#A20 INTEGERS 15 (2015)

THE SMOOTHED PÓLYA–VINOGRADOV INEQUALITY

Kamil Adamczewski
Department of Mathematics, Dartmouth College, Hanover, New Hampshire
kamil.m.adamczewski@gmail.com

Enrique Treviño
Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, Illinois
trevino@mx.lakeforest.edu

Received: 1/31/12, Revised: 10/18/14, Accepted: 4/28/15, Published: 5/8/15

Abstract

Let χ be a primitive Dirichlet character to the modulus q. Let $S_\chi(M,N) = \sum_{M<n\leq N} \chi(n)$. The Pólya-Vinogradov inequality states that $|S_\chi(M,N)| \ll \sqrt{q}\log q$. The smoothed Pólya–Vinogradov inequality, recently introduced by Levin, Pomerance and Soundararajan, is a numerically useful version of the Pólya–Vinogradov inequality that saves a $\log q$ factor. The smoothed Pólya–Vinogradov inequality has been used to settle a conjecture of Brizolis, namely that for every prime $p > 3$, there is a primitive root g and an integer $x \in [1, p-1]$ such that $g^x \equiv x \bmod p$. It has also been used to improve the best known numerically explicit upper bound on the least inert prime in a real quadratic field. In this paper we will prove a smoothed Pólya–Vinogradov inequality which takes into account the arithmetic properties of the modulus and we extend the inequality to imprimitive characters. We also find a lower bound for the inequality.

1. Introduction

Let χ be a non-principal Dirichlet character to the modulus q. It has been the interest of mathematicians to study the sum $\left|\sum_{n=M+1}^{M+N} \chi(n)\right|$. Pólya and Vinogradov independently proved in 1918 that the sum is bounded above by $O(\sqrt{q}\log q)$. Assuming the Riemann Hypothesis for L-functions (GRH), Montgomery and Vaughan [3] showed that the sum is bounded by $O(\sqrt{q}\log\log q)$. This is best possible (up to a constant), because in 1932 Paley [5] proved that there are infinitely many quadratic characters χ such that there exists a constant $c > 0$ that satisfy for some N the inequality $\left|\sum_{n=1}^{N}\chi(n)\right| > c\sqrt{q}\log\log q$.

Recently, in [2], Levin, Pomerance and Soundararajan considered a "smoothed" version of the Pólya–Vinogradov inequality. Instead of considering the character sum over an interval, they consider the following weighted sum

$$S_\chi^*(M,N) := \sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right).$$

The theorem they prove is the following:

Theorem A. *Let χ be a primitive Dirichlet character to the modulus $q>1$ and let M,N be real numbers with $0<N\le q$. Then*

$$\left|S_\chi^*(M,N)\right| = \left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| \le \sqrt{q}-\frac{N}{\sqrt{q}}.$$

Levin, Pomerance and Soundararajan used the inequality to prove that for every prime $p>3$, there is a primitive root g and an integer $x\in[1,p-1]$ such that $g^x \equiv x \bmod p$, i.e., that the discrete logarithm base g has a fixed point. The second author (see [6]) used the smoothed Pólya–Vinogradov inequality to improve an upper bound for the least inert prime in a real quadratic field. The inequality is not new, as it was used by Hua in [1] to improve a bound on the least primitive root $\bmod\, p$. However, while Hua presented his paper as an introduction of a method with numerous applications, we didn't find other papers that used this technique. Hopefully this paper will help bring this useful method to the spotlight it deserves.

In this paper we will prove several related results. In section 2 we will prove a theorem that takes into account arithmetic information from the modulus q to give a better upper bound for some ranges of N:

Theorem 1. *Let χ be a primitive character to the modulus $q>1$, let M,N be real numbers with $0<N\le q$ and let m be a divisor of q such that $1\le m\le \frac{q}{N}$. Then*

$$\left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| \le \frac{\phi(m)}{m}\sqrt{q}.$$

We also prove the following theorem which expands the range of N and will be crucial to extend the inequality to imprimitive characters.

