A Central Limit Theorem for Congruence Subgroups of the Modular Group

Vladimir Lukianov
Tel-Aviv University

March 9, 2005

Abstract

We consider hyperbolic Laplacian on a Riemann surfaces associated to congruence subgroups of the modular group. We establish the Central Limit Theorem for the spectrum of the Laplacian on these surfaces. In the case of the modular group it is done by Z. Rudnick [20]. An important quantity in our work is a weighted multiplicities function for closed geodesics of given length on a finite area Riemann surface. These weighted multiplicities appear naturally in the Selberg trace formula, and in particular their mean square plays an important role in establishing the result.

Contents

1 Introduction

Determining the motion of a particle in microworld differs from that for the macroscopic case. The laws of classical mechanics no longer apply for the atomic scale. There is still no way to describe explicitly the motion or dislocation of a particle. Quantum mechanics offers to measure the probability of the particle to be at the certain place in a given time. In this way one loses the usual concepts of trajectory, coordinates, momentum etc. What remains is a strong analogy with the Hamiltonian formalism of classical mechanics. More precisely, a particle is described at each time by a wave function ψ_t, such that

$$\int_{\mathbb{R}^3} |\psi_t|^2 (\overrightarrow{x})dV = 1,$$

and for a measurable set $B \subseteq \mathbb{R}^3$

$$\int_{B} |\psi_t|^2 (\overrightarrow{x})dV,$$

is the probability of finding the particle inside B at time t.

The wave function satisfies the Schrödinger equation

$$i\hbar\partial_t\psi_t = H\psi_t,$$

where H is the Schrödinger operator, obtained from the classical Hamiltonian of the system by a certain recipe. Hence, one of the natural problems is to find the eigenvalues (energy levels) $E_n(\hbar)$ and the eigenfunctions $\varphi_n^{\hbar} \in L^2(D)$ for this operator and some domain D. In general it is very difficult problem, so one looks for any possible information about these energy levels and eigenfunctions.

There is a strong relation between the energy levels $E_n(\hbar)$ and the eigenvalues of the Laplace operator defined on D. This relation reduces the problem of determining the energy levels statistics for the given quantum system to the studying the eigenvalue statistics of the Laplacian defined on a given domain D. These statistics form one of the intriguing parts of a comparatively young branch of the theoretical physics - "quantum chaos". For more detailed explanation see [2].

In this work we establish the Central Limit Theorem (CLT) for the spectrum of the hyperbolic Laplacian on the fundamental domain of the congruence subgroup of the modular group. For the modular group this was done by Z. Rudnick [20].

We now explain what exactly is proven in this work. Let Q be an odd squarefree integer. Define

$$\Gamma_0(Q) := \left\{ T \in SL_2(\mathbb{Z}) \mid T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, c \equiv 0 (\operatorname{mod} Q) \right\}$$

be the congruence subgroup of level Q of the modular group. Let

$$\Gamma = \Gamma_0(Q) \diagup \{\pm I\},$$

and let

$$y^2 \left(\frac{\partial^2}{\partial^2 x} + \frac{\partial^2}{\partial^2 y} \right)$$

be the hyperbolic Laplacian on the upper complex half plane $\mathbb{H}$. It is known [10], that the discrete spectrum

$$\lambda_0 = 0 < \lambda_1 \leq \lambda_2 \leq ...$$

of the Laplacian on $\Gamma \backslash \mathbb{H}$ satisfies Weyl's law

$$N(T) := \#\{0 \leq r_j \leq T\} = \frac{vol(\Gamma \backslash \mathbb{H})}{4\pi} T^2 + O(T \ln T), \tag{1}$$

where $\lambda_j = 1/4 + r_j^2$. We define a smooth version of the counting function as follows. Let f be an even test function with compactly supported smooth Fourier transform: $\widehat{f} \in C_{00}^{\infty}(\mathbb{R})$. Define

$$N_f(\tau) = \sum_{j \geq 0} f(L(r_j - \tau)) + f(L(-r_j - \tau)).$$

If $f = \mathbf{1}_{(-1/2,1/2)}$ is a characteristic function then $N_f(\tau)$ counts the number of r_j lying in the intervals $\pm(\tau - 1/2L,\ \tau + 1/2L)$. By (1) we expect $N_f(\tau)$ to be asymptotically equal to a multiple of τ/L. To study the fluctuations around this expectation we consider τ as a random variable drawn from a certain distribution on the line. To do this we choose an even weight function $\omega \geq 0$, with

$$\int_{-\infty}^{\infty} \omega(x) dx = 1,$$

such that $\widehat{\omega}$ compactly supported, and consider an averaging operator:

$$\langle F \rangle_T := \frac{1}{T} \int_{-\infty}^{\infty} F(\tau) \omega(\frac{\tau}{T}) d\tau.$$

In particular, for $\omega = \mathbf{1}_{[1,2]}$

$$\langle F \rangle_T = \frac{1}{T}\int\limits_T^{2T} F(\tau)d\tau$$

is the standard arithmetic mean. We wish to study the moments of N_f.

To get an idea what one wants to prove, it is desirable to have some conjecture about the result. In the case of the eigenvalue statistics problem one of the tools for making conjectures is Random Matrix Theory (RMT). The background idea of RMT is simple: we change the eigenvalues of the given operator by the eigenvalues of a random $n \times n$ matrix, and study the statistical properties of eigenvalues of such a matrices as n tends to infinity. Thus we obtain a model for eigenvalue statistics of a "typical" operator.

In part I we introduce an example of such a calculation for a certain random matrices ensemble, the Circular Unitary Ensemble (CUE) and we state the CLT for smooth linear statistics, due to Diaconis and Shahshahani [7]. This example will show what kind of CLT we may expect to prove in our particular case, and the hopes, as we will see below, are fully justified.

In part III we will prove that the limiting value distribution of $N_f(\tau)$ is Gaussian with mean

$$\overline{n}_f := \frac{\tau}{L}\frac{2vol(\Gamma\backslash\mathbb{H})}{4\pi}\int\limits_{-\infty}^{\infty} f(x)dx$$

and variance

$$\sigma_\infty^2(L) := \frac{4\kappa_Q}{\pi L}\int\limits_0^{\infty} \widehat{f}^2(u)e^{\pi L u}du,$$

where

$$\kappa_Q = C_1 \prod_{q|Q} \frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)}, \qquad C_1 = 1.328....$$

Our main result is

Theorem 1.1 *Let $L \to \infty$, as $T \to \infty$, such that $L = o(\ln T)$. Then the moments of $N_f(\tau)$ are those of Gaussian random variable with mean $\overline{n}_f$ and variance $\sigma_\infty^2(L)$.*

$$\lim_{T\to\infty}\left\langle \left(\frac{N_f - \overline{n}_f}{\sigma_\infty(L)}\right)^K \right\rangle_T = \begin{cases} \dfrac{(2k)!}{k!2^k}, & K = 2k \text{ is even} \\ 0, & K \text{ is odd} \end{cases}.$$

Similar eigenvalue statistics may be also established for the arithmetic surfaces derived from indefinite rational quaternion algebras [15].

The main part of the thesis is Part II, which is dedicated to the asymptotic behavior of a weighted multiplicities function $\beta_Q(n)$, connected with the multiplicities of conjugacy classes of matrices of trace n in the congruence group $\Gamma_0(Q)$. This will play a vital role in the proof of the main result. We explain briefly what is done in this part:

Let Γ be a congruence subgroup of $PSL_2(\mathbb{R})$. Put

$$h(r) = f(L(r-\tau)) + f(L(-r-\tau))$$

then we can use the Selberg Trace Formula to express $N_f(\tau)$ as:

$$\begin{aligned} N_f(\tau) = \sum_{j\geq 0} h(r_j) &= \{\textit{identity contribution}\}+ \\ &+ \{\textit{hyperbolic contribution}\}+ \\ &+ \{\textit{elliptic contribution}\}+ \\ &+ \{\textit{parabolic and continuous spectrum contribution}\} \end{aligned} \tag{2}$$

We say that the element T of Γ is hyperbolic if $|trT| > 2$. Such an element is conjugate in $PSL_2(\mathbb{R})$ to a diagonal matrix $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}$, where $\lambda > 1$ is real. For an element T, such that $|trT| = t$ we define the norm[1] of T to be

$$\mathcal{N}(T) = \lambda^2 = \left(\frac{t+\sqrt{t^2-4}}{2}\right)^2.$$

For us the most important term in formula (2) is the hyperbolic contribution term, which is defined explicitly as:

$$\sum_{t>2}\sum_{\substack{\{T\}\ hyperbolic \\ |trT|=t}} \frac{\ln\mathcal{N}(T_0)}{\mathcal{N}(T)^{1/2}-\mathcal{N}(T)^{-1/2}} g(\ln\mathcal{N}(T)).$$

There are in general several conjugacy classes with $|trT| = t$. Define the weighted multiplicity function $\beta_\Gamma(t)$ by:

$$\beta_\Gamma(t) = \frac{1}{4} \sum_{\substack{\{T\}\subset\Gamma \\ T=T_0^k \text{ is hyperbolic} \\ |trT|=t}} \frac{\ln\mathcal{N}(T_0)}{\mathcal{N}(T)^{1/2}-\mathcal{N}(T)^{-1/2}},$$

[1] The number λ^2 is called also a multiplier of T.

where T_0 is a primitive hyperbolic element, that is T_0 is not a power of any other hyperbolic element. In this notation we can rewrite the hyperbolic contribution term as follows

$$\sum_{t>2}\beta_\Gamma(t)g(\ln \mathcal{N}(T)),$$

so the information about the weighted multiplicities will be useful for understanding the behavior of this term.

From the prime geodesic theorem it follows that the mean value of $\beta_\Gamma(t)$ is unity:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2<t\le N}\beta_\Gamma(t)=1.$$

The main result of this part is a computation of the mean square of the weighted multiplicities for the case that $\Gamma=\Gamma_0(Q)$ is a congruence subgroup of the modular group (Theorem 7.1). Namely, designating $\beta_Q=\beta_\Gamma$ for $\Gamma=\Gamma_0(Q)$, we obtain

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2<t\le N}\beta_Q^2(t)=C_1\prod_{q|Q}\frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)}=\kappa_Q.$$

Here

$$C_1=\lim_{N\to\infty}\frac{1}{N}\sum_{2<t\le N}\beta_1^2(t)=\frac{1015}{864}\prod_{p\neq 2}\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}=1.328...$$

which is the mean square of the weighted multiplicities for the modular domain ($Q=1$), proved by M. Peter [16], following a conjecture of Bogomolny et al [3].

We now explain the method of proof. As a first step, we express the weighted multiplicities in terms of Dirichlet's L-functions. For $\Gamma_0(Q)$ the expression is

$$\beta_Q(t)=\sum_{\substack{D,v\ge 1\\ D \text{ is a discriminant}\\ Dv^2=t^2-4}}\frac{1}{v}L(1,\chi_D)\cdot\prod_{q|Q}\left\{\begin{array}{cc} 2, & q^2\mid D\\ 1+\left(\dfrac{D}{q}\right) & q^2\nmid D\end{array}\right\}. \quad (3)$$

This is proved in section 3 by connecting the weighted multiplicities with class numbers and using Dirichlet's class number formula.

The principal tool in our approach, following Peter, is that the formula (3) displays the weighted multiplicity $\beta_Q(t)$ as a "limit periodic function" in a suitable sense (see section 5 for background on these). To show this, we approximate the L-functions by a finite Euler product using a zero-density theorem, in a certain semi-norm coming from the theory of limit periodic functions (section 6). For computing mean squares, this suffices and allows us to use Parseval's equality in this setting to express the mean square as

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le t\le N}\beta_Q^2(t)=\sum_{b\ge 1}\sum_{\substack{1\le a\le b\\ \gcd(a,b)=1}}\left|\widehat{\beta_Q}\left(\frac{a}{b}\right)\right|^2=$$

$$=\prod_{p\text{ - prime}}\left(1+\sum_{c\ge 1}\sum_{\substack{1\le a\le p^c\\ a\not\equiv 0(\bmod p)}}\left|\widehat{\beta_{(p,Q)}}\left(\frac{a}{p^c}\right)\right|^2\right),$$

where $\widehat{\beta}$ are the Fourier coefficients of β, defined in section 5.

We then carry out a length calculation of the Fourier coefficients in section 7.2, finally ending up with rather complicated expressions described in Theorem 7.3.

The result is that the mean square is an Euler product

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=\prod_{p\text{ - prime}}M_p(Q),$$

with

$$M_p(Q)=1+\sum_{c\ge 1}A_Q(p^c),$$

and $A_Q(p^c)$ is given by (20), section 7.3. We evaluate the sum $M_p(Q)$ over prime powers as a rational function of p and find that it depends on divisibility of Q by p, in particular, for $p\nmid Q$, $p\neq 2$,

$$M_p(Q)=M_p(1)=\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}.$$

This will prove Theorem 7.1.

Part I
A statistical model: The Circular Unitary Ensemble (CUE)

In this section we analyze one of the random matrices ensembles and get some knowledge about its statistical behavior. We consider the group $U(n)$ of unitary $n \times n$ matrices, equipped with the unique Haar probability measure d_H. The eigenvalues of the unitary matrix U are

$$e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_3}, ..., e^{i\theta_n},$$

where $\theta_j \in [0, 2\pi)$. All the eigenvalues thus lie on the unit circle, justifying the ensemble's name. Ordering the eigenphases

$$\theta_1 \leq \theta_2 \leq \theta_3 \leq ... \leq \theta_n$$

we study their statistics. To get an averages, we recall Weyl's integration formula

$$\int\limits_{U(n)} g(U) d_H U = \frac{1}{n!(2\pi)^n} \int\limits_0^{2\pi} ... \int\limits_0^{2\pi} g(\theta_1, \theta_2, ..., \theta_n) \prod_{1 \leq j < k \leq n} \left| e^{i\theta_j} - e^{i\theta_k} \right|^2 d\theta_1 ... d\theta_n, \tag{4}$$

where g is a function which depends only on eigenphases $\theta_1, \theta_2, ..., \theta_n$.

Let now f be a real valued trigonometric polynomial, that is

$$f(\theta) = \sum_k f_k e^{ik\theta}.$$

Define a linear statistic of the unitary matrix U by

$$N_f(U) = \sum_{j=1}^n f(\theta_j),$$

where θ_j are eigenphases of U. We may rewrite this in the form

$$N_f(U) = \sum_{j=1}^n \sum_k f_k e^{ik\theta_j} = \sum_k f_k \sum_{j=1}^n e^{ik\theta_j} = \sum_k f_k tr(U^k).$$

The **mean** value of N_f is

$$\langle N_f(U)\rangle = \left\langle \sum_k f_k tr(U^k) \right\rangle = \sum_k f_k \left\langle tr(U^k)\right\rangle . \tag{5}$$

By the invariance of Haar measure under multiplication by a scalar matrix λI we obtain

$$\left\langle tr(U^k)\right\rangle = \left\langle tr((\lambda U)^k)\right\rangle = \lambda^k \left\langle tr(U^k)\right\rangle .$$

Choosing λ not to be a k-th root of unity we conclude, that for $k \neq 0$

$$\left\langle tr(U^k)\right\rangle = 0.$$

Substituting into (5) we find

$$\langle N_f(U)\rangle = nf_0.$$

To obtain the **variance** of $N_f(U)$ we need to compute

$$Var(N_f) = \left\langle |N_f - nf_0|^2 \right\rangle = \sum_{k,l\neq 0} f_k \overline{f_l} \left\langle tr(U^k)\overline{tr(U^l)}\right\rangle .$$

Just as before, using the invariance of Haar measure we get, that for $k \neq l$

$$\left\langle tr(U^k)\overline{tr(U^l)}\right\rangle = 0.$$

Thus

$$Var(N_f) = \sum_{k\neq 0} |f_k|^2 \left\langle \left|tr(U^k)\right|^2 \right\rangle .$$

We will show that for $-n \leq k \leq n,\ k \neq 0$

$$\left\langle \left|tr(U^k)\right|^2 \right\rangle = |k| ,$$

and therefore obtain

$$Var(N_f) = \sum_{k\neq 0} |f_k|^2 |k| =: \sigma_f^2.$$

Lemma 1.2 *Let $1 \leq k \leq n$, then $\left\langle \left|tr(U^k)\right|^2 \right\rangle = k$.*

Proof. By definition

$$\left\langle \left|tr(U^k)\right|^2 \right\rangle = \int_{U(n)} \left|tr(U^k)\right|^2 d_H U.$$

Denoting

$$dA_n := \frac{1}{n!(2\pi)^n} \prod_{1\le j<k\le n} \left|e^{i\theta_j} - e^{i\theta_k}\right|^2 d\theta_1 ... d\theta_n$$

and using formula (4) we have

$$\left\langle \left|tr(U^k)\right|^2 \right\rangle = \int\limits_{[0,2\pi)^n} \sum_{j=1}^n e^{ik\theta_j} \sum_{l=1}^n e^{-ik\theta_l} dA_n = \int\limits_{[0,2\pi)^n} \sum_{j,l=1}^n e^{ik(\theta_j-\theta_l)} dA_n$$

$$= n \cdot \int\limits_{[0,2\pi)^n} dA_n + 2 \cdot \int\limits_{[0,2\pi)^n} \sum_{1\le j<l\le n} \cos k\left(\theta_j - \theta_l\right) dA_n = I_1 + I_2.$$

The first integral is n, since

$$\int\limits_{[0,2\pi)^n} dA_n = 1.$$

For this see for example [6].

We stay with the integral I_2. To handle it we use Gaudin's lemma (see [6]), which allows to restrict the number of integration variables to the number of variables on which the integrand depends. More precise, we have

$$I_2 = 2 \cdot \int\limits_{[0,2\pi)^n} \sum_{1\le j<l\le n} \cos k\left(\theta_j - \theta_l\right) dA_n =$$

$$= 2 \cdot \frac{1}{2!(2\pi)^2} \int\limits_{[0,2\pi)^2} \cos k(\theta_1 - \theta_2)(n^2 - S_n^2(\theta_1 - \theta_2)) d\theta_1 \theta_2,$$

where

$$S_n(\theta) = \frac{\sin(n\theta)/2}{\sin\theta/2}.$$

Changing variables and doing some arithmetic one gets

$$I_2 = -\frac{1}{2\pi} \int\limits_0^{2\pi} \cos ku \cdot S_n^2(u) du.$$

Remembering, that

$$S_n^2(u) = 2n \cdot F_{n-1}(u),$$

where F_{n-1} is the $(n-1)$-th Fejer's kernel, we obtain

$$I_2 = -\frac{n}{\pi} \int\limits_0^{2\pi} \cos ku \cdot F_{n-1}(u) du =$$

$$= -\frac{n}{\pi}\int_{0}^{2\pi} \cos ku \left[\frac{1}{2} + \sum_{j=1}^{n-1}\left(1-\frac{j}{n}\right)\cos ju\right] du = -(n-k).$$

It follows

$$\left\langle \left|tr(U^k)\right|^2 \right\rangle = I_1 + I_2 = n - (n-k) = k,$$

as desired. ■

Diaconis and Shahshahni [7] went on to compute the higher moments of N_f and established the CLT for this ensemble:

Theorem 1.3 *As $n \to \infty$, the moments of N_f converge to those of a Gaussian random variable with mean*

$$nf_0 = \frac{1}{2\pi}\int_{0}^{2\pi} f(\theta)d\theta$$

and variance

$$\sigma_f^2 := \sum_{k\neq 0} \left|f_k\right|^2 |k| \,.$$

That is

$$\left\langle \left|N_f - nf_0\right|^K \right\rangle \underset{n\to\infty}{\to} \begin{cases} \dfrac{(2k)!}{2^k k!}\sigma_f^{2k}, & K = 2k \\ 0, & K = 2k-1 \end{cases} .$$

Part II

The weighted multiplicities function $\beta_Q(t)$

Let $T \in SL_2(\mathbb{Z})$, such that $|t| = |tr(T)| > 2$. For such T the equation $\det(T - \lambda I) = 0$ has two different solutions: $\lambda_{1,2} = \frac{t \pm \sqrt{t^2-4}}{2}$, and so T is diagonalizable. Such T is called hyperbolic. Define $\mathcal{N}(T) := \lambda^2$, where $|\lambda| > 1$. Hence $\mathcal{N}(T) = \frac{\left(|t| + \sqrt{t^2-4}\right)^2}{4}$.

Define the weighted multiplicities function

$$\beta(t) = \frac{1}{4} \sum_{\substack{\{T\} \in SL_2(\mathbb{Z}) \\ |tr(T)| = t}} \frac{\ln \mathcal{N}(T_0)}{\mathcal{N}(T)^{\frac{1}{2}} - \mathcal{N}(T)^{-\frac{1}{2}}}.$$

In his work M. Peter [16] proved that

$$\lim_{N \to \infty} \frac{1}{N} \sum_{2 \le n \le N} \beta^2(n) = \frac{1015}{864} \prod_{p \ne 2} \frac{p^2(p^3 + p^2 - p - 3)}{(p^2-1)^2(p+1)} = C_1, \qquad (6)$$

and the numerical calculation gives $C_1 = 1.328...$.

We generalize this result for a congruence subgroups $\Gamma_0(Q)$ of $SL_2(\mathbb{Z})$, where Q is an odd squarefree integer. In the previous notation we define

$$\beta_Q(t) := \frac{1}{4} \sum_{\substack{\{T\} \in \Gamma_0(Q) \\ |tr(T)| = t \\ hyperbolic,\ doesn't \\ fix\ cusp}} \frac{\ln \mathcal{N}(T_0)}{\mathcal{N}(T)^{\frac{1}{2}} - \mathcal{N}(T)^{-\frac{1}{2}}},$$

where the sum is taken over conjugacy classes of $\Gamma_0(Q)$.

In this part we will calculate (Theorem 7.1) the mean square of weighted multiplicities $\beta_Q(n)$:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{2 \le n \le N} \beta_Q^2(n) = C_1 \prod_{q | Q} \frac{2(q^2 - q - 1)(q+1)^2}{q(q^3 + q^2 - q - 3)}. \qquad (7)$$

This calculation will be done in a few steps. In the first step we use Dirichlet's class number formula to express weighted multiplicities function $\beta_Q(n)$ in terms of Dirichlet's L-function (Theorem 3.1). After that, following M.Peter, we prove that $\beta_Q(n)$ is a "limit periodic function", in the sense that it may be approximated by periodic functions in the suitable norm (Proposition 6.1). A finite Euler product for L-functions is used for these purposes. All that allows us to use Parseval's equality to get a formula for the mean square of weighted multiplicities $\beta_Q(n)$ in terms of Fourier coefficients (see Proposition 6.13) . Routine Fourier coefficient computation lead us to the final result (7).

2 Preliminaries on orders in quaternion algebras

In this section we remind algebraic definitions and results, which we are going to use along this part.

First of all we recall that a ring B with unity is called an algebra of dimension n over a field F, if the following three conditions are satisfied:

1° $B \supset F$,and $1_B = 1_F$;
2° any element of F commutes with all elements of B;
3° B is a vector space over F of dimension n.

Definition 2.1 *Let B be a finite dimensional algebra over $\mathbb{Q}$ with identity element 1_B. A subset $R \subset B$ is called an order in B if the following conditions are satisfied:*
1° R is a finitely generated $\mathbb{Z}$-module;
2° R contains basis of B over $\mathbb{Q}$;
3° R is a subring of B and $1_B \in R$.

For any finite dimensional algebra B over $\mathbb{Q}$ and for each place v of $\mathbb{Q}$ (i.e. $v = \infty$ or $v = p$ a prime) we define $B_v := B \otimes_{\mathbb{Q}} \mathbb{Q}_v$. B_v is an algebra over $\mathbb{Q}_v$ of dimension $\dim_{\mathbb{Q}} B$. For $v = p$ a prime, orders in B_p defined as in the previous definition, replacing $\mathbb{Q}$ and $\mathbb{Z}$ by $\mathbb{Q}_p$ and $\mathbb{Z}_p$. If R is an order of B, we get an order in B_p by the definition

$$R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p = [\text{the closure of } R \text{ in } B_p].$$

We also recall the definition of adele ring B_A [19, pp. 197-198] and [23, p. 62]. As a set this is

$$B_A = \{(b_v) \in \prod_v B_v \mid b_p \in R_p \text{ for almost all primes } p\},$$

where R is any order in B.

Definition 2.2 *A nonzero integer d is called a fundamental discriminant if $d \equiv 1 (\bmod 4), d$ square free, $d \neq 1$; or $d \equiv 0 (\bmod 4)$, $\dfrac{d}{4} \neq 1 (\bmod 4)$, $\dfrac{d}{4}$ squarefree.*

Consider now a quadratic extension of $\mathbb{Q}$ arising as the splitting field over $\mathbb{Q}$ of a polynomial $P(X) = X^2 - tX + 1$, $t \in \mathbb{Z}$. Notice that $P(X)$ is irreducible iff $\sqrt{t^2-4} \notin \mathbb{Q}$. In this case we can write $t^2 - 4 = l^2 d$, $l \in \mathbb{Z}^+$, d is a fundamental discriminant. The splitting field of $P(X)$ is $\mathbb{Q}(\sqrt{d})$ and the zeros of $P(X)$ are

$$x_1 = \frac{t}{2} + l\frac{\sqrt{d}}{2}, \qquad\qquad x_2 = \frac{t}{2} - l\frac{\sqrt{d}}{2}.$$

For each fixed fundamental discriminant d we let for each $f \in \mathbb{Z}^+$

$$\mathfrak{r}[f] := \mathbb{Z} + f\omega\mathbb{Z}, \quad \text{where} \quad \omega = \frac{d+\sqrt{d}}{2}.$$

Then orders in $\mathbb{Q}(\sqrt{d})$ are precisely $\mathfrak{r}[f]$, $f = 1, 2, 3, ...$ [5, pp. 48-49], and in particular $\mathfrak{r}[1]$ is the unique maximal order.[8, pp. 146-147]. The index $[\mathfrak{r}[1] : \mathfrak{r}[f]] = f$, and we call $\mathfrak{r}[f]$ the order of index f in $\mathbb{Q}(\sqrt{d})$. Note that $\mathfrak{r}[f_1] \subset \mathfrak{r}[f_2]$ iff $f_2 \mid f_1$.

For $P(X)$ as above, the roots x_1, x_2 of $P(X)$ satisfy

$$\mathbb{Z} + x_1\mathbb{Z} = \mathbb{Z} + x_2\mathbb{Z} = \mathfrak{r}[l] \qquad (t^2 - 4 = l^2 d).$$

Let $K = \mathbb{Q}(\sqrt{d})$, d as above, then

$$K_\infty = \mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \left\{ \begin{array}{cc} \mathbb{R} \oplus \mathbb{R} & , d > 0 \\ \mathbb{C} & , d < 0 \end{array} \right\},$$

$$K_p = \mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \left\{ \begin{array}{cc} \mathbb{Q}_p \oplus \mathbb{Q}_p & , \left(\frac{d}{p}\right) = 1 \\ \mathbb{Q}_p(\sqrt{d}) & , \left(\frac{d}{p}\right) = -1 \end{array} \right\}.$$

The distinct orders in K_p are

$$\mathfrak{o}[p^n] := \mathbb{Z}_p + p^n \omega \mathbb{Z}_p, n = 0, 1, 2, ... \text{ and } \omega = \frac{d + \sqrt{d}}{2} \text{ as above.}$$

We have

$$\mathfrak{o}[1] \supset \mathfrak{o}[p] \supset \mathfrak{o}[p^2] \supset ... \text{ and } [\mathfrak{o}[1] : \mathfrak{o}[p^n]] = p^n.$$

Combining the definitions of order in K and in K_p we get

$$(\mathfrak{r}[f])_p = \mathfrak{o}[p^n], \text{ where } n = ord_p f.$$

For any order $\mathfrak{r}$ in $K = \mathbb{Q}(\sqrt{d})$ we define

$$\begin{aligned}
\mathfrak{r}_\infty &:= K_\infty \\
\mathfrak{r}_A &:= \prod_v \mathfrak{r}_v \subset K_A \\
\mathfrak{r}^\times_{\infty+} &:= \{x \in K^\times_\infty \mid N(x) > 0\} \\
\mathfrak{r}^\times_{A+} &:= \{(\alpha_v) \in \mathfrak{r}^\times_A \mid N(\alpha_\infty) > 0\} = \mathfrak{r}^\times_{\infty+} \times \prod_p \mathfrak{r}^\times_p \subset \mathfrak{r}^\times_A
\end{aligned}$$

Here N denotes the extension of the norm $N : K \longrightarrow \mathbb{Q}$ to the regular norm in the algebra K_∞ over $\mathbb{Q}_\infty = \mathbb{R}$. [23, p.53].

The subgroup $\mathfrak{r}^\times_{A+} \cdot K^\times$ has finite index in $K^\times_A$, and we set

$$h(\mathfrak{r}) := \left[K^\times_A : (\mathfrak{r}^\times_{A+} \cdot K^\times)\right],$$

the class number of $\mathfrak{r}$.

For $K = \mathbb{Q}(\sqrt{d})$ as above one can also show [4, Chapter 5.2] that $h(\mathfrak{r}[f])$ is equal to the number of inequivalent primitive (and if $d < 0$, positive) quadratic forms $ax^2 + bxy + cy^2$ with discriminant $b^2 - 4ac = df^2$. In other words $h(\mathfrak{r}[f]) = h(df^2)$, where the right-hand side is as in [13, vol I, pp. 127-].

3 Expression of weighted multiplicities function in the terms of Dirichlet's L-functions

In this section we express $\beta_Q(t)$ in the terms of Dirichlet's L-functions. It is a necessary step, which allows to analyze the behavior of $\beta_Q(t)$.

The result is stated in Theorem 3.1, proof of which takes the rest of the section. In the proof we rely extensively on the exposition of Strömbergsson [22].

Theorem 3.1 *For $t \in \mathbb{Z}$,*

$$\beta_Q(t) = \sum_{\substack{D,v\geq 1 \\ D \text{ is a discriminant} \\ Dv^2=t^2-4}} \frac{1}{v} L(1,\chi_D) \cdot \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\},$$

if $\sqrt{t^2-4} \notin \mathbb{Q}$, $t^2-4>0$, and $\beta_Q(t)=0$, otherwise. Here $\left(\frac{\cdot}{\cdot}\right)$ is a Legendre's symbol and χ_D is a quadratic character.

