THE DISTRIBUTION OF SPACINGS BETWEEN QUADRATIC RESIDUES, II

PÄR KURLBERG

Abstract. We study the distribution of spacings between squares in $\mathbf{Z}/Q\mathbf{Z}$ as the number of *prime* divisors of Q tends to infinity. In [3] Kurlberg and Rudnick proved that the spacing distribution for *square free* Q is **Poissonian**, this paper extends the result to *arbitrary* Q.

1. Introduction

This paper studies the distribution of spacings between squares in $\mathbf{Z}/Q\mathbf{Z}$ as $\omega(Q)$, the number of *prime* divisors of Q, tends to infinity. In [3] Kurlberg and Rudnick proved that the spacing distribution for square free Q is **Poissonian**, i.e., the same as for a sequence of independent uniformly distributed real numbers in the unit interval. The purpose of this paper is to extend the result to arbitrary Q.

The spacing distribution is defined as follows: Let $X_Q \subset \{0, 1, \ldots, Q-1\}$ be a set of representatives of the squares in $\mathbf{Z}/Q\mathbf{Z}$. Order the N_Q elements of X_Q so that $x_1 < x_2 < \ldots < x_{N_Q}$ and form the **normalized consecutive spacings** $y_i = (x_{i+1} - x_i)/s$ where $s = (x_{N_Q} - x_1)/N_Q$ is the mean spacing. By putting point mass $(N_Q - 1)^{-1}$ at each y_i we obtain a probability distribution with mean one, and we can now study the limiting distribution as $\omega(Q) \to \infty$.

For prime $Q \to \infty$ the mean spacing is constant and Davenport [1] has proved that the normalized spacing distribution is a sum of point masses at half integers $k/2$ with weight 2^{-k}, and it is easy to see that the same holds true for prime powers. In the highly composite case the mean spacing tends to infinity since s roughly equals $2^{\omega(Q)}$. Hence there is a chance that the limiting distribution has continuous support. Davenport's result in a sense suggests that quadratic residues behave, at least with respect to spacing statistics, like independent fair coin flips. This together with the heuristic that primes are independent suggests that the limiting distribution for highly composite Q should be Poissonian, i.e., the probability density function of the (normalized) spacing to the next square should be given by $P(s) = e^{-s}$.

The definition of the level spacing distribution involves ordering the elements in X_Q. In terms of analysis, ordering is a complicated operation, and it is not

Supported in part by grants from the Israel Science Foundation and by the EC TMR network "Algebraic Lie Representations", EC-contract no ERB FMRX-CT97-010.

so easy to study the level spacings directly. However, using a combinatorial argument one can recover the level spacings from the knowledge of all r**-level correlations.** (For instance, see lemma 14 of [3].)

Fix an integer $r \geq 2$. The r**-level correlation** is defined as follows: let $\mathcal{C} \subset \mathbf{R}^{k-1}$ be a convex set such that $(x_1 - x_2, x_2 - x_3, \ldots, x_{k-1} - x_x) \in \mathcal{C}$ implies that $x_i \neq x_j$ for $i \neq j$. The reason for this condition is that we want to avoid the self correlation of a point with itself. The r-level correlation with respect to $\mathcal{C}$ is given by:

$$R_r(\mathcal{C}, Q) = \frac{1}{N_Q} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} N(h, Q)$$

where $N(h, Q)$ is the number of solutions in squares $s_1, \ldots, s_r$ of the equations

$$s_{i+1} - s_i \equiv h_i \mod Q, \quad i = 1, \ldots, r-1.$$

The main result of this paper is the following:

Theorem 1. *With $\mathcal{C}$ as above there exists a constant $K > 0$, depending only on r and $\mathcal{C}$, such that*

$$R_r(\mathcal{C}, Q) = \mathrm{vol}(\mathcal{C}) + O(\exp(-K\sqrt{\omega(Q)})).$$

As is well known (for instance, see lemma 14 of [3]) this implies:

Corollary 1. *The limiting spacing distribution of squares in $\mathbf{Z}/Q\mathbf{Z}$ as $\omega(Q) \to \infty$ is Poissonian.*

Remark: In the special case that the exponents of the primes dividing Q are bounded then the methods in [3] can be generalized. For the general case one can try to truncate Q, i.e. replace Q by $\tilde{Q}$ in such a way that that the growth of the exponents is controlled. However, new ideas are needed in order to justify that the errors introduced by truncating Q and cutting off certain divisor sums are not too big. Because of the ensuing complications the bound on the error term in theorem 1 is only of sub-exponential decay in $\omega(Q)$, whereas in theorem 1 of [3] the bound decays exponentially.

Contents of the paper: In section 2 we set up the necessary notation, and in section 3 we show that the decomposition of $N(h, p)$ used in [3] is valid for prime powers. Squares that are distinct modulo Q are not necessarily distinct modulo p, and in section 4 we briefly recall some properties of this modulo p degeneracy and its relation to lattices and Möebius inversion. Section 5 deals with truncating Q, i.e., lowering the exponents of the primes dividing Q, as well as truncating sums over sets of lattices and divisors of Q. In section 6 we use the previous results to show that a periodicity heuristic is valid, using it we prove theorem 1. Finally, in the appendix we collect some lemmas on divisor sums used throughout the text.

2. Notation

For n an integer we let $\omega(n)$ be the number of *prime* divisors of n. When writing $p|n$ we will *always* refer to a prime divisor of n. Let $Q = \prod_{p|q} p^{\alpha_p}$ where $q = \mathrm{rad}(Q)$ is the largest square free divisor of Q. (Note that $\omega(Q) = \omega(q)$.) Put $\tilde{Q} = \prod_{p|q} p^{\tilde{\alpha}_p}$ where $\tilde{\alpha}_p \leq \alpha_p$ are to be picked later. If $c|q$ we let $C = \prod_{p|c} p^{\alpha_p}$ and $\tilde{C} = \prod_{p|C} p^{\tilde{\alpha}_p}$.