Theorem 2. *Let χ be a primitive character to the modulus $q>1$ and let M,N be real numbers with $N>0$. Then,*

$$\left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| \le \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right). \tag{1}$$

In particular, $|S_\chi^*(M,N)| < \sqrt{q}$*.*

Remark 1. The theorem was stated without proof as Corollary 3 in [2]. Also note that if $0 < N < q$, then $\left\{\dfrac{N}{q}\right\} = \dfrac{N}{q}$ and therefore Theorem A follows from Theorem 2.

With Theorem 2, we are able to extend the smoothed Pólya–Vinogradov inequality for imprimitive characters, namely we prove

Theorem 3. *Let* χ *be a non-principal Dirichlet character to the modulus* $q > 1$ *and let* M, N *be real numbers with* $N > 0$*. Then,*

$$\left|\sum_{M \le n \le M+2N} \chi(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| < \frac{4}{\sqrt{6}}\sqrt{q}.$$

One of the remarkable things involving the smoothed Pólya–Vinogradov inequality is that it is not very hard to prove and it is a tight inequality, since one can show that there exist M and N such that $\left|S_\chi^*(M,N)\right| > c\sqrt{q}$ for some positive constant c and some character χ mod q. Indeed, in section 3 we will prove that $\left|S_\chi^*(M,N)\right| > \frac{2}{\pi^2}\sqrt{q}$. The proof was motivated by the proof of Theorem 9.23 in [4]. Finally, in the last section, we show a table computing $S_\chi^*(M,N)$ for many moduli.

2. Upper Bound and Corollaries

We begin by recreating the proof of Theorem A. We do so because the proofs of Theorem 1 and Theorem 2 branch out from this proof.

Proof of Theorem A. We follow the proof in [2]. Let

$$H(t) = \max\{0, 1 - |t|\}.$$

We wish to estimate $|S_\chi^*(M,N)|$.

Using the identity (see Corollary 9.8 in [4])

$$\chi(n) = \frac{1}{\tau(\bar\chi)}\sum_{j=1}^{q} \bar\chi(j)e(nj/q),$$

where $e(x) := e^{2\pi i x}$ and $\tau(\chi)$ is the Gauss sum $\displaystyle\sum_{a=1}^{q} \chi(a)e(a/q)$, we can deduce

$$S_\chi^*(M,N) = \frac{1}{\tau(\bar\chi)}\sum_{j=1}^{q} \bar\chi(j)\sum_{n\in\mathbb{Z}} e(nj/q)H\left(\frac{n-M}{N} - 1\right).$$

The Fourier transform (see Appendix D in [4]) of H is

$$\widehat{H}(s) = \int_{-\infty}^{\infty} H(t)e(-st)dt = \frac{1-\cos 2\pi s}{2\pi^2 s^2} \text{ when } s \neq 0,\ \widehat{H}(0) = 1.$$

Therefore $\widehat{H}(s)$ is nonnegative for s real. In general, if

$$f(t) = e(\alpha t)H(\beta t + \gamma), \tag{2}$$

with $\beta > 0$, then

$$\widehat{f}(s) = \frac{1}{\beta} e\left(\frac{s-\alpha}{\beta}\gamma\right) \widehat{H}\left(\frac{s-\alpha}{\beta}\right). \tag{3}$$

Using $\alpha = j/q$, $\beta = 1/N$ and $\gamma = -M/N - 1$, then by Poisson summation (see Appendix D in [4]) we get

$$S_\chi^*(M,N) = \frac{N}{\tau(\bar{\chi})} \sum_{j=1}^{q} \bar{\chi}(j) \sum_{n\in\mathbb{Z}} e\left(-(M+N)\left(n - \frac{j}{q}\right)\right) \widehat{H}\left(\left(s - \frac{j}{q}\right)N\right). \tag{4}$$

Using that $\chi(q) = 0$, that $\widehat{H}$ is nonnegative and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters, we have

$$\left|S_\chi^*(M,N)\right| \leq \frac{N}{\sqrt{q}} \sum_{j=1}^{q-1} \sum_{n\in\mathbb{Z}} \widehat{H}\left(\left(n - \frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}} \sum_{k\in\mathbb{Z}/q\mathbb{Z}} \widehat{H}\left(\frac{kN}{q}\right).$$