We start from noting that

$$\Gamma_0(Q) = \bigsqcup_{t\in\mathbb{Z}} H_t,$$

where

$$H_t = \{T \in \Gamma_0(Q) \mid tr(T) = t\}.$$

So we can write (the change from 1/4 to 1/2 comes from not collecting together t and $-t$)

$$\beta_Q(t) = \frac{1}{2} \sum_{\substack{T\in H_t//\Gamma_0(Q) \\ \text{hyperbolic, doesn't} \\ \text{fix cusp}}} \frac{\ln \mathcal{N}(T_0)}{\mathcal{N}(T)^{\frac{1}{2}} - \mathcal{N}(T)^{-\frac{1}{2}}} \tag{8}$$

Here $H_t//\Gamma_0(Q)$ is the set of $\Gamma_0(Q)$-conjugacy classes of H_t.

Lemma 3.2 *For a hyperbolic element $T \in H_t$ (i.e. $t^2-4>0$) no fixed point of T is a cusp of $\Gamma_0(Q)$.*

Proof. Note, that the cusps of $\Gamma_0(Q)$ are exactly the points in $\{i\infty\} \cup \mathbb{Q}$, by [19, cor. 1.5.5, th. 4.1.3(2)]. Assume $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. First, $c \neq 0$, since we will get T parabolic. So, the fixpoints of T are the two real solutions to $\dfrac{ax+b}{cx+d} = x \Leftrightarrow x = \dfrac{a-d}{2c} \pm \dfrac{\sqrt{t^2-4}}{2|c|}$, which are both irrational, since $\sqrt{t^2-4} \notin \mathbb{Q}$. ∎

Now we want to know when in the sum (8), H_t is not the empty set.

Lemma 3.3 *Let* $t \in \mathbb{Z}$, *such that* $\sqrt{t^2-4} \notin \mathbb{Q}$, *and write* $t^2-4 = l^2 d$, $l \in \mathbb{Z}^+$, d *is a fundamental discriminant. Then* H_t *is not empty iff for all primes* q *divide* Q *we have* $q \mid l$ *or* $\left(\frac{d}{q}\right) \neq -1$.

Proof. $H_t \neq \emptyset$ iff there some $a, b, c \in \mathbb{Z}$, such that $\det \begin{bmatrix} a & b \\ Qc & t-a \end{bmatrix} = 1$. Hence $H_t \neq \emptyset$ iff there is some $a \in \mathbb{Z}$, such that $a(t-a) \equiv 1 (\operatorname{mod} Q) \Leftrightarrow (2a-t)^2 \equiv t^2 - 4 (\operatorname{mod} Q) \Leftrightarrow (2a-t)^2 \equiv l^2 d (\operatorname{mod} Q)$. Since Q is odd squarefree, the last congruence is solvable iff $(2a-t)^2 \equiv l^2 d (\operatorname{mod} q)$ for all primes $q \mid Q$. Or equivalently: the last congruence is solvable iff $q \mid l$ or $\left(\frac{d}{q}\right) \neq -1$, for all $q \mid Q$. ■

Note, that for $T \in H_t$, $\mathcal{N}(T)^{\frac{1}{2}} - \mathcal{N}(T)^{-\frac{1}{2}} = \frac{|t| + \sqrt{t^2-4}}{2} - \frac{2}{|t| + \sqrt{t^2-4}} = \sqrt{t^2-4}$.

So, for fixed $t \in \mathbb{Z}$, such that $\sqrt{t^2-4} \notin \mathbb{Q}$, $t^2 - 4 > 0$, $H_t \neq \emptyset$ we can write (8) in the form

$$\beta_Q(t) = \frac{1}{2} \sum_{T \in H_t // \Gamma_0(Q)} \frac{\ln \mathcal{N}(T_0)}{\sqrt{t^2-4}} \tag{9}$$

We will enumerate the $\Gamma_0(Q)$-conjugacy classes in H_t, and for each conjugacy class will get the number $\mathcal{N}(T_0)$.

Fix some $T_t \in H_t$, and take the polynomial $P(X) = X^2 - tX + 1$, i.e. the characteristic polynomial of T_t, and so $P(T_t) = 0$. $P(X)$ is irreducible, since $\sqrt{t^2-4} \notin \mathbb{Q}$. Hence $\mathbb{Q}[T_t] \cong \mathbb{Q}(\sqrt{d})$, where $t^2 - 4 = l^2 d$.

Define the set $C(T_t) := \{\delta T_t \delta^{-1} \mid \delta \in GL_2(\mathbb{Q})\}$. Then $H_t = R \cap C(T_t)$, where $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) \mid \quad Q \mid c \right\}$ is an order in $M_2(\mathbb{Q})$. For any $\delta \in GL_2(\mathbb{Q})$, $\left(\mathbb{Q}[T_t] \cap \delta R \delta^{-1}\right)$ is an order in $\mathbb{Q}[T_t]$, by the fact, that if A' is a subalgebra of A, and $\mathcal{O}$ is an order in A, then $A' \cap \mathcal{O}$ is an order in A'. For any order $\mathfrak{r}$ in $\mathbb{Q}[T_t]$ define $C(T_t, \mathfrak{r}) := \{\delta T_t \delta^{-1} \mid \delta \in GL_2(\mathbb{Q}), \mathbb{Q}[T_t] \cap \delta^{-1} R \delta = \mathfrak{r}\}$. Following Strömbergsson [22], Miyake [19] we have a

Lemma 3.4

$$C(T_t) = \bigsqcup_{f=1}^{\infty} C(T_t, \mathfrak{r}[f]),$$

$$H_t = \bigsqcup_{f|l} C(T_t, \mathfrak{r}[f]),$$

and each $C(T_t, \mathfrak{r}[f])$ is closed under $\Gamma_0(Q)$-conjugation.[2]

Proof. Clearly, $C(T_t) = \bigcup_{f=1}^{\infty} C(T_t, \mathfrak{r}[f])$, since there are no other orders than $\mathfrak{r}[1]$, $\mathfrak{r}[2]$, ... in $\mathbb{Q}[T_t]$. To prove disjointedness, we must show that if $\delta_1 T_t \delta_1^{-1} = \delta_2 T_t \delta_2^{-1}$ ($\delta_1, \delta_2 \in GL_2(\mathbb{Q})$), then $\delta_1^{-1} R \delta_1$, and $\delta_2^{-1} R \delta_2$ have the same intersection with $\mathbb{Q}[T_t]$. From $\delta_1 T_t \delta_1^{-1} = \delta_2 T_t \delta_2^{-1}$ we get $\delta_1^{-1}\delta_2 \in \mathbb{Q}[T_t]$, since if an element of $M_2(\mathbb{Q})$ commutes with T_t, it is in $\mathbb{Q}[T_t]$, by [19, Lemma 5.2.2(3)], and thus

$$\mathbb{Q}[T_t] \cap \delta_2^{-1} R \delta_2 = (\delta_1^{-1}\delta_2)\left(\mathbb{Q}[T_t] \cap \delta_2^{-1} R \delta_2\right)(\delta_1^{-1}\delta_2)^{-1} = \mathbb{Q}[T_t] \cap \delta_1^{-1} R \delta_1.$$

This prove the first relation.

Next, for any order $\mathfrak{r}$ in $\mathbb{Q}[T_t]$ and any $\delta \in GL_2(\mathbb{Q})$, such that $\delta T_t \delta^{-1} \in C(T_t, \mathfrak{r})$, we have :

$$T_t \in \mathfrak{r} \Leftrightarrow T_t \in \mathbb{Q}[T_t] \cap \delta^{-1} R \delta \Leftrightarrow T_t \in \delta^{-1} R \delta \Leftrightarrow \delta T_t \delta^{-1} \in R \Leftrightarrow \delta T_t \delta^{-1} \in H_t.$$

In other words :

$$\text{if } T_t \in \mathfrak{r}, \text{ then } C(T_t, \mathfrak{r}) \subset H_t;$$
$$\text{if } T_t \notin \mathfrak{r}, \text{ then } C(T_t, \mathfrak{r}) \cap H_t = \emptyset.$$

Note that $T_t \in \mathfrak{r}[l]$, where $t^2 - 4 = l^2 d$, $l \in \mathbb{Z}^+$.So the orders of $\mathfrak{r}$ in $\mathbb{Q}[T_t]$ that contain T_t are exactly $\mathfrak{r}[f]$, such that $\mathfrak{r}[f] \supset \mathfrak{r}[l]$, that is, such that $f \mid l$. By definition $H_t \subset C(T_t)$, and so from the first relation the second relation follows.

Finally, $\gamma^{-1} R \gamma = R$, for any $\gamma \in R^\times$. So we get that each $C(T_t, \mathfrak{r})$ is closed under $R^\times$-conjugation, and in particular under $\Gamma_0(Q)$-conjugation.
■

[2] $\mathsf{r}[f] := \mathbb{Z} + f w \mathbb{Z}$, is an all orders in $\mathbb{Q}(\sqrt{d})$, where $f \in \mathbb{Z}^+$, $w = \frac{d+\sqrt{d}}{2}$. Since $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[T_t]$ we use the symbol $\mathsf{r}[f]$ for the corresponding order in $\mathbb{Q}[T_t]$.

Let $\varepsilon_d = \dfrac{x+y\sqrt{d}}{2}$ be the proper fundamental unit in $\mathbb{Q}(\sqrt{d})$ ((x,y) is the positive integer solution to $x^2-dy^2=4$, for which $y>0$ is minimal). Define

$$\mathfrak{r}[f]^1 := \{\alpha \in \mathfrak{r}[f] \mid N(\alpha)=1\},$$

the units of the order $\mathfrak{r}[f]$. Since

$$\mathfrak{r}[1]^1 = \left\{\pm\varepsilon_d^k \mid k \in \mathbb{Z}\right\},$$

we have

$$\mathfrak{r}[f]^1 = \left\{\pm\left(\varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}\right)^k \mid k \in \mathbb{Z}\right\}.$$

Lemma 3.5 *If T is hyperbolic, i.e. $d>0$, then $\mathcal{N}(T_0) = \varepsilon_d^{2\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}$.*

Proof. Choose some $\delta \in GL_2(\mathbb{Q})$, such that $T=\delta T_t\delta^{-1}$, and $\mathbb{Q}[T_t]\cap\delta R\delta^{-1}=\mathfrak{r}$. Then $Z_{\Gamma_0(Q)}(T)$, the centralizer of T in $\Gamma_0(Q)$ is

$$Z_{\Gamma_0(Q)}(T) = \mathbb{Q}[T]\cap\Gamma_0(Q) = \delta(\mathbb{Q}[T_t]\cap\delta^{-1}\Gamma_0(Q)\delta)\delta^{-1} = \delta\mathfrak{r}[f]\delta^{-1}$$

by [19, lemma 5.2.2(3)].Since

$$\mathfrak{r}[f]^1 = \left\{\pm\left(\varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}\right)^k \mid k \in \mathbb{Z}\right\},$$

for $d>0$ we can take for T_0 the image of $\varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}$ under the composite of the two isomorphisms $\mathbb{Q}[T_t]\cong\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}[T_t]\ni S\longmapsto \delta S\delta^{-1}\in\mathbb{Q}[T]$. Then

$$tr_{M_2(\mathbb{Q})}(T_0) = tr\left(\varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}\right).$$

If we will denote $\varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]} = \alpha+\beta\sqrt{d}\in\mathbb{Q}(\sqrt{d})$, note, that $\alpha,\beta\geq 0$, and $N(\alpha+\beta\sqrt{d}) = \alpha^2-d\beta^2=1$. We have $tr(\alpha+\beta\sqrt{d})=t$, and so

$$\begin{aligned}\mathcal{N}(T_0) &= \frac{\left(|t|+\sqrt{t^2-4}\right)^2}{4} = \frac{\left(2|\alpha|+\sqrt{4\alpha^2-4}\right)^2}{4} = \\ &= \frac{\left(2|\alpha|+\sqrt{4(1+d\beta^2)-4}\right)^2}{4} = \frac{\left(2|\alpha|+2|\beta|\sqrt{d}\right)^2}{4} = \\ &= \left(|\alpha|+|\beta|\sqrt{d}\right)^2 = \left(\alpha+\beta\sqrt{d}\right)^2 = \varepsilon_d^{2\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}.\end{aligned}$$

■

Now we can rewrite (9) in the form

$$\beta_Q(t) = \sum_{f|l} |C(T_t, \mathfrak{r}[f])//\Gamma_0(Q)| \frac{\ln \varepsilon_d^{[\mathfrak{r}[1]^1 : \mathfrak{r}[f]^1]}}{\sqrt{t^2-4}},$$

where we write $t^2 - 4 = dl^2$ with d a fundamental discriminant and $l \geq 1$.

We calculate now the quantity $|C(T_t, \mathfrak{r}[f])//\Gamma_0(Q)|$, in particular we will prove

Proposition 3.6 *Let N be squarefree and $h(df^2)$ the narrow class number of $\mathbb{Q}(\sqrt{d})$. Then*

$$|C(T_t, \mathfrak{r}[f])//\Gamma_0(N)| = h(df^2) \cdot \left\{ \begin{array}{ll} 2, & \textit{if } d < 0 \\ 1, & \textit{if } d > 0 \end{array} \right\} \cdot \prod_{p|N} \left\{ \begin{array}{cc} 2, & p \mid f \\ 1 + \left(\frac{d}{p}\right) & p \nmid f \end{array} \right\}.$$

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and R an order of B of level N, i.e. R_p is a maximal order of B_p if $p \nmid N$, and if $N = \prod p^e$ then R_p is conjugate to an order $\left\{ \begin{bmatrix} a & b \\ p^e c & d \end{bmatrix} \in M_2(\mathbb{Z}_p) \mid a, b, c, d \in \mathbb{Z}_p \right\}$. In the case of $B = M_2(\mathbb{Q})$ we have

$$R_p \simeq M_2(\mathbb{Z}_p), \text{ if } \ p \nmid N,$$

and

$$R_p \simeq \left\{ \begin{bmatrix} a & b \\ p^e c & d \end{bmatrix} \in M_2(\mathbb{Z}_q) \mid a, b, c, d \in \mathbb{Z}_p \right\}, \text{ if } \ p \mid N.$$

Define the subgroups Γ_R and U_R of $B_A^\times$ by

$$\Gamma_R := \left\{ \gamma \in B^\times \mid N(\gamma) = 1 \right\}$$
$$U_R := GL_2^+(\mathbb{R}) \times \prod_p R_p^\times$$

For instance, in the case of modular groups, $B = M_2(\mathbb{Q})$,

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) \mid c \in N\mathbb{Z} \right\},$$

$$R_p = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_p) \mid c \in N\mathbb{Z}_p \right\}.$$

Therefore

$$\Gamma_R = U_R \cap B^\times = \Gamma_0(N).$$

Now, for $\alpha \in \Gamma_R$, put

$$C(\alpha) = \left\{ h\alpha h^{-1} \mid h \in B^\times \right\},$$

$$C(\alpha, \mathfrak{r}) = \left\{ h\alpha h^{-1} \mid h \in B^\times, \mathbb{Q}[\alpha] \cap hRh^{-1} = \mathfrak{r} \right\},$$

$$C_A(\alpha) = \left\{ h\alpha h^{-1} \mid h \in B_A^\times \right\},$$

$$C_A(\alpha, \mathfrak{r}) = \left\{ h\alpha h^{-1} \mid h \in B_A^\times, \mathbb{Q}_A[\alpha] \cap hR_A h^{-1} = \mathfrak{r}_A \right\},$$

$$C_v(\alpha, \mathfrak{r}) = \left\{ h\alpha h^{-1} \mid h \in B_v^\times, \mathbb{Q}_v[\alpha] \cap hR_v h^{-1} = \mathfrak{r}_v \right\},$$

where $v = \infty$ or $v = p$ is prime.

Lemma 3.7 *Let α be an element of Γ_R, then*

$$|C(\alpha, \mathfrak{r})//\Gamma_R| = h(\mathfrak{r}) \prod_{v=\infty,2,3,5,\ldots} \left| C_v(\alpha, \mathfrak{r})//R_v^\times \right|.$$

Proof. Consider the natural mapping

$$\theta : C(\alpha)//\Gamma \longrightarrow C_A(\alpha)//U$$
$$\theta : \gamma^{-1}C(\alpha)\gamma \longmapsto \gamma^{-1}C_A(\alpha)\gamma$$

(here $\Gamma = \Gamma_R$ and $U = U_R, \gamma \in \Gamma \hookrightarrow U$).

Let $g = h\alpha h^{-1}, (h \in B_A^\times)$ be an element of $C_A(\alpha)$. Since $B_A^\times = B^\times \cdot U$ by [19, Th. 5.2.11, a consequence of the approximation theorem] we may write $h = u_0\beta$, where $\beta \in B^\times$ and $u_0 \in U$. So

$$C_U(g) := \left\{ ugu^{-1} \mid u \in U \right\} = \left\{ uu_0\beta\alpha\beta^{-1}u_0^{-1}u^{-1} \mid u \in U \right\} = C_U(\beta\alpha\beta^{-1}).$$

Thus θ is surjective.

For an element $\xi \in B^\times$, we see that

$$C_U(\xi\alpha\xi^{-1}) = C_U(g) \Longleftrightarrow \xi \in Uh\mathbb{Q}_A[\alpha]^\times \cap B^\times.$$

And for two elements $\eta, \xi \in B^\times$

$$C_\Gamma(\xi\alpha\xi^{-1}) = C_\Gamma(\eta\alpha\eta^{-1}) \Longleftrightarrow \Gamma\xi\mathbb{Q}[\alpha]^\times = \Gamma\eta\mathbb{Q}[\alpha]^\times,$$

since

$$\xi \in \Gamma\eta\mathbb{Q}[\alpha]^\times \Leftrightarrow \xi = \gamma\eta\widetilde{\alpha}\ (\gamma \in \Gamma, \widetilde{\alpha} \in \mathbb{Q}[\alpha]^\times) \Leftrightarrow C_\Gamma(\xi\alpha\xi^{-1}) = C_\Gamma(\eta\alpha\eta^{-1}).$$

We have

$$\beta\mathbb{Q}_A[\alpha]\beta^{-1} = \mathbb{Q}_A[\beta\alpha\beta^{-1}],$$

hence

$$\left|\theta^{-1}\left(C_U(g)\right)\right| = \left|\Gamma\backslash Uh\mathbb{Q}_A[\alpha]^\times \cap B^\times/\mathbb{Q}[\alpha]^\times\right| = \left|\Gamma\backslash U\beta\mathbb{Q}_A[\alpha]^\times \cap B^\times/\mathbb{Q}[\alpha]^\times\right| =$$

$$= \left|\Gamma\backslash U\mathbb{Q}_A[\beta\alpha\beta^{-1}]^\times \cap B^\times/\mathbb{Q}[\beta\alpha\beta^{-1}]^\times\right|,$$

where the last equality holds by the following reason:

Let

$$\varphi : U\beta\mathbb{Q}_A[\alpha]^\times \cap B^\times \longrightarrow U\beta\mathbb{Q}_A[\alpha]^\times\beta^{-1} \cap B^\times = U\mathbb{Q}_A[\beta\alpha\beta^{-1}]^\times \cap B^\times$$

$$\varphi : u\beta t \longmapsto u\beta t\beta^{-1},\ u \in U, t \in \mathbb{Q}_A[\alpha]$$

Let $x, y \in U\beta\mathbb{Q}_A[\alpha]^\times \cap B^\times$, then

$$y \equiv x (\operatorname{mod} \mathbb{Q}[\alpha]^\times) \Leftrightarrow y = xa\ (a \in \mathbb{Q}[\alpha]^\times) \Leftrightarrow$$

$$\Leftrightarrow y\beta^{-1} = xa\beta^{-1} \Leftrightarrow y\beta^{-1} = x\beta^{-1}(\beta a\beta^{-1}) \Leftrightarrow$$

$$\Leftrightarrow y\beta^{-1} \equiv x\beta^{-1}(\operatorname{mod} \beta\mathbb{Q}[\alpha]^\times\beta^{-1}) \Leftrightarrow y\beta^{-1} \equiv x\beta^{-1}(\operatorname{mod} \mathbb{Q}[\beta\alpha\beta^{-1}]^\times).$$

Now, since $B_A^\times = B^\times \cdot U$ it follows that for any commutative subgroup E of $B_A^\times$, for any $t \in E$, there is a $u \in U$, such that $ut \in UE \cap B^\times$. Let $t_1, t_2 \in E$ and $u_1, u_2 \in U$. Assume $u_1t_1, u_2t_2 \in UE \cap B^\times$ then

$$\Gamma u_1t_1(E \cap B^\times) = \Gamma u_2t_2(E \cap B^\times) \Longleftrightarrow t_1t_2^{-1} \in (E \cap U)(E \cap B^\times),$$

since $\Gamma = U \cap B^\times$. Thus

$$\left|\Gamma \backslash UE \cap B^\times / E \cap B^\times\right| = \left|E/(E \cap U)(E \cap B^\times)\right|.$$

Since $\mathbb{Q}_A[\beta\alpha\beta^{-1}]^\times \cap B^\times = \mathbb{Q}[\beta\alpha\beta^{-1}]^\times$ we can apply the last result for $E = \mathbb{Q}_A[\beta\alpha\beta^{-1}]^\times$. So we get

$$\begin{aligned}\left|\theta^{-1}\left(C_U(g)\right)\right| &= \left|\mathbb{Q}_A[\beta\alpha\beta^{-1}]^\times / (\mathbb{Q}_A[\beta\alpha\beta^{-1}] \cap U) \cdot \mathbb{Q}[\beta\alpha\beta^{-1}]^\times\right| \\ &= \left|\mathbb{Q}_A[\alpha]^\times / (\mathbb{Q}_A[\alpha] \cap \beta^{-1}U\beta) \cdot \mathbb{Q}[\alpha]^\times\right|.\end{aligned}$$

Since $U = GL_2^+(\mathbb{R}) \times \prod\limits_p R_p^\times$ we have for $g \in C_A(\alpha, \mathfrak{r})$

$$\mathbb{Q}_A[\alpha] \cap \beta^{-1}U\beta = \mathbb{Q}_A[\alpha] \cap h^{-1}Uh = \mathbb{Q}_A[\alpha] \cap h^{-1}\left(GL_2^+(\mathbb{R}) \times \prod_p R_p^\times\right) h = \mathfrak{r}_{A^+}^\times$$

Therefore

$$\left|\theta^{-1}\left(C_U(g)\right)\right| = \left|\mathbb{Q}_A[\alpha]^\times / \mathfrak{r}_{A^+}^\times \cdot \mathbb{Q}[\alpha]^\times\right| = h(\mathfrak{r}).$$

(see the definitions of the Section 2). Thus we have

$$|C(\alpha, \mathfrak{r})//\Gamma| = h(\mathfrak{r}) \; |C_A(\alpha, \mathfrak{r})//U|.$$

Write

$$U = GL_2^+(\mathbb{R}) \times \prod_p R_p^\times = \prod_{v=\infty,2,3,5,\ldots} R_v^\times$$

and we will get the claim of the lemma:

$$|C(\alpha, \mathfrak{r})//\Gamma| = h(\mathfrak{r}) \prod_{v=\infty,2,3,5,\ldots} \left|C_v(\alpha, \mathfrak{r})//R_v^\times\right|.$$

■

Now we calculate each of the factors $|C_v(\alpha, \mathfrak{r})//R_v^\times|$.

Let $v = \infty$.

Lemma 3.8 $|C_\infty(\alpha, \mathfrak{r})//R_\infty^\times| = \left\{\begin{array}{cc} 1, & \alpha \textit{ is hyperbolic} \\ 2, & \alpha \textit{ is parabolic or elliptic} \end{array}\right\}.$

Proof. Since $C_\infty(\alpha, \mathfrak{r}) = C_\infty(\alpha)$ and $R_\infty^\times = GL_2^+(\mathbb{R})$ we have

$$C_\infty(\alpha, \mathfrak{r})//R_\infty^\times = \{x\alpha x^{-1} \mid x \in GL_2(\mathbb{R})\}//GL_2^+(\mathbb{R}).$$

Let $g \in GL_2^+(\mathbb{R})$, then

$$y\alpha y^{-1} = g^{-1}(x\alpha x^{-1})g \Longleftrightarrow \alpha = y^{-1}g^{-1}x\alpha x^{-1}gy$$
$$\Longleftrightarrow x^{-1}gy \in Z(\alpha) \Longleftrightarrow y \in g^{-1}xZ(\alpha).$$

It follows

$$y \in GL_2^+(\mathbb{R})xZ(\alpha).$$

From the other hand, if $y \in GL_2^+(\mathbb{R})xZ(\alpha)$, then there are $z \in Z(\alpha), g \in GL_2^+(\mathbb{R})$ such that $y = gxz$ and

$$y\alpha y^{-1} = gxz\alpha(gxz)^{-1} = gxz\alpha z^{-1}x^{-1}g^{-1} = g(x\alpha x^{-1})g^{-1},$$

and $y\alpha y^{-1}$ is $GL_2^+(\mathbb{R})$-conjugate to $x\alpha x^{-1}$. Thus we have

$$\left|\{x\alpha x^{-1} \mid x \in GL_2(\mathbb{R})\}//GL_2^+(\mathbb{R})\right| = \left|GL_2^+(\mathbb{R})\backslash GL_2(\mathbb{R})/Z(\alpha)\right|.$$

If α is a hyperbolic element, then there is matrix $B \in GL_2(\mathbb{R})$, such that $\alpha = B^{-1}\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}B$. The centralizer Z of $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}$ in $GL_2(\mathbb{R})$ is the set of all invertible diagonal matrices with real entries. Since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in Z$, we see that $\left|GL_2^+(\mathbb{R})\backslash GL_2(\mathbb{R})/Z\right| = 1$. But $Z(\alpha) = B^{-1}ZB$, therefore we also have

$$\left|GL_2^+(\mathbb{R})\backslash GL_2(\mathbb{R})/Z(\alpha)\right| = 1.$$

For α be elliptic or parabolic one shows in a similar manner that

$$\left|GL_2^+(\mathbb{R})\backslash GL_2(\mathbb{R})/Z(\alpha)\right| = 2.$$

Finally,

$$\left|C_\infty(\alpha, \mathfrak{r})//R_\infty^\times\right| = \left\{ \begin{array}{ll} 2, & \alpha \text{ is parabolic or elliptic} \\ 1, & \alpha \text{ is hyperbolic} \end{array} \right\}.$$

■

Now let $\upsilon = p$. We want to know what elements of $M_2(\mathbb{Q}_p)$ are in $C_p(\alpha, \mathfrak{r})$, where α is a non-scalar element of

$$R_p = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_p) \mid c \equiv 0 (\operatorname{mod} p^\nu) \right\}.$$

(if $p \nmid N$ then $\nu = 0$ and $R_p = M_2(\mathbb{Z}_p)$).

Let

$$f_\alpha(X) = X^2 - tX + 1, \qquad (t \in \mathbb{Z}_p),$$

be the minimal polynomial of α, and let $\mathfrak{r}_p$ be an order of $\mathbb{Q}_p[\alpha]$ including an order $\mathbb{Z}_p[\alpha]$. We put

$$[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho, \qquad (\rho \geq 0).$$

Since all orders of $M_2(\mathbb{Q}_p)$ are of the form

$$\mathbb{Z}_p + p^n \omega \mathbb{Z}, \quad (\omega = \frac{d+\sqrt{d}}{2}, t^2 - 4 = dl^2),$$

it follows that $\mathfrak{r}_p$ is uniquely determined by ρ.

Lemma 3.9 *Let R_p be an order of $M_2(\mathbb{Z}_p)$ as above, α be a non-scalar element of R_p, and $\mathfrak{r}_p$ an order of $\mathbb{Q}_p[\alpha]$, such that $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$, and $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$, $(\rho \geq 0)$. For an element $g \in C_p(\alpha)$ the following statements are equivalent:*

(1) $g \in C_p(\alpha, \mathfrak{r})$*;*

(2) $g \in \mathbb{Z}_p + p^\rho R_p$ *and* $g \notin \mathbb{Z}_p + p^{\rho+1} R_p$*;*

(3) if $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *then* $b \equiv a - d \equiv 0 (\operatorname{mod} p^\rho)$, $c \equiv 0 (\operatorname{mod} p^{\rho+\nu})$,

and any one of the following three conditions is satisfied:

(i) $b \not\equiv 0 (\operatorname{mod} p^{\rho+1})$*;*

(ii) $c \not\equiv 0 (\operatorname{mod} p^{\rho+\nu+1})$*;*

(iii) $a - d \not\equiv 0 (\operatorname{mod} p^{\rho+1})$.

Proof. (1) $\Longleftrightarrow$ (2):

Put $g = h\alpha h^{-1}$ with $h \in GL_2(\mathbb{Q}_p)$. Then

$g \in C_p(\alpha, \mathfrak{r}) \Longleftrightarrow \mathbb{Q}_p[\alpha] \cap h^{-1} R_p h = \mathfrak{r}_p \Longleftrightarrow \mathbb{Q}_p[g] \cap R_p = h \mathfrak{r}_p h^{-1} \Longleftrightarrow$

$\Longleftrightarrow [\mathbb{Q}_p[g] \cap R_p : \mathbb{Z}_p[g]] = p^\rho$, since $\left[\mathbb{Q}_p[\alpha] \cap h^{-1} R_p h : \mathbb{Z}_p[\alpha]\right] = p^\rho$.

But

$$[\mathbb{Q}_p[g] \cap R_p : \mathbb{Z}_p[g]] = p^\rho \Longleftrightarrow \mathbb{Z}_p[g] = \mathbb{Z}_p + \mathbb{Q}_p[g] \cap p^\rho R_p,$$

since all orders in $\mathbb{Q}_p[g]$ are of the form $\mathbb{Z}_p + p^n \omega \mathbb{Z}_p$, for suitable ω. This implies the equivalence of (1) and (2).

