Large sieve inequality with characters to square moduli

by

Liangyi Zhao (Piscataway, NJ)

1. Introduction and historical background. It was in 1941 that Yu. V. Linnik [8] originated the idea of large sieve, and he also made an application to the distribution of quadratic non-residues. A. Rényi studied the large sieve extensively and made important applications to the Goldbach problem. Refinements in that direction have later been made by many.

A set of real numbers $\{x_k\}$ is said to be *δ-spaced modulo* 1 if $x_j - x_k$ is at least δ away from any integer, for all $j \neq k$. Hence the set $\{x_k\}$ must be finite with cardinality not exceeding δ^{-1}. Throughout we assume that $0 < \delta \leq 1/2$.

The large sieve inequality, which we henceforth refer to as the classical large sieve inequality, is stated as follows. Different elegant proofs of it can be found in [3], [6], [10], [9]. The theorem, in the following form, was first introduced by Davenport and Halberstam ([4] and [5]).

THEOREM 1. *Let $\{a_n\}$ be an arbitrary sequence of complex numbers, $\{x_k\}$ be a set of real numbers which is δ-spaced modulo* 1*, and M, N be integers with $N > 0$. Then*

$$(1.1) \qquad \sum_k \Big| \sum_{n=M+1}^{M+N} a_n e(x_k n) \Big|^2 \ll (\delta^{-1} + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant is absolute.

Save for the more precise implied constant, the above inequality is the best possible. Moreover, Cohen and Selberg have shown independently that

$$(1.2) \qquad \sum_k \Big| \sum_{n=M+1}^{M+N} a_n e(x_k n) \Big|^2 \leq (\delta^{-1} - 1 + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

which is absolutely the best possible, since Bombieri and Davenport [1] gave examples of $\{x_k\}$ and a_n, with $\delta \to 0$, $N \to \infty$ and $N\delta \to \infty$ such that asymptotic equality holds in (1.2).

This theorem admits corollaries for additive and multiplicative characters. We derive

$$\sum_{q=1}^{Q} \sum_{\substack{a \bmod q \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q}n\right) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2;$$

here and below, $\sum^*$ means that the sum runs over primitive characters modulo the specified modulus only. As usual, $\varphi(q)$ is the Euler φ function.

In this paper, we shall establish a large sieve inequality for additive characters in which the moduli are squares, that is, q^2 rather than q (see Theorem 2 in Section 4). The problem reduces down to the spacing properties of rational numbers with square denominators. The key idea that we employ in resolving such a problem is the Weyl–Hardy–Littlewood method for exponential sums. It is also worth noting that the method that we use in this paper may be generalized to higher power moduli. However, as Weyl's estimates for exponential sums weaken when the polynomial in the amplitude is of high degree, our corresponding results are also weaker. From Theorem 2 we derive a corresponding large sieve type inequality for multiplicative primitive characters (see Corollary 1 in Section 4).

The following notations and conventions are used throughout paper:

• $e(z) = \exp(2\pi i z) = e^{2\pi i z}$.
• $f = O(g)$ means $|f| \le cg$ for some unspecified positive constant c.
• $f \ll g$ means $f = O(g)$.
• $f \asymp g$ means $c_1 g \le f \le c_2 g$ for some unspecified positive constants c_1 and c_2. Unless otherwise stated, all implied constants in $\ll$, O and $\asymp$ are absolute.
• $\|x\| = \inf\{|x - k| : k \in \mathbb{Z}\}$ denotes the distance of a real number x to its closest integer.
• ■ denotes the end of a proof or that the proof is easy and standard.