Therefore

$$\begin{aligned}
\left|S_\chi^*(M,N)\right| &\leq \frac{N}{\sqrt{q}} \left(\sum_{k\in\mathbb{Z}} \widehat{H}\left(\frac{kN}{q}\right) - \sum_{k\in\mathbb{Z}} \widehat{H}(kN)\right) \\
&= \sqrt{q} \left(\sum_{k\in\mathbb{Z}} \frac{N}{q} \widehat{H}\left(\frac{kN}{q}\right) - \frac{N}{q} \sum_{k\in\mathbb{Z}} \widehat{H}(kN)\right) \\
&\leq \sqrt{q} \left(\sum_{k\in\mathbb{Z}} \frac{N}{q} \widehat{H}\left(\frac{kN}{q}\right) - \frac{N}{q} \widehat{H}(0)\right).
\end{aligned}$$

Using $\alpha = \gamma = 0$ and $\beta = \frac{q}{N}$ in (2) and (3) yields that the Fourier transform of $H\left(\frac{qt}{N}\right)$ is

$$\frac{1}{\beta} e\left(\frac{s-0}{\beta} \cdot (0)\right) \widehat{H}\left(\frac{s-0}{\beta}\right) = \frac{N}{q} \widehat{H}\left(\frac{sN}{q}\right).$$

Therefore, by Poisson summation, we have

$$\left|S_\chi^*(M,N)\right| \leq \sqrt{q} \sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) - \frac{N}{\sqrt{q}} = \sqrt{q} H(0) - \frac{N}{\sqrt{q}} = \sqrt{q} - \frac{N}{\sqrt{q}}. \tag{5}$$

We used that $q \geq N$ which implies that for $l \neq 0$ and $l \in \mathbb{Z}$, $\left|\frac{ql}{N}\right| \geq \left|\frac{q}{N}\right| \geq 1$ which implies $H\left(\frac{ql}{N}\right) = 0$. □

Proof of Theorem 1. Following the proof of the previous theorem, we arrive at (4). From there, using that if $(n,m)>1$ then $\chi(n)=0$, that $\widehat{H}$ is nonnegative, and that $|\tau(\bar{\chi})|=\sqrt{q}$ for primitive characters, we have

$$\left|S_{\chi}^{*}(M,N)\right| \le \frac{N}{\sqrt{q}} \sum_{\substack{j=1\\(j,m)=1}}^{q} \sum_{n\in\mathbb{Z}} \widehat{H}\left(\left(n-\frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}} \sum_{\substack{k\in\mathbb{Z}\\(k,m)=1}} \widehat{H}\left(\frac{kN}{q}\right). \qquad (6)$$

Using inclusion-exclusion we get

$$\left|S_{\chi}^{*}(M,N)\right| \le \frac{N}{\sqrt{q}} \sum_{d|m} \mu(d) \sum_{k\in\mathbb{Z}} \widehat{H}\left(\frac{kdN}{q}\right) = \sqrt{q}\sum_{d|m}\frac{\mu(d)}{d}\sum_{k\in\mathbb{Z}}\frac{dN}{q}\widehat{H}\left(\frac{kdN}{q}\right).$$

Since the Fourier transform of $H\left(\frac{qt}{Nd}\right)$ is $\frac{dN}{q}\widehat{H}\left(\frac{sdN}{q}\right)$, by Poisson summation

$$\left|S_{\chi}^{*}(M,N)\right| \le \sqrt{q}\sum_{d|m}\frac{\mu(d)}{d}\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{Nd}\right) = \sqrt{q}\sum_{d|m}\frac{\mu(d)}{d}H(0) = \frac{\phi(m)}{m}\sqrt{q}.$$

We used that $q \ge mN$ which implies that for $l \ne 0$ and $l \in \mathbb{Z}$, $\left|\frac{ql}{Nd}\right| \ge \left|\frac{q}{Nm}\right| \ge 1$, and hence $H\left(\frac{ql}{Nd}\right)=0$. □

Proof of Theorem 2. In the proof of Theorem A, we only used that $N \le q$ in the last inequality of (5). Therefore, from (5), we have

$$|S_{\chi}^{*}(M,N)| \le \sqrt{q}\left(\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) - \frac{N}{q}\right).$$

To get the desired result we need only prove

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) \le \frac{N}{q} + \frac{q}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right).$$

Note that $H\left(\frac{ql}{N}\right)=0$ for $|l| > \frac{N}{q}$. Also $H\left(\frac{ql}{N}\right) = H\left(\frac{-ql}{N}\right)$. Using these two facts together with $H(0)=1$, we get