(2) $\Longleftrightarrow$ (3): It follows from the definition of R_p. ∎

After this lemma we ask ourselves what elements of R_p are in $C_p(\alpha,\mathfrak{r})$. We see that first of all this elements have trace t and determinant 1, and so them of the form

$$\begin{bmatrix} \xi & kp^\rho \\ c & t-\xi \end{bmatrix},$$

where
(*i*) $t-2\xi \equiv 0(\operatorname{mod} p^\rho)$;
(*ii*) $k \in \mathbb{Z}_p^\times$;
(*iii*) $c \equiv 0(\operatorname{mod} p^{\rho+\nu})$;
(*iv*) $\xi(t-\xi) - ckp^\rho = 1$.

From (*iv*) we have $c = -k^{-1}p^{-\rho} f_\alpha(\xi)$, and since (*ii*) and (*iii*) must be satisfied it follows that

$$f_\alpha(\xi) \equiv 0(\operatorname{mod} p^{2\rho+\nu}).$$

We take $k=1$ and put

$$g_\xi = \begin{bmatrix} \xi & p^\rho \\ -p^{-\rho} f_\alpha(\xi) & t-\xi \end{bmatrix} \in R_p,$$

where

$$\xi \in \Omega(\alpha,\mathfrak{r}_p) := \left\{ \xi \in \mathbb{Z}_p \mid f_\alpha(\xi) \equiv 0(\operatorname{mod} p^{2\rho+\nu}), t-2\xi \equiv 0(\operatorname{mod} p^\rho) \right\}.$$

Therefore by definition we have $g_\xi \in C_p(\alpha,\mathfrak{r})$.

Lemma 3.10 *On the conditions of the previous lemma, for $g \in C_p(\alpha)$ we have that $g \in C_p(\alpha,\mathfrak{r})$ iff g is $N(R_p)$-conjugate to g_ξ for some $\xi \in \Omega(\alpha,\mathfrak{r}_p)$. Here*

$$N(R_p) = \left\{ \begin{array}{cc} \mathbb{Q}_p^\times R_p^\times & \text{if } \nu = 0 \\ \mathbb{Q}_p^\times R_p^\times \cup \begin{bmatrix} 0 & 1 \\ p^\nu & 0 \end{bmatrix} \mathbb{Q}_p^\times R_p^\times & \text{if } \nu > 0 \end{array} \right\},$$

the normalizer of the R_p (see [19, Lemma 6.6.2]).

Proof. Let g is $N(R_p)$-conjugate to g_ξ for some $\xi \in \Omega(\alpha,\mathfrak{r}_p)$. That is $g = xg_\xi x^{-1}$ for $x \in N(R_p)$. The direct calculations show that g satisfies condition (3) of the previous lemma, and so $g \in C_p(\alpha,\mathfrak{r})$.

Suppose $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C_p(\alpha,\mathfrak{r})$, then g satisfies condition (3). Let (*i*) is fulfilled. Put

$$b = kp^\rho, k \in \mathbb{Z}_p^\times$$

Since $g \in C_p(\alpha)$, it follows that g is similar to α and

$$f_\alpha(g) = 0.$$

In particular,

$$t = a + d, \text{ and } ad - bc = 1,$$

so that

$$f_\alpha(a) = a^2-(a+d)a+ad-bc = -bc \equiv 0(\operatorname{mod} p^{2\rho+\nu}) \text{ and } t-2a \equiv 0(\operatorname{mod} p^{\rho}).$$

Thus $a \in \Omega(\alpha, \mathfrak{r}_p)$. Moreover we see

$$g = u^{-1} g_\xi u, \text{ for } u = \begin{bmatrix} 1 & 0 \\ 0 & k \end{bmatrix} \in R_p^\times.$$

Let now (ii) is fulfilled. We have $\begin{bmatrix} 0 & 1 \\ p^\nu & 0 \end{bmatrix} \in N(R_p)$. Put

$$\widetilde{g} = \begin{bmatrix} 0 & 1 \\ p^\nu & 0 \end{bmatrix} g \begin{bmatrix} 0 & 1 \\ p^\nu & 0 \end{bmatrix}^{-1} = \begin{bmatrix} d & cp^{-\nu} \\ p^\nu & a \end{bmatrix}.$$

Since $c \equiv 0(\operatorname{mod} p^{\rho+\nu})$, we get

$$cp^{-\nu} = c_1 p^{\rho+\nu} p^{-\nu} = c_1 p^\rho \quad (c_1 \in \mathbb{Z}_p^\times).$$

So we have

$$cp^{-\nu} \equiv 0(\operatorname{mod} p^\rho) \text{ and } cp^{-\nu} \not\equiv 0(\operatorname{mod} p^{\rho+1}),$$

that is $\widetilde{g}$ satisfies (i). Therefore $\widetilde{g}$ is $R_p^\times$-conjugate to g_d as before, and thus g is $N(R_p)$-conjugate to g_d.

Lastly assume condition (iii). We may suppose that

$$b \equiv 0(\operatorname{mod} p^{\rho+1}) \text{ and } c \equiv 0(\operatorname{mod} p^{\nu+\rho+1}).$$

Let $u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in R_p^\times$. Then

$$ugu^{-1} = \begin{bmatrix} a+c & -a+d+b-c \\ c & -c+d \end{bmatrix},$$

we see that $-a+d+b-c \not\equiv 0(\operatorname{mod} p^{\rho+1})$, and so ugu^{-1} satisfies (i). We finish as in the previous cases. ■

For $\nu \geq 1$, we put $w = \begin{bmatrix} 0 & 1 \\ p^{\nu} & 0 \end{bmatrix} \in N(R_p)$. Then for $\xi \in \Omega(\alpha, \mathfrak{r}_p)$,

$$wg_{\xi}w^{-1} = \begin{bmatrix} t-\xi & -f_{\alpha}(\xi)p^{-\rho-\nu} \\ p^{\rho+\nu} & \xi \end{bmatrix} \in C_p(\alpha, \mathfrak{r}).$$

And so we have

$$C_p(\alpha, \mathfrak{r}) = \left\{ \begin{array}{cc} \{g_{\xi} \mid \xi \in \Omega(\alpha, \mathfrak{r}_p)\} //R_p^{\times}, & \nu = 0 \\ \{g_{\xi}, wg_{\xi}w^{-1} \mid \xi \in \Omega(\alpha, \mathfrak{r}_p)\} //R_p^{\times}, & \nu \geq 1 \end{array} \right\}.$$

Now we will conclude some results about $R_p^{\times}$-conjugation in $\Omega(\alpha, \mathfrak{r}_p)$.

Lemma 3.11 *Let ξ, η be two elements of $\Omega(\alpha, \mathfrak{r}_p)$.*
(1) *g_{ξ} and g_{η} are $R_p^{\times}$-conjugate iff $\xi \equiv \eta (\operatorname{mod} p^{\rho+\nu})$;*
(2) *Suppose $\nu \geq 1$. Then g_{ξ} and $wg_{\eta}w^{-1}$ are $R_p^{\times}$-conjugate iff ξ and η satisfy the following two conditions:*
(i) $t^2 - 4 \not\equiv 0 (\operatorname{mod} p^{2\rho+1})$ or $f_{\alpha}(\eta) \not\equiv 0 (\operatorname{mod} p^{2\rho+\nu+1})$;
(ii) $\xi \equiv t - \eta (\operatorname{mod} p^{\rho+\nu})$.

Proof. (1) Suppose $\xi \equiv \eta (\operatorname{mod} p^{\rho+\nu})$. Then for

$$u = \begin{bmatrix} 1 & 0 \\ -p^{-\rho}(\xi - \eta) & 1 \end{bmatrix} \in R_p^{\times}$$

we have $ug_{\xi}u^{-1} = g_{\eta}$.

Conversely assume $g_{\eta} = ug_{\xi}u^{-1}$ with $u \in R_p^{\times}$. We have

$$g_{\xi} - \xi = \begin{bmatrix} 0 & p^{\rho} \\ -p^{-\rho}f_{\alpha}(\xi) & t - 2\xi \end{bmatrix} \equiv 0 (\operatorname{mod} p^{\rho}),$$

hence

$$p^{-\rho}(g_{\xi} - \xi) \in R_p,$$

so that

$$p^{-\rho}(g_{\eta} - \xi) = up^{-\rho}(g_{\xi} - \xi)u^{-1} \in R_p.$$

We calculate

$$p^{-\rho}(g_{\eta} - \xi) = \begin{bmatrix} p^{-\rho}(\eta - \xi) & * \\ * & * \end{bmatrix}.$$

In other hand for $u = \begin{bmatrix} a & b \\ cp^{\nu} & d \end{bmatrix} \in R_p^{\times}$

$$up^{-\rho}(g_{\xi} - \xi)u^{-1} = \frac{p^{-\rho}}{ad - bcp^{\nu}} \begin{bmatrix} a & b \\ cp^{\nu} & d \end{bmatrix} \begin{bmatrix} 0 & p^{\rho} \\ -p^{-\rho}f_{\alpha}(\xi) & t - 2\xi \end{bmatrix} \begin{bmatrix} d & -b \\ -cp^{\nu} & a \end{bmatrix} =$$

$$= \frac{1}{ad - bcp^{\nu}} \begin{bmatrix} -bdp^{-2\rho} f_{\alpha}(\xi) - cap^{\nu} - cbp^{\nu-\rho}(t-2\xi) & * \\ * & * \end{bmatrix}.$$

So we see that

$$p^{-\rho}(\eta - \xi) \equiv 0 (\operatorname{mod} p^{\nu}),$$

and thus

$$\xi \equiv \eta (\operatorname{mod} p^{\rho+\nu}).$$

(2) We will show first that $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C_p(\alpha, \mathfrak{r})$ is $R_p^{\times}$-conjugate to g_{ξ} for some $\xi \in \Omega(\alpha, \mathfrak{r}_p)$ iff

$$b \not\equiv 0 (\operatorname{mod} p^{\rho+1}) \text{ or } \; a - d \not\equiv 0 (\operatorname{mod} p^{\rho+1}).$$

The if-part was proved in the previous lemma. Assume

$$b \equiv a - d \equiv 0 (\operatorname{mod} p^{\rho+1}),$$

and

$$ugu^{-1} = g_{\xi} \qquad (u = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in R_p^{\times}, \xi \in \Omega(\alpha, \mathfrak{r}_p)).$$

By previous lemma $c \equiv 0 (\operatorname{mod} p^{\rho+\nu})$ and so

$$g_{\xi} = ugu^{-1} \equiv \begin{bmatrix} * & (-a'b'(a-d) + a'^2 b)/(a'd' - b'c') \\ * & * \end{bmatrix} (\operatorname{mod} p^{\rho+\nu}),$$

but

$$-a'b'(a-d) + a'^2 b \equiv 0 (\operatorname{mod} p^{\rho+1}),$$

and this contradicts the definition of g_{ξ}.

By definition we have

$$w g_{\eta} w^{-1} = \begin{bmatrix} t - \eta & -p^{-\rho-\nu} f_{\alpha}(\eta) \\ p^{\rho+\nu} & \eta \end{bmatrix} \in C_p(\alpha, \mathfrak{r}),$$

and so

$$-p^{-\rho-\nu} f_{\alpha}(\eta) \not\equiv 0 (\operatorname{mod} p^{\rho+1}) \text{ or } \; 2\eta - t \not\equiv 0 (\operatorname{mod} p^{\rho+1}).$$

Equivalently:

$$f_{\alpha}(\eta) \not\equiv 0 (\operatorname{mod} p^{2\rho+\nu+1}) \text{ or } \; 2\eta - t \not\equiv 0 (\operatorname{mod} p^{\rho+1}),$$

and since

$$\eta(t-\eta) \equiv 1 (\operatorname{mod} p^{\nu+2\rho}),$$

we see that

$$(2\eta - t)^2 = 4\eta^2 - 4\eta t + t^2 = t^2 - 4\eta(t-\eta) \equiv t^2 - 4 (\operatorname{mod} p^{\nu+2\rho}).$$

Thus we see that

$$2\eta - t \not\equiv 0 (\operatorname{mod} p^{\rho+1}) \Longleftrightarrow t^2 - 4 \not\equiv 0 (\operatorname{mod} p^{2\rho+1}),$$

and we have condition (i).

Condition (ii) we get by argument similar to part (1) of the lemma. ■

Now assume $\Omega(\alpha, \mathfrak{r}_p) \neq \emptyset$ and let $\xi \in \Omega(\alpha, \mathfrak{r}_p)$. Then

$$t^2 - 4 \equiv (t - 2\xi)^2 (\operatorname{mod} p^{2\rho+\nu}),$$

and by definition of $\Omega(\alpha, \mathfrak{r}_p)$ we have $t^2 - 4 \equiv 0 (\operatorname{mod} p^{2\rho})$.

Conversely, suppose that α such that $t^2 - 4 \equiv 0 (\operatorname{mod} p^{2\rho})$. If $\xi \in \mathbb{Z}_p$ satisfies

$$f_\alpha(\xi) \equiv 0 (\operatorname{mod} p^{2\rho+\nu}),$$

then

$$\xi(t-\xi) \equiv 1 (\operatorname{mod} p^{2\rho+\nu}) \equiv 1 (\operatorname{mod} p^{2\rho}),$$

and

$$(t-2\xi)^2 = t^2 - 4\xi(t-\xi) \equiv t^2 - 4 (\operatorname{mod} p^{2\rho}) \equiv 0 (\operatorname{mod} p^{2\rho}).$$

Thus

$$t - 2\xi \equiv 0 (\operatorname{mod} p^{\rho}).$$

Therefore

$$\Omega(\alpha, \mathfrak{r}_p) = \left\{ \begin{array}{cc} \left\{\xi \in \mathbb{Z}_p \mid f_\alpha(\xi) \equiv 0 (\operatorname{mod} p^{2\rho+\nu})\right\}, & t^2 - 4 \equiv 0 (\operatorname{mod} p^{2\rho}) \\ \emptyset, & \text{otherwise} \end{array} \right\}.$$

We also put

$$\Omega'(\alpha, \mathfrak{r}_p) = \left\{ \begin{array}{cc} \left\{\xi \in \mathbb{Z}_p \mid f_\alpha(\xi) \equiv 0 (\operatorname{mod} p^{2\rho+\nu+1})\right\}, & t^2 - 4 \equiv 0 (\operatorname{mod} p^{2\rho+1}), \nu \geq 1 \\ \emptyset, & \text{otherwise} \end{array} \right\}.$$

Combining we have

Proposition 3.12 *Assume $\nu \geq 1$. Let α be a non-scalar element of R_p and $f_\alpha(X) = X^2 - tX + 1$ the minimal polynomial of α. For any order $\mathfrak{r}_p$ of $\mathbb{Q}_p[\alpha]$ including $\mathbb{Z}_p[\alpha]$ such that $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$, $(\rho \geq 0)$, we can take as a complete set of representatives of $C_p(\alpha, \mathfrak{r})//R_p^\times$ the set*

$$\left\{ g_\xi \mid \xi \in \Omega/p^{\rho+\nu} \right\} \cup \left\{ w g_\xi w^{-1} \mid \xi \in \Omega'/p^{\rho+\nu} \right\},$$

where $\Omega/p^{\rho+\nu}$ (resp. $\Omega'/p^{\rho+\nu}$) is a complete set of representatives of $\Omega(\alpha, \mathfrak{r}_p) \bmod p^{\rho+\nu}$ (resp. $\Omega'(\alpha, \mathfrak{r}_p) \bmod p^{\rho+\nu}$).

Now we can return to our case, i.e.

$$R_p = M_2(\mathbb{Z}_p) \qquad \text{if} \qquad p \nmid N,$$

and

$$R_p = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_p) \mid c \equiv 0 (\operatorname{mod} p^\nu) \right\} \text{ if } p \mid N \text{ and } ord_p N = \nu.$$

Lemma 3.13 *If $R_p = M_2(\mathbb{Z}_p)$ then $\left| C_p(\alpha, \mathfrak{r})//R_p^\times \right| = 1$.*

Proof. Since any order $\mathfrak{r}_p$ of $\mathbb{Q}_p[\alpha]$ is a $\mathbb{Z}_p$-free module we can write

$$\mathfrak{r}_p = \mathbb{Z}_p[\beta] \text{ with } \beta \in \mathbb{Q}_p[\alpha].$$

Put

$$\beta = a + b\alpha \qquad\qquad (a, b \in \mathbb{Q}_p).$$

Then $C_p(\alpha, \mathfrak{r})//R_p^\times$ corresponds bijectively to $C_p(\beta, \mathfrak{r})//R_p^\times$ through the correspondence $g \longmapsto a + bg$. Since $[\mathfrak{r}_p : \mathbb{Z}_p[\beta]\ ] = 1$ we see that $\rho = 0$, and $\Omega(\beta, \mathfrak{r}_p) = \mathbb{Z}_p$. Then by previous lemma we have

$$\left| C_p(\alpha, \mathfrak{r})//R_p^\times \right| = \left| C_p(\beta, \mathfrak{r})//R_p^\times \right| = 1.$$

■

Now we are left with $p \mid N$. Since N is squarefree we see that $\nu = 1$. We will show

Lemma 3.14 *Let N be squarefree. For prime number p, such that $p \mid N$ we have*

$$\left| C_p(\alpha, \mathfrak{r})//R_p^\times \right| = \left\{ \begin{array}{cc} 2, & p \mid f \\ 1 + \left(\frac{d}{p}\right), & p \nmid f \end{array} \right\}.$$

Proof. We proved that

$$\left|C_p(\alpha,\mathfrak{r})//R_p^{\times}\right| = \left|\Omega/p^{1+\rho}\right| + \left|\Omega'/p^{1+\rho}\right|.$$

Let

$$\mathfrak{r}_p = (\mathfrak{r}[f])_p = \mathbb{Z}_p + f\omega\mathbb{Z}_p \qquad (\omega = \frac{d+\sqrt{d}}{2}, t^2-4 = l^2 d).$$

In other hand $(\mathfrak{r}[f])_p = \mathfrak{o}[p^n]$, where $n = ord_p f$. Since

$$\mathbb{Z}_p[\alpha] = (\mathfrak{r}[l])_p = \mathbb{Z}_p + l\omega\mathbb{Z}_p,$$

we see that

$$\rho = ord_p \frac{l}{f}.$$

We have

$$\Omega = \{\xi \in \mathbb{Z}_p \mid \xi^2 - t\xi + 1 \equiv 0 (\operatorname{mod} p^{2\rho+1})\},$$

the condition $t^2-4 \equiv 0(\operatorname{mod} p^{2\rho})$ is fulfilled, since $t^2-4 = dl^2 = df^2p^{2\rho}$.

$$\Omega' = \left\{ \begin{array}{lr} \{\xi \in \mathbb{Z}_p \mid \xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+2})\}, & t^2-4 = l^2 d \equiv 0(\operatorname{mod} p^{2\rho+1}) \\ \emptyset, & \text{otherwise} \end{array} \right\}.$$

Assume $p \neq 2$. For $\xi \in \mathbb{Z}_p$ we find

$$\begin{aligned} \xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+1}) &\Longleftrightarrow (2\xi - t)^2 \equiv l^2 d(\operatorname{mod} p^{2\rho+1}) \\ &\Longleftrightarrow (2\xi - t)^2 \equiv df^2p^{2\rho}(\operatorname{mod} p^{2\rho+1}). \end{aligned}$$

If $p \mid f$ then

$$\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+1}) \Longleftrightarrow \xi = \frac{t}{2}(\operatorname{mod} p^{\rho+1}).$$

(Note that $\frac{t}{2} \in \mathbb{Z}_p$, since $p \neq 2$). If $p \mid d$ then

$$\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+1}) \Longleftrightarrow \xi = \frac{t}{2}(\operatorname{mod} p^{\rho+1}).$$

If $p \nmid f, p \nmid d$ then the congruence $\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+1})$ has two incongruent solutions $\operatorname{mod} p^{\rho+1}$ if $\left(\frac{d}{p}\right) = 1$, and no solutions if $\left(\frac{d}{p}\right) = -1$. So we have

$$\left|\Omega/p^{1+\rho}\right| = \left\{ \begin{array}{lc} 1, & p \mid f \\ 2, & p \nmid f, \left(\frac{d}{p}\right) = 1 \\ 0, & p \nmid f, \left(\frac{d}{p}\right) = -1 \\ 1, & p \nmid f, \left(\frac{d}{p}\right) = 0 \end{array} \right\}.$$

In the similar way

$$\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+2}) \Longleftrightarrow (2\xi - t)^2 \equiv l^2 d(\operatorname{mod} p^{2\rho+2})$$
$$\Longleftrightarrow (2\xi - t)^2 \equiv df^2 p^{2\rho}(\operatorname{mod} p^{2\rho+2}).$$

If $p \nmid f$ and $d = ps$, where $p \nmid s$. We have that the congruence $\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+2})$ is equivalent to the congruence

$$(2\xi - t)^2 \equiv sf^2 p^{2\rho+1}(\operatorname{mod} p^{2\rho+2}),$$

but thus we see that

$$(2\xi - t)^2 \equiv 0(\operatorname{mod} p^{2\rho+1}) \text{ and so } (2\xi - t)^2 \equiv 0(\operatorname{mod} p^{2\rho+2}).$$

The last congruence is impossible, since $p \nmid f$ and $p \nmid s$. Hence $\Omega' = \emptyset$.

If $p \nmid f$ and $p \nmid d$ we have that $p^{2\rho+1} \nmid l^2 d$ and so $\Omega' = \emptyset$.

If $p \mid f$ then $l^2 d \equiv 0(\operatorname{mod} p^{2\rho+2})$ and

$$\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} p^{2\rho+2}) \Longleftrightarrow \xi = \frac{t}{2}(\operatorname{mod} p^{\rho+1}).$$

We get

$$\left|\Omega'/p^{1+\rho}\right| = \left\{ \begin{array}{ll} 1, & p \mid f \\ 0, & p \nmid f \end{array} \right\}.$$

Combining together we have that for $p \nmid N$

$$\left|C_p(\alpha, \mathfrak{r})//R_p^\times\right| = \left\{ \begin{array}{ll} 2, & p \mid f \\ 2, & p \nmid f, \left(\frac{d}{p}\right) = 1 \\ 0, & p \nmid f, \left(\frac{d}{p}\right) = -1 \\ 1, & p \nmid f, \left(\frac{d}{p}\right) = 0 \end{array} \right\} = \left\{ \begin{array}{ll} 2, & p \mid f \\ 1 + \left(\frac{d}{p}\right), & p \nmid f \end{array} \right\}.$$

For $p = 2$ we consider two cases:

(i) $2 \mid f$. In this case we have that $\frac{t}{2} \in \mathbb{Z}_2$, since $t^2 - 4 = dl^2$, and $f \mid l$.

We also have that for the set Ω

$$\xi^2 - t\xi + 1 \equiv 0(\operatorname{mod} 2^{2\rho+1}) \Longleftrightarrow (2\xi - t)^2 \equiv l^2 d(\operatorname{mod} 2^{2\rho+3})$$
$$\Longleftrightarrow (2\xi - t)^2 \equiv df^2 2^{2\rho}(\operatorname{mod} 2^{2\rho+3}) \Longleftrightarrow$$
$$\Longleftrightarrow (2\xi - t)^2 \equiv df'^2 2^{2\rho+2}(\operatorname{mod} 2^{2\rho+3}).$$

If $d \equiv 1 (\bmod 8)$ the last congruence have two incongruent solutions for $2\xi - t$ modulo $2^{2\rho+3}$, which imply only one solution ξ modulo $2^{\rho+1}$.

If $d \equiv 5 (\bmod 8)$ then $d \equiv 1 (\bmod 4)$ and

$$(2\xi - t)^2 \equiv f'^2 2^{2\rho+2}(2^2 d' + 1)(\bmod 2^{2\rho+3}) \equiv f'^2 2^{2\rho+2}(\bmod 2^{2\rho+3}),$$

and there are two solutions for $2\xi - t$ modulo $2^{2\rho+3}$, which imply only one solution ξ modulo $2^{\rho+1}$.

If $d \equiv 0 (\bmod 4)$ there is one solution $\xi \equiv \frac{t}{2} (\bmod 2^{\rho+1})$.

For the set Ω' we have that

$$\xi^2 - t\xi + 1 \equiv 0(\bmod 2^{2\rho+2}) \Longleftrightarrow (2\xi - t)^2 \equiv df'^2 2^{2\rho+2}(\bmod 2^{2\rho+4}),$$

and by the same arguments we have exactly the same results.

(ii) $2 \nmid f$. For the set Ω'

$$\begin{aligned} \xi^2 - t\xi + 1 \equiv 0(\bmod 2^{2\rho+2}) &\Longleftrightarrow (2\xi - t)^2 \equiv l^2 d(\bmod 2^{2\rho+4}) \\ &\Longleftrightarrow (2\xi - t)^2 \equiv df^2 2^{2\rho}(\bmod 2^{2\rho+4}). \end{aligned}$$

If $d \equiv 1, 5 (\bmod 8)$ we have $\Omega' = \emptyset$, since $2^{2\rho+1} \nmid dl^2$.

If $d \equiv 0 (\bmod 8)$ then $(2\xi - t)^2 \equiv 0(\bmod 2^{2\rho+3})$, and then $(2\xi - t)^2 \equiv 0(\bmod 2^{2\rho+4})$, that contradicts either the definition of the fundamental discriminant or the assumption $2 \nmid f$.

If $d \equiv 4 (\bmod 8)$ we have that $d \equiv -4 (\bmod 16)$ or $d \equiv 4 (\bmod 16)$. If $d \equiv -4 (\bmod 16)$, then has no solution, since -1 is not a square $\bmod 2^{2\rho+4}$.

If $d \equiv 4 (\bmod 16)$ we have $\dfrac{d}{4} \equiv 1 (\bmod 4)$, that contradicts the definition of the fundamental discriminant.

For the set Ω, if $2 \nmid f$, we consider two cases: $\rho \neq 0$ and $\rho = 0$.

Let $\rho \neq 0$, we still have $\dfrac{t}{2} \in \mathbb{Z}_2$, since $4 \mid t^2 - 4 = dl^2$.

$$\begin{aligned} \xi^2 - t\xi + 1 \equiv 0 (\operatorname{mod} 2^{2\rho+1}) &\Longleftrightarrow (2\xi - t)^2 \equiv l^2 d (\operatorname{mod} 2^{2\rho+3}) \\ &\Longleftrightarrow (2\xi - t)^2 \equiv df^2 2^{2\rho} (\operatorname{mod} 2^{2\rho+3}). \end{aligned}$$

If $d \equiv 1 (\operatorname{mod} 8)$ we have two incongruent solution for $2\xi - t$ modulo $2^{2\rho+3}$, which imply two incongruent solutions ξ modulo $2^{\rho+1}$.

If $d \equiv 5 (\operatorname{mod} 8)$ there is no solution, since $\left(\dfrac{5}{2}\right) = -1$.

If $d \equiv 0 (\operatorname{mod} 8)$ we have one solution ξ modulo $2^{\rho+1}$.

If $d \equiv 4 (\operatorname{mod} 8)$ we have two solutions for $2\xi - t$ modulo $2^{2\rho+3}$, which imply only one solution ξ modulo $2^{\rho+1}$.

In the case of $\rho = 0$ we want to be sure that if $d \equiv 1 (\operatorname{mod} 8)$ we still have two incongruent solutions ξ modulo $2^{\rho+1}$. Indeed

$$(2\xi - t)^2 \equiv df^2 (\operatorname{mod} 2^3) \Longleftrightarrow 2\xi \equiv t \pm f (\operatorname{mod} 2^3),$$

but $\dfrac{t \pm f}{2} \in \mathbb{Z}_2$, since $2 \nmid f$ and $2 \nmid t$, and we have the desired. ■

This finishes the proof of the Proposition 3.6.

Now we can apply the above results for $\alpha = T_t$ and $N = Q$ be an odd squarefree number. So we find:

Lemma 3.15

$$\beta_Q(t) = \sum_{f \mid l} h(df^2) \frac{\ln \varepsilon_d^{\left[\mathfrak{r}[1]^1 : \mathfrak{r}[f]^1\right]}}{\sqrt{t^2 - 4}} \cdot \prod_{q \mid Q} \left\{ \begin{array}{cc} 2, & q \mid f \\ 1 + \left(\dfrac{d}{q}\right) & q \nmid f \end{array} \right\},$$

where we write $t^2 - 4 = dl^2$ with d a fundamental discriminant and $l \geq 1$.

Proof. Immediately from proposition 3.6. ■

We can continue the process

$$\sum_{f|l} h(df^2)\frac{\ln \varepsilon_d^{\left[\mathfrak{r}[1]^1:\mathfrak{r}[f]^1\right]}}{\sqrt{t^2-4}} \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q \mid f \\ 1+\left(\dfrac{d}{q}\right) & q \nmid f \end{array}\right\} =$$

$$= \sum_{f|l}\frac{h(df^2)\ln \varepsilon_{df^2}}{l\sqrt{d}} \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q \mid f \\ 1+\left(\dfrac{d}{q}\right) & q \nmid f \end{array}\right\} =$$

$$= \sum_{\substack{f|l \\ (D=df^2)}} \frac{h(D)\ln \varepsilon_D}{l\cdot \frac{\sqrt{D}}{f}} \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q \mid f \\ 1+\left(\dfrac{d}{q}\right) & q \nmid f \end{array}\right\}.$$

Now using Dirichlet's class number formula $h(D)\ln \varepsilon_D = \sqrt{D}L(1,\chi_D)$, we get

$$\beta_Q(t) = \sum_{\substack{f|l \\ (D=df^2)}} L(1,\chi_D)\frac{f}{l} \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q \mid f \\ 1+\left(\dfrac{D}{q}\right) & q \nmid f \end{array}\right\} =$$

$$= \sum_{\substack{D,v\geq 1 \\ Dv^2=t^2-4}} \frac{1}{v}L(1,\chi_D) \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q \mid f \\ 1+\left(\dfrac{D}{q}\right) & q \nmid f \end{array}\right\} =$$

$$= \sum_{\substack{D,v\geq 1 \\ Dv^2=t^2-4}} \frac{1}{v}L(1,\chi_D) \cdot \prod_{q|Q}\left\{\begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array}\right\},$$

and the theorem 3.1 follows.