2. Heuristics and "trivial" bounds. As stated earlier, we are interested in having an estimate of the following kind:

$$(2.1) \qquad \sum_{q=1}^{Q} \sum_{\substack{a \bmod q^2 \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^2}\, n\right) \right|^2 \ll \Delta \sum_{n=M+1}^{M+N} |a_n|^2.$$

It is a remark attributed to Borel that the rational numbers on the real line are like stars in the heavens "to illuminate the mystery of the continuum." Indeed, we must investigate the well-spacedness of some of these "stars." As it certainly suffices to consider only q's in dyadic intervals, we set

$$S_Q = \{a/q^2 \in \mathbb{Q} : \gcd(a,q) = 1,\ 1 \le a < q^2,\ Q < q \le 2Q\}.$$

We easily see that if x and x' are two distinct elements of S_Q, then $\|x-x'\| \ge Q^{-4}$. Therefore, just from the classical large sieve inequality, we may take

$$(2.2) \qquad\qquad\qquad \Delta = Q^4 + N$$

in (2.1). On the other hand, all rational numbers a/q^2 in S_Q with a fixed denominator q^2 are clearly q^{-2}-spaced. Therefore, again by virtue of the classical large sieve inequality, we may also take in (2.1) after summing over q,

$$(2.3) \qquad\qquad\qquad \Delta = Q(Q^2 + N).$$

It is worth noting that when $N \asymp Q^3$, both (2.2) and (2.3) can be interpreted as Q^4. However, neither (2.2) nor (2.3) exploit the fact that squares are so sparsely distributed among the integers. One easily deduces that there are $\asymp Q^3$ rational numbers between 0 and 1 with square denominators and height at most Q^2. Hence, these rational numbers are "on average" Q^{-3}-spaced. Therefore, we aim to exploit these "facts" and improve the estimates in (2.2) and (2.3). Toward that end, we "divide and conquer."

3. Preliminary lemmas. We begin by quoting the duality principle, which says that the norm of a bounded linear operator in a Banach space is the same as that of its adjoint operator. To us, it amounts to swapping summations. More precisely, we have

LEMMA 1 (Duality Principle, [7]). *Let $T = [t_{mn}]$ be a finite square matrix with complex entries. The following two statements are equivalent:*

1. *For any complex numbers $\{a_n\}$, we have*

$$\sum_m \left| \sum_n a_n t_{mn} \right|^2 \le D \sum_n |a_n|^2.$$

2. *For any complex numbers $\{b_n\}$, we have*

$$\sum_n \left| \sum_m b_m t_{mn} \right|^2 \leq D \sum_m |b_m|^2. \quad \blacksquare$$

We shall need the Poisson summation formula, which asserts that if $f(x)$ is a reasonably well-behaved function, then summing $f(n)$ over all integers n is the same as summing the Fourier transform of $f(x)$ over all integers n. More precisely, we have

LEMMA 2 (Poisson Summation Formula, [2]). *Let $f(x)$ be a function on the real numbers that is piecewise continuous with only finitely many discontinuities and for all real numbers a satisfies*

$$f(a) = \frac{1}{2}[\lim_{x \to a-} f(x) + \lim_{x \to a+} f(x)].$$

Moreover, $f(x) \ll (1 + |x|)^{-c}$ for some $c > 1$ with an absolute implied constant. Then

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}(n),$$

where

$$\widehat{f}(x) = \int_{-\infty}^{\infty} f(y)e(xy)\,dy,$$

the Fourier transform of $f(x)$. $\blacksquare$

Both of the above lemmas are proved using standard means. The following lemma is crucial to the proof of our result.

LEMMA 3 (Weyl Shift, [12, Lemma 5.6]). *Let I be an interval of length N and $f(x)$ be a polynomial of degree $k \geq 2$ with real coefficients. Set $\kappa = 2^{k-1}$ and let α be the leading coefficient of $f(x)$. Also set*

$$S = \sum_{n \in I} e(f(n)).$$

Then

$$|S|^\kappa \leq 2^{2\kappa} N^{\kappa-1} + 2^\kappa N^{\kappa-k} \sum_{r_1,\ldots,r_{k-1}} \min\left(N, \frac{1}{\|\alpha k! r_1 \ldots r_{k-1}\|}\right),$$

where each r runs from 1 to $N - 1$. $\blacksquare$

In short, if $f(x)$ is a linear polynomial, then S is none other than a geometric series. But if $f(x)$ is a polynomial of degree $k > 1$, then $f(x) - f(x+h)$ will be a polynomial of degree $k-1$ in x. If we iterate this process $k-1$ times, we get a geometric series and obtain some saving in the estimate of the modulus of S.