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) = 1 + 2\sum_{l\le\frac{N}{q}} H\left(\frac{ql}{N}\right) = 1 + 2\sum_{l\le\frac{N}{q}}\left(1-\frac{ql}{N}\right).$$

Therefore

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) = 1 + 2\left\lfloor\frac{N}{q}\right\rfloor - \frac{2q}{N}\sum_{l\le\frac{N}{q}} l = 1 + 2\left\lfloor\frac{N}{q}\right\rfloor - \frac{q}{N}\left(\left\lfloor\frac{N}{q}\right\rfloor\right)\left(\left\lfloor\frac{N}{q}\right\rfloor+1\right).$$

Letting $\theta = \frac{N}{q}$ and using that $\frac{N}{q} = \left\lfloor \frac{N}{q} \right\rfloor + \theta$, we get

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) = 1 + \frac{2N}{q} - 2\theta - \frac{q}{N}\left(\frac{N^2}{q^2} + \frac{N}{q}(1-2\theta) - \theta(1-\theta)\right)$$
$$= \frac{2N}{q} + 1 - 2\theta - \frac{N}{q} - (1-2\theta) + \frac{q}{N}\theta(1-\theta) = \frac{N}{q} + \frac{q}{N}\theta(1-\theta).$$

Therefore (1) is true. Once we have (1), we can conclude that $|S^*_\chi(M,N)| < \sqrt{q}$. Indeed, if $N < q$, then

$$S^*_\chi(M,N) \leq \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1 - \left\{\frac{N}{q}\right\}\right) = \sqrt{q} - \frac{N}{\sqrt{q}} < \sqrt{q};$$

and if $N \geq q$, we have

$$S^*_\chi(M,N) \leq \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1 - \left\{\frac{N}{q}\right\}\right) \leq \frac{q^{3/2}}{4N} \leq \frac{\sqrt{q}}{4} < \sqrt{q}.$$

□

We finish the section with the proof of Theorem 3 :

Proof of Theorem 3. In this proof, we follow the ideas used in [4] (page 307) to extend the Pólya–Vinogradov inequality from primitive characters to general characters.

Let χ be induced by a primitive character χ^* of modulus $d > 1$. This is possible since χ is non-principal. In the case that χ is primitive, then $\chi^* = \chi$. Letting χ_0 be the principal character mod q, we have that $\chi = \chi^*\chi_0$. Therefore $\chi(n) = \chi^*(n)$ for n an integer coprime to q, and $\chi(n) = 0$ otherwise.

Let r be the product of primes that divide q but not d. Then when $(n,r) > 1$, we have $\chi(n) = 0$. If $(n,r) = 1$, then $\chi(n) = \chi^*(n)$. Therefore

$$\sum_{n=M}^{M+2N} \chi(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right) = \sum_{\substack{M\leq n\leq M+2N \\ (n,r)=1}} \chi^*(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)$$
$$= \sum_{M\leq n\leq M+2N} \chi^*(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)\sum_{k|(n,r)} \mu(k)$$
$$= \sum_{k|r} \mu(k) \sum_{\substack{M\leq n\leq M+2N \\ k|n}} \chi^*(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right).$$

Now, writing $n = km$ and using that χ^* is totally multiplicative, we get

$$\sum_{k|r} \mu(k)\chi^*(k) \sum_{\frac{M}{k}\leq m\leq \frac{M+2N}{k}} \chi^*(m)\left(1 - \left|\frac{m - \frac{M}{k}}{\frac{N}{k}} - 1\right|\right) = \sum_{k|r} \mu(k)\chi^*(k) S_{\chi^*}\left(\frac{M}{k}, \frac{N}{k}\right).$$

By Theorem 2, $|S_{\chi^*}(M/k, N/k)| < \sqrt{d}$. Hence, taking absolute value, we have

$$|S^*_\chi(M,N)| < \sum_{k|r} \sqrt{d} = 2^{\omega(r)}\sqrt{d} \leq 2^{\omega(r)}\sqrt{\frac{q}{r}}. \tag{7}$$