In what follows we will use the following convention: If a function, say f, is defined for prime arguments we let

$$f(c) = \prod_{p|c} f(p).$$

If the function is defined for prime powers, let

$$f(C) = \prod_{p|c} f(p^{\alpha_p})$$

and

$$f(\tilde{C}) = \prod_{p|c} f(p^{\tilde{\alpha}_p}).$$

For instance, we let $\sigma(p) = 1 + p^{-1}$; by the above convention $\sigma(q) = \prod_{p|q} \sigma(p) = \sum_{c|q} c^{-1}$.

We let $s = Q/N_Q$ denote the mean spacing. (This is slightly different from what is used in the introduction, but in the limit $\omega(Q) \to \infty$ the two definitions agree.) It is easy to see that $N_{p^k} = p^k \frac{\sigma(p)}{2}\left(1 + O(p^{-2})\right)$, with the error term always positive, and therefore

$$2^{\omega(q)(1-\epsilon)} \ll \frac{2^{\omega(q)}}{\sigma(q)} \leq s \ll \frac{2^{\omega(q)}}{\sigma(q)} \leq 2^{\omega(q)}. \tag{1}$$

Finally, we let

$$F(q,t) = \sum_{p|q} p^{-t}.$$

3. Analyzing $N(h, Q)$

Since x is a square modulo Q if and only if it is a square modulo P for all $P|Q$, we see that $N(h, Q)$ is multiplicative. For primes we have:

Lemma 1. *We can write*

$$N(h,p) = \frac{\Delta(h,p)}{2^r} p\left(1 + \epsilon(h,p)\right)$$

where

$$\epsilon(h,p) \ll_r p^{-1/2} \qquad \text{as } p \to \infty,$$

and $\Delta(h,p) = 2^k$ *for some* $0 \leq k \leq r$.

Proof. See proposition 4 in [3]. □

Remark: For $p \neq 2$ the bound on $\epsilon(h,p)$ follows from the Weil bounds on the number of points on curves over finite fields. For $p = 2$ the curve is highly singular, but the bound holds trivially by choosing a large enough constant.

For prime powers Hensel's lemma can be used to lift solutions. However, there are complications due to singularities arising for certain choices of h. (Note that if all points were smooth, then $N(h,p^k) = p^{k-1}N(h,p)$.) The following lemma shows that there are few solutions that do not lift.

Proposition 1. *If $b \geq a$ then*

$$|N(h,p^b) - p^{b-a}N(h,p^a)| \ll_r p^{b-a}.$$

Proof. Recall that $N(h,p^b)$ is the number of solutions in squares $s_1,\dots,s_r$ of the equations

$$s_{i+1} - s_i \equiv h_i \mod p^b, \quad i = 1,\dots,r-1,$$

which we may rewrite as

$$y_i^2 \equiv t_i + x^2 \mod p^b, \quad i = 1,\dots,r-1,$$

where $t_i = \sum_{j=1}^{i} h_j$ and we think of x as a preferred parameter. For most values of x, the equations in y_i are *smooth*, and Hensel's lemma can be applied to lift solutions modulo p to solutions for arbitrary high powers. However, at the non-smooth points the analysis is more involved.

Assume first that $p \neq 2$. For the pair correlation we get the equation

$$y^2 \equiv x^2 + t \mod p^b.$$

If $x^2 + t \not\equiv 0 \mod p$, we're in the smooth case. If not, then we can write $x^2 + t = up^k$, where u is invertible modulo p and $1 \leq k \leq b$. Now, $y^2 \equiv up^k \mod p^b$ has a solution iff k is even and u is a square in F_p, or $k = b$. Thus, if $y^2 \equiv x^2 + t \mod p^a$ has a solution which does not lift, this implies that $k \geq a$. The x^2 for which solutions cannot be lifted are contained in the (p^b)-cosets generated by $-t + (p^a)$, and there are at most $|(p^a)/(p^b)| = p^{b-a}$ such elements in $\mathbf{Z}/p^b\mathbf{Z}$. For $r \geq 3$ we observe that the "bad" x^2 are contained in the p^b-cosets generated by $\cup_{i=1}^{r-1}(-t_i + (p^a))$, and there are at most $(r-1)p^{b-a}$ such x^2.

For $p = 2$ the difference is that a unit has to be a square modulo 8 in order to be a dyadic square, and we therefore lose a factor of 4 when bounding the number of "bad" squares. $\square$

Corollary 2. *We can write*

$$N(h,p^k) = \frac{\Delta(h,p)}{2^r} p^k \left(1 + \epsilon(h,p^k)\right)$$

where

$$\epsilon(h,p^k) \ll_r p^{-1/2}.$$

Corollary 3. *There exists $K_1 > 0$ such that*

$$\epsilon(h,C) \leq K_1^{\omega(c)} c^{-1/2}$$

for all $c|q$.

4. Δ, lattices and Möbius inversion

In this section we briefly explain $\Delta(h,p)$, which measures how many extra solutions in squares s_i of the system

$$s_{i+1} - s_i \equiv h_i \mod p, \quad i = 1, \ldots, r-1,$$

there are. (For full details see section 4.1 in [3].) For the pair correlation it works as follows: if $h \not\equiv 0 \mod p$ then there are roughly $N_p/2 \simeq p/4$ solutions of $s_2 \equiv s_1 + h \mod p$ since the "probability" of $s_1 + h$ being a square modulo p is roughly $1/2$. However, if $h \equiv 0 \mod p$ there is degeneracy; $s_2 = s_1$ is *automatically* a square. Hence there are $N_p \simeq p/2$ solutions in this case, and $\Delta(0,p) = 2$ is the corresponding correction factor.

For the higher correlations the "probability" of $s_1, s_1+h_1, s_1+h_1+h_2, \ldots, s_1+h_1+\ldots h_{r-1}$ all being squares is roughly 2^{-r}, *unless* the values of the h_i's forces some of the s_i's to be equal. More precisely, if we let $\mathcal{H}_p$ be the union of linear subspaces in $(\mathbf{Z}/p\mathbf{Z})^{r-1}$ that corresponds to some s_i's being equal, then the condition for degeneracy translates into h lying in a unique smallest linear subspace $H \in \mathcal{H}_p$, and the corresponding correction factor is $2^{\operatorname{codim}(H)}$.