4. The main contention. Again, we are interested in having an estimate of the following kind:

$$\sum_{\substack{q=1}}^{Q} \sum_{\substack{a \bmod q^2 \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^2}n\right) \right|^2 \ll \Delta \sum_{n=M+1}^{M+N} |a_n|^2.$$

Before we state and prove our main contention of this section, we first estimate

$$(4.1) \qquad M(Q,N) = \max_{x \in S_Q} \#\left\{ x' \in S_Q : \|x - x'\| < \frac{1}{2N} \right\},$$

which is the central issue of our theorem.

LEMMA 4. *Given $\varepsilon > 0$ and $N \in \mathbb{N}$, we have*

$$(4.2) \qquad M(Q,N) \ll \frac{Q^3}{N} + \left(\sqrt{Q} + \frac{Q^2}{\sqrt{N}}\right)N^\varepsilon,$$

where the implied constant in (4.2) depends on ε alone.

Proof. The task before us is as follows. Let $x = a/q^2$ and $x' = a_1/q_1^2$, with $\gcd(a,q) = \gcd(a_1,q_1) = 1$. Let $aq_1^2 - a_1q^2 \equiv b \pmod{q^2 q_1^2}$ with $|b| \le \frac{1}{2}q^2 q_1^2$. We have

$$(4.3) \qquad 0 \le \left\| \frac{a}{q^2} - \frac{a_1}{q_1^2} \right\| = \frac{|b|}{q^2 q_1^2} < \frac{1}{2N}.$$

This yields $|b| \ll q^2 Q^2 N^{-1} = B$, say. We want to estimate, for each a/q^2, the number of fractions $a_1/q_1^2 \in S_Q$ satisfying (4.3). Let $b = aq_1^2 - a_1q^2$. We have $|b| < B$ and

$$(4.4) \qquad q^2 \equiv -b\bar{a}_1 \pmod{q_1^2}, \qquad b \equiv aq_1^2 \pmod{q^2},$$

where $\bar{a}_1$ is the multiplicative inverse of a_1 modulo q_1^2.

We shall estimate the number of b's and q_1's that satisfy the second congruence relation in (4.4) with $q_1 < Q$ and $|b| < B$, which clearly majorizes the maximum that we need to estimate in (4.1).

First, we set $\phi(x) = \left(\frac{\sin \pi x}{2x}\right)^2$, a constant multiple of the Féjer kernel. We note that $\phi(x)$ is non-negative, $\phi(x) \ge 1$ for $|x| \le 1/2$ and $\phi(0) = \pi^2/4$. Therefore

$$(4.5) \qquad \sum_{n \equiv aq_1^2 \bmod q^2} \phi\left(\frac{n}{2B}\right)$$

majorizes $M(Q)$. There is certainly no unique choice for this test function $\phi(x)$. However, as we shall presently apply the Poisson summation formula, we find it most convenient to choose $\phi(x)$ this way, since its Fourier transform has compact support, specifically $\widehat{\phi}(s) = (\pi^2/4)\max(1 - |s|, 0)$.

Now we apply Poisson summation (Lemma 2) with a linear change of variable, to (4.5) and sum q_1 over dyadic intervals. We get

$$(4.6) \qquad \frac{2B}{q^2} \sum_{Q < q_1 \leq 2Q} \sum_j e\left(\frac{ajq_1^2}{q^2}\right) \widehat{\phi}\left(\frac{2jB}{q^2}\right).$$

More precisely, the above is

$$\frac{\pi^2 B}{2q^2} \sum_{|j| < q^2/(2B)} \sum_{Q < q_1 \leq 2Q} \left(1 - \frac{2|j|B}{q^2}\right) e\left(\frac{ajq_1^2}{q^2}\right)$$

$$= \frac{\pi^2 Q^2}{2N} \sum_{|j| < N/(4Q^2)} \sum_{Q < q_1 \leq 2Q} \left(1 - \frac{4|j|Q^2}{N}\right) e\left(\frac{ajq_1^2}{q^2}\right)$$

$$\leq \frac{\pi^2 Q^3}{2N} + \frac{\pi^2 Q^2}{N} \sum_{0 < j < N/(4Q^2)} \left|\sum_{Q < q_1 \leq 2Q} e\left(\frac{ajq_1^2}{q^2}\right)\right|,$$

where the first term above corresponds to the contribution of $j = 0$. Applying the Cauchy–Schwarz inequality, we see that the square of the above expression is bounded by

$$\ll \frac{Q^6}{N^2} + \frac{Q^2}{N} \sum_{0 < j < N/(4Q^2)} \left|\sum_{Q < q_1 \leq 2Q} e\left(\frac{ajq_1^2}{q^2}\right)\right|^2.$$