Remark 3.16 *Here D is a discriminant, i.e. $D \equiv 0, 1 (\mathrm{mod}\, 4)$. We assume it from now on.*

4 Factorization of weighted multiplicities

Here we factorize (lemma 4.1) the weighted multiplicities function as a finite products of a local terms, defined below.

We have

$$\beta_Q(n) = \sum_{\substack{D,v\geq 1\\ Dv^2=n^2-4}} \frac{1}{v} L(1,\chi_D) \cdot \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\}.$$

We use now the Euler product formula for $L(1,\chi_D)$. For $n \geq 3, P \geq Q$, define

$$\beta_{P,Q}(n) := \sum_{\substack{D,v\geq 1\\ Dv^2=n^2-4\\ p|v \Longrightarrow p\leq P}} \left(\frac{1}{v} \prod_{p\leq P} \left(1 - \frac{\chi_D(p)}{p}\right)^{-1} \right) \cdot \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\}.$$

Note, that

$$q^2 \mid D \Longleftrightarrow q^2 \mid (n^2-4)v^{-2} \Longleftrightarrow q^2 \mid (n^2-4) \prod_{\substack{p\leq P\\ p|v}} p^{-2b_p}$$

$$\Longleftrightarrow \left\{ \begin{matrix} q^2 \mid n^2-4 & , \ b_q = 0 \\ q^2 \mid (n^2-4)q^{-2b_q}, & b_q \neq 0 \end{matrix} \right\} \Longleftrightarrow q^2 \mid (n^2-4)q^{-2ord_q v}.$$

Hence

$$\beta_{P,Q}(n) = \sum_{\substack{D,v\geq 1\\ Dv^2=n^2-4\\ p|v \Longrightarrow p\leq P}} \left(\frac{1}{v} \prod_{p\leq P} \left(1 - \frac{\chi_D(p)}{p}\right)^{-1} \right) \times$$

$$\times \prod_{q|Q} \left\{ \begin{array}{cl} 2 & , \ q^2 \mid (n^2-4)q^{-2ord_q v} \\ 1+\left(\dfrac{(n^2-4)q^{-2ord_q v}}{q}\right) & , \ q^2 \nmid (n^2-4)q^{-2ord_q v} \end{array} \right\} .$$

Define a function

$$\beta_{(p,Q)}(n) := \sum_{b\geq 0} \frac{1}{p^b} \left(1 - \frac{1}{p}\chi_{(n^2-4)p^{-2b}}(p)\right)^{-1} \cdot \mathbb{I}_{p^b}(n) \ ,$$

where

$$\mathbb{I}_{p^b}(n) := \left\{ \begin{array}{ll} 1 & ,n^2 = 4(\bmod p^{2b}) \\ 0 & , \text{else} \end{array} \right\} \text{ , for } p \neq 2, p \nmid Q$$

$$\mathbb{I}_{2^b}(n) := \left\{ \begin{array}{lll} 1 & , n^2 = 4(\bmod\ 2^{2b}) & , (n^2-4)2^{-2b} \text{ is a discriminant} \\ 0 & , \text{else} & \end{array} \right\},$$

and for $q \mid Q$

$$\mathbb{I}_{q^b}(n) := \left\{ \begin{array}{lll} 2 & , n^2 = 4(\bmod\ q^{2b}) & , q^2 \mid (n^2-4)q^{-2b} \\ 1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right) & , n^2 = 4(\bmod\ q^{2b}) & , q^2 \nmid (n^2-4)q^{-2b} \\ 0 & , \text{else} & \end{array} \right\}.$$

Lemma 4.1 *For Q odd squarefree and $P \geq Q$ we have*

$$\beta_{P,Q}(n) = \prod_{\substack{p \leq P \\ p \nmid Q}} \beta_{(p,Q)}(n) \cdot \prod_{q \mid Q} \beta_{(q,Q)}(n).$$

Proof.

$$\prod_{\substack{p \leq P \\ p \nmid Q}} \beta_{(p,Q)}(n) \cdot \prod_{q \mid Q} \beta_{(q,Q)}(n) = \prod_{\substack{p \leq P \\ p \nmid Q}} \left(\sum_{b \geq 0} \frac{1}{p^b} \left(1 - \frac{1}{p}\chi_{(n^2-4)p^{-2b}}(p)\right)^{-1} \cdot \mathbb{I}_{p^b}(n) \right) \times$$

$$\prod_{q \mid Q} \left(\sum_{b \geq 0} \frac{1}{q^b} \left(1 - \frac{1}{q}\chi_{(n^2-4)q^{-2b}}(q)\right)^{-1} \mathbb{I}_{q^b}(n) \right).$$

After opening the brackets, we will get the sum of terms of the form:

$$\frac{1}{p_1^{b_1}} \left(1 - \frac{1}{p_1}\chi_{(n^2-4)p_1^{-2b_1}}(p_1)\right)^{-1} \mathbb{I}_{p_1^{b_1}}(n) \cdot \frac{1}{p_2^{b_2}} \left(1 - \frac{1}{p_2}\chi_{(n^2-4)p_2^{-2b_2}}(p_2)\right)^{-1} \mathbb{I}_{p_2^{b_2}}(n) \cdot \ldots \cdot$$

$$\frac{1}{p_k^{b_k}} \left(1 - \frac{1}{p_k}\chi_{(n^2-4)p_k^{-2b_k}}(p_k)\right)^{-1} \mathbb{I}_{p_k^{b_k}}(n) \cdot \frac{1}{q_1^{b_{q_1}}} \left(1 - \frac{1}{q_1}\chi_{(n^2-4)q_1^{-2b_{q_1}}}(q_1)\right)^{-1} \mathbb{I}_{q_1^{b_{q_1}}}(n) \cdot \ldots \cdot$$

$$\frac{1}{q_l^{b_{q_l}}} \left(1 - \frac{1}{q_l}\chi_{(n^2-4)q_l^{-2b_{q_l}}}(q_l)\right)^{-1} \mathbb{I}_{q_l^{b_{q_l}}}(n).$$

Therefore, since $P \geq Q$ we have

$$\prod_{\substack{p \leq P \\ p \nmid Q}} \beta_{(p,Q)}(n) \cdot \prod_{q \mid Q} \beta_{(q,Q)}(n) =$$

$$\sum_{b\geq 0}\prod_{\substack{p\leq P\\ n^2=4(\text{mod } p^{2b})\\ (n^2-4)2^{-2b}\text{ is}\\ \text{a discriminant}}}\frac{1}{p^b}\left(1-\frac{1}{p}\chi_{(n^2-4)p^{-2b}}(p)\right)^{-1}\times$$

$$\times\prod_{q|Q}\left\{\begin{array}{ll} 2 & ,\ q^2\mid(n^2-4)q^{-2ord_q v}\\ 1+\left(\dfrac{(n^2-4)q^{-2ord_q v}}{q}\right) & ,\ q^2\nmid(n^2-4)q^{-2ord_q v}\end{array}\right\}=$$

$$\sum_{\substack{D,v\geq 1\\ Dv^2=n^2-4\\ p|v\Longrightarrow p\leq P}}\left[\frac{1}{v}\prod_{p\leq P}\left(1-\frac{1}{p}\chi_D(p)\right)^{-1}\right]\times$$

$$\times\prod_{q|Q}\left\{\begin{array}{ll} 2 & ,\ q^2\mid(n^2-4)q^{-2ord_q v}\\ 1+\left(\dfrac{(n^2-4)q^{-2ord_q v}}{q}\right) & ,\ q^2\nmid(n^2-4)q^{-2ord_q v}\end{array}\right\}=\beta_{P,Q}(n).$$

■

5 Limit periodic functions and Fourier analysis

Let $s\geq 1$. For $f:\mathbb{N}\longrightarrow\mathbb{C}$, define the seminorm

$$\|f\|_s:=\left(\limsup_{N\to\infty}\frac{1}{N}\sum_{1\leq n\leq N}|f(n)|^s\right)^{1/s}\in[0,\infty).$$

A function f is called s-limit periodic if for every $\varepsilon>0$ there is a periodic function h with $\|f-h\|_s\leq\varepsilon$. The set $\mathcal{D}^s$ of all s-limit periodic functions becomes a Banach space with norm $\|\cdot\|_s$ if functions f_1, f_2 with $\|f_1-f_2\|_s=0$ are identified. If $1\leq s_1\leq s_2<\infty$, we have $\mathcal{D}^1\supseteq\mathcal{D}^{s_1}\supseteq\mathcal{D}^{s_2}$ as sets (but they are endowed with different norms). For all $f\in\mathcal{D}^1$, the mean value

$$M(f):=\lim_{N\to\infty}\frac{1}{N}\sum_{1\leq n\leq N}f(n)$$

exists. The space $\mathcal{D}^2$ is a Hilbert space with inner product

$$\langle f,h\rangle:=M(f\overline{h}),\qquad f,h\in\mathcal{D}^2\ .$$

For $u \in \mathbb{R}$, define $e_u(n) := e^{2\pi i u n}$, $n \in \mathbb{N}$. In $\mathcal{D}^2$, we have canonical orthonormal base $\left\{e_{a/b}\right\}$, where $1 \le a \le b$ and $\gcd(a,b) = 1$.

For all $f \in \mathcal{D}^1$, the Fourier coefficients $\widehat{f}(u) := M(fe_{-u})$, $u \in \mathbb{R}$, exist.

Lemma 5.1 *For $f \in \mathcal{D}^1, u \notin \mathbb{Q}$, we have $\widehat{f}(u) = 0$*

Proof. Let $f \in \mathcal{D}^1$. For any $\varepsilon > 0$ there is a linear combination $\sum_{1\le v\le V} e_v(n)$, such that $\left\|f - \sum_{1\le v\le V} e_v\right\|_1 < \varepsilon$, where $v \in \mathbb{Q}$. So$\left|f(n) - \sum_{1\le v\le V} e_v(n)\right| < \varepsilon$, for all $1 \le n \le N$. Therefore we have

$$\left|\widehat{f}(u) - \lim_{N\to\infty} \frac{1}{N} \sum_{1\le n\le N} \sum_{1\le v\le V} e_v(n)e_{-u}(n)\right| =$$

$$= \lim_{N\to\infty} \frac{1}{N} \left| \sum_{1\le n\le N} \left(f(n) - \sum_{1\le v\le V} e_v(n) \right) e_{-u}(n) \right| \le$$

$$\le \lim_{N\to\infty} \frac{1}{N} \sum_{1\le n\le N} \varepsilon\left|e_{-u}(n)\right| \le \varepsilon.$$

Let $u \notin \mathbb{Q}$, since $v - u \notin \mathbb{Q}$ we have

$$\left|\lim_{N\to\infty} \frac{1}{N} \sum_{1\le n\le N} \sum_{1\le v\le V} e_v(n)e_{-u}(n)\right| = \left|\lim_{N\to\infty} \frac{1}{N} \sum_{1\le n\le N} \sum_{1\le v\le V} e^{2\pi i n(v-u)}\right| =$$

$$= \left|\lim_{N\to\infty} \frac{1}{N} \sum_{1\le v\le V} \frac{1 - e^{2\pi i N(v-u)}}{1 - e^{2\pi i(v-u)}}\right| \le \lim_{N\to\infty} \frac{1}{N} \sum_{1\le v\le V} \frac{2}{const} = 0,$$

and the lemma follows. ■

6 Limit periodicity of weighted multiplicities

In this section we will prove that the weighted multiplicities function $\beta_Q(n)$ is limit periodic (prop. 6.1), and as consequence, we will obtain the formula (17) for calculating its mean square (end of the section).

Proposition 6.1 *The functions $\beta_Q(n) \in \mathcal{D}^1$ and for $1 \le s \le 2$, $\lim_{P\to\infty} \|\beta_Q - \beta_{P,Q}\|_s = 0$ holds.*

Write $\beta_Q(n) - \beta_{P,Q}(n) = \triangle_P^{(1)}(n) + \triangle_P^{(2)}(n)$, where

$$\triangle_P^{(1)}(n) := \sum_{\substack{D,v\ge 1; Dv^2=n^2-4 \\ p|v \text{ for some } p>P}} \frac{1}{v} \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\frac{D}{q}\right) & q^2 \nmid D \end{array} \right\} L(1,\chi_D)$$

and

$$\triangle_P^{(2)}(n) := \sum_{\substack{D,v\ge 1; Dv^2=n^2-4 \\ p|v \Rightarrow p\le P}} \frac{1}{v} \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\frac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \left(L(1,\chi_D) - \prod_{p\le P} \left(1 - \frac{\chi_D(p)}{p}\right)^{-1} \right).$$

Lemma 6.2 *For $P \ge Q$ we have*

$$\frac{1}{x} \sum_{2<n\le x} \left| \triangle_P^{(1)}(n) \right|^2 \ll \sum_{v>P} \frac{1}{v^2}.$$

Proof. Note that

$$\triangle_P^{(1)}(n) \le \sum_{\substack{D,v\ge 1; Dv^2=n^2-4 \\ p|v \text{ for some } p>P}} \frac{2^{\omega(Q)}}{v} L(1,\chi_D), \tag{10}$$

where $\omega(Q)$ is the number of prime divisors of Q. Cauchy's inequality gives

$$\left| \triangle_P^{(1)}(n) \right| \le \left(\sum_{\substack{D,v\ge 1; Dv^2=n^2-4 \\ p|v \text{ for some } p>P}} \frac{2^{2\omega(Q)}}{v^2} \right)^{1/2} \left(\sum_{\substack{D,v\ge 1; Dv^2=n^2-4 \\ p|v \text{ for some } p>P}} L(1,\chi_D)^2 \right)^{1/2}.$$

For $x \ge 1$, this gives

$$\sum_{2<n\le x} \left| \triangle_P^{(1)}(n) \right|^2 \le \sum_{v>P} \frac{2^{2\omega(Q)}}{v^2} \sum_{\substack{2<n\le x \\ D,v\ge 1; Dv^2=n^2-4}} L(1,\chi_D)^2.$$

M.Peter shows [16],[17] that the last sum is

$$\sum_{\substack{2<n\le x \\ D,v\ge 1; Dv^2=n^2-4}} L(1,\chi_D)^2 \sim const \cdot x,$$

as $x \to \infty$. Therefore we have the claim of the lemma. ■

In order to estimate $\triangle_P^{(2)}(n)$ we must compare $L(1,\chi_D)$ with a partial product of its Euler products. This is done by comparing both terms with a smoothed version of the Dirichlet series for $L(1,\chi_D)$. Let $N \geq 1$. Then

$$\triangle_P^{(2)}(n) = \triangle_{P,N}^{(2,1)}(n) + \triangle_{P,N}^{(2,2)}(n) + \triangle_{P,N}^{(2,3)}(n),$$

where

$$\triangle_{P,N}^{(2,1)}(n) := \sum_{\substack{D,v\geq 1; Dv^2=n^2-4 \\ p|v \Rightarrow p\leq P}} \frac{1}{v} \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \left(L(1,\chi_D) - \sum_{l\geq 1} \frac{\chi_D(l)}{l} e^{-l/N} \right),$$

$$\triangle_{P,N}^{(2,2)}(n) := \sum_{\substack{D,v\geq 1; Dv^2=n^2-4 \\ p|v \Rightarrow p\leq P}} \frac{1}{v} \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \sum_{l\geq 1: p|l \ \text{ for some } p>P} \frac{\chi_D(l)}{l} e^{-l/N},$$

$$\triangle_{P,N}^{(2,3)}(n) := \sum_{\substack{D,v\geq 1; Dv^2=n^2-4 \\ p|v \Rightarrow p\leq P}} \frac{1}{v} \prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \sum_{l\geq 1: p|l \Rightarrow p\leq P} \frac{\chi_D(l)}{l} \left(e^{-l/N} - 1 \right);$$

Lemma 6.3 (Sarnak [21])

$$\sum_{\substack{2<n\leq x \\ d,v\geq 1 \\ dv^2=n^2-4}} 1 \sim const \cdot x$$

Proof. $\displaystyle\sum_{\substack{2<n\leq x \\ d,v\geq 1 \\ dv^2=n^2-4}} 1 = N(x) :=$

$$= \# \left\{ (n,v,d) \mid n \leq x, \ n^2-4 = dv^2, \ n,v>0, \ d \text{ is a discriminant} \right\} \tag{11}$$

First, we notice that in counting solutions to (11) we may include the case of d being a perfect square without altering the behavior of $N(x)$. So for these purposes we may think of d as being positive integer congruent to 0 or $1 (\bmod 4)$.

Let $S(v)$ denote the number of solutions of (11) in the variables n and d, for fixed v.

$$N(t)=\sum_{v=1}^{t}S(v)=\sum_{v\le t^{1/2}}S(v)+\sum_{t^{1/2}\le v\le t}S(v)=N_1+N_2.$$

We prove first that

$$N_2=O(t^{2/3+\varepsilon}).$$

To see this, let

$$S^*(v):=\#\left\{(n,k)\mid 0<n\le t,\ n^2-4=kv^2\right\}$$

so that

$$N_2\le\sum_{t^{1/2}\le v\le t}S^*(v).$$

Let $T^*(v)$ is the number of residue class solutions of $n^2\equiv 4(\operatorname{mod} v^2).T^*$ is multiplicative and one easily checks that $T^*(v)=O(v^{\varepsilon})$ for any $\varepsilon>0$.

For $t^{1/2}<v$,

$$S^*(v)\le T^*(v).$$

Now

$$N_2\le\sum_{t^{1/2}\le v\le t^{2/3}}S^*(v)+\sum_{t^{2/3}<v\le t}S^*(v)=O(t^{2/3+\varepsilon})+\sum_{t^{2/3}<v\le t}S^*(v).$$

The latter term is the number of solutions of

$$n^2-kv^2=4,\qquad n\le t,t^{2/3}<v\le t \tag{12}$$

or

$$kv^2=(n-2)(n+2),\qquad n\le t,t^{2/3}<v\le t.$$

So we may write

$$v=yz\qquad\text{with}\qquad y^2\mid(n+2),\ z^2\mid(n-2),$$

or

$$v=2yz\qquad\text{with}\qquad\left\{\begin{array}{l}2y^2\mid(n+2),\ z^2\mid(n-2),\\ y^2\mid(n+2),\ 2z^2\mid(n-2),\end{array}\right\}.$$

In any case, one y or $z>t^{1/3}/2$. Thus the n's which are solutions of (12) are among those n's satisfying

$$n\equiv\pm2(\operatorname{mod} m^2),\qquad\text{where}\qquad t^{1/3}\le m\le t^{1/2}.$$

Given such n and m, there are clearly at most $\tau(m \pm 2)$ solutions of (12) in v and k. Now $\tau(l) = O(l^{\varepsilon})$ for any $\varepsilon > 0$. Therefore the number of solutions of (12) is at most

$$t^{\varepsilon} \sum_{t^{1/3}<m<t^{1/2}} \#\{n \le t \mid n \equiv \pm 2 (\operatorname{mod} m^2)\} = t^{\varepsilon} \sum_{t^{1/3} \le m \le t^{1/2}} \left\{ \frac{t}{m^2} + O(1) \right\} =$$

$$= \frac{t^{1+\varepsilon}}{t^{1/3}} + O(t^{1/2+\varepsilon}) = O(t^{2/3+\varepsilon}).$$

So we get that $N_2 = O(t^{2/3+\varepsilon})$ as we desired.

Now we discuss the term $N_1 = \sum_{v \le t^{1/2}} S(v)$. To calculate $S(v)$, let $S_1(v)$ be the number of solutions of

$$n^2 - 4kv^2 = 4, \qquad k \ge 1, n \le t, \tag{13}$$

and $S_2(v)$ be the number of solutions of

$$n^2 - (4k+1)v^2 = 4, \qquad k \ge 1, n \le t. \tag{14}$$

So that $S(v) = S_1(v) + S_2(v)$. A solution (n, k, v) of (13) must have n even, $n = 2n'$, and so we are looking at

$$(n')^2 - kv^2 = 1, \qquad n' \le t/2.$$

Let $T_1(v)$ be the number of residue class solutions of $(n')^2 \equiv 1 (\operatorname{mod} v^2)$. Clearly, for any $\varepsilon > 0$

$$S_1(v) = \frac{tT_1(v)}{2v^2} + O(T_1(v)) = \frac{t}{2}\frac{T_1(v)}{v^2} + O(v^{\varepsilon}).$$

Let $T_2(v)$ be the number of residue class solutions of $n^2 \equiv (v^2 + 4)(\operatorname{mod} 4v^2)$. Then from (14), for any $\varepsilon > 0$

$$S_2(v) = \frac{tT_2(v)}{4v^2} + O(T_2(v)) = \frac{t}{4}\frac{T_2(v)}{v^2} + O(v^{\varepsilon}).$$

Therefore,

$$N_1 = \sum_{v \le t^{1/2}} \left(\frac{tT_1(v)}{2v^2} + \frac{tT_2(v)}{4v^2} + O(v^{\varepsilon}) \right) = t \sum_{v=1}^{\infty} \left(\frac{T_1(v)}{2v^2} + \frac{T_2(v)}{4v^2} \right) + O(t^{1/2+\varepsilon}).$$

P.Sarnak [21] proves that

$$\sum_{v=1}^{\infty} \frac{T_1(v)}{v^2} = \frac{11}{4}, \text{ and } \sum_{v=1}^{\infty} \frac{T_2(v)}{v^2} = \frac{13}{4}.$$

Finally, we have

$$N_1 = t\left(\frac{11}{8} + \frac{13}{16}\right) + O(t^{1/2+\varepsilon}) = \frac{35}{16}t + O(t^{1/2+\varepsilon}),$$

and so

$$N(t) = \frac{35}{16}t + O(t^{2/3+\varepsilon}),$$

proving the lemma. ∎

Lemma 6.4 *For $P \geq Q$ and $x, N \geq 1$, we have*

$$\frac{1}{x} \sum_{2<n\leq x} \left|\triangle_{P,N}^{(2,3)}(n)\right|^2 \ll \left(N^{-1/2} + \sum_{l>\sqrt{N}:p|l\Rightarrow p\leq P} \frac{1}{l}\right)^2.$$

Proof. Since $|e^{-u} - 1| \ll u$ for $0 \leq u \leq 1$, we see that for $n > 2$ the inner sum in $\triangle_{P,N}^{(2,3)}(n)$ is

$$\ll \sum_{l\geq 1:p|l\Rightarrow p\leq P} \frac{1}{l}\left|e^{-l/N} - 1\right| \ll \sum_{l>\sqrt{N}:p|l\Rightarrow p\leq P} \frac{2}{l} + \sum_{1<l\leq\sqrt{N}:p|l\Rightarrow p\leq P} \frac{1}{l}\frac{l}{N}$$

$$\ll \sum_{l>\sqrt{N}:p|l\Rightarrow p\leq P} \frac{1}{l} + N^{-1/2} =: c_1(P,N).$$

Cauchy's inequality and (10) give

$$\sum_{2<n\leq x} \left|\triangle_{P,N}^{(2,3)}(n)\right|^2 \ll \sum_{2<n\leq x} \left(\sum_{D,v\geq 1;Dv^2=n^2-4} \frac{2^{\omega(Q)}}{v}\right)^2 c_1(P,N)^2 \ll$$

$$\ll c_1(P,N)^2 \sum_{2<n\leq x} \left(\sum_{D,v\geq 1;Dv^2=n^2-4} \frac{2^{2\omega(Q)}}{v^2}\right)\left(\sum_{D,v\geq 1;Dv^2=n^2-4} 1\right) \ll$$

$$\ll c_1(P,N)^2 \sum_{\substack{2<n\leq x \\ D,v\geq 1;Dv^2=n^2-4}} 1.$$

By using the previous lemma the result follows. ∎

Lemma 6.5 (Peter [12]) *For $l, v \in \mathbb{N}$ and $x \geq 3$, we have*

$$\sum_{\substack{2<n\leq x \\ d\geq 1 \\ dv^2=n^2-4}} \chi_d(l) \ll \frac{x}{v^{2-\varepsilon}K(l)} + v^\varepsilon l,$$

where $K(l)$ is the squarefree kernel of l and $\varepsilon > 0$ is arbitrary.

Proof. Let $d_j = \left\{ \begin{array}{ll} 0, & j=1 \\ 1, & j=2 \end{array} \right\}$. Write

$$\sum_{\substack{2<n\leq x \\ d\geq 1 \\ dv^2=n^2-4}} \chi_d(l) = \sum_{j=1}^{2} \sum_{\substack{d=d_j (\mathrm{mod}\, 4) \\ 2<n\leq x \\ dv^2=n^2-4}} \chi_d(l).$$

Let $s_j(v)$ be the number of the solution of the congruence $m^2 \equiv d_j v^2 + 4 (\mathrm{mod}\, 4v^2)$, and let $m_{ij}(v), 1 \leq i \leq s_j(v)$ be all it's solutions. Divide the interval of the summation to intervals of the length $4v^2$. We get that our expression is equal to

$$\sum_{j=1}^{2} \sum_{i=1}^{s_j(v)} \sum_{\substack{t\in\mathbb{Z}: \\ m_{ij}(v)+4v^2t\leq x}} \chi_{p_{ijv}(t)}(l),$$

where

$$p_{ijv}(t) = \frac{(m_{ij}(v)+4v^2t)^2-4}{v^2} = 16v^2t^2 + 8m_{ij}(v)t + \frac{m_{ij}(v)^2-4}{v^2} \in \mathbb{Z}[t].$$

Divide the interval of the summation on t to intervals of the length $4l$. We get

$$\sum_{j=1}^{2} \sum_{i=1}^{s_j(v)} \sum_{\substack{t\in\mathbb{Z}: \\ m_{ij}(v)+4v^2t\leq x}} \chi_{p_{ijv}(t)}(l) = \sum_{j=1}^{2} \sum_{i=1}^{s_j(v)} \left(\frac{x}{16v^2 l} \sum_{t (\mathrm{mod}\, 4l)} \left(\frac{p_{ijv}(t)}{l}\right) + O(l) \right) =$$

$$= \frac{x}{16v^2 l} \left(\sum_{j=1}^{2} \sum_{i=1}^{s_j(v)} \sum_{t (\mathrm{mod}\, 4l)} \left(\frac{p_{ijv}(t)}{l}\right) \right) + O((s_1(v)+s_2(v))\cdot l) =$$

$$= \frac{x}{16v^2 l} c(v,l) + O(l \cdot s(v)),$$

where

$$s(v) := s_1(v) + s_2(v), \quad c(v,l) := c_1(v,l) + c_2(v,l),$$

and

$$c_j(v,l) := \sum_{i=1}^{s_j(v)} \sum_{t (\bmod 4l)} \left(\frac{p_{ijv}(t)}{l}\right).$$

Calculation shows that $c(v,l) \ll 2^{v(v)} \dfrac{l}{K(l)} \ll v^{\varepsilon} \dfrac{l}{K(l)}$, and $s(v) \ll 2^{v(v)} \ll v^{\varepsilon}$, where $v(v)$ is the number of distinct prime factors of v. Therefore we have

$$\sum_{\substack{2<n\le x\\ d\ge 1\\ dv^2=n^2-4}} \chi_d(l) \ll \frac{x}{v^{2-\varepsilon}K(l)} + v^{\varepsilon} l,$$

as claimed in the lemma. ■

Lemma 6.6 *For $P \ge Q$ and $x, N \ge 1$, we have*

$$\frac{1}{x}\sum_{2<n\le x} \left|\triangle_{P,N}^{(2,2)}(n)\right|^2 \ll \sum_{l>P^2} \frac{\tau(l)}{lK(l)} + \frac{1}{x^{1/3-\varepsilon}} N^2$$

where $\tau(l)$ is the number of positive divisors of l.