Using Möbius inversion we can express the function $\Delta(h,p) = 2^{\operatorname{codim}(H)}$ as a linear combination of characteristic functions of the linear subspaces in $\mathcal{H}_p$. Pulling the subspaces in $(\mathbf{Z}/p\mathbf{Z})^{r-1}$ back to $\mathbf{Z}^{r-1}$ gives a set of lattices $\mathcal{L}_p$, and $\Delta(h,p) = \sum_{L\in\mathcal{L}_p} \lambda(L)\delta_L(h)$ where δ_L is the characteristic function of the lattice and $\lambda(L)$ are certain coefficients (see section 4.1 in [3].) Note that the set of values $\{\, \lambda(L) \colon L \in \mathcal{L}_p \,\}$ is independent of p, and that $\lambda(L) = 1$ for the the maximal lattice $L = \mathbf{Z}^{r-1}$.

For divisors $c|q$, we then have

$$\Delta(h,c) = \prod_{p|c} \Delta(h,p) = \prod_{p|c} \left(\sum_{L_p \in \mathcal{L}_p} \lambda(L_p)\delta_{L_p}(h) \right) = \sum_{g|c} \sum_{\substack{L\in\mathcal{L} \\ \operatorname{supp}(L)=g}} \lambda(L)\delta_L(h)$$

where the inner sum is over the collection $\mathcal{L}$ of all lattices of the form $\cap_{p|q} L_p$, $L_p \in \mathcal{L}_p$, the coefficient $\lambda(\cap_{p|q} L_p)$ is given by $\prod_{p|q} \lambda(L_p)$, and where we let $\operatorname{supp}(L)$, the support of L, be the largest square free divisor of the discriminant $\operatorname{disc}(L)$. (The discriminant is as usual the volume of the fundamental domain of the lattice.)

Remark: If $L = \cap_{p|q} L_p$ and p does not divide $\operatorname{supp}(L)$ then $L_p = \mathbf{Z}^{r-1}$ and $\lambda(L_p) = 1$. Consequently, $L = \cap_{p|\operatorname{supp}(L)} L_p$ and $\lambda(L) = \prod_{p|\operatorname{supp}(L)} \lambda(L_p)$.

For future reference we have the following lemmas:

Lemma 2.

$$|\lambda(L)| \ll_r \operatorname{supp}(L)^\epsilon,$$

and

$$\sum_{\substack{L\in\mathcal{L} \\ \operatorname{supp}(L)=g}} 1 \ll_r g^\epsilon.$$

Proof. Immediate by the previous remark and the fact that $\lambda(L_p), |\mathcal{L}_p| \ll_r 1$. □

Lemma 3. *The following bound holds:*

$$\Delta(h, c) \ll c^{\epsilon}.$$

Proof. By the previous remark there exists a constant K_2, depending only on r, such that $\Delta(h, p) \leq K_2$. Hence $\Delta(h, c) = \prod_{p|c} \Delta(h, p) \leq K_2^{\omega(c)} \ll c^{\epsilon}$. □

By assumption the convex set $\mathcal{C}$ has empty intersection with the linear subspaces, or walls, corresponding to $\sum_{i \leq j \leq k} h_j = 0$ for $1 \leq i \leq k \leq r-1$. The lattices in $\mathcal{L}$ correspond to integer points that are congruent to the walls modulo some divisor of Q. Thus, if the support of a lattice is sufficiently large compared to the size of $s\mathcal{C}$ we expect it to have empty intersection with $s\mathcal{C}$, and this is in fact true:

Lemma 4. *If $\mathcal{C}$ does not intersect with the walls and* $\operatorname{supp}(L) \gg_{\mathcal{C}} s^{r(r-1)/2}$ *then* $s\mathcal{C} \cap L = \emptyset$.

Proof. See lemma 7 in [3]. □

If $L \subset \mathbf{R}^n$ is a lattice and $X \subset \mathbf{R}^n$ is a set with nice boundary, for instance if X is convex, then it is well known that the number of lattice points in $t \cdot X$ equals $t^n \frac{\operatorname{vol}(X)}{\operatorname{disc}(L)} + O_{X,L}(t^{n-1})$, where the error term depends on the set X *and* the lattice L. The Lipschitz principle (Davenport [2], Schmidt [4]) allows us to bound the error uniformly with respect to *integer lattices* $L \subset \mathbf{Z}^n$:

Proposition 2. *Let $L \subset \mathbf{Z}^n$ be a lattice of discriminant* $\operatorname{disc}(L)$*, and $\mathcal{C}$ a convex set. Suppose that $\mathcal{C}$ lies in a ball of radius R. Then*

$$\#(L \cap \mathcal{C}) = \frac{\operatorname{vol}(\mathcal{C})}{\operatorname{disc}(L)} + O_{\mathcal{C}}(R^{n-1})$$

where the error term only depends on $\mathcal{C}$.

Proof. For details see lemma 16 in [3]. □

The following bounds the sum of $\Delta(h, q)$ over all integer points in $s\mathcal{C}$.

Lemma 5.

$$\sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h, q) \ll_r s^{r-1} \exp\left(O\left(\log\log\left(\omega(q)\right)\right)\right)$$

Proof. Rewriting the sum using Möbius inversion and using proposition 2 we get

$$\sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h, q) = \sum_{g|q} \sum_{\substack{L \in \mathcal{L} \\ \operatorname{supp}(L) = g}} \lambda(L) \sum_{h \in s\mathcal{C} \cap L} 1$$

$$= \sum_{g|q} \sum_{\substack{L \in \mathcal{L} \\ \operatorname{supp}(L) = g}} \lambda(L) \left(\frac{\operatorname{vol}(s\mathcal{C})}{\operatorname{disc}(L)} + O(s^{r-2}) \right).$$