Applying Weyl shift (Lemma 3) to the innermost sum of the second term, we see that the double sum of the second term is

$$\ll \sum_j Q + \sum_j \sum_{0 < l < Q} \min\left\{Q, \left\|\frac{2ajl}{q^2}\right\|^{-1}\right\}$$

$$\ll \frac{N}{Q} + \sum_{0 < m < NQ^{-1}} \tau(m) \min\left\{Q, \left\|\frac{am}{q^2}\right\|^{-1}\right\},$$

where $\tau(m)$, the divisor function, is $O(m^\varepsilon)$ and estimates the multiplicity of representations of $m = 2jl$. The inequalities go in the correct direction by positivity.

What still remains is to estimate the sum over m. We have, with $am \equiv d$ $(\mathrm{mod}\, q^2)$ and $|d| \leq q^2/2$,

$$\sum_m \leq \sum_{|d| < q^2} \min\left\{Q, \frac{q^2}{|d|}\right\} \sum_{0 < m < NQ^{-1}} \tau(m)$$

$$\ll q^{-2} N^{1+\varepsilon} + \sum_{0 < d < q^2} \frac{q^2}{d}\left(q^{-2}\frac{N}{Q} + 1\right)\left(\frac{N}{Q}\right)^\varepsilon$$

$$\ll q^{-2} N^{1+\varepsilon} + \left(\frac{N}{Q} + q^2\right) N^\varepsilon \ll \left(\frac{N}{Q} + Q^2\right) N^\varepsilon.$$

Recall that we are only considering the q's in the dyadic interval $Q < q \leq 2Q$. Combining everything and taking the square root, we infer that for every $x \in S_Q$,

$$\#\left\{x' \in S_Q : \|x - x'\| < \frac{1}{2N}\right\} \ll \frac{Q^3}{N} + \left(\sqrt{Q} + \frac{Q^2}{\sqrt{N}}\right)N^\varepsilon,$$

from which we infer the lemma. ■

Now we are able to state and prove our main result. The beginning of the proof will go very much like that of the classical large sieve inequalities. As far as that part is concerned, we are following the proof given in [7].

THEOREM 2. *With $\{a_n\}$, Q, M, and N defined as before, we have*

$$(4.7) \quad \sum_{\substack{q=1}}^{Q} \sum_{\substack{a \bmod q^2 \\ \gcd(a,q)=1}} \left|\sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^2}n\right)\right|^2$$

$$\ll \log 2Q[Q^3 + (N\sqrt{Q} + \sqrt{N}Q^2)N^\varepsilon]\sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant depends on ε alone.

Proof. It is easily observed that after breaking the summation over q into dyadic intervals with $Q < q \leq 2Q$ and applying the duality principle (Lemma 1), and by assuming $M = 0$ via the shift $n \mapsto n - M$, it suffices to show that

$$(4.8) \quad \sum_{0 < n \leq N} \left|\sum_{x \in S_Q} b_x e(xn)\right|^2 \ll [Q^3 + (N\sqrt{Q} + \sqrt{N}Q^2)N^\varepsilon]\sum_{x \in S_Q} |b_x|^2,$$

for any sequence of complex numbers $\{b_x\}$.