Since $2^{\omega(r)}$ is a multiplicative function, and for $p \geq 5$, $2 < \sqrt{p}$, we have

$$\frac{2^{\omega(r)}}{\sqrt{r}} = \prod_{p|r} \frac{2}{\sqrt{p}} \leq \frac{2}{\sqrt{2}} \times \frac{2}{\sqrt{3}} = \frac{4}{\sqrt{6}}. \tag{8}$$

Combining (7) with (8) yields the desired result. □

3. Lower Bound

Theorem 4. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be positive integers. Then*

$$S_2(N) := \max_{1\leq M\leq q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right| \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin\frac{\pi N}{q}\right)^2}{\left(\sin\frac{\pi}{q}\right)^2}. \tag{9}$$

Proof. Let

$$S_3(N) := \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right),$$

and note that

$$\begin{aligned}|S_3(N)| &\leq \sum_{M=1}^{q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right| \\ &\leq q \max_{1\leq M\leq q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right| = qS_2(N).\end{aligned}$$

Therefore we can focus on $S_3(N)$:

$$\begin{aligned}S_3(N) &= \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \\ &= \sum_{n=0}^{2N} \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \chi(n+M) \left(1 - \left|\frac{n}{N} - 1\right|\right).\end{aligned}$$

Now we can do a change of variable, to go from M to $L-n$:

$$\begin{aligned}S_3(N) &= \sum_{n=0}^{2N}\sum_{L=1}^{q} e\left(\frac{L-n}{q}\right)\chi(L)\left(1-\left|\frac{n}{N}-1\right|\right)\\ &= \sum_{n=0}^{2N} e\left(-\frac{n}{q}\right)\left(1-\left|\frac{n}{N}-1\right|\right)\sum_{L=1}^{q} e\left(\frac{L}{q}\right)\chi(L).\end{aligned}$$

Therefore,

$$S_3(N) = \tau(\chi)\sum_{n=0}^{2N} e\left(-\frac{n}{q}\right)\left(1-\left|\frac{n}{N}-1\right|\right) = \tau(\chi)S_4(N).$$

Now it's time to work on $S_4(N)$:

$$S_4(N) = \sum_{n=0}^{2N} e\left(-\frac{n}{q}\right)\left(1-\left|\frac{n}{N}-1\right|\right) = \sum_{n=0}^{N} e\left(-\frac{n}{q}\right)\frac{n}{N} + \sum_{n=N+1}^{2n} e\left(-\frac{n}{q}\right)\left(2-\frac{n}{N}\right).$$

By making the change of variable $m = 2N-n$, we get

$$S_4(N) = \frac{1}{N}\sum_{n=0}^{N} e\left(-\frac{n}{q}\right) n \; + \; \frac{e\left(-\frac{2N}{q}\right)}{N}\sum_{m=0}^{N-1} e\left(\frac{m}{q}\right) m.$$

Using the identity

$$\sum_{n=0}^{N} nx^n = x\frac{Nx^{N+1}-(N+1)x^N+1}{(x-1)^2} = \frac{Nx^{N+1}-(N+1)x^N+1}{(x^{1/2}-x^{-1/2})^2},$$

with $x = e(\alpha)$ and $\alpha = -\frac{1}{q}$, we get

$$\begin{aligned}S_4(N) = \frac{1}{N}&\frac{Ne\left((N+1)\alpha\right)-(N+1)e\left(N\alpha\right)+1}{\left(e\left(\frac{\alpha}{2}\right)-e\left(-\frac{\alpha}{2}\right)\right)^2}\\ &+ \; \frac{e\left(2N\alpha\right)}{N}\frac{(N-1)e\left(-N\alpha\right)-Ne\left(-(N-1)\alpha\right)+1}{\left(e\left(-\frac{\alpha}{2}\right)-e\left(\frac{\alpha}{2}\right)\right)^2}.\end{aligned}$$