By lemma 4 we may assume that $g \leq s^{r(r-1)/2}$, and we may estimate the terms involving $O(s^{r-2})$ by

$$\sum_{\substack{g|q \\ g \leq s^{r(r-1)/2}}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} |\lambda(L)| s^{r-2} \ll s^{r-2} \sum_{\substack{g|q \\ g \leq s^{r(r-1)/2}}} g^{2\epsilon}$$

using lemma 2. But

$$\sum_{\substack{g|q \\ g \leq s^{r(r-1)/2}}} g^{2\epsilon} \ll s^{2\epsilon r(r-1)/2} \sum_{\substack{g|q \\ g \leq s^{r(r-1)/2}}} 1 \ll s^{\epsilon'}$$

by lemma 13 and hence the error terms only contribute $O(s^{r-2+\epsilon})$. The main term

$$\sum_{\substack{g|q \\ g \leq s^{r(r-1)/2}}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(L)}$$

is trivially bounded by

$$\mathrm{vol}(s\mathcal{C}) \sum_{g|q} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{|\lambda(L)|}{\mathrm{disc}(L)}.$$

Using multiplicativity once more we get

$$\sum_{g|q} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{|\lambda(L)|}{\mathrm{disc}(L)} = \prod_{p|q} \left(\sum_{L \in \mathcal{L}_p} \frac{|\lambda(L)|}{\mathrm{disc}(L)} \right).$$

Now, if $L \in \mathcal{L}_p$ then $\mathrm{disc}(L)$ is a power of p, and unless $L = \mathbf{Z}^{r-1}$ the power is ≥ 1. Since $\lambda(\mathbf{Z}^{r-1}) = 1$ we see that $\sum_{L \in \mathcal{L}_p} \frac{|\lambda(L)|}{\mathrm{disc}(L)} = 1 + O(p^{-1})$. Recalling that the number of lattices in $\mathcal{L}_p$ and the set of values $\{\, \lambda(L) \colon L \in \mathcal{L}_p \,\}$ are independent of p we see that the error is uniform in p. Thus

$$\begin{aligned} \sum_{g|q} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{|\lambda(L)|}{\mathrm{disc}(L)} &\ll \prod_{p|q} \left(1 + O(p^{-1})\right) \\ &\ll \exp\left(\sum_{p|q} O(p^{-1}) \right) = \exp\left(O\left(F_q(1)\right)\right) \end{aligned}$$

By lemma 10, $F_q(1) = O\left(\log\log\left(\omega(q)\right)\right)$ and we are done. □

5. Truncations

In order to use periodicity in section 6 we will need to control the error when we replace $Q = \prod_{p|q} p^{\alpha_p}$ by $\tilde{Q} = \prod_{p|q} p^{\tilde{\alpha}_p}$, where

$$\tilde{\alpha}_p = \min(\lceil 1/2 + \tfrac{\sqrt{\omega(q)}}{7 \log_2 p} \rceil, \alpha_p).$$

We will also need to show that sums over large divisors and lattices are small.

5.1. **Truncating Q.** First note that if $\tilde{\alpha}_p < \alpha_p$ then

$$p^{-\tilde{\alpha}_p} \leq p^{-1/2} \exp\left(-\frac{\sqrt{\omega(q)}}{K_3}\right)$$

for $K_3 > \frac{7}{\log 2}$. The following shows that we are not committing too large of an error when we truncate Q.

Proposition 3. *There exists $K_4 > 0$ such that*

$$R_r(\mathcal{C}, Q) = s \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \frac{N(h, \tilde{Q})}{\tilde{Q}} + O\left(\exp(-K_4\sqrt{\omega(q)})\right).$$

Proof. First we prove the following claim:

$$|\frac{N(h,Q)}{Q} - \frac{N(h,\tilde{Q})}{\tilde{Q}}| = \frac{1}{Q}\left|\prod_{p|q} N(h, p^{\alpha_p}) - \prod_{p|q} N(h, p^{\tilde{\alpha}_p})p^{\alpha_p - \tilde{\alpha}_p}\right|$$

$$\ll \frac{\Delta(h,q)}{2^{r\omega(q)}} \exp\left(K_5\sqrt{\frac{\omega(q)}{\log \omega(q)}} - \frac{\sqrt{\omega(q)}}{K_3+1}\right).$$

Letting $A_p = N(h, p^{\alpha_p})$ and $B_p = N(h, p^{\tilde{\alpha}_p})p^{\alpha_p - \tilde{\alpha}_p}$ we have $|A_p - B_p| \ll_r p^{\alpha_p - \tilde{\alpha}_p}$ by proposition 1. We may assume that B_p is nonzero for all p since $B_p = 0$ implies that $A_p = 0$ (there are no solutions to lift), and if $A_p = B_p = 0$ the bound holds trivially. Now,

$$|\prod_{p|q} A_p - \prod_{p|q} B_p| = \left(\prod_{p|q} B_p\right)\left|\prod_{p|q}\left(1 + \frac{A_p - B_p}{B_p}\right) - 1\right|$$

$$= \left(\prod_{p|q} B_p\right)\left|\exp\left(\sum_{p|q} \log\left(\frac{A_p - B_p}{B_p} + 1\right)\right) - 1\right| \ll \left(\prod_{p|q} B_p\right)\sum_{p|q}\left|\frac{A_p - B_p}{B_p}\right|$$

Thus

$$|\frac{N(h,Q)}{Q} - \frac{N(h,\tilde{Q})}{\tilde{Q}}| \ll \sum_{p_0|q}\left(\prod_{p|\frac{q}{p_0}} \frac{B_p}{p^{\alpha_p}}\right)\frac{|A_{p_0} - B_{p_0}|}{p_0^{\alpha_{p_0}}}$$

$$\ll \sum_{p_0|q}\left(\prod_{p|\frac{q}{p_0}} \frac{N(h, p^{\tilde{\alpha}_p})}{p^{\tilde{\alpha}_p}}\right) p_0^{-\tilde{\alpha}_{p_0}}$$

$$\ll \sum_{p_0|q} \prod_{p|\frac{q}{p_0}} \frac{\Delta(h,p)}{2^r}(1 + K_1 p^{-1/2}) \exp\left(-\frac{\sqrt{\omega(q)}}{K_3}\right)$$

by corollary 3 and since we can assume that $\tilde{\alpha}_p < \alpha_p$. (If they are equal then $A_p = B_p$.) This is in turn bounded by

$$\omega(q) \exp\left(-\frac{\sqrt{\omega(q)}}{K_3}\right) \prod_{p|q}(1 + K_1 p^{-1/2})$$

since $\frac{\Delta(h,p)}{2^r} \leq 1$. By lemma 12

$$\prod_{p|q}(1 + K_1 p^{-1/2}) \ll \exp\left(K_5 \sqrt{\frac{\omega(q)}{\log \omega(q)}}\right)$$

and we have proved the claim.