As before, we take $\phi(x) = \left(\frac{\sin \pi x}{2x}\right)^2$. By positivity, the left-hand side of (4.8) is majorized by

$$\sum_{n=-\infty}^{\infty} \phi\left(\frac{n}{2N}\right)\left|\sum_{x \in S_Q} b_x e(nx)\right|^2 = \sum_x \sum_{x'} b_x \overline{b}_{x'} V(x - x'),$$

where $V(y) = \sum_n \phi\left(\frac{n}{2N}\right)e(ny)$. Apply the Poisson summation formula and a change of variables to obtain

$$V(y) = 2N \sum_m \widehat{\phi}\,[2N(m + y)]$$

$$= \frac{\pi^2 N}{2} \sum_{|m+y| < (2N)^{-1}} (1 - 2N|m + y|) = \frac{\pi^2 N}{2}(1 - 2N\|y\|).$$

if $\|y\| < (2N)^{-1}$ and $V(y) = 0$ otherwise. Hence the left-hand side of (4.8) is majorized by

$$\frac{\pi^2 N}{2} \sum_{\substack{x \quad x' \\ \|x-x'\|<(2N)^{-1}}} |b_x b_{x'}| \leq \frac{\pi^2 N}{2} \sum_x |b_x|^2 M(Q, N),$$

where $M(Q, N)$ is as defined in Lemma 4. We insert the result of the afore-mentioned lemma, and the theorem is proved. ∎

The greatest strength of our result lies in the range where $N \asymp Q^3$. There, our result gives the majorant of $O(Q^{7/2+\varepsilon})$ while both (2.2) and (2.3) give the majorant of $O(Q^4)$.

In the same spirit that the classical large sieve inequality for additive characters implies one for multiplicative characters, we have the following easy corollary.

COROLLARY 1. *For any sequence of complex numbers $\{a_n\}$, we have*

$$(4.9) \quad \sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi \bmod q^2} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2$$

$$\ll \log 2Q [Q^3 + (N\sqrt{Q} + \sqrt{N}Q^2)N^\varepsilon] \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant depends on ε alone.

Proof. Using the Gauss sums $G(\chi)$, we have

$$\chi(n) = \frac{1}{G(\overline{\chi})} \sum_{a \bmod q^2} \overline{\chi}(a) e\left(\frac{an}{q^2}\right).$$

It is an elementary fact that the modulus of the Gauss sum $G(\chi)$ is the square root of its modulus, q in our case. Hence

$$\sideset{}{^*}\sum_{\chi \bmod q^2} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \leq \frac{1}{q^2} \sum_{\chi \bmod q^2} \left| \sum_{a \bmod q^2} \overline{\chi}(a) \sum_n a_n e\left(\frac{an}{q^2}\right) \right|^2$$

$$= \frac{\varphi(q)}{q} \sum_{\substack{a \bmod q^2 \\ \gcd(a,q)=1}} \left| \sum_n a_n e\left(\frac{an}{q^2}\right) \right|^2.$$

The last equality is obtained by opening the squared modulus and applying the orthogonality of Dirichlet characters. Note also that $\varphi(q^2) = q\varphi(q)$. The corollary now follows from Theorem 2. ∎

We do not believe (4.7) is the best possible result. In fact, in Section 6 we shall make stronger conjectures based on computational evidence.

5. Higher power moduli. We mentioned that our method of the previous section may be generalized to investigate large sieve inequalities with higher power moduli. We substantiate that comment below. "Since brevity is the soul of wit and tediousness the limbs and outward flourishes, I will be brief." ([11, *Hamlet*, II, ii, 91–93]). Therefore we shall not provide all details of the proof as the proof goes *à la* previous section. First we write down a lemma concerning the spacing of special fractions.

First set

$$S_{Q,k} = \{a/q^k \in \mathbb{Q} : \gcd(a,q) = 1,\ 1 \le a < q^k,\ Q < q \le 2Q\},$$

$$M_k(Q, N) = \max_{x' \in S_{Q,k}} \# \left\{ x \in S_{Q,k} : \|x - x'\| < \frac{1}{2N} \right\}.$$

We have the following lemma.

LEMMA 5. *Given* $\varepsilon > 0$, $N \in \mathbb{N}$ *and setting* $\kappa = 2^{k-1}$, *we have*

$$(5.1) \qquad M_k(Q, N) \ll \frac{Q^{k+1}}{N} + \left(Q^{(\kappa-1)/\kappa} + \frac{Q^{(\kappa+k)/\kappa}}{N^{1/\kappa}} \right) N^\varepsilon,$$

where the implied constant in (5.1) *depends on* ε *and* k.

From the above lemma, we have the following theorem.