Proof. Let $\alpha > \frac{1}{2}$. We write

$$\triangle_{P,N}^{(2,2)}(n) = \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v\le n^{\alpha}}} \frac{1}{v}\prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \sum_{\substack{l\ge 1: p|l \text{ for}\\ \text{some } p>P}} \frac{\chi_D(l)}{l} e^{-l/N} +$$

$$+ \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v> n^{\alpha}}} \frac{1}{v}\prod_{q|Q} \left\{ \begin{array}{cc} 2, & q^2 \mid D \\ 1+\left(\dfrac{D}{q}\right) & q^2 \nmid D \end{array} \right\} \sum_{\substack{l\ge 1: p|l \text{ for}\\ \text{some } p>P}} \frac{\chi_D(l)}{l} e^{-l/N} =$$

$$= \triangle_{P,N}^{(2,2,1)}(n) + \triangle_{P,N}^{(2,2,2)}(n).$$

A trivial estimate gives

$$\triangle_{P,N}^{(2,2,2)}(n) \le \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v> n^{\alpha}}} \frac{2^{\omega(Q)}}{v} \sum_{\substack{l\ge 1: p|l \text{ for}\\ \text{some } p>P}} \frac{\chi_D(l)}{l} e^{-l/N} \ll \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v> n^{\alpha}}} \frac{1}{v} \sum_{\substack{l\ge 1: p|l \text{ for}\\ \text{some } p>P}} \frac{1}{l} e^{-l/N} \ll$$

$$\log N \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v> n^{\alpha}}} \frac{1}{v} \ll \log N \cdot \frac{1}{n^{\alpha}} \tau(n^2-4) \ll \log N \cdot \frac{1}{n^{\alpha-\varepsilon}}.$$

Thus , since $\alpha > \frac{1}{2}$, we have

$$\sum_{2<n\le x} \left|\triangle_{P,N}^{(2,2,2)}(n)\right|^2 \ll (\log N)^2 \cdot \sum_{2<n\le x} \frac{1}{n^{2(\alpha-\varepsilon)}} \ll (\log N)^2 . \qquad (15)$$

By Cauchy's inequality

$$\left|\triangle_{P,N}^{(2,2,1)}(n)\right| \le \sum_{\substack{D,v\ge 1\\ Dv^2=n^2-4\\ v\le n^\alpha}} \frac{2^{\omega(Q)}}{v} \left| \sum_{l\ge 1:p|l \text{ for some } p>P} \frac{\chi_D(l)}{l} e^{-l/N} \right| \le$$

$$\left(\sum_{D,v\ge 1; Dv^2=n^2-4} \frac{2^{2\omega(Q)}}{v^2} \right)^{\frac{1}{2}} \cdot \left(\sum_{D,v\ge 1; Dv^2=n^2-4; v\le n^\alpha} \left(\sum_{l\ge 1:p|l \text{ for some } p>P} \frac{\chi_D(l)}{l} e^{-l/N} \right)^2 \right)^{\frac{1}{2}} .$$

Thus for $x \ge 1$,

$$\sum_{2<n\le x} \left|\triangle_{P,N}^{(2,2,1)}(n)\right|^2 \ll \sum_{2<n\le x} \sum_{D,v\ge 1; Dv^2=n^2-4; v\le x^\alpha} \left(\sum_{l\ge 1:p|l \text{ for some } p>P} \frac{\chi_D(l)}{l} e^{-l/N} \right)^2 =$$

$$= \sum_{\substack{l_1,l_2:p_i|l_i\\ \text{for some } p_i>P}} \frac{1}{l_1 l_2} e^{-(l_1+l_2)/N} \sum_{1\le v\le x^\alpha} \sum_{\substack{2<n\le x\\ D\ge 1\\ Dv^2=n^2-4}} \chi_D(l_1 l_2).$$

Applying Peter's lemma 6.5 to the innermost sum gives the estimate

$$\sum_{2<n\le x} \left|\triangle_{P,N}^{(2,2,1)}(n)\right|^2 \ll \sum_{l>P^2} \frac{1}{l}\tau(l) \sum_{1\le v\le x^\alpha} \frac{x}{v^{2-\varepsilon}K(l)} + \sum_{l_1,l_2\ge 1} \frac{l_1 l_2}{l_1 l_2} e^{-(l_1+l_2)/N} \sum_{1\le v\le x^\alpha} v^\varepsilon$$

$$\ll x \sum_{l>P^2} \frac{\tau(l)}{lK(l)} + N^2 x^{\alpha(1+\varepsilon)}.$$

Thus together with (15), for $\alpha = 2/3 > 1/2$ we have

$$\frac{1}{x} \sum_{2<n\le x} \left|\triangle_{P,N}^{(2,2)}(n)\right|^2 \ll \sum_{l>P^2} \frac{\tau(l)}{lK(l)} + \frac{1}{x}(\log N)^2 + \frac{1}{x^{1/3-\varepsilon}} N^2.$$

■

In order to estimate $\triangle^{(2,1)}_{P,N}(n)$ we must show that the error

$$I(D,N) := L(1,\chi_D) - \sum_{l\geq 1} \frac{\chi_D(l)}{l} e^{-l/N},$$

which comes from smoothing Dirichlet series expansion of $L(1,\chi_D)$, is small for large N.

Lemma 6.7 *For $1/2 < \sigma_0 < 1$ define the rectangle*

$$R_x := \{s \in \mathbb{C} \mid \sigma_0 \leq \mathrm{Re}(s) \leq 1, |\mathrm{Im}(s)| \leq \log^2 x\}.$$

(a) If $L(s,\chi_D)$ has no zeros in R_x and $D \leq x^2$, then for

$$\mathrm{Re}(s) = \kappa, |\mathrm{Im}(s)| \leq \frac{(\log x)^2}{2}$$

holds

$$I(D,N) \ll x^{\varepsilon} N^{(\kappa-1)};$$

(b) If $L(s,\chi_D)$ has zeros in R_x, then

$$\#\{(n,v,D) \mid 2 < n \leq x, D,v \geq 1, n^2 - Dv^2 = 4, \\ L(s,\chi_D) \text{ has zeros in } R_x\} \ll x^{\mu+\varepsilon},$$

where $\mu := 8(1-\sigma_0)/\sigma_0 < 1$, $\sigma_0 < \kappa < 1$.

Proof. See [16, Lemma 3.6]. ■

Lemma 6.8 *There are $0 < \kappa, \mu < 1$ such that for $P \geq Q, x, N \geq 1$ and $\varepsilon > 0$ we have*

$$\frac{1}{x} \sum_{2<n\leq x} \left|\triangle^{(2,1)}_{P,N}(n)\right|^2 \ll x^{\varepsilon} N^{2(\kappa-1)} + x^{\mu-1+\varepsilon} (\log(x^2 N))^2.$$

Proof. Note that a trivial estimation gives $I(D,N) \ll \log(DN)$. Cauchy's inequality, previous lemma and (10) give

$$\sum_{2<n\leq x} \left|\triangle^{(2,1)}_{P,N}(n)\right|^2 \ll \sum_{2<n\leq x} \left(\sum_{D,v\geq 1; Dv^2 = n^2-4} \frac{2^{2\omega(Q)}}{v^2} \right) \left(\sum_{D,v\geq 1; Dv^2=n^2-4} |I(D,N)|^2 \right) \ll$$

$$\ll \sum_{\substack{2<n\leq x; D,v\geq 1: Dv^2=n^2-4 \\ L(s,\chi_D) \text{ has no zeros in } R_x}} \left(x^{\varepsilon} N^{(\kappa-1)}\right)^2 + \sum_{\substack{2<n\leq x; D,v\geq 1: Dv^2=n^2-4 \\ L(s,\chi_D) \text{ has a zero in } R_x}} \log^2(DN) \ll$$

$$\ll x\left(x^{\varepsilon}N^{(\kappa-1)}\right)^{2}+x^{\mu+\varepsilon}(\log(x^{2}N))^{2},$$

which proves the lemma. ■

Now the results are collected.

Lemma 6.9 *For $P\geq Q$, we have*

$$\|\beta_Q-\beta_{P,Q}\|_2\ll\left(\sum_{v>P}\frac{1}{v^2}\right)^{1/2}+\left(\sum_{l>P^2}\frac{\tau(l)}{lK(l)}\right)^{1/2}.$$

Proof. For $x\geq 1$ choose $N:=x^{1/8}$. Then previous lemmas show that

$$\frac{1}{x}\sum_{2<n\leq x}\left|\triangle_P^{(2)}(n)\right|^2\ll\left(x^{-1/16}+\sum_{l>x^{1/16}:p|l\Rightarrow p\leq P}\frac{1}{l}\right)^2+\sum_{l>P^2}\frac{\tau(l)}{lK(l)}+$$

$$+\frac{1}{x}(\log x)^2+\frac{1}{x^{1/12-\varepsilon}}+x^{(\kappa-1)/4+\varepsilon}+x^{\mu-1+\varepsilon}(\log x)^2.$$

Since the series

$$\sum_{l\geq 1:p|l\Rightarrow p\leq P}\frac{1}{l}$$

converges, we have for $P\geq Q$ fixed

$$\left\|\triangle_P^{(2)}(n)\right\|_2^2\ll\sum_{l>P^2}\frac{\tau(l)}{lK(l)}.$$

Together with Lemma 6.2 this proves the claim. ■

Corollary 6.10 *The functions $\beta_Q(n)\in\mathcal{D}^1$ and for $1\leq s\leq 2$, $\lim\limits_{P\to\infty}\|\beta_Q-\beta_{P,Q}\|_s=0$ holds.*

Proof. By previous lemma we have

$$\|\beta_Q-\beta_{P,Q}\|_2\ll\left(\sum_{v>P}\frac{1}{v^2}\right)^{1/2}+\left(\sum_{l>P^2}\frac{\tau(l)}{lK(l)}\right)^{1/2};$$

here

$$\sum_{v>P}\frac{1}{v^2}\longrightarrow 0,$$

as $P \to \infty$, since the series $\sum_{v \geq 1} \frac{1}{v^2}$ converges. Furthermore,

$$\sum_{l > P^2} \frac{\tau(l)}{lK(l)} \longrightarrow 0,$$

as $P \to \infty$, since

$$\sum_{l \geq 1} \frac{\tau(l)}{lK(l)} = \sum_{a,b \geq 1 : a \text{ squarefree}} \frac{\tau(ab^2)}{ab^2 \cdot a} \ll \sum_{a \geq 1} \frac{a^{\varepsilon}}{a^2} \sum_{b \geq 1} \frac{b^{2\varepsilon}}{b^2} < \infty.$$

Thus $\lim_{P \to \infty} \|\beta_Q - \beta_{P,Q}\|_2 = 0$. For $f : \mathbb{N} \longrightarrow \mathbb{C}$ arbitrary and $1 \leq s \leq 2$ we have $\|f\|_s \leq \|f\|_2$ by Hölder's inequality. Thus $\lim_{P \to \infty} \|\beta_Q - \beta_{P,Q}\|_s = 0$, for all $1 \leq s \leq 2$ and, in particular $\lim_{P \to \infty} \|\beta_Q - \beta_{P,Q}\|_1 = 0$.

Since the b-th summand of $\beta_{(p,Q)}$ is p^{2b+1}-periodic for $p \nmid Q$, 2^{2b+3}-periodic in case $p = 2$, and p^{2b+2}-periodic in case $p \mid Q$, and the series representing $\beta_{(p,Q)}$ is uniformly convergent, the function $\beta_{(p,Q)}$ is uniformly limit periodic, i.e. $\beta_{(p,Q)} \in \mathcal{D}^u$; here $\mathcal{D}^u$ is the set of all functions which can be approximated to an arbitrary accuracy by periodic functions with respect to the supremum norm. Since $\mathcal{D}^u$ is closed under multiplication it follows from Lemma 4.1, that $\beta_{P,Q} \in \mathcal{D}^u$ for all $P \geq Q$. This gives $\beta_Q \in \mathcal{D}^s$ for all $1 \leq s \leq 2$. ■

So we have now

$$\widehat{\beta_Q}(0) := M(\beta_Q) := \lim_{N \to \infty} \frac{1}{N} \sum_{1 \leq n \leq N} \beta_Q(n).$$

One can prove the

Lemma 6.11 *For $b \in \mathbb{N}$, $a \in \mathbb{Z}$, $\gcd(a,b) = 1$, choose $a_p \in \mathbb{Z}$ for all $p \mid b$ such that $\sum_{p \mid b} a_p p^{-ord_p b} \equiv ab^{-1} (\operatorname{mod} 1)$. Then*

$$\widehat{\beta_Q}\left(\frac{a}{b}\right) = \prod_{p \mid b} \widehat{\beta_{(p,Q)}}\left(\frac{a_p}{p^{ord_p b}}\right). \tag{16}$$

Proof. Word by word the proof of the same fact in [16, Lemma 4.3] ■

Corollary 6.12

$$\lim_{N \to \infty} \frac{1}{N} \sum_{1 \leq n \leq N} \beta_Q(n) = \widehat{\beta_Q}(0) = 1$$

Proposition 6.13

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=\prod_{p\ \text{-prime}}\left(1+\sum_{c\ge 1}\sum_{\substack{1\le a\le p^c\\ a\ne 0 (\mathrm{mod}\, p)}}\left|\widehat{\beta_{(p,Q)}}\left(\frac{a}{p^c}\right)\right|^2\right). \tag{17}$$

Proof. By Parseval's equality and by previous lemma and corollary

$$M(\beta\overline{\beta}):=\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=\sum_{b\ge 1}\sum_{\substack{1\le a\le b\\ \gcd(a,b)=1}}\left|\widehat{\beta_Q}\left(\frac{a}{b}\right)\right|^2=$$

$$=\prod_{p\ \text{- prime}}\left(1+\sum_{c\ge 1}\sum_{\substack{1\le a\le p^c\\ a\ne 0 (\mathrm{mod}\, p)}}\left|\widehat{\beta_{(p,Q)}}\left(\frac{a}{p^c}\right)\right|^2\right).$$

Here the term 1 in a brackets is a contribution of $c=0$, that is $\left|\widehat{\beta_{(p,Q)}}(0)\right|^2$. ■

7 Calculating the mean square of weighted multiplicities $\beta_Q(n)$

In this section we will prove

Theorem 7.1 *Let Q be an odd squarefree number. Then the mean square of weighted multiplicities function is*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=C_1\prod_{q|Q}\frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)},$$

where $C_1=1.328...$, is defined in (6).

Define a functions

$$\beta_{(p,Q,b)}(n):=\left(1-\frac{1}{p}\chi_{(n^2-4)p^{-2b}}(p)\right)^{-1}\cdot\mathbb{I}_{p^b}(n),$$

and calculate the Fourier coefficients of the $\beta_{(p,Q)}(n)$ by the Fourier coefficients of the $\beta_{(p,Q,b)}(n)$.

$$\widehat{\beta_{(p,Q)}}(r) = \sum_{b\geq 0} \frac{1}{p^b} \widehat{\beta_{(p,Q,b)}}(r) \tag{18}$$

In [16] was proved that for all $p \nmid Q$,

$$\widehat{\beta_{(p,Q)}}(0) = 1 \tag{19}$$

We will prove that $\widehat{\beta_{(q,Q)}}(0) = 1$ holds as well, for all $q \mid Q$.

7.1 Calculation of the period of the $\beta_{(q,Q,b)}(n)$

Let us calculate now the minimal period of the function defined above:

$$\beta_{(q,Q,b)}(n) := \left(1 - \frac{1}{q}\chi_{(n^2-4)q^{-2b}}(q)\right)^{-1} \cdot \mathbb{I}_{q^b}(n)$$

Lemma 7.2 *For $q \mid Q$ the minimal period of the $\beta_{(q,Q,b)}(n)$ is q^{2b+2}.*

Proof. a) we will find a period of a χ. We will look for a minimal k ,such that $\chi(n+k) = \chi(n)$ for all n. That is

$$\left(\frac{\left(n^2-4\right)q^{-2b}}{q}\right) = \left(\frac{\left((n+k)^2-4\right)q^{-2b}}{q}\right) = \left(\frac{\left(n^2-4\right)q^{-2b} + \left(2nk+k^2\right)q^{-2b}}{q}\right)$$

and it's true for $k = q^{2b+1}$.

b) we will find a period of the $\mathbb{I}_{q^b}(n)$. We will look for a minimal k ,such that $\mathbb{I}_{q^b}(n+k) = \mathbb{I}_{q^b}(n)$ for all n.

$$n^2 - 4 \equiv 0(\bmod q^{2b}) \Longleftrightarrow (n+k)^2 - 4 \equiv 0(\bmod q^{2b}) \Longleftrightarrow$$

$$n^2 - 4 + 2nk + k^2 \equiv 0(\bmod q^{2b}) \Longleftrightarrow 2nk + k^2 \equiv 0(\bmod q^{2b}),$$

and it's true for $k = q^{2b}$.

$$\left(n^2-4\right)q^{-2b} \equiv 0(\bmod q^2) \Longleftrightarrow \left((n+k)^2-4\right)q^{-2b} \equiv 0(\bmod q^2) \Longleftrightarrow$$

$$\left(n^2-4\right)q^{-2b} + \left(2nk+k^2\right)q^{-2b} \equiv 0(\bmod q^2) \Longleftrightarrow \left(2nk+k^2\right)q^{-2b} \equiv 0(\bmod q^2),$$

and it's true for $k = q^{2b+2}$.

So the minimal period of the $\beta_{(q,Q,b)}(n)$ is q^{2b+2} that is $\beta_{(q,Q,b)}(n + q^{2b+2}) = \beta_{(q,Q,b)}(n)$ for all n. ■

7.2 Calculation of the Fourier coefficients $\widehat{\beta_{(q,Q,b)}}(r)$ and $\widehat{\beta_{(q,Q)}}(r)$

Theorem 7.3 *For any prime $q \mid Q$ the Fourier coefficients $\widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c})$ are:*

$$c=0, \qquad b=0, \qquad \widehat{\beta_{(q,Q,0)}}(0) = 1 - \frac{2}{q^2(q-1)}$$

$$c=0, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(0) = \frac{2(q^2+q+1)}{q^{2b+2}}$$

$$c=2b+2, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right)$$

$$c=2b+1, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{1}{q^{2b+2}}\left(\left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}}\epsilon_q \times \right.$$
$$\left. \times\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q}) + e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right] - \frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\right),$$

$$\text{where} \quad \epsilon_q = \left\{\begin{array}{ll} 1, & q\equiv 1 (\mathrm{mod}\, 4) \\ i, & q\equiv 3 (\mathrm{mod}\, 4) \end{array}\right\}$$

$$c\leq 2b, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1)$$

$$c=1, \qquad b=0, \qquad \widehat{\beta_{(q,Q,0)}}(\frac{a}{q}) = -\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right) + $$
$$+\frac{1}{q-1}\sum_{n (\mathrm{mod}\, q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}$$

$$c=2, \qquad b=0, \qquad \widehat{\beta_{(q,Q,0)}}(\frac{a}{q^2}) = \frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right).$$

First we calculate the $\widehat{\beta_{(q,Q,b)}}(0)$.

Remark 7.4 *In all of the sums below we want to be sure that the function $\beta_{(q,Q,b)}(n)$ is defined at n, that is n is a trace of some element of $\Gamma_0(Q)$. The necessary and sufficient condition for n to be a trace of some element of $\Gamma_0(Q)$ is the condition that $\left(\frac{n^2-4}{q}\right)\neq -1$ for all $q\mid Q$. We will easily see that those n, for which $\left(\frac{n^2-4}{q}\right)\neq -1$ do not contribute to the sum. That is why we can sum over all n of the given range without any restriction.*

a) $b=0$,

$$\widehat{\beta_{(q,Q,0)}}(0)=\frac{1}{q^2}\sum_{n(\operatorname{mod}q^2)}\left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\cdot\left\{\begin{array}{cc} 2, & q^2\mid n^2-4 \\ \left(\frac{n^2-4}{q}\right)+1, & q^2\nmid n^2-4 \end{array}\right\}$$

$$=\frac{1}{q^2}\sum_{n(\operatorname{mod}q^2)}\left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\cdot\left\{\begin{array}{cc} 2, & n=\pm 2,\ \text{or}\ \left(\frac{n^2-4}{q}\right)=1 \\ 1, & n\neq\pm 2,\ q\mid n^2-4 \end{array}\right\}$$

$$=\frac{1}{q^2}\left(2\cdot 2+2\cdot\#\{n(\operatorname{mod}q^2)\mid\left(\frac{n^2-4}{q}\right)=1\}\left(1-\frac{1}{q}\right)^{-1}+\right.$$

$$\left.\#\{n\neq\pm 2(\operatorname{mod}q^2)\mid q\mid n^2-4\}\right)=\frac{1}{q^2}(2\cdot 2+2\frac{q-3}{2}\cdot q\left(1-\frac{1}{q}\right)^{-1}+2(q-1)\Bigg)$$

$$=\frac{1}{q^2}\left(4+q(q-3)\frac{q}{q-1}+2(q-1)\right)=1-\frac{2}{q^2(q-1)}.$$

b) $b\neq 0$,

$$\widehat{\beta_{(q,Q,b)}}(0)=\frac{1}{q^{2b+2}}\sum_{n(\operatorname{mod}q^{2b+2})}\left(1-\frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1}\times$$

$$\times\left\{\begin{array}{ccc} 2 & ,\ n^2=4(\operatorname{mod}\ q^{2b}) & ,\ q^2\mid(n^2-4)q^{-2b} \\ 1+\left(\frac{(n^2-4)q^{-2b}}{q}\right) & ,\ n^2=4(\operatorname{mod}\ q^{2b}) & ,\ q^2\nmid(n^2-4)q^{-2b} \\ 0 & ,\ \text{else} & \end{array}\right\}=$$

$$=\frac{1}{q^{2b+2}}\left(2\cdot 2+2\left(1-\frac{1}{q}\right)^{-1}\#\left\{n(\operatorname{mod}q^{2b+2})\mid\left\{\begin{array}{c} n^2\equiv 4(\operatorname{mod}q^{2b}) \\ \left(\frac{(n^2-4)q^{-2b}}{q}\right)=1 \end{array}\right\}\right\}+\right.$$

$$\left.\#\left\{n\neq\pm 2(\operatorname{mod}q^{2b+2})\mid\left\{\begin{array}{c} n^2\equiv 4(\operatorname{mod}q^{2b}) \\ q^{2b+1}\mid n^2-4 \end{array}\right\}\right\}\right).$$

Lemma 7.5 *The cardinality of the set*

$$\left\{ n (\bmod q^{2b+2}) \mid \left\{ \begin{array}{c} n^2 \equiv 4 (\bmod q^{2b}) \\ \left(\dfrac{(n^2-4)q^{-2b}}{q} \right) = 1 \end{array} \right\} \right\} \quad \textit{is } q(q-1),$$

and the cardinality of the set

$$\left\{ n \neq \pm 2 (\bmod q^{2b+2}) \mid \left\{ \begin{array}{c} n^2 \equiv 4 (\bmod q^{2b}) \\ q^{2b+1} \mid n^2 - 4 \end{array} \right\} \right\} \quad \textit{is } 2q-2.$$

Proof.

a) There are $2q^2$ numbers n modulo q^{2b+2} such that $n^2-4 = 0 (\bmod q^{2b})$. They are of the form kq^{2b}, where $k = \pm 1, \pm 2, ..., \pm q^2$.So it's need to check how many of the k's are squares modulo q. There are $(q-1)/2$ squares modulo q, hence there are $2q(q-1)/2 = q(q-1)$ numbers in the first set.

b) The number of $n \neq \pm 2$ modulo q^{2b+2} such that $n^2 = 4$ modulo q^{2b+1} is $2q-2$. ■

So

$$\widehat{\beta_{(q,Q,b)}}(0) = \frac{1}{q^{2b+2}} \left(4 + 2\frac{q}{q-1} q(q-1) + 2q - 2 \right) = \frac{2(q^2+q+1)}{q^{2b+2}}.$$

From the relation (18) it follows that

$$\widehat{\beta_{(q,Q)}}(0) = \sum_{b \geq 0} \frac{1}{q^b} \widehat{\beta_{(q,Q,b)}}(0) = 1 - \frac{2}{q^2(q-1)} + \sum_{b \geq 1} \frac{1}{q^b} \frac{2(q^2+q+1)}{q^{2b+2}} =$$

$$1 - \frac{2}{q^2(q-1)} + \frac{2(q^2+q+1)}{q^2} \sum_{b \geq 1} \frac{1}{q^{3b}} = 1 - \frac{2}{q^2(q-1)} + \frac{2(q^2+q+1)}{q^2} \frac{1}{q^3-1} = 1.$$

Now we will compute the Fourier coefficients $\widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c})$.

a) $b \neq 0$, $c = 2b+2$.

We will need a lemmas before we will start .

Lemma 7.6 *If $q \nmid a$, then*

$$\sum_{k=1}^{q^2} \left(\frac{k}{q}\right) e^{-2\pi i k \frac{a}{q^2}} = 0,$$

for q prime.

Proof. Note that

$$\left(\frac{m}{q}\right) = \left(\frac{m+lq}{q}\right),$$

for $l \in \mathbb{Z}$. Now we can write

$$\sum_{k=1}^{q^2} \left(\frac{k}{q}\right) e^{-2\pi i k \frac{a}{q^2}} = \sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{m+lq}{q}\right) e^{-2\pi i (m+lq) \frac{a}{q^2}} =$$

$$\sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{m}{q}\right) e^{-2\pi i m \frac{a}{q^2}} \cdot e^{-2\pi i l \frac{a}{q}} = \sum_{m=1}^{q} \left(\frac{m}{q}\right) e^{-2\pi i m \frac{a}{q^2}} \sum_{l=0}^{q-1} e^{-2\pi i l \frac{a}{q}}.$$

But

$$\sum_{l=0}^{q-1} e^{-2\pi i l \frac{a}{q}} = 0$$

and hence

$$\sum_{k=1}^{q^2} \left(\frac{k}{q}\right) e^{-2\pi i k \frac{a}{q^2}} = 0,$$

as desired. ■

Lemma 7.7 *For $c = 2b+2$*

$$\sum_{\substack{n \not\equiv \pm 2 (\mathrm{mod}\, q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} \mid n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} = 0.$$

Proof.

$$\sum_{\substack{n \not\equiv \pm 2 (\mathrm{mod}\, q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} \mid n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} =$$

$$e^{-4\pi i \frac{a}{q^c}} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(1 + \left(\frac{k}{q}\right)\right) \left(1 - \frac{1}{q}\left(\frac{k}{q}\right)\right)^{-1} e^{-2\pi i k a q^{2b-c}} +$$

$$e^{4\pi i\frac{a}{q^c}}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}\left(1+\left(\frac{-k}{q}\right)\right)\left(1-\frac{1}{q}\left(\frac{-k}{q}\right)\right)^{-1}e^{-2\pi ika q^{2b-c}}=\{c=2b+2\}=$$

$$e^{-4\pi i\frac{a}{q^c}}\sum_{k=1,\left(\frac{k}{q}\right)=1}^{q^2-1}2\left(1-\frac{1}{q}\right)^{-1}e^{-2\pi ik\frac{a}{q^2}}+e^{4\pi i\frac{a}{q^c}}\sum_{k=1,\left(\frac{-k}{q}\right)=1}^{q^2-1}2\left(1-\frac{1}{q}\right)^{-1}e^{-2\pi ik\frac{a}{q^2}}=$$

$$e^{-4\pi i\frac{a}{q^c}}\cdot 2\left(1-\frac{1}{q}\right)^{-1}\cdot\frac{1}{2}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}e^{-2\pi ik\frac{a}{q^2}}\left(1+\left(\frac{k}{q}\right)\right)+$$

$$e^{4\pi i\frac{a}{q^c}}\cdot 2\left(1-\frac{1}{q}\right)^{-1}\cdot\frac{1}{2}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}e^{-2\pi ik\frac{a}{q^2}}\left(1+\left(\frac{-k}{q}\right)\right)$$

$$=e^{-4\pi i\frac{a}{q^c}}\left(1-\frac{1}{q}\right)^{-1}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}\left(\frac{k}{q}\right)e^{-2\pi ik\frac{a}{q^2}}+e^{-4\pi i\frac{a}{q^c}}\left(1-\frac{1}{q}\right)^{-1}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}e^{-2\pi ik\frac{a}{q^2}}+$$

$$e^{4\pi i\frac{a}{q^c}}\left(1-\frac{1}{q}\right)^{-1}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}\left(\frac{-k}{q}\right)e^{-2\pi ik\frac{a}{q^2}}+e^{4\pi i\frac{a}{q^c}}\left(1-\frac{1}{q}\right)^{-1}\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}e^{-2\pi ik\frac{a}{q^2}}.$$

By the previous lemma and the fact that

$$\sum_{\substack{k=1\\ q\nmid k}}^{q^2-1}e^{-2\pi ik\frac{a}{q^2}}=0$$

the expression we want to compute is equal to 0. ∎

Now it will be much easier to compute what we want to compute:

$$\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q^c}\right)=\frac{1}{q^{2b+2}}\sum_{n(\operatorname{mod} q^{2b+2})}\left(1-\frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1}\times$$

$$\times\begin{Bmatrix} 2 & ,\, n^2=4(\operatorname{mod}\ q^{2b}) & ,\, q^2\mid(n^2-4)q^{-2b}\\ 1+\left(\frac{(n^2-4)q^{-2b}}{q}\right) & ,\, n^2=4(\operatorname{mod}\ q^{2b}) & ,\, q^2\nmid(n^2-4)q^{-2b}\\ 0 & ,\, \text{else} & \end{Bmatrix}\cdot e^{-2\pi in\frac{a}{q^c}}$$

$$= \frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n \frac{a}{q^c}} + \right.$$

$$\left. \sum_{\substack{n (\mathrm{mod}\, q^{2b+2}) \\ n^2=4 (\mathrm{mod}\, q^{2b}) \\ q^2 \nmid (n^2-4)q^{-2b}}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} \right)$$

$$= \frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n \frac{a}{q^c}} + \sum_{\substack{n \neq \pm 2 (\mathrm{mod}\, q^{2b+2}) \\ q^{2b+1} | n^2-4}} e^{-2\pi i n \frac{a}{q^c}} + \right.$$

$$\left. \sum_{\substack{n \neq \pm 2 (\mathrm{mod}\, q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} | n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} \right) =$$

$$\frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n \frac{a}{q^c}} + 2\cos\left(\frac{4\pi a}{q^c}\right) \sum_{k=1}^{q-1} e^{-2\pi i k a q^{2b-c+1}} + 0 \right).$$

by the previous lemma. Note that

$$\sum_{k=1}^{q-1} e^{-2\pi i k a q^{2b-c+1}} = -1$$

when $c = 2b+2$. Therefore

$$\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q^c}\right) = \frac{1}{q^{2b+2}} \left(2e^{-4\pi i \frac{a}{q^c}} + 2e^{4\pi i \frac{a}{q^c}} + 2\cos\left(\frac{4\pi a}{q^c}\right) \cdot (-1) \right) =$$

$$\frac{1}{q^{2b+2}} \cos\left(\frac{4\pi a}{q^c}\right)(4-2) = \frac{2}{q^{2b+2}} \cos\left(\frac{4\pi a}{q^c}\right).$$

b) $b \neq 0$, $c = 2b+1$.