Summing over all h and applying lemma 5 gives that

$$s \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \frac{\Delta(h,q)}{2^{r\omega(q)}} \ll \frac{s^r}{2^{r\omega(q)}} \exp\left(O(\log\log \omega(q))\right) \ll \exp\left(O(\log\log \omega(q))\right).$$

Hence

$$s \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \left|\frac{N(h,Q)}{Q} - \frac{N(h,\tilde{Q})}{\tilde{Q}}\right|$$

$$\ll \exp\left(O\left(\log\log(\omega(q))\right) + K_5 \frac{\sqrt{\omega(q)}}{\log \omega(q)} - \frac{\sqrt{\omega(q)}}{K_3 + 1}\right).$$

and we are done as $s = Q/N_Q$ and thus

$$R_r(\mathcal{C}, Q) = \frac{1}{N_Q} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} N(h,Q) = s \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \frac{N(h,Q)}{Q}.$$

□

Corollary 4. *There exists $K_4 > 0$ such that*

$$R_r(\mathcal{C}, Q) = \frac{s}{2^{r\omega(q)}} \sum_{c|q} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q)\epsilon(h,\tilde{C}) + O\left(\exp(-K_4\sqrt{\omega(q)})\right).$$

Proof. Immediate since

$$\frac{N(h,\tilde{Q})}{\tilde{Q}} = \prod_{p|q} \frac{\Delta(h,p)}{2^r}\left(1 + \epsilon(h, p^{\tilde{\alpha}_p})\right) = \frac{\Delta(h,q)}{2^{r\omega(q)}} \sum_{c|q} \epsilon(h,\tilde{C}).$$

□

The choice of $\tilde{\alpha}_p$ also gives some control of the size of $\tilde{C}$ when $\omega(c) \leq \sqrt{\omega(q)}$:

Lemma 6. *If $c|q$ and $\omega(c) \leq \sqrt{\omega(q)}$ then $\tilde{C} \leq c^{3/2}s^{1/6}$.*

Proof. We have $\tilde{\alpha}_p \leq 3/2 + \frac{\sqrt{\omega(q)}}{7\log_2 p}$ and thus

$$\log_2 \tilde{C} \leq 3/2 \log_2 c + \sum_{p|c} \log_2 p \frac{\sqrt{\omega(q)}}{7 \log_2 p} \leq 3/2 \log_2 c + \omega(c) \frac{\sqrt{\omega(q)}}{7}$$
$$\leq 3/2 \log_2 c + \frac{\omega(q)}{7}.$$

Exponentiating we get $\tilde{C} \leq c^{3/2} 2^{\omega(q)/7} \ll c^{3/2} s^{1/7+\epsilon} \ll c^{3/2} s^{1/6}$. □

5.2. **Truncating divisor sums.** In order to use periodicity in section 6 we need the product of $\tilde{C}$ and certain discriminants of lattices to be small. We will prove that the contribution of terms where this is not the case is negligible. First we show that c with many divisors, or of large size, can be neglected.

Lemma 7. *There exists $K_6 > 0$ such that*

$$\frac{s}{2^{r\omega(q)}} \sum_{c|q} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q) \epsilon(h, \tilde{C})$$
$$= \frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c \leq s^{1/3} \\ \omega(c) \leq \sqrt{\omega(q)}}} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q) \epsilon(h, \tilde{C}) + O\left(\exp\left(-\frac{K_6}{2}\sqrt{\omega(q)}\right)\right).$$

Proof. By corollary 3,

$$\sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \left|\Delta(h,q)\epsilon(h,\tilde{C})\right|$$
$$\ll c^{-1/2} K_1^{\omega(c)} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q).$$

Moreover,

$$\frac{s}{2^{r\omega(q)}} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q) \ll \frac{s^r}{2^{r\omega(q)}} \exp\left(O(\log\log\omega(q))\right)$$
$$\ll \exp\left(O(\log\log\omega(q))\right)$$

by lemma 5 and the result now follows from lemma 12. □

5.3. **Truncating lattice sums.** Writing $\Delta(h,q) = \Delta(h,c) \cdot \Delta(h, \frac{q}{c})$ and expanding the second term

$$\Delta(h, \frac{q}{c}) = \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L) = g}} \lambda(L) \delta_L(h)$$

we get

$$\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c \leq s^{1/3} \\ \omega(c) \leq \sqrt{\omega(q)}}} \sum_{h \in s\mathcal{C} \cap \mathbf{Z}^{r-1}} \Delta(h,q) \epsilon(h, \tilde{C})$$

$$= \frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} \sum_{g|\frac{q}{c}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c).$$

We now show that lattices with large discriminants can be neglected:

Lemma 8.

$$\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} \sum_{g|\frac{q}{c}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c)$$

$$= \frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c} \\ g\le s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g \\ \mathrm{disc}(L)\le s^{1/3}}} \lambda(L) \sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c)$$
$$+ O(s^{-1/3+\epsilon}).$$

Proof. By lemma 4, we may assume that $g \le s^{r(r-1)/2}$. By corollary 3, and lemma 3 $\epsilon(h,\tilde{C})\Delta(h,c) \ll c^{-1/2+\epsilon}$, thus

$$\sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c) \ll c^{-1/2+\epsilon} \sum_{h\in s\mathcal{C}\cap L} 1.$$

By proposition 2

$$\sum_{h\in s\mathcal{C}\cap L} 1 = \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(L)} + O(s^{r-2}).$$