THEOREM 3. *Let* $\{a_n\}$ *be an arbitrary sequence of complex numbers*, Q, M, N *positive integers, and* $k \ge 2$. *Set* $\kappa = 2^{k-1}$. *Then*

$$(5.2) \quad \sum_{q=1}^{Q} \sum_{\substack{a \bmod q^k \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^k} n \right) \right|^2$$

$$\ll \log 2Q [Q^{k+1} + N^\varepsilon (NQ^{(\kappa-1)/\kappa} + N^{1-1/\kappa} Q^{(\kappa+k)/\kappa})] \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant will depend on k *and* ε.

Of course, in the same spirit as Corollary 1, Theorem 3 also admits the following corollary for multiplicative characters.

COROLLARY 2. *With the same notation as before, we have*

$$(5.3) \quad \sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\chi \bmod q^k}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2$$

$$\ll \log 2Q [Q^{k+1} + N^\varepsilon (NQ^{(\kappa-1)/\kappa} + N^{1-1/\kappa} Q^{(\kappa+k)/\kappa})] \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant depends on ε *and* k.

As an application of the classical large sieve inequality, we can take

$$(5.4) \qquad \Delta = Q^{2k} + N,$$

as all fractions with k-power denominator not greater than Q^k will be Q^{-2k}-spaced modulo 1. Alternatively, as before, since fractions with height exactly q^k between 0 and 1, for $1 \leq q \leq Q$, are q^{-k}-spaced, we may take

$$(5.5) \qquad \Delta = Q(Q^k + N).$$

It is clear that the virtue of (5.4), for large k's, is limited when compared with (5.5).

As before, our result is most useful when $N \asymp Q^{k+1}$. In this case, (5.5) gives $\Delta = O(Q^{k+2})$, and (5.4) gives the extremely poor $\Delta = O(Q^{2k})$, while our result gives $\Delta = O(Q^{k+1+(\kappa-1)/\kappa})$, where κ is defined as before.

6. Conjectures based on heuristics and empirical evidence. If we take $N = Q^3$ in Lemma 4, we have

$$(6.1) \qquad M(Q) := \max_{x' \in S_Q} \#\{x \in S_Q : 2\|x - x'\| < Q^{-3}\} \ll Q^{1/2+\varepsilon},$$

and the implied constant in (6.1) depends on ε alone. With this, we can arrive at something slightly different.

PROPOSITION 1. *With $\{a_n\}$, Q, M, and N defined as before, we have*

$$(6.2) \qquad \sum_{q=1}^{Q} \sum_{\substack{a \bmod q^2 \\ \gcd(a,q)=1}} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^2} n\right) \right|^2 \ll Q^{1/2+\varepsilon}(Q^3 + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant depends on ε alone.

Proof. The proposition follows easily from Theorem 2 together with the observation that $Q^2 \sqrt{N} \leq \max\{Q^{7/2}, \sqrt{Q}N\}$. However, if one follows a different line of proof and partitions the interval $(0, 1]$ into $2Q^3$ subintervals of equal size, say K_i, $i = 1, \ldots, 2Q^3$, then $\#\{K_i \cap S_Q\} = O(Q^{1/2+\varepsilon})$ for all i, by (6.1). Picking one element from $K_i \cap S_Q$ for each even and then odd i would ensure the well-spacedness of the resulting set, and such a "picking" process terminates after $O(Q^{1/2+\varepsilon})$ times. Thus, one can also infer the result of the proposition; the factor of $Q^{1/2+\varepsilon}$ in (6.2) comes from that in (6.1). ∎

The above gives the significance of the majorant (6.1) which will facilitate our conjecture making. Table 1 below lists some values of $M(Q)$ for some small values of Q, where $M(Q)$ is as in (6.1). We see that $M(Q)$ increases rather slowly and it is our belief that $M(Q) = O(Q^\varepsilon)$ with the implied constant depending on ε alone. Indeed, there are about Q^3 elements in S_Q, and "on average," they are Q^{-3}-spaced. Hence, there should be not many