Therefore, by taking common denominator and multiplying out, we get that $S_4(N)$ equals

$$\frac{Ne\left((N+1)\alpha\right)-(N+1)e\left(N\alpha\right)+1+(N-1)e(N\alpha)-Ne((N+1)\alpha)+e(2N\alpha)}{N\left(e\left(\frac{\alpha}{2}\right)-e\left(-\frac{\alpha}{2}\right)\right)^2},$$

which equals

$$\frac{e(2N\alpha)-2e(N\alpha)+1}{N\left(e\left(\frac{\alpha}{2}\right)-e\left(-\frac{\alpha}{2}\right)\right)^2} = \frac{e(N\alpha)}{N}\frac{\left(e\left(\frac{N\alpha}{2}\right)-e\left(-\frac{N\alpha}{2}\right)\right)^2}{\left(e\left(\frac{\alpha}{2}\right)-e\left(-\frac{\alpha}{2}\right)\right)^2} = \frac{e(N\alpha)}{N}\frac{\left(\sin N\pi\alpha\right)^2}{\left(\sin\pi\alpha\right)^2}. \tag{10}$$

From earlier we know, $qS_2(N) \geq |S_3(N)| = |\tau(\chi)||S_4(N)|$. Using $|\tau(\chi)| = \sqrt{q}$, that $|e(x)| = 1$ and (10) yields the theorem. □

Now we are ready to prove our main lower bound result.

Corollary 1. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be positive integers. Then*

$$\max_{M,N} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right) \right| \geq \frac{2}{\pi^2}\sqrt{q}.$$

Proof. If q is even, let $N = \frac{q}{2}$. Therefore (9) becomes

$$S_2(N) \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin \frac{\pi N}{q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2} = \frac{2}{q\sqrt{q}} \frac{1}{\left(\sin \frac{\pi}{q}\right)^2} \geq \frac{2}{\pi^2}\sqrt{q}.$$

The last inequality comes from $\frac{1}{\sin x} \geq \frac{1}{x}$.

If q is odd, let $N = \frac{q-1}{2}$. Then

$$S_2(N) \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin \frac{\pi N}{q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2} = \frac{2}{(q-1)\sqrt{q}} \frac{\left(\cos \frac{\pi}{2q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2}.$$

From this and $\sin \frac{\pi}{q} = 2 \sin \frac{\pi}{2q} \cos \frac{\pi}{2q}$, we get

$$S_2(N) \geq \frac{2}{4(q-1)\sqrt{q}} \frac{1}{\left(\sin \frac{\pi}{2q}\right)^2} \geq \frac{2}{\pi^2} \frac{q}{q-1}\sqrt{q} > \frac{2}{\pi^2}\sqrt{q}.$$

□

Remark 2. If we consider $N = \frac{q}{3}$ for $3 \mid q$, $N = \frac{q-1}{3}$ for $q \equiv 1 \pmod 3$ and $N = \frac{q-2}{3}$ for $q \equiv 2 \pmod 3$, then we can improve the constant from $\frac{2}{\pi^2} \approx 0.202642$ to $\frac{9}{4\pi^2} \approx 0.227973$. With N around $\frac{2q}{5}$ the constant improves a bit more to $\frac{5(5+\sqrt{5})}{16\pi^2} \approx 0.229115$. The optimal value for N under this technique is around $N = .371q$ where the constant is approximately 0.230651.

4. Numerics

Let χ be a Dirichlet character mod q and let

$$F(\chi) = \max_{M,2N \in \mathbb{Z}} \frac{\left|S_\chi^*(M,N)\right|}{\sqrt{q}}.$$

Note that $F(\chi)$ exists because $|S_\chi(M,N)|/\sqrt{q}$ is a bounded continuous function, periodic in M and going to 0 as $N \to \infty$ (by Theorem 2). In the previous sections we gave upper and lower bounds for $F(\chi)$. Indeed
$\frac{2}{\pi^2} \leq F(\chi) < 1$. Now, let

$$G(q) = \max_{\chi} F(\chi),$$

and

$$H(q) = \min_{\chi} F(\chi),$$

where the max and the min range over primitive characters mod q. By writing a program in Java we created Table 1 (below) giving values for $G(q)$ and $H(q)$ which show that there's room for improvement in the upper and lower bounds, for example it seems $\frac{2}{5} < F(q) < \frac{4}{5}$. The reason a program could be written to find $G(q)$ and $H(q)$ even though M and N range through all integers is that the periodicity of χ mod q allows us to restrict ourselves to $0 \leq M < q$ and $M \leq 2N < M + q$ with $M, 2N \in \mathbb{N}$.

Acknowledgements We would like to thank Carl Pomerance for his useful comments regarding this paper and his encouragement.