Now,

$$\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} c^{-1/2+\epsilon} \sum_{\substack{g|\frac{q}{c} \\ g\le s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g \\ \mathrm{disc}(L)\ge s^{1/3}}} |\lambda(L)| \left(\frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(L)} + O(s^{r-2})\right)$$

$$\ll \frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} c^{-1/2+\epsilon} \sum_{\substack{g|\frac{q}{c} \\ g\le s^{r(r-1)/2}}} g^{2\epsilon} \left(\frac{\mathrm{vol}(s\mathcal{C})}{s^{1/3}} + O(s^{r-2})\right)$$

by lemma 2. Thus we need to show that

$$\frac{\mathrm{vol}(\mathcal{C})s^r}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\le s^{1/3} \\ \omega(c)\le\sqrt{\omega(q)}}} c^{-1/2+\epsilon} \sum_{\substack{g|\frac{q}{c} \\ g\le s^{r(r-1)/2}}} O(s^{-1/3}) = O(s^{-1/3+\epsilon}).$$

By lemma 13

$$\sum_{\substack{g|\frac{q}{c}\\ g\leq s^{r(r-1)/2}}} s^{-1/3} \ll s^{-1/3+\epsilon},$$

and

$$\sum_{\substack{c|q\\ c\leq s^{1/3}\\ \omega(c)\leq\sqrt{\omega(q)}}} c^{-1/2+\epsilon} \ll \sum_{\substack{c|q\\ c\leq s^{1/3}\\ \omega(c)\leq\sqrt{\omega(q)}}} O(1) \ll s^{\epsilon}.$$

Since $\frac{\mathrm{vol}(\mathcal{C})s^r}{2^{r\omega(q)}} \leq \frac{\mathrm{vol}(\mathcal{C})}{\sigma(q)^r} \leq 1$ we see that the sum over L such that $\mathrm{disc}(L) \geq s^{1/3}$ is $O(s^{-1/3+\epsilon})$. □

6. Periodicity

We are now in the position of using periodicity of $\epsilon(h,\tilde{C})\Delta(h,c)$ modulo $\tilde{C}$, i.e. if $\mathrm{disc}(L)\cdot\tilde{C} \leq s$ then

$$\sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c) \simeq \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c),$$

which is made rigorous by:

Proposition 4. *If* $\mathrm{disc}(L)\cdot\tilde{C} \leq s$ *then*

$$\sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c) = \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c) + O(\tilde{C}c^{-1/2+\epsilon}s^{r-2})$$

Proof. See 6.10 in [3]. □

Summing over c, g and L we get:

Corollary 5.

$$\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q\\ c\leq s^{1/3}\\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c}\\ g\leq s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L}\\ \mathrm{supp}(L)=g\\ \mathrm{disc}(L)\leq s^{1/3}}} \lambda(L) \sum_{h\in s\mathcal{C}\cap L} \epsilon(h,\tilde{C})\Delta(h,c)$$

$$= \frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q\\ c\leq s^{1/3}\\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c}\\ g\leq s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L}\\ \mathrm{supp}(L)=g\\ \mathrm{disc}(L)\leq s^{1/3}}} \lambda(L) \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c)$$

$$+O\left(\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q\\ c\leq s^{1/3}\\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c}\\ g\leq s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L}\\ \mathrm{supp}(L)=g\\ \mathrm{disc}(L)\leq s^{1/3}}} |\lambda(L)|\tilde{C}c^{-1/2+\epsilon}s^{r-2} \right).$$

Proof. Immediate since the bounds on $c, \omega(c)$ and $\mathrm{disc}(L)$ forces $\tilde{C} \cdot \mathrm{disc}(L)$ to be smaller than s by lemma 6. □

6.1. **Estimating the error term.** By lemma 6, $\tilde{C}c^{-1/2+\epsilon} \leq cs^{1/6+\epsilon} \leq s^{1/2+\epsilon}$. This together with lemma 2 gives that the error term is bounded by

$$\frac{s^{r-1}}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\leq s^{1/3} \\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c} \\ g\leq s^{r(r-1)/2}}} g^{2\epsilon}s^{1/2+\epsilon} \ll \frac{s^{r-1}}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\leq s^{1/3} \\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c} \\ g\leq s^{r(r-1)/2}}} s^{1/2+2\epsilon}$$

which, by lemma 13, is

$$\ll \frac{s^{r-1}}{2^{r\omega(q)}} s^{1/2+3\epsilon} \ll s^{-1/2+3\epsilon}$$

and can thus be neglected.

6.2. **The main term.** In order to evaluate the main term we need to complete the sum, i.e. extend it to all lattices and divisors:

Lemma 9. *There exists $K_7 > 0$ such that*

$$\frac{s}{2^{r\omega(q)}} \sum_{\substack{c|q \\ c\leq s^{1/3} \\ \omega(c)\leq\sqrt{\omega(q)}}} \sum_{\substack{g|\frac{q}{c} \\ g\leq s^{r(r-1)/2}}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g \\ \mathrm{disc}(L)\leq s^{1/3}}} \lambda(L)\frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c)$$

$$= \frac{s}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L)\frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c)$$

$$+O\left(\exp\left(-K_7\sqrt{\omega(q)}\right)\right).$$

Proof. By lemma 3 and corollary 3,

$$\frac{1}{\tilde{C}^{r-1}} \sum_{h \mod \tilde{C}} \epsilon(h,\tilde{C})\Delta(h,c) \ll c^{1/2+\epsilon}$$

and we can therefore use the same bounds as in lemma 8 to include the terms for which $\mathrm{disc}(L) \geq s^{1/3}$. Since

$$\sum_{\substack{L\in\mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{\lambda(L)}{\mathrm{disc}(\tilde{C}L)} \ll g^{2\epsilon-1}$$

we can use lemma 13 to include $g \geq s^{r(r-1)/2}$. Finally, similar bounds used in lemma 7 allows us to extend the sum to include all $c, \tilde{C}$. □

The completed sum is multiplicative, and we can evaluate it as follows: Expanding $N(h, \tilde{Q})$ we see that

$$\frac{1}{N_{\tilde{Q}}} \sum_{h \in (\mathbf{Z}/\tilde{Q}\mathbf{Z})^{r-1}} N(h, \tilde{Q}) = \frac{s_{\tilde{Q}}}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \sum_{\substack{h \mod \tilde{Q} \\ h \in L}} \epsilon(h, \tilde{C}) \Delta(h, c).$$