Table 1. $M(Q)$ for some small Q's

Q	$M(Q)$	Q	$M(Q)$	Q	$M(Q)$	Q	$M(Q)$	Q	$M(Q)$
1	0	2	0	3	1	4	1	5	2
6	1	7	1	8	2	9	2	10	2
11	2	12	2	13	2	14	2	15	2
16	2	17	2	18	2	19	2	20	2
21	2	22	2	23	2	24	3	25	2
26	2	27	3	28	2	29	2	30	2
31	2	32	2	33	2	34	2	35	2
36	2	37	3	38	3	39	3	40	3
41	3	42	3	43	3	44	3	45	2
46	3	47	3	48	3	49	3	50	3
51	3	52	3	53	4	54	3	55	3
56	3	57	3	58	3	59	3	60	3
61	3	62	3	63	3	64	3	65	3
66	3	67	3	68	3	69	3	70	3
71	3	72	3	73	3	74	3	75	3
76	3	77	3	78	3	79	3	80	3
81	3	82	3	83	4	84	4	85	3
86	3	87	3	88	3	89	4	90	4
91	4	92	4	93	4	94	3	95	3
96	3	97	4	98	4	99	4	100	4

pairs of elements in S_Q that are spaced too closely. The readers should allow my making the following analogy. If we are using a sieve with Q^3 holes of equal size in it and sift out the elements of S_Q with it, then "not many" rational numbers should fall through the same hole. This is precisely the meaning of the conjectures in this section.

We believe the growth of $M(Q)$, as defined in (6.1), is of independent interest. Therefore, we record the following conjectures.

CONJECTURE 1. *Let S_Q be defined as before. Then*

$$(6.3) \qquad \max_{x \in S_Q} \#\{x' \in S_Q : \|x - x'\| < Q^{-3}\} \ll Q^\varepsilon,$$

where the implied constant depends on ε alone.

In the same spirit, we also express, but with less confidence, the following conjecture for higher power moduli.

CONJECTURE 2. *Let*

$$S_{k,Q} = \{a/q^k \in \mathbb{Q} : \gcd(a, q) = 1,\ 1 \le a < q^k,\ Q < q \le 2Q\}.$$

Then

$$(6.4) \qquad \max_{x \in S_{k,Q}} \#\{x' \in S_{k,Q} : \|x - x'\| < Q^{-k-1}\} \ll Q^\varepsilon,$$

where the implied constant depends only on k and ε.

If we assume the truth of Conjecture 2, then we would have

CONJECTURE 3. *Let $\{a_n\}$ be an arbitrary sequence of complex numbers, and Q, $N \in \mathbb{N}$ and $M \in \mathbb{Z}$. Then*

$$(6.5) \quad \sum_{q=1}^{Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q^k} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{a}{q^k}\, n \right) \right|^2 \ll Q^\varepsilon (Q^{k+1} + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

where the implied constant depends only on ε and k.

References

[1]   E. Bombieri and H. Davenport, *Some inequalities involving trigonometrical polynomials*, Ann. Scuola Norm. Sup. Pisa 23 (1969), 223–241.

[2]   D. Bump, *Automorphic Forms and Representations*, Cambridge Stud. Adv. Math. 55, Cambridge Univ. Press, Cambridge, 1996.

[3]   H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, Berlin, 2000.

[4]   H. Davenport and H. Halberstam, *The values of a trigonometrical polynomial at well spaced points*, Mathematika 13 (1966), 91–96.

[5]   —, —, *Corrigendum and addendum*, ibid. 14 (1967), 229–232.

[6]   P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14–20.

[7]   H. Iwaniec, *Introduction to the Prime Number Theory*, in: Lecture notes from a course on Special Topics of Number Theory, Rutgers University, 1994 (unpublished).

[8]   Yu. V. Linnik, *The large sieve*, Dokl. Akad. Nauk SSSR 36 (1941), 119–120 (in Russian).

[9]   H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, Berlin, 1971.

[10]   —, *The analytic principles of large sieve*, Bull. Amer. Math. Soc. 84 (1978), 547–567.

[11]   W. Shakespeare, *The Norton Shakespeare*, W. W. Norton & Co., New York, 1997.

[12]   E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, 2nd ed., Clarendon Press, Oxford, 1986.

Department of Mathematics
Hill Center, Busch Campus
Rutgers University
110 Frelinghuysen Road
Piscataway, NJ 08854-8019, U.S.A.
E-mail: lzhao@math.rutgers.edu