LARGE SIEVE INEQUALITIES FOR SPECIAL CHARACTERS TO PRIME SQUARE MODULI

LIANGYI ZHAO

Abstract: In this paper, we develop a large sieve type inequality for some special characters whose moduli are squares of primes. Our result gives a non-trivial estimate in certain ranges.
Keywords: large sieve inequality.

1. Introduction and historical background

It was in 1941 that Yuri Vladimirovich Linnik [8] originated the idea of large sieve. It is as follows. 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 $j \neq k$.

The large sieve inequality, which we henceforth refer to as the classical large sieve inequality, is stated as follows. Different elegant proofs of the theorem can be found in [1], [4], [10], [9]. The theorem, in the following form, was first introduced by Davenport and Halberstam, [2] and [3].

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 $M \in \mathbb{Z}$, $N \in \mathbb{N}$. Then we have*

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

where the implied constant is absolute.

Save for the more precise implied constant, the above inequality is the best possible. This theorem admits corollaries for multiplicative characters. We derive

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\chi \bmod q}^{\star} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2, \qquad (1.1)$$

where here and later, $\sum^*$ means that the sum runs over primitive characters modulo the specified modulus only. Note that the sum is over only the primitive characters is a vital feature of the theorem.

Also, large sieve type inequalities for the complete set of characters to square, and higher power, moduli were investigated by L. Zhao in [12].

In this paper, we aim to have a result of the following kind.

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sideset{}{'}\sum_{\chi \bmod q^2} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll \Delta \sum_{n=M+1}^{M+N} |a_n|^2, \tag{1.2}$$

where the $\sum'$ runs over some special Dirichlet characters, to be specified in the next section, and as usual Δ will be in terms of Q and N.

In all of our investigations of this paper, we shall restrict our attention to prime square moduli only. The result can be generalized, but restricting the prime square moduli gives us great convenience in estimates; that is, two prime squares are not co-prime if and only if they are the same.

The idea of studying character sums to prime-power moduli was started in a paper by A. G. Postnikov [11]. He gave formulas on the decomposition of groups of characters of powerful moduli. P. X. Gallagher [5] also studied characters of this type. Iwaniec [6] expanded the Postnikov-Gallagher idea to composite moduli.

The author also thanks his thesis adviser, Henryk Iwaniec, who first suggested this problem and who, of his advise and support, has been most generous.

2. Heuristics

First we note that there are $\varphi(q^2) = q\varphi(q)$ Dirichlet characters modulo q^2 which is the same as the order of the group $G = (\mathbb{Z}/q^2\mathbb{Z})^*$. The group G contains the following subgroup $H = \{x \in G \mid x \equiv 1 (\bmod q)\}$, which is isomorphic to the additive group $\mathbb{Z}/q\mathbb{Z}$. The isomorphism is given by

$$H \longrightarrow \mathbb{Z}/q\mathbb{Z} : x \longrightarrow \frac{x-1}{q}.$$

Any Dirichlet character ξ on G induces an additive character on H. So we have, for any $x \in H$,

$$\xi(x) = e\left[\frac{a(x-1)}{q^2}\right], \tag{2.1}$$

for some $a(\bmod q)$. If $\xi'(\bmod q^2)$ is another character satisfying (2.1) with the same $a(\bmod q)$. Then $\xi'\xi^{-1}$ is a character on G that is trivial on H. Therefore, $\xi' = \xi\chi$ where χ is induced by a character on $(\mathbb{Z}/q\mathbb{Z})^*$. Let G_a be the set of characters

$\xi(\mathrm{mod}\,q^2)$ satisfying (2.1). G_a has $\varphi(q)$ elements, and that every element of G_a is obtained in a unique way by multiplying a fixed character $\xi \in G_a$ by a character χ on $(\mathbb{Z}/q\mathbb{Z})^*$.

Therefore, the context in which we shall consider the sum in the left-hand side of (1.2) is with $a = 1$ in (2.1); namely, we shall study the following sum

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \in G_1} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 .$$

The more general case in which one considers characters in G_a is similar to the investigation for G_1. Also, we note that the characters being summed are not necessarily primitive, a feature that the classical large sieve inequality, (1.1), does not possess.