Lemma 7.8

$$\sum_{k=1}^{q^2}\left(\frac{k}{q}\right)e^{-2\pi ik\frac{a}{q}}=q^{\frac{3}{2}}(\frac{-a}{q})\epsilon_q,\ where\ \epsilon_q=\left\{\begin{array}{ll}1, & q\equiv 1(\bmod 4)\\ i, & q\equiv 3(\bmod 4)\end{array}\right\}.$$

Proof.

$$\sum_{k=1}^{q^2}\left(\frac{k}{q}\right)e^{-2\pi ik\frac{a}{q}}=\sum_{m=1}^{q}\sum_{l=0}^{q-1}\left(\frac{m+lq}{q}\right)e^{-2\pi i(m+lq)\frac{a}{q}}=$$

$$=\sum_{m=1}^{q}\sum_{l=0}^{q-1}\left(\frac{m}{q}\right)e^{-2\pi im\frac{a}{q}}\cdot e^{-2\pi ila}=q\sum_{m=1}^{q}\left(\frac{m}{q}\right)e^{-2\pi im\frac{a}{q}}=$$

$$=q(\frac{-1}{q})\sum_{m=1}^{q}\left(\frac{-m}{q}\right)e^{2\pi i(-m)\frac{a}{q}}=q(\frac{-1}{q})\sum_{m=1}^{q}\left(\frac{m}{q}\right)e^{2\pi im\frac{a}{q}}=$$

$$=q(\frac{-1}{q})(\frac{a}{q})\sum_{m=1}^{q}\left(\frac{m}{q}\right)e^{2\pi i\frac{m}{q}}.$$

The equality holds by using of property of the Gaussian sum. The value of the last sum is $\epsilon_q\sqrt{q}$, where ϵ_q defined as above. For this see, for example,[11, chapter 6]. Hence

$$\sum_{k=1}^{q^2}\left(\frac{k}{q}\right)e^{-2\pi ik\frac{a}{q}}=q(\frac{-1}{q})(\frac{a}{q})\epsilon_q\sqrt{q}=q^{\frac{3}{2}}(\frac{-a}{q})\epsilon_q,$$

and we have the claim of the lemma. ■

Lemma 7.9 *For $c=2b+1$, and ϵ_q defined as before*

$$\sum_{\substack{n\neq\pm 2(\bmod q^{2b+2})\\ q^{2b+1}\nmid n^2-4\\ q^{2b}|n^2-4}}\left(1-\frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1}\left(1+\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)e^{-2\pi in\frac{a}{q^c}}=$$

$$=\left(1-\frac{1}{q}\right)^{-1}q^{\frac{3}{2}}\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-2q\left(1-\frac{1}{q}\right)^{-1}\cos\left(\frac{4\pi a}{q^c}\right).$$

Proof.

$$\sum_{\substack{n\neq\pm 2(\bmod q^{2b+2})\\ q^{2b+1}\nmid n^2-4\\ q^{2b}|n^2-4}}\left(1-\frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1}\left(1+\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)e^{-2\pi in\frac{a}{q^c}}=$$

$$= e^{-4\pi i \frac{a}{q^c}} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(1 + \left(\frac{k}{q}\right)\right) \left(1 - \frac{1}{q}\left(\frac{k}{q}\right)\right)^{-1} e^{-2\pi i k a q^{2b-c}} +$$

$$e^{4\pi i \frac{a}{q^c}} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(1 + \left(\frac{-k}{q}\right)\right) \left(1 - \frac{1}{q}\left(\frac{-k}{q}\right)\right)^{-1} e^{-2\pi i k a q^{2b-c}} = \{c = 2b{+}1\} =$$

$$= e^{-4\pi i \frac{a}{q^c}} \sum_{k=1, \left(\frac{k}{q}\right)=1}^{q^2-1} 2 \left(1 - \frac{1}{q}\right)^{-1} e^{-2\pi i k \frac{a}{q}} +$$

$$e^{4\pi i \frac{a}{q^c}} \sum_{k=1, \left(\frac{-k}{q}\right)=1}^{q^2-1} 2 \left(1 - \frac{1}{q}\right)^{-1} e^{-2\pi i k \frac{a}{q}} =$$

$$= e^{-4\pi i \frac{a}{q^c}} \cdot 2 \left(1 - \frac{1}{q}\right)^{-1} \cdot \frac{1}{2} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} e^{-2\pi i k \frac{a}{q}} \left(1 + \left(\frac{k}{q}\right)\right) +$$

$$e^{4\pi i \frac{a}{q^c}} \cdot 2 \left(1 - \frac{1}{q}\right)^{-1} \cdot \frac{1}{2} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} e^{-2\pi i k \frac{a}{q}} \left(1 + \left(\frac{-k}{q}\right)\right) =$$

$$= e^{-4\pi i \frac{a}{q^c}} \left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(\frac{k}{q}\right) e^{-2\pi i k \frac{a}{q}} + e^{-4\pi i \frac{a}{q^c}} \left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} e^{-2\pi i k \frac{a}{q}} +$$

$$e^{4\pi i \frac{a}{q^c}} \left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(\frac{-k}{q}\right) e^{-2\pi i k \frac{a}{q}} + e^{4\pi i \frac{a}{q^c}} \left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} e^{-2\pi i k \frac{a}{q}}.$$

By the previous lemma and the fact that

$$\sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} e^{-2\pi i k \frac{a}{q}} = -q$$

we can write that our expression is equal to

$$\left(1 - \frac{1}{q}\right)^{-1} q^{\frac{3}{2}} \epsilon_q \left[e^{-4\pi i \frac{a}{q^c}} (\frac{-a}{q}) + e^{4\pi i \frac{a}{q^c}} (\frac{a}{q}) \right] - 2q \left(1 - \frac{1}{q}\right)^{-1} \cos\left(\frac{4\pi a}{q^c}\right),$$

proving the claim. ■

By using the same arguments as in the case a) we will get

$$\widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n \frac{a}{q^c}} + \sum_{\substack{n\neq\pm 2 (\bmod q^{2b+2}) \\ q^{2b+1} | n^2-4}} e^{-2\pi i n\frac{a}{q^c}} + \right.$$

$$\left. \sum_{\substack{n\neq\pm 2 (\bmod q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} | n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} \right) =$$

$$= \frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n\frac{a}{q^c}} + 2\cos\left(\frac{4\pi a}{q^c}\right) \sum_{k=1}^{q-1} e^{-2\pi i k a} + \right.$$

$$\left. \left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}} \epsilon_q \left[e^{-4\pi i \frac{a}{q^c}} (\frac{-a}{q}) + e^{4\pi i \frac{a}{q^c}} (\frac{a}{q}) \right] - 2q\left(1-\frac{1}{q}\right)^{-1} \cos\left(\frac{4\pi a}{q^c}\right) \right).$$

by using previous lemma. Note that

$$\sum_{k=1}^{q-1} e^{-2\pi i k a} = q-1,$$

so

$$\widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{1}{q^{2b+2}} \left(4\cos\left(\frac{4\pi a}{q^c}\right) + 2(q-1)\cos\left(\frac{4\pi a}{q^c}\right) + \right.$$

$$\left. \left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}} \epsilon_q \left[e^{-4\pi i \frac{a}{q^c}} (\frac{-a}{q}) + e^{4\pi i \frac{a}{q^c}} (\frac{a}{q}) \right] - 2q\left(1-\frac{1}{q}\right)^{-1} \cos\left(\frac{4\pi a}{q^c}\right) \right) =$$

$$= \frac{1}{q^{2b+2}} \left(\left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}} \epsilon_q \left[e^{-4\pi i \frac{a}{q^c}} (\frac{-a}{q}) + e^{4\pi i \frac{a}{q^c}} (\frac{a}{q}) \right] - \frac{2}{q-1} \cos\left(\frac{4\pi a}{q^c}\right) \right).$$

c) $b \neq 0$, $2b \geq c$.

By doing the same steps as before we can write

Lemma 7.10 *For $2b \geq c$,*

$$\sum_{\substack{n \not\equiv \pm 2 (\operatorname{mod} q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} | n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} =$$

$$= 2q^2 \cos\left(\frac{4\pi a}{q^c}\right).$$

Proof.

$$\sum_{\substack{n \not\equiv \pm 2 (\operatorname{mod} q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} | n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} =$$

$$= e^{-4\pi i \frac{a}{q^c}} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(1 + \left(\frac{k}{q}\right)\right) \left(1 - \frac{1}{q}\left(\frac{k}{q}\right)\right)^{-1} e^{-2\pi i k a q^{2b-c}} +$$

$$e^{4\pi i \frac{a}{q^c}} \sum_{\substack{k=1 \\ q \nmid k}}^{q^2-1} \left(1 + \left(\frac{-k}{q}\right)\right) \left(1 - \frac{1}{q}\left(\frac{-k}{q}\right)\right)^{-1} e^{-2\pi i k a q^{2b-c}} = \{2b \geq c\} =$$

$$= e^{-4\pi i \frac{a}{q^c}} \sum_{k=1, \left(\frac{k}{q}\right)=1}^{q^2-1} 2\left(1 - \frac{1}{q}\right)^{-1} + e^{4\pi i \frac{a}{q^c}} \sum_{k=1, \left(\frac{-k}{q}\right)=1}^{q^2-1} 2\left(1 - \frac{1}{q}\right)^{-1} =$$

$$= 2\frac{q}{q-1} \#\{k (\operatorname{mod} q^2) \mid (\frac{k}{q}) = 1\} 2\cos\left(\frac{4\pi a}{q^c}\right) = 4\frac{q}{q-1}\frac{q(q-1)}{2} \cos\left(\frac{4\pi a}{q^c}\right) =$$

$$= 2q^2 \cos\left(\frac{4\pi a}{q^c}\right).$$

■

And gathering all together we have

$$\widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c}) = \frac{1}{q^{2b+2}} \left(\sum_{\substack{n=2 \\ n=-2+q^{2b+2}}} 2e^{-2\pi i n \frac{a}{q^c}} + 2\cos\left(\frac{4\pi a}{q^c}\right) \sum_{k=1}^{q-1} e^{-2\pi i k a q^{2b-c+1}} + \right.$$

$$\left. \sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^{2b+2}) \\ q^{2b+1} \nmid n^2-4 \\ q^{2b} | n^2-4}} \left(1 - \frac{1}{q}\left(\frac{(n^2-4)q^{-2b}}{q}\right)\right)^{-1} \left(1 + \left(\frac{(n^2-4)q^{-2b}}{q}\right)\right) e^{-2\pi i n \frac{a}{q^c}} \right)$$

$$= \frac{1}{q^{2b+2}} \left(4\cos\left(\frac{4\pi a}{q^c}\right) + 2(q-1)\cos\left(\frac{4\pi a}{q^c}\right) + 2q^2\cos\left(\frac{4\pi a}{q^c}\right)\right) =$$

$$= \frac{1}{q^{2b+2}} \cos\left(\frac{4\pi a}{q^c}\right) [4+2(q-1)+2q^2] = \frac{2}{q^{2b+2}} \cos\left(\frac{4\pi a}{q^c}\right) (q^2+q+1).$$

d) $b = 0$, $c = 1$.

As always we need two lemmas:

Lemma 7.11

$$\sum_{n (\operatorname{mod} q^2)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q}} = q \sum_{n (\operatorname{mod} q)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q}}.$$

Proof.

$$\sum_{n (\operatorname{mod} q^2)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q}} = \sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{(m+lq)^2-4}{q}\right) e^{-2\pi i (m+lq) \frac{a}{q}} =$$

$$= \sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{m^2-4}{q}\right) e^{-2\pi i m \frac{a}{q}} = q \sum_{m=1}^{q} \left(\frac{m^2-4}{q}\right) e^{-2\pi i m \frac{a}{q}} =$$

$$= q \sum_{n (\operatorname{mod} q)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q}}.$$

■

Lemma 7.12

$$\sum_{\substack{n\neq\pm 2 (\operatorname{mod} q^2)\\ q\nmid n^2-4}} \left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\left(\left(\frac{n^2-4}{q}\right)+1\right)e^{-2\pi i n\frac{a}{q}} =$$

$$= q\left(1-\frac{1}{q}\right)^{-1}\left(-2\cos\left(\frac{4\pi a}{q}\right)+\sum_{n (\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}\right).$$

.

Proof.

$$\sum_{\substack{n\neq\pm 2 (\operatorname{mod} q^2)\\ q\nmid n^2-4}} \left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\left(\left(\frac{n^2-4}{q}\right)+1\right)e^{-2\pi i n\frac{a}{q}} =$$

$$= \sum_{\substack{n (\operatorname{mod} q^2)\\ n\neq\pm 2 (\operatorname{mod} q)}} \left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\left(\left(\frac{n^2-4}{q}\right)+1\right)e^{-2\pi i n\frac{a}{q}} =$$

$$= \sum_{\substack{n (\operatorname{mod} q^2)\\ \left(\frac{n^2-4}{q}\right)=1}} 2\left(1-\frac{1}{q}\right)^{-1}e^{-2\pi i n\frac{a}{q}} =$$

$$= 2\cdot\frac{1}{2}\left(1-\frac{1}{q}\right)^{-1}\sum_{\substack{n (\operatorname{mod} q^2)\\ n\neq\pm 2 (\operatorname{mod} q)}}\left(\left(\frac{n^2-4}{q}\right)+1\right)e^{-2\pi i n\frac{a}{q}} =$$

$$= \left(1-\frac{1}{q}\right)^{-1}\left(\sum_{\substack{n (\operatorname{mod} q^2)\\ n\neq\pm 2 (\operatorname{mod} q)}} e^{-2\pi i n\frac{a}{q}}+\sum_{\substack{n (\operatorname{mod} q^2)\\ n\neq\pm 2 (\operatorname{mod} q)}}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}\right) =$$

$$= \left(1-\frac{1}{q}\right)^{-1}\left(-2q\cos\left(\frac{4\pi a}{q}\right)+\right.$$

$$\left.\sum_{n (\operatorname{mod} q^2)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}-\sum_{\substack{n (\operatorname{mod} q^2)\\ n=\pm 2 (\operatorname{mod} q)}}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}\right)$$

$$= \left(1-\frac{1}{q}\right)^{-1}\left(-2q\cos\left(\frac{4\pi a}{q}\right)+\sum_{n (\operatorname{mod} q^2)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}-0\right) =$$

$$= \left(1-\frac{1}{q}\right)^{-1}\left(-2q\cos\left(\frac{4\pi a}{q}\right)+q\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}\right).$$

by previous lemma, and that's it. ■

Now we can gather the results

$$\widehat{\beta_{(q,Q,0)}}\left(\frac{a}{q}\right)=\frac{1}{q^2}\sum_{n(\operatorname{mod} q^2)}\left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\times$$
$$\times\begin{Bmatrix} 2, & q^2 \mid n^2-4 \\ \left(\frac{n^2-4}{q}\right)+1, & q^2\nmid n^2-4\end{Bmatrix}\cdot e^{-2\pi i n\frac{a}{q}}$$

$$=\frac{1}{q^2}\left(\sum_{\substack{n=2\\ n=-2+q^2}}2e^{-2\pi i n\frac{a}{q}}+\sum_{\substack{n\neq\pm 2(\operatorname{mod} q^2)\\ q\mid n^2-4}}e^{-2\pi i n\frac{a}{q}}+\right.$$
$$\left.\sum_{\substack{n\neq\pm 2(\operatorname{mod} q^2)\\ q\nmid n^2-4}}\left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1}\left(\left(\frac{n^2-4}{q}\right)+1\right)e^{-2\pi i n\frac{a}{q}}\right)$$

$$=\frac{1}{q^2}\left(4\cos\left(\frac{4\pi a}{q}\right)+2(q-1)\cos\left(\frac{4\pi a}{q}\right)+\right.$$
$$\left.q\left(1-\frac{1}{q}\right)^{-1}\left[-2\cos\left(\frac{4\pi a}{q}\right)+\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}\right]\right)$$

$$=-\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right)+\frac{1}{q-1}\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}.$$

e) $b=0$, $c=2$.

Lemma 7.13

$$\sum_{\substack{n\neq\pm 2(\operatorname{mod} q^2)\\ q\mid n^2-4}}e^{-2\pi i n\frac{a}{q^2}}=-2\cos\left(\frac{4\pi a}{q^2}\right).$$

Proof. Rewrite the condition $\{ n \neq \pm 2 (\operatorname{mod} q^2),\ q \mid n^2-4\}$ in the form $\{ n = \pm 2 + kq,\ k = 1, ..., q-1\}$. Thus

$$\sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^2) \\ q \mid n^2-4}} e^{-2\pi i n \frac{a}{q^2}} = \sum_{k=1}^{q-1} e^{-2\pi i (\pm 2 + kq) \frac{a}{q^2}} =$$

$$= 2 \cos\left(\frac{4\pi a}{q^2}\right) \sum_{k=1}^{q-1} e^{-2\pi i k \frac{a}{q}} = -2 \cos\left(\frac{4\pi a}{q^2}\right),$$

and we are done. ■

Lemma 7.14

$$\sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^2) \\ q \nmid n^2-4}} \left(1 - \frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1} \left(\left(\frac{n^2-4}{q}\right) + 1\right) e^{-2\pi i n \frac{a}{q^2}} = 0.$$

Proof.

$$\sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^2) \\ q \nmid n^2-4}} \left(1 - \frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1} \left(\left(\frac{n^2-4}{q}\right) + 1\right) e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \sum_{\substack{n (\operatorname{mod} q^2) \\ n \neq \pm 2 (\operatorname{mod} q)}} \left(1 - \frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1} \left(\left(\frac{n^2-4}{q}\right) + 1\right) e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \sum_{\substack{n (\operatorname{mod} q^2) \\ \left(\frac{n^2-4}{q}\right) = 1}} 2 \left(1 - \frac{1}{q}\right)^{-1} e^{-2\pi i n \frac{a}{q^2}} =$$

$$= 2 \cdot \frac{1}{2} \left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{n (\operatorname{mod} q^2) \\ n \neq \pm 2 (\operatorname{mod} q)}} \left(\left(\frac{n^2-4}{q}\right) + 1\right) e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \left(1 - \frac{1}{q}\right)^{-1} \left(\sum_{\substack{n (\operatorname{mod} q^2) \\ n \neq \pm 2 (\operatorname{mod} q)}} e^{-2\pi i n \frac{a}{q^2}} + \sum_{\substack{n (\operatorname{mod} q^2) \\ n \neq \pm 2 (\operatorname{mod} q)}} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q^2}} \right).$$

The first sum in the brackets is 0, and so we need to compute an expression

$$\left(1 - \frac{1}{q}\right)^{-1} \sum_{\substack{n (\operatorname{mod} q^2) \\ n \neq \pm 2 (\operatorname{mod} q)}} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \left(1-\frac{1}{q}\right)^{-1} \sum_{n (\operatorname{mod} q^2)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \left(1-\frac{1}{q}\right)^{-1} \sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{(m+lq)^2-4}{q}\right) e^{-2\pi i (m+lq) \frac{a}{q^2}} =$$

$$= \left(1-\frac{1}{q}\right)^{-1} \sum_{m=1}^{q} \sum_{l=0}^{q-1} \left(\frac{m^2-4}{q}\right) e^{-2\pi i m \frac{a}{q^2}} \cdot e^{-2\pi i l \frac{a}{q}} =$$

$$= \left(1-\frac{1}{q}\right)^{-1} \sum_{m=1}^{q} \left(\frac{m^2-4}{q}\right) e^{-2\pi i m \frac{a}{q^2}} \sum_{l=0}^{q-1} e^{-2\pi i l \frac{a}{q}} = 0,$$

since the last sum is 0. ■

$$\widehat{\beta_{(q,Q,0)}}\left(\frac{a}{q^2}\right) = \frac{1}{q^2} \sum_{n (\operatorname{mod} q^2)} \left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1} \cdot \begin{Bmatrix} 2, & q^2 \mid n^2-4 \\ \left(\frac{n^2-4}{q}\right)+1, & q^2 \nmid n^2-4 \end{Bmatrix} \cdot e^{-2\pi i n \frac{a}{q^2}} =$$

$$= \frac{1}{q^2} \left(\sum_{\substack{n=2 \\ n=-2+q^2}} 2e^{-2\pi i n \frac{a}{q^2}} + \sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^2) \\ q \mid n^2-4}} e^{-2\pi i n \frac{a}{q^2}} + \right.$$

$$\left. \sum_{\substack{n \neq \pm 2 (\operatorname{mod} q^2) \\ q \nmid n^2-4}} \left(1-\frac{1}{q}\left(\frac{n^2-4}{q}\right)\right)^{-1} \left(\left(\frac{n^2-4}{q}\right)+1\right) e^{-2\pi i n \frac{a}{q^2}} \right) =$$

$$= \frac{1}{q^2}\left(4\cos\left(\frac{4\pi a}{q^2}\right) - 2\cos\left(\frac{4\pi a}{q^2}\right) + 0\right) = \frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right).$$

Now we can compute the $\widehat{\beta_{(q,Q)}}(r)$. Summarize the above results:

$$c = 0, \qquad b = 0, \qquad \widehat{\beta_{(q,Q,0)}}(0) = 1 - \frac{2}{q^2(q-1)}$$

$$c=0, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(0)=\frac{2(q^2+q+1)}{q^{2b+2}}$$

$$c=2b+2,\ b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c})=\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right)$$

$$c=2b+1,\ b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c})=\frac{1}{q^{2b+2}}\left(\left(1-\frac{1}{q}\right)^{-1}q^{\frac{3}{2}}\epsilon_q\times\right.$$

$$\left.\times\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\right)$$

$$c\leq 2b, \qquad b\neq 0, \qquad \widehat{\beta_{(q,Q,b)}}(\frac{a}{q^c})=\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1)$$

$$c=1, \qquad b=0, \qquad \widehat{\beta_{(q,Q,0)}}(\frac{a}{q})=-\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right)+$$

$$\frac{1}{q-1}\sum_{n(\bmod q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi in\frac{a}{q}}$$

$$c=2, \qquad b=0, \qquad \widehat{\beta_{(q,Q,0)}}(\frac{a}{q^2})=\frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right).$$

And the theorem is completely proved.

Now we can to compute the $\widehat{\beta_{(q,Q)}}(r)$.

Theorem 7.15 *The Fourier coefficients* $\widehat{\beta_{(q,Q)}}(\frac{a}{q^c})$ *are:*

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q}\right)=\frac{1}{q-1}\sum_{n(\bmod q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi in\frac{a}{q}}$$

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^2}\right)=\frac{2}{q(q-1)}\cos\left(\frac{4\pi a}{q^2}\right)$$

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^c}\right)=\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\frac{1}{q^{\frac{3c-4}{2}}},\ \textit{for } c>2, c \textit{ even}$$

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^c}\right)=\frac{1}{q-1}\frac{1}{q^{\frac{3c-4}{2}}}\epsilon_q\left(\frac{a}{q}\right)\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-1}{q})+e^{4\pi i\frac{a}{q^c}}\right],\ \textit{for } c>2, c \textit{ odd}$$

Proof. By using (18) we get

a) for $c = 1$,

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q}\right) = \sum_{b\geq 0}\frac{1}{q^b}\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q}\right) =$$

$$= -\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right)+\frac{1}{q-1}\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}+\sum_{b\geq 1}\frac{1}{q^b}\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q}\right)$$

$$= -\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right)+\frac{1}{q-1}\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}} + \sum_{b\geq 1}\frac{1}{q^b}\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q}\right)(q^2+q+1)$$

$$= -\frac{2}{q^2(q-1)}\cos\left(\frac{4\pi a}{q}\right)+\frac{1}{q-1}\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}} + 2\cos\left(\frac{4\pi a}{q}\right)(q^2+q+1)\frac{1}{q^2(q^3-1)}$$

$$= \frac{1}{q-1}\sum_{n(\operatorname{mod} q)}\left(\frac{n^2-4}{q}\right)e^{-2\pi i n\frac{a}{q}}.$$

b) for $c = 2$,

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^2}\right) = \sum_{b\geq 0}\frac{1}{q^b}\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q^2}\right) = \frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right)+\sum_{b\geq 1}\frac{1}{q^b}\widehat{\beta_{(q,Q,b)}}\left(\frac{a}{q^2}\right) =$$

$$= \frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right)+\sum_{b\geq 1}\frac{1}{q^b}\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^2}\right)(q^2+q+1) =$$

$$= \frac{2}{q^2}\cos\left(\frac{4\pi a}{q^2}\right)+2\cos\left(\frac{4\pi a}{q^2}\right)(q^2+q+1)\frac{1}{q^2(q^3-1)} = \frac{2}{q(q-1)}\cos\left(\frac{4\pi a}{q^2}\right).$$

c) for $c > 2$,

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^c}\right) = \sum_{0\leq b<\frac{c-2}{2}} \frac{1}{q^b}\cdot 0 + \sum_{b=\frac{c-2}{2}} \frac{1}{q^b}\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right) +$$

$$+\sum_{b=\frac{c-1}{2}} \frac{1}{q^b}\left[\frac{1}{q^{2b+2}}\left(\left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}}\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\right)\right]+$$

$$+\sum_{b\geq\frac{c}{2}}\frac{1}{q^b}\frac{2}{q^{2b+2}}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1).$$

For c even we have

$$\widehat{\beta_{(q,Q)}}\left(\frac{a}{q^c}\right) = \frac{1}{q^{\frac{c-2}{2}}}\frac{2}{q^c}\cos\left(\frac{4\pi a}{q^c}\right)+\frac{2}{q^2}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1)\sum_{b\geq\frac{c}{2}}\frac{1}{q^{3b}} =$$

$$= 2\cos\left(\frac{4\pi a}{q^c}\right)\left[\frac{1}{q^{\frac{3c-2}{2}}}+\frac{1}{q^2}(q^2+q+1)\frac{1}{q^{\frac{3c-6}{2}}}\frac{1}{q^3-1}\right] = \frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\frac{1}{q^{\frac{3c-4}{2}}}.$$

And for c odd

$$\frac{1}{q^{\frac{c-1}{2}}}\left[\frac{1}{q^{c+1}}\left(\left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}}\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\right)\right]+$$

$$+\frac{2}{q^2}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1)\sum_{b\geq\frac{c+1}{2}}\frac{1}{q^{3b}} =$$

$$= \frac{1}{q^{\frac{3c+1}{2}}}\left(1-\frac{1}{q}\right)^{-1} q^{\frac{3}{2}}\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-\frac{1}{q^{\frac{3c+1}{2}}}\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)+$$

$$+\frac{2}{q^2}\cos\left(\frac{4\pi a}{q^c}\right)(q^2+q+1)\frac{1}{q^{\frac{3c-3}{2}}}\frac{1}{q^3-1} =$$

$$= \frac{1}{q^{\frac{3c-4}{2}}}\frac{1}{q-1}\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-a}{q})+e^{4\pi i\frac{a}{q^c}}(\frac{a}{q})\right]-$$

$$-\frac{1}{q^{\frac{3c+1}{2}}}\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)+\frac{1}{q^{\frac{3c+1}{2}}}\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)=$$

$$=\frac{1}{q-1}\frac{1}{q^{\frac{3c-4}{2}}}\epsilon_q\left(\frac{a}{q}\right)\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-1}{q})+e^{4\pi i\frac{a}{q^c}}\right]. \blacksquare$$

7.3 Calculating the mean square of weighted multiplicities function

In this subsection we will calculate the mean-square of the weighted multiplicities $\beta_Q(n)$.