References

[1] Loo-Keng Hua, *On the least primitive root of a prime*, Bull. Amer. Math. Soc. **48** (1942), 726–730.

[2] M. Levin, C. Pomerance, and K. Soundararajan, *Fixed points for discrete logarithms*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, 2010, pp. 6–15.

[3] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), no. 1, 69–82.

[4] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[5] R.E.A.C. Paley, *A theorem on characters*, J. Lond. Math. Soc. **7** (1932), 28–32.

[6] Enrique Treviño, *The least inert prime in a real quadratic field*, Math. Comp. **81** (2012), no. 279, 1777–1797.

q	G(q)	H(q)	q	G(q)	H(q)	q	G(q)	H(q)
3	0.577	0.577	63	0.610	0.481	123	0.627	0.473
4	0.500	0.500	64	0.481	0.449	124	0.488	0.448
5	0.596	0.500	65	0.624	0.478	125	0.697	0.471
7	0.567	0.500	67	0.678	0.470	127	0.709	0.464
8	0.471	0.471	68	0.480	0.448	128	0.484	0.453
9	0.533	0.509	69	0.638	0.474	129	0.647	0.485
11	0.603	0.484	71	0.681	0.472	131	0.708	0.474
12	0.462	0.462	72	0.466	0.463	132	0.470	0.455
13	0.666	0.474	73	0.720	0.475	133	0.694	0.465
15	0.516	0.506	75	0.607	0.465	135	0.615	0.471
16	0.452	0.452	76	0.487	0.450	136	0.488	0.456
17	0.610	0.493	77	0.676	0.483	137	0.711	0.471
19	0.622	0.489	79	0.683	0.475	139	0.704	0.478
20	0.461	0.447	80	0.481	0.463	140	0.480	0.458
21	0.635	0.495	81	0.634	0.470	141	0.645	0.472
23	0.615	0.480	83	0.684	0.469	143	0.706	0.472
24	0.467	0.467	84	0.470	0.461	144	0.474	0.455
25	0.628	0.493	85	0.701	0.479	145	0.747	0.472
27	0.615	0.473	87	0.611	0.480	147	0.620	0.466
28	0.481	0.460	88	0.487	0.451	148	0.488	0.451
29	0.640	0.484	89	0.689	0.470	149	0.690	0.471
31	0.654	0.485	91	0.656	0.479	151	0.717	0.474
32	0.476	0.472	92	0.483	0.448	152	0.485	0.451
33	0.604	0.476	93	0.621	0.465	153	0.629	0.469
35	0.653	0.486	95	0.669	0.482	155	0.701	0.468
36	0.470	0.459	96	0.474	0.460	156	0.483	0.454
37	0.701	0.473	97	0.718	0.468	157	0.703	0.464
39	0.604	0.490	99	0.630	0.480	159	0.636	0.466
40	0.484	0.459	100	0.484	0.452	160	0.478	0.451
41	0.652	0.479	101	0.685	0.480	161	0.715	0.476
43	0.655	0.487	103	0.688	0.466	163	0.724	0.465
44	0.482	0.455	104	0.485	0.452	164	0.483	0.448
45	0.603	0.479	105	0.619	0.478	165	0.623	0.479
47	0.669	0.474	107	0.696	0.476	167	0.698	0.475
48	0.473	0.473	108	0.473	0.458	168	0.468	0.462
49	0.675	0.474	109	0.716	0.473	169	0.715	0.466
51	0.588	0.481	111	0.630	0.472	171	0.636	0.472
52	0.479	0.457	112	0.482	0.456	172	0.487	0.449
53	0.639	0.466	113	0.697	0.474	173	0.711	0.460
55	0.644	0.487	115	0.688	0.470	175	0.691	0.466
56	0.478	0.467	116	0.486	0.449	176	0.484	0.452
57	0.626	0.482	117	0.624	0.478	177	0.636	0.466
59	0.672	0.477	119	0.692	0.471	179	0.721	0.466
60	0.471	0.463	120	0.476	0.464	180	0.472	0.455
61	0.694	0.486	121	0.690	0.475	181	0.714	0.466

Table 1: A table showing the max and min of $G(q)$ and $H(q)$ for all moduli $q \leq 181$ that have primitive characters. It is worth noting that the reason the moduli divisible by 4 has such a small $G(q)$ is Theorem 1.