Next, we observe the following.

$$\frac{q}{\varphi(q)} \sum_{\xi \in G_1} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = \frac{q}{\varphi(q)} \sum_{n} \sum_{n'} \bar{a}_n a_{n'} \xi(\bar{n}n') \sum_{\chi} \chi(\bar{n}n'),$$

where ξ is a fixed character in G_1 and χ runs over Dirichlet characters of $(\mathbb{Z}/q\mathbb{Z})^*$. The inner-most sum vanishes unless $n \equiv n'(\mathrm{mod}\,q)$, in which case it yields $\varphi(q)$ and

$$\xi(\bar{n}n') = e\left(\frac{\bar{n}n' - 1}{q} \right) = e\left(\frac{\bar{n}}{q} \frac{n' - n}{q} \right)$$

by (2.1). Note that $\frac{n'-n}{q}$ is an integer. Hence, we have

$$\frac{q}{\varphi(q)} \sum_{\xi \,\mathrm{mod}\, q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = q \sum_{\substack{n \\ n \equiv n' \,\mathrm{mod}\, q}} \sum_{n'} \bar{a}_n a_{n'} e\left(\frac{\bar{n}}{q} \frac{n' - n}{q} \right), \qquad (2.2)$$

where henceforth $\sum^{(1)}$ denotes sum over characters $\xi \in G_1$. Trivially estimating the contribution of the above sum gives

$$\frac{q}{\varphi(q)} \sum_{\xi \,\mathrm{mod}\, q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = [q + O(N)] \sum_{\gcd(n,q)=1} |a_n|^2. \qquad (2.3)$$

Estimating thus gives that

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \,\mathrm{mod}\, q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 \ll (Q^2 + QN) \sum_{n} |a_n|^2. \qquad (2.4)$$

Although (2.3) is obtained trivially, it is an asymptotic formula rather than simply an upper bound, a main feature of the classical large sieve inequalities. The inequality (2.4) is of interest when $N \ll Q$. Moreover, in the light of (2.3), we see that any improvement upon the exponent of Q is not possible and any improvement upon this trivial bound has to come from that on N. Toward that end, we shall use the results in the following section.

3. Preliminaries Lemmas

First, we shall need the estimate for Kloosterman sums.

Theorem 2. [Weil] *For any* $c \in \mathbb{N}$, m *and* n, *we have*

$$\left| \sum_{ad \equiv 1 \bmod c} e\left(\frac{ma + nd}{c}\right) \right| \leqslant [\gcd(m, n, c)]^{\frac{1}{2}} c^{\frac{1}{2}} \tau(c),$$

where $\tau(c)$ *is the divisor function.*

Proof. This is quoted from [7] and is deduced from the celebrated Riemann hypothesis for curves over finite fields proved by A. Weil in 1948.   ∎

Next we shall also need the following estimate for Ramanujan's Sums.

Lemma 1. *For any* $n, q \in \mathbb{N}$, *we have*

$$\left| \sum_{\substack{a(\bmod q) \\ \gcd(a,q)=1}} e\left(\frac{an}{q}\right) \right| \leqslant \gcd(n, q). \tag{3.1}$$

Proof. This estimate is easy, standard, and best possible.   ∎

4. Main Result

We now state and prove the theorem of this paper. Throughout, q runs over prime numbers only.

Theorem 3. *Suppose* $Q, N \in \mathbb{N}$, $M \in \mathbb{Z}$ *and* $\{a_n\}$ *be a sequence of complex numbers. We have*

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \bmod q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2$$
$$\ll Q^\epsilon \left(NQ^{\frac{1}{2}} + N^{\frac{1}{4}} Q^2 + N^{\frac{3}{4}} Q^{\frac{11}{8}} \right) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{4.1}$$

with any $\epsilon > 0$, *and the implied constant depends on* ϵ *alone.*

Proof. For the proof, it suffices to consider $q \in (Q/2, Q]$. The size of the sum resulted from breaking the left-hand side of (4.1) into dyadic intervals is majorized by $QT(N,Q)$, with

$$T(N,Q) = \sum_{Q/2 < q \leqslant Q} \frac{1}{\varphi(q)} \sum_{\xi \bmod q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 .$$

From (2.2), we have

$$T(N,Q) = \sum_q \sum_n \sum_{\substack{n' \\ n \equiv n' \bmod q}} \bar{a}_n a_{n'} e\left(\frac{\overline{n'}(nn'-1)}{q^2} \right)$$

$$= \sum_n \sum_{n'} \sum_{q | (n-n')} \bar{a}_n a_{n'} e\left(\frac{\overline{n'}(nn'-1)}{q^2} \right)$$

$$= \sum_{|l| \leqslant 2N/Q} \sum_{\substack{q \\ ql = n - n'}} \sum_n \sum_{n'} \bar{a}_n a_{n'} e\left(\frac{\overline{n}l}{q} \right) .$$

We get, by applying Cauchy's inequality,

$$T^2(N,Q) \leqslant \left(\sum_{n'} |a_{n'}|^2 \right) \sum_{n'} \left| \sum_{n-n'=lq} \sum \sum a_n e\left(\frac{\overline{n}l}{q} \right) \right|^2$$

$$= \left(\sum_{n'} |a_{n'}|^2 \right) \sum \sum \sum \sum \sum \sum_{n_1 - n_2 = l_1 q_1 - l_2 q_2} a_{n_1} \bar{a}_{n_2} e\left(\frac{\overline{n_1} l_1}{q_1} - \frac{\overline{n_2} l}{q_2} \right) .$$