To calculate the limit

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\leq n\leq N}\beta_Q^2(n)$$

we will use (17). Let us define the function

$$A_Q(p^c):=\sum_{\substack{1\leq a\leq p^c\\ p\nmid a}}\left|\widehat{\beta_{(p,Q)}}(\frac{a}{p^c})\right|^2. \tag{20}$$

So we have that

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\leq n\leq N}\beta_Q^2(n)=\prod_{p\text{ - prime}}\left(1+\sum_{c\geq 1}A_Q(p^c)\right).$$

The values of the $A_Q(p^c)$ for $p\nmid Q$ were calculate by M.Peter [16]. They are:

$$p\neq 2, p\nmid Q;\quad A_Q(p)=\frac{p^2-2p-1}{(p^2-1)^2},\quad A_Q(p^c)=\frac{2(p-1)}{(p^2-1)^2p^{2c-3}}$$

$$p=2;\qquad A_Q(2)=\frac{1}{9},\qquad A_Q(4)=\frac{1}{18},$$

$$A_Q(8)=0,\qquad A_Q(16)=\frac{1}{9\cdot 16},$$

$$A_Q(32)=0,\qquad A_Q(2^c)=\frac{1}{9\cdot 2^{2c-5}}, c\geq 6.$$

We just need to complete his work by adding the case $q\mid Q$.

a) $c = 1$;

$$A_Q(q) = \sum_{\substack{1\le a\le q\\ q\nmid a}} \left|\widehat{\beta_{(q,Q)}}(\frac{a}{q})\right|^2 = \sum_{\substack{1\le a\le q\\ q\nmid a}} \left|\frac{1}{q-1}\sum_{n(\mathrm{mod}\,q)} \left(\frac{n^2-4}{q}\right) e^{-2\pi i n\frac{a}{q}}\right|^2 =$$

$$= \frac{1}{(q-1)^2}\sum_{\substack{1\le a\le q\\ q\nmid a}}\sum_{n_1,n_2(\mathrm{mod}\,q)} \left(\frac{n_1^2-4}{q}\right)\left(\frac{n_2^2-4}{q}\right) e^{2\pi i(n_1-n_2)\frac{a}{q}} =$$

$$= \frac{1}{(q-1)^2}\sum_{n_1,n_2(\mathrm{mod}\,q)} \left(\frac{n_1^2-4}{q}\right)\left(\frac{n_2^2-4}{q}\right)\sum_{a=1}^{q-1} e^{2\pi i(n_1-n_2)\frac{a}{q}}.$$

The sum

$$\sum_{a=1}^{q-1} e^{2\pi i(n_1-n_2)\frac{a}{q}} = \begin{cases} q-1, & n_1=n_2=n(\mathrm{mod}\,q)\\ -1, & \text{else}\end{cases}.$$

Note that

$$\sum_{n(\mathrm{mod}\,q)}\left(\frac{n^2-4}{q}\right) = \frac{q-3}{2} - \frac{q-1}{2} = -1,$$

hence

$$A_Q(q) = \frac{1}{(q-1)^2}\left((q-1)\sum_{n(\mathrm{mod}\,q)}\left(\frac{n^2-4}{q}\right)^2 - \right.$$

$$\left. - \sum_{n_1(\mathrm{mod}\,q)}\sum_{n_2\ne n_1(\mathrm{mod}\,q)}\left(\frac{n_1^2-4}{q}\right)\left(\frac{n_2^2-4}{q}\right)\right)$$

$$= \frac{1}{(q-1)^2}\left((q-1)(q-2) - \sum_{n_1(\mathrm{mod}\,q)}\left(\sum_{n_2(\mathrm{mod}\,q)}\left(\frac{n_1^2-4}{q}\right)\left(\frac{n_2^2-4}{q}\right) - \left(\frac{n_1^2-4}{q}\right)^2\right)\right) =$$

$$= \frac{1}{(q-1)^2}\left((q-1)(q-2) - \left(1 - \sum_{n_1(\mathrm{mod}\,q)}\left(\frac{n_1^2-4}{q}\right)^2\right)\right) =$$

$$= \frac{1}{(q-1)^2}\left(q^2-3q+2-(1-(q-2))\right) = \frac{q^2-2q-1}{(q-1)^2}.$$

b) $c=2$;

$$A_Q(q^2) = \sum_{\substack{1\le a\le q^2\\ q\nmid a}} \left|\widehat{\beta_{(q,Q)}}(\frac{a}{q^2})\right|^2 = \sum_{\substack{1\le a\le q^2\\ q\nmid a}} \left|\frac{2}{q(q-1)}\cos\left(\frac{4\pi a}{q^2}\right)\right|^2 =$$

$$= \frac{4}{q^2(q-1)^2}\sum_{\substack{1\le a\le q^2\\ q\nmid a}} \left|\cos\left(\frac{4\pi a}{q^2}\right)\right|^2 = \frac{1}{q^2(q-1)^2}\sum_{\substack{1\le a\le q^2\\ q\nmid a}}\left(e^{8\pi i\frac{a}{q^2}}+e^{-8\pi i\frac{a}{q^2}}+2\right) =$$

$$= \frac{1}{q^2(q-1)^2}\left(2(q^2-q)+\sum_{\substack{1\le a\le q^2\\ q\nmid a}}\left(e^{8\pi i\frac{a}{q^2}}+e^{-8\pi i\frac{a}{q^2}}\right)\right) = \frac{2(q^2-q)}{q^2(q-1)^2} = \frac{2}{q(q-1)}.$$

c1) $c>2$, c even;

$$A_Q(q^c) = \sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left|\widehat{\beta_{(q,Q)}}(\frac{a}{q^c})\right|^2 = \sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left|\frac{2}{q-1}\cos\left(\frac{4\pi a}{q^c}\right)\frac{1}{q^{\frac{3c-4}{2}}}\right|^2 =$$

$$= \frac{1}{q^{3c-4}}\frac{4}{(q-1)^2}\sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left|\cos\left(\frac{4\pi a}{q^c}\right)\right|^2 =$$

$$= \frac{1}{q^{3c-4}}\frac{1}{(q-1)^2}\sum_{\substack{1\le a\le q^c\\ q\nmid a}}\left(e^{8\pi i\frac{a}{q^c}}+e^{-8\pi i\frac{a}{q^c}}+2\right) =$$

$$= \frac{1}{q^{3c-4}}\frac{1}{(q-1)^2}\left(2(q^c-q^{c-1})+\sum_{\substack{1\le a\le q^c\\ q\nmid a}}\left(e^{8\pi i\frac{a}{q^c}}+e^{-8\pi i\frac{a}{q^c}}\right)\right)$$

$$= \frac{2q^{c-1}(q-1)}{q^{3c-4}(q-1)^2} = \frac{2}{q^{2c-3}(q-1)}.$$

c2) $c > 2$, c odd;

$$A_Q(q^c) = \sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left|\widehat{\beta_{(q,Q)}}(\frac{a}{q^c})\right|^2 =$$

$$= \sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left|\frac{1}{q-1}\frac{1}{q^{\frac{3c-4}{2}}}\epsilon_q\left(\frac{a}{q}\right)\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-1}{q}) + e^{4\pi i\frac{a}{q^c}}\right]\right|^2 =$$

$$= \frac{1}{(q-1)^2}\frac{1}{q^{3c-4}}\sum_{\substack{1\le a\le q^c\\ q\nmid a}} \epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-1}{q}) + e^{4\pi i\frac{a}{q^c}}\right]\cdot\overline{\epsilon_q\left[e^{-4\pi i\frac{a}{q^c}}(\frac{-1}{q}) + e^{4\pi i\frac{a}{q^c}}\right]} =$$

$$= \frac{1}{(q-1)^2}\frac{1}{q^{3c-4}}\sum_{\substack{1\le a\le q^c\\ q\nmid a}} \left(2 + \left(\frac{-1}{q}\right)\left[e^{8\pi i\frac{a}{q^c}} + e^{-8\pi i\frac{a}{q^c}}\right]\right) =$$

$$= \frac{2q^{c-1}(q-1)}{q^{3c-4}(q-1)^2} = \frac{2}{q^{2c-3}(q-1)}.$$

And we can see that for $c > 2$, $A_Q(q^c)$ does not depend on parity of c. Now we have by [16]

$$p \ne 2, p\nmid Q; \quad A_Q(p) = \frac{p^2-2p-1}{(p^2-1)^2}, \quad A_Q(p^c) = \frac{2(p-1)}{(p^2-1)^2 p^{2c-3}}$$

$$p = 2; \qquad A_Q(2) = \frac{1}{9}, \qquad A_Q(4) = \frac{1}{18},$$

$$A_Q(8) = 0, \qquad A_Q(16) = \frac{1}{9\cdot 16},$$

$$A_Q(32) = 0, \qquad A_Q(2^c) = \frac{1}{9\cdot 2^{2c-5}}, c \ge 6.$$

and what we have find, for $q \mid Q$,

$$A_Q(q) = \frac{q^2-2q-1}{(q-1)^2}, \quad A_Q(q^2) = \frac{2}{q(q-1)}, \quad A_Q(q^c) = \frac{2}{q^{2c-3}(q-1)}.$$

Now we can calculate

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=\prod_{p\text{ - prime}}\left(1+\sum_{c\ge1}A_Q(p^c)\right)=$$

$$=\left(1+\frac{1}{9}+\frac{1}{18}+\frac{1}{9\cdot16}+\sum_{c\ge6}\frac{1}{9\cdot2^{2c-5}}\right)\times$$
$$\times\prod_{q|Q}\left(1+\frac{q^2-2q-1}{(q-1)^2}+\frac{2}{q(q-1)}+\sum_{c>2}\frac{2}{q^{2c-3}(q-1)}\right)\times$$
$$\times\prod_{\substack{p\ne2\\p\nmid Q}}\left(1+\frac{p^2-2p-1}{(p^2-1)^2}+\sum_{c\ge2}\frac{2(p-1)}{(p^2-1)^2p^{2c-3}}\right)$$

$$=\frac{1015}{864}\prod_{q|Q}\frac{2q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{p\ne2\\p\nmid Q}}\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}.$$

That is

$$\lim_{N\to\infty}\frac{1}{N}\sum_{2\le n\le N}\beta_Q^2(n)=\frac{1015}{864}\prod_{q|Q}\frac{2q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{p\ne2\\p\nmid Q}}\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}=$$

$$=\frac{1015}{864}\prod_{q|Q}\frac{2q(q^2-q-1)}{(q+1)(q-1)^2}\frac{(q^2-1)^2(q+1)}{q^2(q^3+q^2-q-3)}\prod_{p\ne2}\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}=$$

$$=\frac{1015}{864}\prod_{q|Q}\frac{2\left(q+1\right)^2\left(q^2-q-1\right)}{q\left(q^3+q^2-q-3\right)}\prod_{p\ne2}\frac{p^2(p^3+p^2-p-3)}{(p^2-1)^2(p+1)}$$

$$=\left(\prod_{q|Q}\frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)}\right)\cdot1.328...=C_1\prod_{q|Q}\frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)},$$

proving the result pointed out at the beginning of this part.

Part III
Central Limit Theorem for the spectrum of the Laplacian

8 The Selberg Trace Formula for $\Gamma_0(Q)$

Let $g \in C_{00}^{\infty}(\mathbb{R})$ be a smooth even function with compact support, and let

$$h(r) = \int_{-\infty}^{\infty} g(u)e^{iru}du$$

so that

$$g(u) = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)e^{-iru}dr.$$

Then the Selberg Trace Formula for $\Gamma_0(Q)$ is the identity

$$\begin{aligned}\sum_{j\geq 0} h(r_j) = \\ &= \{\textit{central term (identity contribution)}\} + \\ &\{\textit{hyperbolic contribution}\} + \{\textit{elliptic contribution}\} + \\ &\{\textit{parabolic and continuous spectrum contribution}\}.\end{aligned}$$

For Q squarefree, the terms are:

1. The central term is

$$\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty} h(r)r\tanh(\pi r)dr.$$

2. The hyperbolic term can be written as

$$\sum_{t>2}\sum_{\substack{\{T\}\ hyperbolic \\ |trT|=t}} \frac{\ln \mathcal{N}(T_0)}{\mathcal{N}(T)^{1/2} - \mathcal{N}(T)^{-1/2}} g(\ln \mathcal{N}(T)) = 2\sum_{t>2}\beta_Q(t)g(\ln \mathcal{N}(T)).$$

3. The elliptic term is

$$\sum_{\{E\}\ elliptic} \frac{1}{4M_E \sin\theta(E)} \int_{-\infty}^{\infty} \frac{e^{-2\theta(E)r}}{1+e^{-2\pi r}} h(r)dr.$$

Here $\theta(E)$ is the unique angle $\theta \in (0,\pi)$, such that E is $SL_2(\mathbb{R})$ - conjugate to $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$. It is clear that $\theta(E) = \{\frac{\pi}{2}, \frac{\pi}{3}\}$, since $trE = 2\cos\theta$. Also $M_E = \left|Z_{\Gamma_0(Q)}(E)\right| = \{2,3\}$ is the order of the centralizer of E in $\Gamma_0(Q)$.

4. The contribution of the parabolic terms and continuous spectrum is (see[9])

$$2^{\omega(Q)}\left(-g(0)\ln 2 - \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} h(r)\left(\frac{\Gamma'}{\Gamma}(1+ir) - \frac{1}{2}\frac{\varphi'}{\varphi}(\frac{1}{2}+ir)\right)dr\right) -$$

$$-\,2^{\omega(Q)}g(0)\ln Q - 2^{\omega(Q)}\sum_{p|Q}\sum_{n=p^r}\frac{\Lambda(n)}{n}g(2\ln n).$$

Here $2^{\omega(Q)}$ is the number of inequivalent cusps of $\Gamma_0(Q)$ for Q square-free, $\Lambda(n) = \left\{\begin{array}{ll} \ln p, & n = p^r \\ 0, & n \neq p^r \end{array}\right\}$, and $\varphi(s) = \frac{\Lambda(1-s)}{\Lambda(s)}$, $\Lambda(s) = \pi^{-s}\Gamma(s)\zeta(2s)$.

9 Applying the Selberg Trace Formula for the Counting Function

Let us set

$$h(r) = f(L(r-\tau)) + f(L(-r-\tau)),$$

where f is even function, such that $f \in C^{\infty}_{00}(\mathbb{R})$.

Lemma 9.1 *In above conditions on f and g, it follows that*

$$g(u) = \frac{1}{2\pi L}\widehat{f}\left(\frac{u}{2\pi L}\right)\left(e^{iu\tau} + e^{-iu\tau}\right).$$

Proof. We have

$$g(u) = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} h(r)e^{-iru}dr = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\left[f(L(r-\tau)) + f(L(-r-\tau))\right]e^{-iru}dr$$

$$= \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} f(L(r-\tau))e^{-iru}dr + \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} f(L(-r-\tau))e^{-iru}dr.$$

Put in the second integral $\rho = -r$ and get

$$g(u) = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} f(L(r-\tau))e^{-iru}dr + \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} f(L(\rho-\tau))e^{i\rho u}d\rho$$

$$= \frac{1}{2\pi}\int_{-\infty}^{\infty} f(L(r-\tau))(e^{iru}+e^{-iru})dr.$$

Write $L(r-\tau)=t$, we obtain

$$g(u) = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(t)\left[e^{iu(\frac{t}{L}+\tau)}+e^{-iu(\frac{t}{L}+\tau)}\right]\frac{dt}{L}$$

$$= \frac{1}{2\pi L}e^{iu\tau}\int_{-\infty}^{\infty} f(t)e^{2\pi it\frac{u}{2\pi L}}\,dt + \frac{1}{2\pi L}e^{-iu\tau}\int_{-\infty}^{\infty} f(t)e^{-2\pi it\frac{u}{2\pi L}}\,dt.$$

Since f is an even function we can write

$$g(u) = \frac{1}{2\pi L}\left(e^{iu\tau}+e^{-iu\tau}\right)\int_{-\infty}^{\infty} f(t)e^{2\pi it\frac{u}{2\pi L}}\,dt.$$

And finally

$$g(u) = \frac{1}{2\pi L}\widehat{f}\left(\frac{u}{2\pi L}\right)\left(e^{iu\tau}+e^{-iu\tau}\right),$$

proving the lemma. ∎

Now we can rewrite N_f by the new terms:

$$\begin{aligned}
N_f(\tau) &= \sum_{j\geq 0} h(r_j) = \sum_{j\geq 0}\left[f(L(r_j-\tau))+f(L(-r_j-\tau))\right]\\
&= \frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty}\left[f(L(r-\tau))+f(L(-r-\tau))\right]r\tanh(\pi r)dr\\
&+ 2\frac{1}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\left(e^{i\tau\ln\mathcal{N}(t)}+e^{-i\tau\ln\mathcal{N}(t)}\right)\\
&+ \sum_{\{E\}\text{ is elliptic}}\frac{1}{4M_E\sin\theta(E)}\int_{-\infty}^{\infty}\frac{e^{-2\theta(E)r}}{1+e^{-2\pi r}}\left[f(L(r-\tau))+f(L(-r-\tau))\right]dr\\
&- 2^{\omega(Q)}g(0)(\ln 2+\ln Q) - 2^{\omega(Q)}\sum_{p|Q}\sum_{n=p^r}\frac{\Lambda(n)}{n}g(2\ln n)\\
&- 2^{\omega(Q)}\frac{1}{2\pi}\int_{-\infty}^{\infty}\left\{f(L(r-\tau))+f(L(-r-\tau))\right\}\left\{\frac{\Gamma'}{\Gamma}(1+ir)-\frac{1}{2}\frac{\varphi'}{\varphi}(\frac{1}{2}+ir)\right\}dr.
\end{aligned}$$

Now we will try to estimate the contribution of each term above.

9.1 The Identity Term Contribution

Here we estimate the identity term, in particular we will prove

Lemma 9.2 *As $\tau \to \infty$ we have*

$$\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty}\left[f(L(r-\tau))+f(L(-r-\tau))\right]r\tanh(\pi r)dr$$

$$=\frac{2\tau}{L}\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty}f(x)dx+O(\tau e^{-2\pi\tau}).$$

Proof. Since f is an even function we get

$$\int_{-\infty}^{\infty}\left[f(L(r-\tau))+f(L(-r-\tau))\right]r\tanh(\pi r)dr$$

$$=2\int_{-\infty}^{\infty}f(L(r-\tau))r\tanh(\pi r)dr=\begin{bmatrix} x=L(r-\tau) & r=\frac{x}{L}+\tau \\ dx=Ldr & \end{bmatrix}$$

$$=2\int_{-\infty}^{\infty}f(x)\left(\frac{x}{L^2}+\frac{\tau}{L}\right)\tanh(\pi\frac{x+L\tau}{L})dx$$

$$=\frac{2}{L^2}\int_{-\infty}^{\infty}f(x)x\tanh(\pi\frac{x+L\tau}{L})dx+\frac{2\tau}{L}\int_{-\infty}^{\infty}f(x)\tanh(\pi\frac{x+L\tau}{L})dx.$$

Now we can write

$$\tanh(\pi\frac{x+L\tau}{L})=1-\frac{2}{e^{2\pi(\frac{x}{L}+\tau)}+1},$$

and so the contribution of the identity term is

$$\frac{2}{L^2}\int_{-\infty}^{\infty}f(x)xdx-\frac{4}{L^2}\int_{-\infty}^{\infty}\frac{f(x)x}{e^{2\pi(\frac{x}{L}+\tau)}+1}dx+\frac{2\tau}{L}\int_{-\infty}^{\infty}f(x)dx-\frac{4\tau}{L}\int_{-\infty}^{\infty}\frac{f(x)}{e^{2\pi(\frac{x}{L}+\tau)}+1}dx.$$

The first integral is equal to 0, since $xf(x)$ is an odd continuous function. The second and the fourth integrals are correspondingly $O(e^{-2\pi\tau})$ and $O(\tau e^{-2\pi\tau})$ as $\tau\to\infty$.

Finally we have

$$\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty}\left[f(L(r-\tau))+f(L(-r-\tau))\right]r\tanh(\pi r)dr$$
$$=\frac{2\tau}{L}\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int_{-\infty}^{\infty}f(x)dx+O(\tau e^{-2\pi\tau}),$$

as $\tau\to\infty$, proving the claim of the lemma. ■

9.2 The Elliptic Terms Contribution

Now we estimate the contribution of the elliptic terms. We consider two cases, namely $\theta(E)=\dfrac{\pi}{2}$ and $\theta(E)=\dfrac{\pi}{3}$.

Lemma 9.3 *As $\tau\to\infty$ the elliptic terms contribution is*

$$\sum_{\{E\}\ is\ elliptic}\frac{1}{4M_E\sin\theta(E)}\int_{-\infty}^{\infty}\frac{e^{-2\theta(E)r}}{1+e^{-2\pi r}}\left[f(L(r-\tau))+f(L(-r-\tau))\right]dr=O(\frac{e^{-\frac{2}{3}\pi\tau}}{L}).$$

Proof.

a) Let $\theta(E)=\dfrac{\pi}{2}$, then the integral within the sum is

$$\int_{-\infty}^{\infty}\frac{e^{-\pi r}}{1+e^{-2\pi r}}\left[f(L(r-\tau))+f(L(-r-\tau))\right]dr$$
$$=\int_{-\infty}^{\infty}f(L(r-\tau))\frac{e^{-\pi r}}{1+e^{-2\pi r}}dr+\int_{-\infty}^{\infty}f(L(-r-\tau))\frac{e^{-\pi r}}{1+e^{-2\pi r}}dr$$
$$=2\int_{-\infty}^{\infty}f(L(r-\tau))\frac{e^{-\pi r}}{1+e^{-2\pi r}}dr=\begin{bmatrix} x=L(r-\tau) & r=\dfrac{x}{L}+\tau \\ dx=Ldr & \end{bmatrix}$$
$$=\frac{2}{L}\int_{-\infty}^{\infty}f(x)\frac{e^{-\pi(\frac{x}{L}+\tau)}}{1+e^{-2\pi(\frac{x}{L}+\tau)}}dr=\frac{2}{L}\int_{-A}^{A}\frac{e^{-\pi(\frac{x}{L}+\tau)}}{1+e^{-2\pi(\frac{x}{L}+\tau)}}dr,$$

since the function f has a compact support. By changing variables in the last integral, namely by setting

$$t=e^{-\pi(\frac{x}{L}+\tau)}$$

we get

$$\frac{2}{L}\int_{-A}^{A}\frac{e^{-\pi(\frac{x}{L}+\tau)}}{1+e^{-2\pi(\frac{x}{L}+\tau)}}dr=\frac{2}{\pi}\int_{e^{-\pi(\tau+\frac{A}{L})}}^{e^{-\pi(\tau-\frac{A}{L})}}\frac{dt}{1+t^2}.$$

The last integral is positive and equal to

$$\begin{aligned}&\frac{2}{\pi}\left(\arctan e^{-\pi(\tau-\frac{A}{L})}-\arctan e^{-\pi(\tau+\frac{A}{L})}\right)\\&<\frac{2}{\pi}\left(e^{-\pi(\tau-\frac{A}{L})}-e^{-\pi(\tau+\frac{A}{L})}\right)\\&=\frac{2}{\pi}e^{-\pi\tau}\left(e^{\frac{A\pi}{L}}-e^{-\frac{A\pi}{L}}\right)=\frac{4}{\pi}e^{-\pi\tau}\sinh\frac{A\pi}{L}=O(\frac{e^{-\pi\tau}}{L}),\end{aligned}$$

as $\tau\to\infty$.

b) Consider now the case of $\theta(E)=\frac{\pi}{3}$, and transform the integral within the sum

$$\begin{aligned}&\int_{-\infty}^{\infty}\frac{e^{-\frac{2}{3}\pi r}}{1+e^{-2\pi r}}\left[f(L(r-\tau))+f(L(-r-\tau))\right]dr\\&=\int_{-\infty}^{\infty}f(L(r-\tau))\frac{e^{-\frac{2}{3}\pi r}}{1+e^{-2\pi r}}dr+\int_{-\infty}^{\infty}f(L(-r-\tau))\frac{e^{-\frac{2}{3}\pi r}}{1+e^{-2\pi r}}dr.\end{aligned}$$

By changing r with $-r$ in the second integral we will get

$$\begin{aligned}&\int_{-\infty}^{\infty}f(L(r-\tau))\left(\frac{e^{-\frac{2}{3}\pi r}}{1+e^{-2\pi r}}+\frac{e^{\frac{2}{3}\pi r}}{1+e^{2\pi r}}\right)dr\\&=\int_{-\infty}^{\infty}f(L(r-\tau))\left(\frac{e^{-\frac{2}{3}\pi r}}{1+e^{-2\pi r}}+\frac{e^{-\frac{4}{3}\pi r}}{1+e^{-2\pi r}}\right)dr=\begin{bmatrix}x=L(r-\tau) & r=\frac{x}{L}+\tau\\ dx=Ldr & \end{bmatrix}\\&=\frac{1}{L}\int_{-\infty}^{\infty}f(x)\frac{e^{-\frac{2}{3}\pi(\frac{x}{L}+\tau)}+e^{-\frac{4}{3}\pi(\frac{x}{L}+\tau)}}{1+e^{-2\pi(\frac{x}{L}+\tau)}}dx=\frac{1}{L}\int_{-A}^{A}\frac{e^{-\frac{2}{3}\pi(\frac{x}{L}+\tau)}+e^{-\frac{4}{3}\pi(\frac{x}{L}+\tau)}}{1+e^{-2\pi(\frac{x}{L}+\tau)}}dx,\end{aligned}$$

since f compactly supported. Changing variables by substituting

$$t=e^{-\frac{2}{3}\pi(\frac{x}{L}+\tau)}$$

we obtain

$$-\frac{3}{2\pi}\int_{e^{-\frac{2}{3}\pi(\tau-\frac{A}{L})}}^{e^{-\frac{2}{3}\pi(\tau+\frac{A}{L})}}\frac{t+t^2}{1+t^3}\frac{1}{t}dt=\frac{3}{2\pi}\int_{e^{-\frac{2}{3}\pi(\tau+\frac{A}{L})}}^{e^{-\frac{2}{3}\pi(\tau-\frac{A}{L})}}\frac{dt}{t^2-t+1}$$

$$= \frac{\sqrt{3}}{\pi}\left\{\arctan\frac{2}{\sqrt{3}}(e^{-\frac{2}{3}\pi(\tau-\frac{A}{L})}-\frac{1}{2}) - \arctan\frac{2}{\sqrt{3}}(e^{-\frac{2}{3}\pi(\tau+\frac{A}{L})}-\frac{1}{2})\right\} \leq$$

$$\leq \frac{2}{\pi}\left(e^{-\frac{2}{3}\pi(\tau-\frac{A}{L})} - e^{-\frac{2}{3}\pi(\tau+\frac{A}{L})}\right) =$$

$$= \frac{2}{\pi}e^{-\frac{2}{3}\pi\tau}\left(e^{\frac{2\pi A}{3L}} - e^{-\frac{2\pi A}{3L}}\right) = \frac{4}{\pi}e^{-\frac{2}{3}\pi\tau}\sinh\frac{2\pi A}{3L} = O(\frac{e^{-\frac{2}{3}\pi\tau}}{L}),$$

as $\tau \to \infty$.

Thus we see that the elliptic terms contribution is $O(\frac{e^{-\frac{2}{3}\pi\tau}}{L})$, as desired.

$\blacksquare$

9.3 Contribution of the Parabolic Terms and of the Continuous Spectrum.

In this subsection we will prove the

Theorem 9.4 *Contribution of the parabolic terms and of the continuous spectrum is*

$$O\left(\frac{\ln(1+\tau)}{L}\right),\ \textit{as}\ \tau \to \infty.$$

We start from the estimation of the integral

$$\int\limits_{-\infty}^{\infty} h(r)\frac{\Gamma'}{\Gamma}(1+ir)dr.$$

We will prove the following lemma:

Lemma 9.5 *As $\tau \to \infty$ we have*

$$\int\limits_{-\infty}^{\infty} h(r)\frac{\Gamma'}{\Gamma}(1+ir)dr = O\left(\frac{\ln(1+\tau)}{L}\right).$$

Proof. We will use here a certain form of Stirling's formula. By [1, 358-360] for s being not on the negative real axis there is an absolute constant A, such that

$$\ln\Gamma(s) = \left(s - \frac{1}{2}\right)\ln s - s + A - \int_0^\infty \frac{x - [x] + \frac{1}{2}}{x+s}dx.$$

Integrating by parts the integral here we obtain

$$\int_0^\infty \frac{x - [x] + \frac{1}{2}}{x+s}dx = \int_0^\infty \frac{\varphi(x)}{(x+s)^2}dx,$$

where

$$\varphi(x) := \int_1^x \left(u - [u] - \frac{1}{2}\right)du,$$

and, in fact,

$$|\varphi(x)| \le \frac{1}{2}.$$

By the mean-value theorem we get

$$\int_0^\infty \frac{x - [x] + \frac{1}{2}}{x+s}dx = \mu\int_0^\infty \frac{1}{(x+s)^2}dx, \text{ for some } |\mu| \le \frac{1}{2}.$$

Thus, one can conclude that

$$\frac{\Gamma'}{\Gamma}(s) = (\ln\Gamma(s))' = \ln s - \frac{1}{2s} + O\left(\frac{1}{|s|^2}\right).$$

Rewrite now the source integral as follows:

$$\int_{-\infty}^\infty h(r)\frac{\Gamma'}{\Gamma}(1+ir)dr = \int_{-\infty}^\infty h(r)\left[\ln(1+ir) - \frac{1}{2(1+ir)} + O\left(\frac{1}{1+r^2}\right)\right]dr,$$

and consider each term independently. Designate this terms I_1, I_2, I_3 correspondingly.

$$
\begin{aligned}
I_1 &= \int_{-\infty}^{\infty} h(r)\ln(1+ir)dr = \int_{-\infty}^{\infty} \left(f(L(r-\tau)) + f(L(-r-\tau))\right)\ln(1+ir)dr \\
&= \int_{-\infty}^{\infty} f(L(r-\tau))\ln(1+ir)dr + \int_{-\infty}^{\infty} f(L(-r-\tau))\ln(1+ir)dr \\
&= \int_{-\infty}^{\infty} f(L(r-\tau))\ln(1+ir)dr + \int_{-\infty}^{\infty} f(L(r-\tau))\ln(1-ir)dr \\
&= \int_{-\infty}^{\infty} f(L(r-\tau))\ln(1+r^2)dr = \begin{bmatrix} x = L(r-\tau) & dr = \frac{1}{L}dx \\ r = \frac{x}{L}+\tau & 1+r^2 = 1+\left(\frac{x}{L}+\tau\right)^2 \end{bmatrix} \\
&= \frac{1}{L}\int_{-\infty}^{\infty} f(x)\ln\left[1+\left(\frac{x}{L}+\tau\right)^2\right]dx = O\left(\frac{\ln(1+\tau)}{L}\right), \text{ as } \tau\to\infty.
\end{aligned}
$$

The last equality we obtain, for example, after integration by parts and estimation of the each term.

$$
\begin{aligned}
I_2 &= \int_{-\infty}^{\infty} h(r)\frac{1}{2(1+ir)}dr = \int_{-\infty}^{\infty} \frac{f(L(r-\tau)) + f(L(-r-\tau))}{2(1+ir)}dr \\
&= \int_{-\infty}^{\infty} \frac{f(L(r-\tau))}{2(1+ir)}dr + \int_{-\infty}^{\infty} \frac{f(L(r-\tau))}{2(1-ir)}dr \\
&= \int_{-\infty}^{\infty} f(L(r-\tau))\frac{2}{2(1+r^2)}dr = \int_{-\infty}^{\infty} \frac{f(L(r-\tau))}{1+r^2}dr = \begin{bmatrix} x = L(r-\tau) \\ dr = \frac{1}{L}dx \end{bmatrix}
\end{aligned}
$$

$$
= \frac{1}{L}\int_{-\infty}^{\infty} \frac{f(x)}{1+\left(\frac{x}{L}+\tau\right)^2}dx = \frac{1}{L}\int_{-A}^{A} \frac{1}{1+\left(\frac{x}{L}+\tau\right)^2}dx = \int_{-A}^{A} \frac{d\left(\frac{x}{L}+\tau\right)}{1+\left(\frac{x}{L}+\tau\right)^2}
$$

$$
= \arctan\left(\frac{A}{L}+\tau\right) - \arctan\left(-\frac{A}{L}+\tau\right) \le \frac{2A}{L}.
$$

And thus

$$
I_2 = O\left(\frac{1}{L}\right).
$$

Finally,

$$I_3 = O\left(\int\limits_{-\infty}^{\infty} \frac{h(r)}{1+r^2}dr\right) = O\left(\int\limits_{-\infty}^{\infty} \frac{f(L(r-\tau))+f(L(-r-\tau))}{1+r^2}dr\right)$$
$$= O\left(\int\limits_{-\infty}^{\infty} \frac{f(L(r-\tau))}{1+r^2}dr + \int\limits_{-\infty}^{\infty} \frac{f(L(-r-\tau))}{1+r^2}dr\right) = O\left(2\int\limits_{-\infty}^{\infty} \frac{f(L(r-\tau))}{1+r^2}dr\right) = O\left(\frac{1}{L}\right),$$

exactly as in the previous case.

Now one can see that we proved the lemma. ■

For the following estimation of the parabolic terms and continuous spectrum contribution, note that after certain number of steps, one obtain

$$-\frac{1}{4\pi}\int\limits_{-\infty}^{\infty} h(r)\frac{\varphi'}{\varphi}(\frac{1}{2}+ir)dr = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} h(r)\frac{\Gamma'}{\Gamma}(\frac{1}{2}+ir)dr - 2\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n}g(2\ln n) - \ln\pi g(0).$$

By the same argument as in the lemma we conclude that

$$\int\limits_{-\infty}^{\infty} h(r)\frac{\Gamma'}{\Gamma}(\frac{1}{2}+ir)dr = O\left(\frac{\ln(1+\tau)}{L}\right), \text{ as } \tau\to\infty.$$

and the sum in the right-hand side is finite, since g has a compact support. Thus

$$\int\limits_{-\infty}^{\infty} h(r)\frac{\varphi'}{\varphi}(\frac{1}{2}+ir)dr = O\left(\frac{\ln(1+\tau)}{L}\right), \text{ as } \tau\to\infty.$$

Since the non-integral part of the parabolic terms and continuous spectrum contribution is a constant for the fixed Q we have the desired claim of the theorem.