Since $\mathrm{disc}(L)$ and c are coprime the intersection of a fundamental domain of $\tilde{C}L$ with L consists of a full set of representatives of $\mathbf{Z}^{r-1}/\tilde{C}\mathbf{Z}^{r-1}$ (see lemma 8 in [3].) Now, $\mathbf{R}^{r-1}/\tilde{Q}\mathbf{Z}^{r-1}$ can be expressed as a disjoint union of $\frac{\tilde{Q}^{r-1}}{\mathrm{disc}(\tilde{C}L)}$ translates of the fundamental domain for $\tilde{C}L$, and thus

$$\sum_{\substack{h \mod \tilde{Q} \\ h \in L}} \epsilon(h, \tilde{C}) \Delta(h, c) = \frac{\tilde{Q}^{r-1}}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h, \tilde{C}) \Delta(h, c).$$

Hence

$$\frac{1}{N_{\tilde{Q}}} \sum_{h \in (\mathbf{Z}/\tilde{Q}\mathbf{Z})^{r-1}} N(h, \tilde{Q})$$

$$= \frac{s_{\tilde{Q}}}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \frac{\tilde{Q}^{r-1}}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h, \tilde{C}) \Delta(h, c).$$

On the other hand,

$$\sum_{h \in (\mathbf{Z}/\tilde{Q}\mathbf{Z})^{r-1}} N(h, \tilde{Q}) = N_{\tilde{Q}}^r$$

since all r-tuples of squares are accounted for when we sum over all h. Hence

$$\frac{s_{\tilde{Q}}}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{\lambda(L)}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h, \tilde{C}) \Delta(h, c) = \left(\frac{N_{\tilde{Q}}}{\tilde{Q}} \right)^{r-1} = \frac{1}{s_{\tilde{Q}}^{r-1}},$$

and thus

$$\frac{s}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \lambda(L) \frac{\mathrm{vol}(s\mathcal{C})}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h, \tilde{C}) \Delta(h, c)$$

$$= \frac{\mathrm{vol}(\mathcal{C}) s^r}{2^{r\omega(q)}} \sum_{c|q} \sum_{g|\frac{q}{c}} \sum_{\substack{L \in \mathcal{L} \\ \mathrm{supp}(L)=g}} \frac{\lambda(L)}{\mathrm{disc}(\tilde{C}L)} \sum_{h \mod \tilde{C}} \epsilon(h, \tilde{C}) \Delta(h, c)$$

$$= \mathrm{vol}(\mathcal{C}) \frac{s^r}{s_{\tilde{Q}}} \frac{1}{s_{\tilde{Q}}^{r-1}} = \mathrm{vol}(\mathcal{C}) \left(\frac{s}{s_{\tilde{Q}}} \right)^r,$$

and we will be done if we can show that $\frac{s}{s_{\tilde{Q}}} = 1 + O(\exp(-C\sqrt{\omega(q)})$ for some $C > 0$. Now, it is easy to see that

$$N_{p^k} = p^{k-1}\frac{p-1}{2} + p^{k-1-2}\frac{p-1}{2} + \ldots + \frac{p-1}{2}p^{k-1-2(\lceil k/2\rceil -1)} + 1,$$

which implies that

$$\frac{N_{p^k}}{p^k} = \frac{\sigma(p)}{2}\left(1 + p^{-2} + \ldots + p^{-2(\lceil k/2\rceil -1)} + \frac{2}{\sigma(p)}p^{-k}\right).$$

We may assume that $\tilde{\alpha}_p < \alpha_p$, hence

$$\begin{aligned}\frac{s}{s_{\tilde{Q}}} &= \prod_{p|q}\left(1 + O(p^{-\tilde{\alpha}_p})\right) = \exp\left(\sum_{p|q}\log\left(1 + O(p^{-\tilde{\alpha}_p})\right)\right) \\ &= \exp\left(\sum_{p|q} O(p^{-\tilde{\alpha}_p})\right).\end{aligned}$$

But

$$\begin{aligned}\sum_{p|q} p^{-\tilde{\alpha}_p} &\ll \sum_{p|q} p^{-1/2}\exp\left(-\frac{\sqrt{\omega(q)}}{K_3}\right) \ll \omega(q)\exp\left(-\frac{\sqrt{\omega(q)}}{K_3}\right) \\ &\ll \exp\left(-\frac{\sqrt{\omega(q)}}{K_3+1}\right).\end{aligned}$$

Thus

$$\frac{s}{s_{\tilde{Q}}} = 1 + O\left(\exp\left(-\frac{\sqrt{\omega(q)}}{K_3+1}\right)\right)$$

and we have proved theorem 1.

Appendix

Recall that q is assumed to be *square free.* (See section 2.)

Lemma 10. *Let p_1 be the smallest prime dividing q. With $F(q,t) = \sum_{p|q} p^{-t}$ and $k > 0$ an integer we have*

$$F(q,k/2) \le \begin{cases} O\left(\sqrt{\frac{\omega(q)}{\log\omega(q)}}\right) & \text{if } k = 1, \\ O\left(\log(\log(\omega(q)))\right) & \text{if } k = 2, \\ 3p_1^{1-k/2} & \text{if } k \ge 3. \end{cases}$$

Proof. For the cases $k = 1$ and $k = 2$ we may assume that q is the product of the first $\omega(q)$ primes, and the bounds are then immediate consequences of the prime number theorem, together with the fact that the $\omega(q)$-th prime is roughly of size $\omega(q)\log\omega(q)$. For $k \ge 3$, we note that the sum is bounded by $p_1^{-k/2} + \int_{p_1}^{\infty} x^{-k/2}dx < p_1^{-k/2} + (k/2-1)^{-1}p_1^{1-k/2} < 3p_1^{1-k/2}$. $\square$

Corollary 6. *There exist $K_5 > 0$ such that*

$$\prod_{p|q}(1+K_1 p^{-1/2}) \ll \exp\left(K_5\sqrt{\frac{\omega(q)}{\log(\omega(q))}}\right).$$

Proof.

$$\prod_{p|q}(1+K_1 p^{-1/2}) = \exp\left(\sum_{p|q}\log(1+K_1 p^{-1/2})\right)$$
$$\ll \exp\left(\sum_{p|q} K_1 p^{-1/2}\right) = \exp\left(K_1 F(q,1/2)\right).$$