From the above, we get that

$$T^2(N,Q) \leqslant$$

$$\leqslant \left(\sum_n |a_n|^2 \right) \sum_{n_1} \sum_{n_2} |a_{n_1} a_{n_2}| \sum_{q_1} \left| \sum_{\substack{l_1 q_1 - l_2 q_2 = n_1 - n_2}} \sum \sum e\left(\frac{\overline{(n_2 - l_2 q_2)} l_1}{q_1} - \frac{\overline{n_2} l_2}{q_2} \right) \right| .$$

Here, we apply once again, the Cauchy-Schwartz inequality, getting

$$T^4(N,Q) \leqslant \left(\sum_n |a_n|^2 \right)^4 Q \sum_{n_1} \sum_{n_2} \sum_q \left| \sum_{\substack{l_1 q_1 - l_2 q_2 = n_1 - n_2}} \sum_{q_1} \sum_{l_1} \sum_l e\left(\frac{\overline{(n_1 - lq)} l}{q_1} - \frac{\overline{n_2} l}{q} \right) \right|^2 .$$

Opening the square modulus, we get

$$T^4(N,Q) \leqslant \left(\sum_n |a_n|^2 \right)^4 Q \sum_q \sum_{q_1} \sum_{q_2} \sum_{l_1} \sum_{l_2} \sum_{l'} \sum_{l''} \left\{ \sum_n \right\} , \qquad (4.2)$$
$$l_1 q_1 - l_2 q_2 = q(l' - l'')$$

where the inner-most sum is

$$\sum_n e\left[\frac{\overline{(n-l'q)}l_1}{q_1} - \frac{\overline{n}l'}{q} - \frac{\overline{(n-l''q)}l_2}{q_2} + \frac{\overline{n}l''}{q}\right],$$

which is an incomplete Kloosterman type sum and may be completed by Fourier techniques.

It suffices to estimate a sum of the following form

$$\sum_{N\leqslant n\leqslant N_1} e\left[\frac{\overline{(n-l'q)}l_1}{q_1} - \frac{\overline{n}l'}{q} - \frac{\overline{(n-l''q)}l_2}{q_2} + \frac{\overline{n}l''}{q}\right], \tag{4.3}$$

where $N < N_1 \leqslant 2N$. Our sum may be written as

$$\frac{1}{q_1q_2q} \sum_{a \bmod q_1q_2q} \sum_n e\left(\frac{an}{q_1q_2q}\right) \sum_{x \bmod q_1q_2q} e\left[f(x) - \frac{ax}{q_1q_2q}\right], \tag{4.4}$$

where $f(x)$ is the amplitude in (4.3) and the range of summation for n is the same as in (4.3). The main contribution will come from the part where $a \equiv 0 (\bmod q_1 q_2 q)$. That part in (4.3) is the following

$$\frac{N}{q_1q_2q} \sum_{x \bmod q_1q_2q} e\left[f(x)\right]. \tag{4.5}$$

The other parts are

$$\ll \sum_{0<|a|\leqslant q_1q_2q/2} \left|\frac{1}{a} \sum_{x \bmod q_1q_2q} e\left[f(x) - \frac{ax}{q_1q_2q}\right]\right| \tag{4.6}$$

where we have applied the bound for the geometric series over n. The sum in (4.5) is a Ramanujan type sum while the one in (4.6) may be estimated via Weil's bound for Kloosterman sums, given by Theorem 2.

Making the change of variable from x into $x + l''q$, the inner-most sum of (4.6) becomes

$$e\left(\frac{al''}{qq_1q_2}\right) \sum_{x \bmod q_1q_2q} e\left[\left(\frac{\overline{(x+lq)}l_1}{q_1} - \frac{\overline{x}l_2}{q_2} + \frac{\overline{x}l}{q}\right) - \frac{ax}{q_1q_2q}\right],$$

where $l = l'' - l'$. The above is a complete Kloosterman sum of modulus qq_1q_2.

Hence we apply Weil's bound for Kloosterman sums and the above is $\ll \gcd(a, q_1 q_2 q)^{\frac{1}{2}} Q^{\frac{3}{2}}$. Recall that we are assuming that q_1, q_2 and q are primes. Summing over a, we get that the sum in (4.6) is $\ll Q^{\frac{3}{2}+\epsilon}$.

It still remains to estimate the sum in (4.5). The sum simplifies to

$$\sum_{x \bmod q_1 q_2 q} e\left[\overline{\frac{(x+lq)l_1}{q_1}} - \frac{\overline{x}l_2}{q_2} + \frac{\overline{x}l}{q}\right]. \tag{4.7}$$

If q_1, q_2 and q_3 are pair-wise co-prime, that is distinct, we write

$$x = x_1 \overline{q_2 q} q_2 q + x_2 \overline{q_1 q} q_1 q + y \overline{q_1 q_2} q_1 q_2,$$

where $x_1(\bmod q_1)$, $x_2(\bmod q_2)$ and $y(\bmod q)$. The sum of our interest in (4.7) factors into the product of three Ramanujan type sums

$$R\left(\frac{l_1}{q_1}\right) R\left(\frac{l_2}{q_2}\right) R\left(\frac{l}{q}\right),$$

where

$$R\left(\frac{l}{q}\right) = \sum_{\substack{n(\bmod q) \\ \gcd(n,q)=1}} e\left(\frac{nl}{q}\right), \text{ and } \left|R\left(\frac{l}{q}\right)\right| \leqslant \gcd(l, q)$$

by the virtue of (3.1) and we also note the following almost trivial estimate.

$$\sum_{d \bmod q} \gcd(d, q) \leqslant \sum_{l|q} \frac{q}{l} l = q\tau(q) \ll q^{1+\epsilon}.$$

Hence, summing over all relevant variables, we have the contribution of (4.5) to the majorant of $T^4(N, Q)$ is

$$QN \left(\frac{N}{Q} + Q\right)^3 \left(\sum_n |a_n|^2\right)^4.$$

If some of the q's are not pair-wise distinct, then the estimate will essentially go the same way as before, but the contribution to the majorant will be different. If two of the q's are the same, then the contribution of the majorant is

$$Q^\epsilon \left(N^4 Q^{-2} + N^2 Q^2\right) \left(\sum_n |a_n|^2\right)^4,$$

and similarly if all q's are the same, the contribution is

$$Q^\epsilon \left(N^4 Q^{-2} + N^3\right) \left(\sum_n |a_n|^2\right)^4.$$

Combining everything, the left-hand side of (4.1) is

$$\ll Q^\epsilon \left(NQ^{\frac{1}{2}} + N^{\frac{1}{4}} Q^2 + N^{\frac{1}{2}} Q^{\frac{3}{2}} + N^{\frac{3}{4}} Q^{\frac{11}{8}}\right) \sum_n |a_n|^2. \tag{4.8}$$

The last term in the majorant of (4.8) comes from the contribution of (4.6). The third term in (4.8) is not needed, as if $N^{\frac{1}{2}} Q^{\frac{3}{2}} \gg N^{\frac{1}{4}} Q^2$, then $N^{\frac{1}{4}} \gg Q^{\frac{1}{2}}$. In that case, $N^{\frac{3}{4}} Q^{\frac{11}{8}} \gg N^{\frac{3}{4}} Q \gg N^{\frac{1}{2}} Q^{\frac{3}{2}}$. Our result follows. ∎

5. Notes

The asymptotic formula of (2.3) is useful when $N \ll Q$. Theorem 3 is better than (2.3) when $Q^{\frac{3}{2}+\epsilon} \ll N$. We would certainly hope to have a result that is useful whenever (2.3) does not hold, namely whenever $Q \ll N$. However, since we already have to resort to the strength of Weil's bound for our present result, any desire for improvement is perhaps too greedy.

References

[1] H. Davenport, *Multiplicative Number Theory*, Third Edition, Graduate Texts in Mathematics, Springer-Verlag, Berlin, etc., 2000.

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

[3] H. Davenport and H. Halberstam, *Corrigendum and addendum*, Mathematika **14** (1967), 229–232.

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

[5] P.X. Gallagher, *Primes in progressions to prime-power modulus*, Inventiones Mathematicae **16** (1972), 191–201.

[6] H. Iwaniec, *On zeros of Dirichlet's L series*, Inventiones Mathematicae **23** (1974), 97–104.

[7] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, vol. 17, American Mathematical Society, Providence, 1997.

[8] J.V. Linnik, *The large sieve*, Doklady Akademii Nauk Soiuza Sovetskikh Sotsialisticheskikh Respublik, **36** (1941), 119–120 (Russian).

[9] H.L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics, Spring-Verlag, Berlin, etc., 1971.

[10] H.L. Montgomery, *The Analytic Priciples of Large Sieve*, Bulletin of the American Mathematical Society **84** (July 1978), 547–567.

[11] A.G. Postnikov, *On the sum of the characters for a prime power modulus*, Izvestiya Akademii Nauk. Soiuza Sovetskikh Sotsialisticheskikh Respublik, Seriya Matematicheskaya, **19** (1955), 11–16, (Russian).

[12] L. Zhao, *Large sieve inequalities with characters for square moduli*, Accepted for publication and to appear in Acta Arithmetica (2002).

Address: Dept. Math., U.S. Military Academy, West Point, NY 10996
E-mail: al1526@usma.edu