9.4 Estimation of the counting function

Applying the above estimations we obtain

$$N_f(\tau) - 2\frac{vol(\Gamma\backslash\mathbb{H})}{4\pi}\int\limits_{-\infty}^{\infty} f(x)dx\frac{\tau}{L} = S_f(\tau) + O\left(\frac{\ln(1+\tau)}{L}\right), \text{ as } \tau\to\infty,$$

where S_f is the hyperbolic terms contribution, that is

$$S_f(\tau) = 2\frac{1}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\left(e^{i\tau\ln\mathcal{N}(t)} + e^{-i\tau\ln\mathcal{N}(t)}\right). \quad (21)$$

10 The mean and variance of S_f

10.1 The expected value of S_f

To calculate the mean value of S_f we consider a following averaging operator. Choose an even weight function $\omega \geq 0$, with

$$\int\limits_{-\infty}^{\infty}\omega(x)dx = 1,$$

and $\widehat{\omega}$ compactly supported, and define an operator:

$$\langle F\rangle_T := \frac{1}{T}\int\limits_{-\infty}^{\infty}F(\tau)\omega(\frac{\tau}{T})d\tau.$$

For example, $\langle N_f(\tau)\rangle_T$ is the expectation of that all of $N_f(T\tau)$ eigenvalues are in the "window" of the length T.

Lemma 10.1 *The mean value of $S_f(\tau)$ is zero, for $T \gg 1$.*

Proof. By the above definition

$$\begin{aligned}
\langle S_f(\tau)\rangle_T &= \frac{1}{T}\int\limits_{-\infty}^{\infty}2\frac{1}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\left(e^{i\tau\ln\mathcal{N}(t)} + e^{-i\tau\ln\mathcal{N}(t)}\right)\omega(\frac{\tau}{T})d\tau \\
&= \frac{1}{T}\cdot\frac{2}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\int\limits_{-\infty}^{\infty}\omega(\frac{\tau}{T})\left(e^{i\tau\ln\mathcal{N}(t)} + e^{-i\tau\ln\mathcal{N}(t)}\right)d\tau \\
&= \frac{2}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\int\limits_{-\infty}^{\infty}\omega(\frac{\tau}{T})\left(e^{2\pi i\frac{\tau}{T}\ln\mathcal{N}(t)\frac{T}{2\pi}} + e^{-2\pi i\frac{\tau}{T}\ln\mathcal{N}(t)\frac{T}{2\pi}}\right)d(\frac{\tau}{T}) \\
&= 2\cdot\frac{2}{2\pi L}\sum_{t>2}\beta_Q(t)\widehat{f}\left(\frac{\ln\mathcal{N}(t)}{2\pi L}\right)\widehat{\omega}\left(\frac{T}{2\pi}\ln\mathcal{N}(t)\right).
\end{aligned}$$

Since $\widehat{\omega}$ has a compact support, it follows that

$$\langle S_f(\tau)\rangle_T = 0,$$

for T sufficiently large. ∎

10.2 The variance of S_f

Proposition 10.2 *If $L = o(\ln T)$, then for sufficiently large T*

$$\langle S_f^2(\tau)\rangle_T = \sigma_L^2,$$

where

$$\sigma_L^2 = 2\left(\frac{2}{2\pi L}\right)^2 \sum_{n>2} \beta_Q^2(n)\widehat{f}^2\left(\frac{\ln\mathcal{N}(n)}{2\pi L}\right).$$

Proof. Handle $\left\langle S_f^2(\tau)\right\rangle_T$ by the following way:

$$\langle S_f^2(\tau)\rangle_T = \frac{1}{T}\int_{-\infty}^{\infty}\left(\frac{2}{2\pi L}\right)^2 \sum_{m,n>2} \beta_Q(m)\beta_Q(n)\widehat{f}\left(\frac{\ln\mathcal{N}(m)}{2\pi L}\right)\widehat{f}\left(\frac{\ln\mathcal{N}(n)}{2\pi L}\right)\times$$
$$\times\left(e^{i\tau\ln\mathcal{N}(m)} + e^{-i\tau\ln\mathcal{N}(m)}\right)\left(e^{i\tau\ln\mathcal{N}(n)} + e^{-i\tau\ln\mathcal{N}(n)}\right)\omega(\frac{\tau}{T})d\tau$$

$$= \left(\frac{2}{2\pi L}\right)^2 \sum_{m,n>2} \beta_Q(m)\beta_Q(n)\widehat{f}\left(\frac{\ln\mathcal{N}(m)}{2\pi L}\right)\widehat{f}\left(\frac{\ln\mathcal{N}(n)}{2\pi L}\right)\times$$
$$\times\int_{-\infty}^{\infty}\left(e^{i\tau\ln\mathcal{N}(m)} + e^{-i\tau\ln\mathcal{N}(m)}\right)\left(e^{i\tau\ln\mathcal{N}(n)} + e^{-i\tau\ln\mathcal{N}(n)}\right)\omega(\frac{\tau}{T})\frac{d\tau}{T}$$

$$= \left(\frac{2}{2\pi L}\right)^2 \sum_{m,n>2} \beta_Q(m)\beta_Q(n)\widehat{f}\left(\frac{\ln\mathcal{N}(m)}{2\pi L}\right)\widehat{f}\left(\frac{\ln\mathcal{N}(n)}{2\pi L}\right)\times$$
$$\times\sum_{\varepsilon_1,\varepsilon_2=\pm1}\widehat{\omega}\left(\frac{T}{2\pi}(\varepsilon_1\ln\mathcal{N}(m) + \varepsilon_2\ln\mathcal{N}(n))\right).$$

Consider two cases: $\varepsilon_1 = \varepsilon_2$ and $\varepsilon_1 = -\varepsilon_2$.

a) Let $\varepsilon_1 = \varepsilon_2$, then

$$\widehat{\omega}\left(\frac{T}{2\pi}(\varepsilon_1\ln\mathcal{N}(m) + \varepsilon_2\ln\mathcal{N}(n))\right) = \widehat{\omega}\left(\frac{T}{2\pi}(\ln\mathcal{N}(m) + \ln\mathcal{N}(n))\right),$$

vanishes, since $\widehat{\omega}$ has compact support.

b) Let $\varepsilon_1 = -\varepsilon_2$.

(i) Let first $m \neq n$. We will show that these term do not contribute to the sum. To do this we estimate the difference

$$|\ln \mathcal{N}(m) - \ln \mathcal{N}(n)| .$$

Remember that

$$\mathcal{N}(n) = \left(\frac{|n| + \sqrt{n^2 - 4}}{2} \right)^2 ,$$

and thus

$$\begin{aligned} \ln \mathcal{N}(n) &= \ln \left(\frac{|n| + \sqrt{n^2 - 4}}{2} \right)^2 = 2 \ln \left(\frac{|n| + \sqrt{n^2 - 4}}{2} \right) \\ &= 2 \ln |n| \frac{1 + \sqrt{1 - \dfrac{4}{n^2}}}{2} = 2 \ln |n| + 2 \ln \frac{1 + \sqrt{1 - \dfrac{4}{n^2}}}{2} . \end{aligned}$$

For $n > 2$ we have $|n| = n$, and using Taylor's expansion we obtain

$$\ln \mathcal{N}(n) = 2 \ln n + O\left(\frac{1}{n^2} \right) .$$

Thus for $m > n$ we have

$$\ln \mathcal{N}(m) - \ln \mathcal{N}(n) = 2 \ln \frac{m}{n} + O\left(\frac{1}{n^2} \right) .$$

Since

$$\ln \frac{m}{n} \geq \ln \frac{n+1}{n} \gg \frac{1}{n} - \frac{1}{2n^2} \gg \frac{1}{\mathcal{N}(n)},$$

we conclude that for any $m \neq n$

$$|\ln \mathcal{N}(m) - \ln \mathcal{N}(n)| \gg \max \left\{ \frac{1}{\mathcal{N}(n)}, \frac{1}{\mathcal{N}(m)} \right\} . \tag{22}$$

To get a non-zero contribution to the sum we need

$$\ln \mathcal{N}(m), \ln \mathcal{N}(n) \ll L \text{ or } \ln \left(\mathcal{N}(m) \mathcal{N}(n) \right) \ll L , \tag{23}$$

since$\widehat{f}$ has compact support, and

$$\ln \left(\mathcal{N}(m) \mathcal{N}(n) \right) \gg \ln T, \tag{24}$$

by (22) and since $\widehat{\omega}$ has compact support. The estimations (24), (23) contradict $L = o(\ln T)$, and thus the terms, for which $m \neq n$ do not contribute.

(ii) We stay with the case $m = n$.

$$\begin{aligned}\left\langle S_f^2(\tau)\right\rangle_T &= \left(\frac{2}{2\pi L}\right)^2 \sum_{n>2} \beta_Q^2(n) \widehat{f}^2\left(\frac{\ln \mathcal{N}(n)}{2\pi L}\right) \sum_{\varepsilon_1=-\varepsilon_2=\pm 1} \widehat{\omega}\,(0) \\ &= 2\left(\frac{2}{2\pi L}\right)^2 \sum_{n>2} \beta_Q^2(n) \widehat{f}^2\left(\frac{\ln \mathcal{N}(n)}{2\pi L}\right) = \sigma_L^2,\end{aligned}$$

proving the proposition. ■

10.3 The asymptotics of σ_L

We can evaluate the asymptotics of σ_L as $L \to \infty$, using the formula

$$\lim_{N\to\infty} \frac{1}{N} \sum_{2\le n\le N} \beta_Q^2(n) = C_1 \prod_{q|Q} \frac{2(q^2-q-1)(q+1)^2}{q(q^3+q^2-q-3)} =: \kappa_Q,$$

which proved earlier. (Here $C_1 = \kappa_1 = 1.328...$ was analytically calculated by Manfred Peter.)

Using the partial summation formula for σ_L^2 one obtains

$$\sigma_L^2 \sim \sigma_\infty^2 := 2\left(\frac{2}{2\pi L}\right)^2 \kappa_Q \pi L \int_0^\infty \widehat{f}^2(u) e^{\pi L u} du = \frac{4\kappa_Q}{\pi L} \int_0^\infty \widehat{f}^2(u) e^{\pi L u} du. \tag{25}$$

Define the "spectral radius" ρ of f by

$$\rho := \sup\{|\xi| : \widehat{f}(\xi) \neq 0\}.$$

Then the sum (21) contains only terms with $\ln \mathcal{N}(t) \le 2\pi\rho L$. From (25) it follows now, that as $L \to \infty$

$$\sigma_L \gg\ll \frac{e^{\pi\rho L/2}}{L}.$$

11 Background from Diophantine approximation theory

In order to compute higher moments, we need to recall some basic facts about Diophantine approximation, specifically the basic machinery of heights and Liouville's theorem.

Let K be a finite extension of $\mathbb{Q}$. Denote by M_K the set of all proper absolute values on K. The height of a number $x \in K$ is defined as

$$H_K(x) := \prod_{\upsilon \in M_K} \max\{1, \|x\|_\upsilon\} \tag{26}$$

If $f(T) = a_d T^d + a_{d-1}T^{d-1} + ... + a_1 T + a_0 \in \mathbb{Z}[T]$ is the minimal polynomial of $\alpha \in K$, that is a_i coprime integers, $a_d > 0$, $f(\alpha) = 0$, then one has (see [14][3])

$$H_K(\alpha) := a_d \prod_{j=1}^{d} \max\{1, |\alpha_j|\}, \tag{27}$$

where $|\cdot|$ is the complex absolute value, and $\alpha_1, \alpha_2, ..., \alpha_d$ are the distinct Galois conjugates of α.

We define the height of the above polynomial f to be

$$H(f) := \max\{|a_j| : 0 \leq j \leq d\},$$

and the length of f to be

$$L(f) := L(\alpha) = \sum_{j=0}^{d} |a_j|\,. \tag{28}$$

It is clear that

$$L(\alpha) \leq (d+1)H(f).$$

Here we recall some basic properties of heights.

1. If $x \neq 0$, then

$$H_K(x) = H_K(x^{-1}).$$

Indeed, since for $x \neq 0$ we have $\prod_{\upsilon \in M_K} \|x\|_\upsilon = 1$ and $\left\|x^{-1}\right\|_\upsilon = \|x\|_\upsilon^{-1}$ we obtain

$$1 = \prod_{\upsilon \in M_K} \|x\|_\upsilon = \prod_{\upsilon : \|x\|_\upsilon > 1} \|x\|_\upsilon \cdot \prod_{\upsilon : \|x\|_\upsilon < 1} \|x\|_\upsilon =$$

$$= \prod_{\upsilon : \|x\|_\upsilon > 1} \|x\|_\upsilon \cdot \prod_{\upsilon : \|x^{-1}\|_\upsilon > 1} \frac{1}{\|x^{-1}\|_\upsilon},$$

and thus

$$H_K(x) = \prod_{\upsilon : \|x\|_\upsilon > 1} \|x\|_\upsilon = \prod_{\upsilon : \|x^{-1}\|_\upsilon > 1} \left\|x^{-1}\right\|_\upsilon = H_K(x^{-1}).$$

[3] The definitions in [14] quite more general. For our purposes we need no generalization.

2. For any $x, y \in K$

$$H_K(xy) \leq H_K(x)H_K(y).$$

This is a straightforward conclusion from the definitions of height and absolute value.

3. If $L \supset K$ is a finite extension of K of index $[L:K]$, then

$$H_L(x) = H_K(x)^{[L:K]}.$$

The proof one can find in [14, page 51].

From the third property we see that the height defined above depends on a field extension. Define the absolute height of x by taking any number field K containing x and setting

$$H(x) := H_K(x)^{\frac{1}{[K:\mathbb{Q}]}}, \tag{29}$$

which is well defined.

Example 11.1 *We compute the height of* $\mathcal{N}(n) = \left(\dfrac{n+\sqrt{n^2-4}}{2}\right)^2$.

Taking $K = \mathbb{Q}(\mathcal{N}(n))$ *and noting that* $\mathcal{N}(n)$ *is an algebraic integer we get* $\|\mathcal{N}(n)\|_\upsilon \leq 1$ *for all non-archimedean absolute value* υ *on* K*. Since the Galois conjugate of* $\mathcal{N}(n)$ *is* $\mathcal{N}(n)^{-1}$ *we have*

$$H(\mathcal{N}(n)) = H_K(\mathcal{N}(n))^{\frac{1}{2}} = \left(\max\{1, \mathcal{N}(n)\} \cdot \max\{1, \mathcal{N}(n)^{-1}\}\right)^{\frac{1}{2}} = \mathcal{N}(n)^{\frac{1}{2}}.$$

4. If $f \in \mathbb{Z}[T]$ is the minimal polynomial of α of degree d, then

$$H(f) \leq 2^{d-1}H(\alpha)^d.$$

For proof we recall that the coefficients of $f(x) = a_d(x-\alpha_1)(x-\alpha_2)\cdot \ldots \cdot (x-\alpha_d)$ is the symmetric functions of $\alpha_1, \alpha_2, \ldots, \alpha_d$ up to the factor

a_d, and that the maximum of the number of factors in such a functions is

$$\begin{cases} \binom{2k}{k}, & d = 2k \\ \binom{2k-1}{k}, & d = 2k-1 \end{cases}.$$

Since

$$\binom{2k}{k} = \frac{(k+1)\cdot \ldots \cdot (2k)}{k!} \le 2^k \le 2^{d-1},$$

and

$$\binom{2k-1}{k} = \frac{(k+1)\cdot \ldots \cdot (2k-1)}{(k-1)!} \le 2^{k-1} \le 2^{d-1}$$

we have

$$H(f) \le 2^{d-1} H_K(\alpha) = 2^{d-1} H(\alpha)^d.$$

Finally, we recall Liouville's theorem on the approximation of algebraic integers by rationals.

Theorem 11.2 (Liouville) *Let α be a real algebraic number of degree d. Then for any rational $\frac{p}{q} \neq \alpha$ we have*

$$\left|\alpha - \frac{p}{q}\right| \ge \frac{1}{(1+|\alpha|)^{d-1}\cdot dL(\alpha)} \cdot \frac{1}{q^d},$$

where $L(\alpha)$ defined as in (28).

12 Higher moments

In this section we will show that $S_f(\tau)$ has a Gaussian distribution:

Theorem 12.1 *For $K \ge 3$ the K-th moment of S_f/σ_L converges to that of a normal Gaussian provided that $T, L \to \infty$, such that $L = o(\ln T)$:*

$$\left\langle \left(\frac{S_f(\tau)}{\sigma_L}\right)^K \right\rangle_T = \begin{cases} \frac{(2k)!}{k!2^k} + O(\sigma_L^{-1+\varepsilon}), & K = 2k \text{ is even} \\ O(\sigma_L^{-1+\varepsilon}), & K \text{ is odd} \end{cases},$$

for any $\varepsilon > 0$.

By (21) the K-th moment of S_f is given by

$$\left\langle S_f^K(\tau)\right\rangle_T = \left(\frac{2}{2\pi L}\right)^K \sum_{n_1,n_2,\ldots,n_K} \prod_{j=1}^{K} \beta_Q(n_j)\widehat{f}\left(\frac{\ln\mathcal{N}(n_j)}{2\pi L}\right)\times \qquad (30)$$
$$\times \sum_{\eta_j=\pm1} \widehat{\omega}\left(\frac{T}{2\pi}\left(\sum_{j=1}^{K}\eta_j \ln\mathcal{N}(n_j)\right)\right).$$

We will show that for $T \gg 1$ the only contribution to (30) is for terms satisfying:

$$\sum_{j=1}^{K}\eta_j \ln\mathcal{N}(n_j) = 0.$$

To do this we need a following lemma:

Lemma 12.2 *Suppose that*

$$\sum_{j=1}^{K}\eta_j \ln\mathcal{N}(n_j) \neq 0.$$

Then

$$\left|\sum_{j=1}^{K}\eta_j \ln\mathcal{N}(n_j)\right| \geq C(K)\left(\prod_{j=1}^{K}\mathcal{N}(n_j)\right)^{-2^{K-1}},$$

where

$$C(K) = \frac{1}{(5/2)^{2^K-1}\cdot 2^{2^K+k-1}(2^K+1)}.$$

Proof. Let

$$\alpha = \prod_{j=1}^{K}\mathcal{N}(n_j)^{\eta_j}.$$

If $|\alpha-1| \leq \frac{1}{2}$ then

$$\left|\sum_{j=1}^{K}\eta_j \ln\mathcal{N}(n_j)\right| = |\ln\alpha| \gg |\alpha-1|.$$

By Liouville's theorem (11.2) for $\frac{p}{q}=1$ we have

$$|\alpha-1| \geq \frac{1}{(1+|\alpha|)^{d-1}dL(\alpha)},$$

where d is degree of α and $L(\alpha)$ defined in preliminaries. Since α lies in the compositum of the quadratic fields $\mathbb{Q}(\mathcal{N}(n_j))$ we have

$$d \leq 2^K.$$

Assuming that $|\alpha - 1| \leq \frac{1}{2}$ and using the facts

$$L(\alpha) \leq (d+1)H(f) \text{ and } H(f) \leq 2^{d-1}H(\alpha)^d$$

we obtain

$$|\alpha - 1| \geq \frac{1}{(5/2)^{2^K-1} \cdot 2^K(2^K+1) \cdot 2^{2^K-1}H(\alpha)^{2^K}}. \tag{31}$$

Estimate now the absolute height of α:

$$H(\alpha) \leq \prod_{j=1}^{K} H\left(\mathcal{N}(n_j)^{\eta_j}\right) = \prod_{j=1}^{K} H\left(\mathcal{N}(n_j)\right),$$

and using the example (11.1) we find that

$$H(\alpha) \leq \prod_{j=1}^{K} \mathcal{N}(n_j)^{\frac{1}{2}}.$$

By substituting this into (31) we derive

$$\left|\sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j)\right| \geq \frac{1}{(5/2)^{2^K-1} \cdot 2^{2^K+k-1}(2^K+1)} \left(\prod_{j=1}^{K} \mathcal{N}(n_j)\right)^{-2^{K-1}},$$

as desired. ∎

To contribute to (30) it must be satisfied

$$\left|\sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j)\right| \ll \frac{1}{T},$$

since $\widehat{\omega}$ has compact support. By the above lemma

$$\left|\sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j)\right| \gg_K \left(\prod_{j=1}^{K} \mathcal{N}(n_j)\right)^{-2^{K-1}},$$

which implies

$$\frac{1}{T} \gg_K \left(\prod_{j=1}^{K} \mathcal{N}(n_j) \right)^{-2^{K-1}}.$$

Taking logarithm and using $\ln \mathcal{N}(n_j) \ll L$ we obtain

$$\ln T \ll K 2^{K-1} L + O_K(1),$$

which contradicts the assumption $L = o(\ln T)$.

So, we stay only with the terms, such that

$$\sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j) = 0,$$

that is

$$\left\langle S_f^K(\tau) \right\rangle_T = \left(\frac{2}{2\pi L} \right)^K \sum_{n_1, n_2, \ldots, n_K} \sum_{\substack{\eta_j = \pm 1: \\ \sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j) = 0}} \prod_{j=1}^{K} \beta_Q(n_j) \widehat{f} \left(\frac{\ln \mathcal{N}(n_j)}{2\pi L} \right) \tag{32}$$

We start to handle the sum (32) from understanding the relation

$$\sum_{j=1}^{K} \eta_j \ln \mathcal{N}(n_j) = 0.$$

Rewrite this condition in the form

$$\prod_{j=1}^{K} \mathcal{N}(n_j)^{\eta_j} = 1,$$

and partition the set $\{1, 2, ..., K\}$ into disjoint union of the sets S_j, that is

$$\{1, 2, ..., K\} = \coprod_j S_j,$$

such that

$$\prod_{i \in S_j} \mathcal{N}(n_i)^{\eta_i} = 1. \tag{33}$$

We assume here that for any proper subset S of S_j

$$\prod_{i \in S} \mathcal{N}(n_i)^{\eta_i} \neq 1.$$

Under this condition it is possible to prove that all the numbers $\mathcal{N}(n_i)$, $i \in S_j$ lie in the same real quadratic field $\mathbb{Q}(\sqrt{d_j})$.

Consider now two cases:

(i) In the sum (32) there is at least one index j, such that $n_j \neq n_i$ for any $i \neq j$. We call this case an off-diagonal case. In this case there is at least one subset S_j, which contains at least 3 elements. Then the number r of subsets must satisfy

$$K \geq 2(r-1)+3, \text{ that is } r \leq \frac{K-1}{2}.$$

For each subset S_j we denote by d_j the square-free kernel of $n_i^2 - 4$, $i \in S_j$ and write

$$n_i^2 - 4 = d_j f_i^2,\ i \in S_{j.}$$

Let $\varepsilon(d_j)$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d_j})$. We can write thus

$$\mathcal{N}(n_i) = \varepsilon(d_j)^{2k_i},\ i \in S_j.$$

We saw before that $\ln \mathcal{N}(n_i) \ll L$, which implies

$$k_i \ll \frac{L}{\ln \varepsilon(d_j)},\ i \in S_j.$$

From (33) we have

$$\sum_{i \in S_j} \eta_i k_i = \sum_{i \in S_j} \pm k_i = 0,$$

and thus for $\ln \mathcal{N}(n_i) \ll L$ there are at most $O\left((L/\ln \varepsilon(d_j))^{|S_j|-1}\right)$ solutions of (33) for each subset S_j. Taking to account that we have a non-zero contribution for $\ln \mathcal{N}(n_i) \leq 2\pi\rho L$, where ρ is the spectral radius of f, and using $\beta_Q(n_i) \ll \ln^2(n_i)$ and $2\ln n_i \sim \ln \mathcal{N}(n_i) \ll L$ we obtain that the off-diagonal contribution to the sum is

$$\sum_{j=1}^{r} \prod_{i \in S_j} \beta_Q(n_i) \widehat{f}\left(\frac{\ln \mathcal{N}(n_i)}{2\pi L}\right) \ll L^2 \prod_{j=1}^{r} \sum_{\varepsilon(d_j) \leq e^{\pi L \rho}} \left(\frac{L}{\ln \varepsilon(d_j)}\right)^{|S_j|-1}$$

$$\ll L^k \left(\#\left\{d \text{ is the fundamental discriminant } \mid \varepsilon(d) \leq e^{\pi L \rho}\right\}\right)^r,$$

where $r \leq (k-1)/2$.

Using Sarnak's lemma (6.3) we have

$$\#\left\{d \text{ is the fundamental discriminant } \mid \varepsilon(d) \leq e^{\pi L\rho}\right\} \ll e^{\pi L\rho},$$

and thus we obtain that the contribution of the off-diagonal terms is bounded by

$$L^K e^{\pi L\rho r} \ll L^K e^{\pi L\rho \frac{K-1}{2}}.$$

Since $\sigma_L \gg\ll \dfrac{e^{\pi L\rho/2}}{L}$, it follows that the off-diagonal contribution is $O(\sigma_L^{K-1+\varepsilon})$, for any $\varepsilon > 0$.

(ii) Consider now the diagonal terms contribution, that is the case in which all of S_j consist of two elements, i.e. $K = 2k$. We can write $S_j = \{j, k+j\}$ for $j = 1, ..., k$, for example. We may assume now that there is the same number of "+" signs and "-" signs, and thus there are $\binom{2k}{k}$ such choices of signs. Take for convenience the first k signs to be "+" and the last k to be "-". It follows that we have to evaluate the sum

$$\left(\frac{2}{2\pi L}\right)^{2k} \sum_{\prod_{j=1}^{k} \mathcal{N}(n_j) = \prod_{j=k+1}^{2k} \mathcal{N}(n_j)} \prod_{j=1}^{2k} \beta_Q(n_j) \widehat{f}\left(\frac{\ln \mathcal{N}(n_j)}{2\pi L}\right).$$

There are $k!$ ways to build the correspondence between the first k numbers and the last k numbers, such as $n_j = n_{k+j}$. For each such correspondence we obtain the term

$$\left(\frac{2}{2\pi L}\right)^{2k} \left(\sum_{n>2} \beta_Q^2(n) \widehat{f}^2\left(\frac{\ln \mathcal{N}(n)}{2\pi L}\right)\right)^k = \left(\frac{\sigma_L^2}{2}\right)^k.$$

For the overlapping of such a correspondences we calculated the contribution in the off-diagonal case. Thus the total contribution of the diagonal terms is

$$\binom{2k}{k} k! \left(\frac{\sigma_L^2}{2}\right)^k + O(\sigma_L^{2k-1+\varepsilon}) = \frac{(2k)!}{k! 2^k} \sigma_L^{2k} + O(\sigma_L^{2k-1+\varepsilon}),$$

for any $\varepsilon > 0$, proving the theorem.

References

[1] Ayoub.R.: An introduction to the analytic theory of numbers, American Mathematical Society, Mathematical Surveys, num 10, 1963.

[2] De Bièvre.S: Quantum chaos: a brief first visit, Second Summer School in Analysis and Mathematical Physics (Cuernavaca, 2000), 161–218, Contemp. Math., 289, Amer. Math. Soc., Providence, RI, 2001.

[3] Bogomolny.E., Leyvraz.F., Schmit.C.:Distribution of eigenvalues for the modular group. Comm. Math. Phys. 176 (1996), no. 3, 577-617.

[4] Cohen.H.:A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.

[5] Cohn.H.:Advanced Number Theory, Dover Publications Inc.,1980.

[6] Conrey.B.: A guide to random matrix theory for number theorists, www.ma.utexas.edu/~kumchev/Notes.pdf

[7] Diaconis.P., Shahshahani.M.: On the eigenvalues of random matrices, J. Appl. Probab. 31A (1994) 49-62.

[8] Dedekind.K.:Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers, in Gesammelte matematische Werke, Vol I, Chelsea Publishing Co., New York, 1968, 105-158.

[9] Hejhal.D.A.: The Selberg Trace Formula for congruence subgroups, Bulletin of the American Mathematical Society, vol. 81, num. 4, 752-755, 1975.

[10] Hejhal.D.A.: The Selberg Trace Formula for $PSL(2, \mathbb{R})$, vol. 1, 2, Lecture Notes in Math. Springer-Verlag, Berlin, 1976, 1983.

[11] Ireland,K., Rosen,M.: A classical introduction to modern number theory, 2nd ed., Springer-Verlag, Berlin-Heidelberg-New York, 1990.

[12] Kallies.J., Özlük.A., Peter.M., Snyder.C.: On asymptotic properties of a number theoretic function arising out of a spin chain model in statistical mechanics, Comm. Math. Phys., 222, 9-43 (2001).

[13] Landau,E.: Vorlesungen über Zahlentheorie, vols. 1-3, S.Hirzel, Leipzig,1927.

[14] Lang.S.: Fundamentals of Diophantine geometry, Springer, New York, 1983.

[15] Lukianov.V.:A Mean Value Theorem for Closed Geodesics on Congruence Surfaces (preprint).

[16] Peter.M.: The correlation between multiplicities of closed geodesics on the modular surface. Comm.Math.Phys. 225(2002), no.1, 171-189.

[17] Peter.M: Momente der Klassenzahlen binärerquadratischer Formen mit ganzalgebraischen Koeffizienten. Acta Arith. 70, 43-77 (1995).

[18] Peter.M: The limit distribution of a number theoretic functions arising from a problem in statistical mechanics. J. Number Th. 90, 265-280 (2001).

[19] Miyake.T.:Modular forms, Springer-Verlag, New York, 1989.

[20] Rudnick.Z.: A central limit theorem for the spectrum of the modular domain. Park City lectures 2002, to appear in Annales Henri Poincare.

[21] Sarnak.P.: Class number of indefinite binary quadratic forms. J. Number Th.15, 229-247 (1982).

[22] Strömbergsson.A.: Some remarks on a spectral correspondence for Maass waveforms. Internat. Math. Res. Notices 2001, no.10, 505-517.

[23] Weil.A.:Basic Number Theory, 3rd ed., Springer-Verlag, New York, 1974.