□

Lemma 11. *There exists $C > 0$ such that*

$$\sum_{\substack{c|q \\ \omega(c)\geq\sqrt{\omega(q)}}} K_1^{\omega(c)} c^{-1/2} \ll_{K_1} \exp(-C\sqrt{\omega(q)}).$$

Proof. Let

$$f(z) = \prod_{p|q}(1+zK_1 p^{-1/2}) = \sum_{k=0}^{\omega(q)} z^k a_k$$

where $a_k = \sum_{c|q,\omega(c)=k} K_1^{\omega(q)} c^{-1/2}$. By Cauchy's theorem

$$a_n = \frac{1}{2\pi i}\int_{|z|=2}\frac{f(z)}{z^{n+1}}dz$$

and thus

$$|a_n| \leq \frac{1}{2\pi}\int_{|z|=2}\frac{|f(z)|}{2^{n+1}}|dz|.$$

Write $q = q_1 \cdot q_2$ where $q_1 = \prod_{\substack{p|q \\ p\leq 9K_1^2}} p$, $q_2 = \prod_{\substack{p|q \\ p>9K_1^2}} p$ and let

$$f_i = \prod_{p|q_i}(1+zK_1 p^{-1/2}).$$

Clearly $|f_1(z)| \ll_{K_1} 1$ for $|z| \leq 2$. Moreover,

$$f_2(z) = \prod_{p|q_2}(1+zK_1 p^{-1/2}) = \exp\left(\sum_{p|q_2}\log(1+zK_1 p^{-1/2})\right)$$
$$= \exp\left(\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}F(q_2,k/2)(zK_1)^k\right).$$

By lemma 10, $F(q_2, k/2) \le 3(9K_1^2)^{1-k/2}$ for $k \ge 3$ and thus

$$f_2(z) = \exp\left(zK_1F(q_2, 1/2) - \frac{(zK_1)^2}{2}F(q_2, 1) + g(z)\right)$$

where $g(z)$ is an analytic function whose n-th coefficient of its power series expansion around zero is bounded by $K_1^2 \cdot 3^{3-n}$. Consequently, $|g(z)|$ is uniformly bounded in q as well as z for $|z| \le 2$. Hence

$$|a_n| \ll \frac{\exp\left(2K_1F(q,1/2) + \frac{(2K_1)^2}{2}F(q,1)\right)}{2^{n+1}}$$

for $|z| \le 2$. By the bounds on $F(q, 1/2)$ and $F(q, 1)$ in lemma 10 we see that

$$|a_n| \ll \frac{\exp\left(O\left(\sqrt{\frac{\omega(q)}{\log\omega(q)}}\right)\right)}{2^n}.$$

Thus,

$$\sum_{\substack{c|q\\ \omega(c)\ge\sqrt{\omega(q)}}} K_1^{\omega(c)}c^{-1/2} = \sum_{k=\sqrt{\omega(q)}}^{\omega(q)} a_k \ll \exp\left(O\left(\sqrt{\frac{\omega(q)}{\log\omega(q)}}\right)\right)\sum_{k=\sqrt{\omega(q)}}^{\infty}\frac{1}{2^n}$$

$$\ll \exp\left(O\left(\sqrt{\frac{\omega(q)}{\log\omega(q)}}\right)\right)\frac{1}{2^{\sqrt{\omega(q)}}}$$

$$\ll \exp\left(O\left(\sqrt{\frac{\omega(q)}{\log\omega(q)}}\right) - \sqrt{\omega(q)}\log(2)\right) \ll \exp(-C\sqrt{\omega(q)})$$

for any $C < \log 2$. □

Lemma 12. *Let f be a multiplicative function such that $f(c) \le c^{-1/2}K_1^{\omega(c)}$ for some constant $K_1 > 0$. Then there exists constants K_5, K_6 such that for all q*

$$\sum_{c|q} f(c) = \sum_{\substack{c|q\\ c\le s^{1/3}}} f(c) + O(s^{-1/6+\epsilon}) = \sum_{\substack{c|q\\ c\le s^{1/3}\\ \omega(c)\le\sqrt{\omega(q)}}} f(c) + O\left(\exp\left(-K_6\sqrt{\omega(q)}\right)\right)$$

and

$$\sum_{c|q} f(c) \ll \exp\left(K_5\sqrt{\frac{\omega(q)}{\log(\omega(q))}}\right).$$

Proof. For the first assertion we note that $f(c) \le c^{-1/2}K_1^{\omega(c)}$ implies that

$$\sum_{\substack{c|q\\ c\ge s^{1/3}}} |f(c)| \ll \sum_{\substack{c|q\\ c\ge s^{1/3}}} c^{-1/2}K_1^{\omega(c)} \ll \sum_{\substack{c|q\\ c\ge s^{1/3}}} c^{-1/2+\epsilon},$$

which by lemma 13 is bounded by $s^{-1/6+\epsilon}$. The second assertion follows from lemma 11, and the last follows from corollary 6. $\square$

Lemma 13. *Let q be the largest square free divisor of Q, and let $s = Q/N_Q$ where N_Q is the number of squares modulo Q (see section 2 for more details.) Let $\alpha, \beta > 0$. Then*

$$\sum_{\substack{c|q \\ c \geq s^\alpha}} c^{-\beta} \ll s^{-\alpha\beta+\epsilon}.$$

Moreover,

$$\sum_{\substack{c|q \\ c \leq s^\alpha}} 1 \ll s^{\epsilon}.$$

Proof. For Q square free (i.e. $Q = q$ and $s = 2^{\omega(q)}/\sigma(q)$) this is lemma 18 and 19 in [3], and the general case then follows from equation 1. $\square$

Acknowledgement. The author wishes to thank Zeév Rudnick for helpful discussions and comments.

References

[1] H. Davenport, *On the distribution of quadratic residues* (mod p), Jour. London Math. Soc. **6** (1931), 49-54, *ibid.* **8** (1933), 46-52.

[2] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.

[3] P. Kurlberg, Z. Rudnick, *The distribution of spacings between quadratic residues*, submitted for publication.

[4] W. M. Schmidt, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.

E-mail address: `kurlberg@alumni.stanford.org`

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel