PÓLYA-VINOGRADOV AND THE LEAST QUADRATIC NONRESIDUE

JONATHAN W. BOBER AND LEO GOLDMACHER

Abstract. It is well-known that cancellation in short character sums (e.g. Burgess’ estimates) yields bounds on the least quadratic nonresidue. Scant progress has been made on short character sums since Burgess’ work, so it is desirable to find a new approach to nonresidues. The goal of this note is to demonstrate a new line of attack via long character sums, a currently active area of research. Among other results, we demonstrate that improving the constant in the Pólya-Vinogradov inequality would lead to significant progress on nonresidues. Moreover, conditionally on a conjecture on long character sums, we show that the least nonresidue for any odd primitive character (mod \(k\)) is bounded by \((\log k)^{1.4}\).

1. The case of the odd character

It is a long-standing open problem (first studied by Gauss as a key step in his first proof of Quadratic Reciprocity) to determine strong bounds on the least quadratic nonresidue modulo \(p\), which we denote \(n_p\). The celebrated Pólya-Vinogradov bound on character sums immediately implies the bound \(n_p \ll \sqrt{p} \log p\), and an innovation due to Vinogradov reduced this to \(n_p \ll p^{1/(2\sqrt{e})} \log^2 p\). Burgess’ character sum bound further improved this to \(n_p \ll p^{1/4+\epsilon}\), and applying Vinogradov’s trick gives \(n_p \ll p^{1/(4\sqrt{e})+\epsilon}\). Finally, Hildebrand observed [Hil86] that mean values of character sums vary slowly, from which he deduced

\[
n_p \ll p^{1/(4\sqrt{e})-o(1)}.
\]

This bound remains the state of the art.

From this history one might infer that the way forward is to improve Burgess’ theorem by exhibiting cancellation in shorter character sums. This seems to be a difficult problem, however, as no one has made progress on short character sums in a long time. By contrast, there have been a number of recent breakthroughs on long character sums (discussed below), and it is likely that more are on the horizon. The goal of the present note is to show that cancellation in long character sums can lead to strong bounds on \(n_p\). To state our results more precisely, we need some notation. Given a character \(\chi \pmod{q}\), set

\[
S_{\chi}(t) := \sum_{n \leq t} \chi(n), \quad M(\chi) := \max_{t \leq q} |S_{\chi}(t)|, \quad \text{and} \quad n_{\chi} := \min\{n \in \mathbb{N} : \chi(n) \neq 0, 1\}. \tag{2}
\]

In this notation, the Pólya-Vinogradov inequality asserts the bound \(M(\chi) \ll \sqrt{q} \log q\). Our main result is the following.

Theorem 1. Fix notation as in (2), and suppose \(M(\chi) \leq \sqrt{q} \cdot \frac{\log x}{f(q)}\) for all primitive even characters \(\chi \pmod{q}\) of order \(g\), where \(f\) is some function satisfying \(f'(x) \geq 0\) for all sufficiently large \(x\). Then for all odd primitive Dirichlet characters \(\xi \pmod{k}\) of order \(g\) with \(3 \nmid k\) we have

\[
n_\xi \ll \exp\left(\frac{\pi \sqrt{3}}{2(\sqrt{e} - 1)} \cdot \frac{\log k}{f(k)}\right).
\]
In other words, improvements to the Pólya-Vinogradov inequality (even of the implicit constant) would yield improvements of bounds on the least nonresidue. To get a feel for the strength of Theorem 1, we explore several consequences.

First, we consider the constant in the Pólya-Vinogradov inequality. Hildebrand proved [Hil88, Corollary 5] that for all primitive even quadratic $\chi \pmod{q}$ one has

$$M(\chi) \leq \left( C + o(1) \right) \sqrt{q} \log q$$

with $C = \frac{\sqrt{e} - 1}{2\pi\sqrt{3}e} \approx 0.036$. Applying Theorem 1 to Hildebrand’s bound recovers the Burgess bound $n_p \ll p^{\frac{1}{4}\sqrt{e} + o(1)}$ for all $p \equiv 3 \pmod{4}$. Thus, any improvement over Hildebrand’s constant – for example, to $C = \frac{1}{9\pi} \approx 0.035$ – would immediately yield an improvement of the Burgess exponent $\frac{1}{4\sqrt{e}}$ for primes $p \equiv 3 \pmod{4}$. (Hildebrand asserts, without proof, that the same is true for primes $p \equiv 1 \pmod{4}$; this is presumably a typo.)

If we are more optimistic, we might hope to improve Pólya-Vinogradov further. In recent years, several infinite families of characters (namely, characters of odd order [GS07, Gol12] and characters with smooth conductor [Gol10]) have been shown to satisfy

$$M(\chi) = o\left(\sqrt{q} \log q\right).$$

If we could prove such a bound for the family of all even characters $\chi \pmod{q}$, Theorem 1 would imply

$$n_\xi \ll k^{o(1)}$$

for all odd $\xi \pmod{k}$.

We conclude our discussion by exploring the limitations of Theorem 1. Working under the Generalized Riemann Hypothesis, Granville and Soundararajan have shown that

$$M(\chi) \leq \left( \frac{2e^\gamma}{\pi\sqrt{3}} + o(1) \right) \sqrt{q} \log \log q$$

for every even primitive character and conjecture that this can be improved to

$$M(\chi) \leq \left( \frac{e^\gamma}{\pi\sqrt{3}} + o(1) \right) \sqrt{q} \log \log q. \quad (3)$$

Applying Theorem 1 yields the following.

**Corollary 2.** Suppose that the bound (3) holds for all primitive even characters $\chi \pmod{q}$. Then for all odd primitive characters $\xi \pmod{k}$ we have

$$n_\xi \ll (\log k)^{c + o(1)},$$

where $c = \frac{e^\gamma}{2(\sqrt{e} - 1)} \approx 1.37$.

Note that this is stronger than Ankeny’s [Ank52] long-standing GRH bound $n_p \ll (\log p)^2$. On the other hand, we fall short of achieving the conjectured bound $n_p \ll_\epsilon (\log p)^{1+\epsilon}$. In fact, Corollary 2 is the strongest consequence one could hope to derive from Theorem 1 since Granville and Soundararajan have unconditionally proved that equality is attained in (3) for infinitely many primitive even $\chi \pmod{q}$; this follows immediately from equation (1.8) of [GS07].

\footnote{Although not explicitly stated, this is easily derived from the proof of Theorem 6 in [GS07].}
The maximum size of the least nonresidue seems to be intimately linked with the maximum size of Dirichlet $L$-functions at 1. Given an odd character $\xi (\text{mod } p)$ with large least nonresidue, we construct an even character $\chi (\text{mod } 3p)$ for which $S_{\chi}(\alpha p)$ is large for some $\alpha$. In fact, it follows from work of the first author [Bob] that we can take $\alpha$ very close to 1.

Since $S_{\chi}(p) = \frac{\pi}{\sqrt{3}} L(1, \xi)$, one expects that $L(1, \xi)$ is also large; however, we are not able to prove this. If we were, we would be able to recover the Burgess exponent $\frac{1}{4\sqrt{e}} + o(1)$ from Stephens’ work [Ste72] on the size of $L(1, \chi)$.

At the heart of the proof of Theorem 1 is the following result, which provides an upper bound on the least nonresidue for an odd character in terms of the maximum size of a related character sum.

**Theorem 3.** Suppose $\xi (\text{mod } k)$ and $\psi (\text{mod } \ell)$ are odd primitive Dirichlet characters such that $(k, \ell) = 1$. Then

$$\log n_{\xi} \leq \frac{\pi}{2(\sqrt{e} - 1)} \cdot \frac{M(\xi \psi)}{\sqrt{k}} + O(\sqrt{\ell}).$$

This demonstrates that we can improve bounds on $n_{\xi}$ by finding a single twist of $\xi$ for which Pólya-Vinogradov can be beaten. Although this seems stronger than Theorem 1, we have not been able to exploit the extra flexibility.

We expect that neither Theorem 1 nor Theorem 3 is optimal. In Section 3 we give a heuristic argument which suggests the following.

**Conjecture 4.** Let $\chi(n) := \xi(n) \left(\frac{a}{3}\right)$, where $\xi (\text{mod } k)$ is an odd primitive character such that $3 \nmid k$. Then

$$\log n_{\xi} \leq \left(\frac{\pi}{e\gamma} + o(1)\right) \frac{M(\chi)}{\sqrt{k}}.$$

Combined with the conjectural bound (5) on long character sums, this would yield

$$n_p \leq (\log p)^{1+o(1)} \quad \text{for all } p \equiv 3 \pmod 4.$$

**Acknowledgements.** We are grateful to Soundararajan for encouragement and some helpful suggestions. The second author is partially supported by an NSERC Discovery Grant.

## 2. Proofs of Theorems 1 and 3

We begin by showing that Theorem 1 is an easy consequence of Theorem 3.

**Proof of Theorem 1.** Let $h(x) := \frac{\log x}{f(x)}$, so that our hypothetical improvement of Pólya-Vinogradov becomes: for all primitive even $\chi (\text{mod } q)$,

$$M(\chi) \leq \sqrt{q} \cdot h(q).$$

Note that we may (and will) assume that $h(x) \leq \log x$, or equivalently that $f(x) \geq 1$, for all sufficiently large $x$.

Given any odd primitive characters $\xi (\text{mod } k)$ and $\psi (\text{mod } \ell)$ with $(k, \ell) = 1$, set $\chi := \xi \psi$ and $q := k\ell$. It follows that $\chi (\text{mod } q)$ is a primitive even character, so by Theorem 3 combined with our hypothesis on $M(\chi)$, we deduce

$$\log n_{\xi} \leq \frac{\pi \sqrt{\ell}}{2(\sqrt{e} - 1)} \cdot h(q) + O(\sqrt{\ell}).$$
We now show that $h(q) = h(k) + O(\ell)$. First, observe that
\[ h'(x) = \frac{1}{x \cdot f(x)} - \frac{f'(x) \log x}{f(x)^2} \leq \frac{1}{x}, \]
since $f(x) \geq 1$ and $f'(x) \geq 0$. The Mean Value theorem implies that for some $x_k \in [k, q]$,
\[ h(q) - h(k) = k(\ell - 1) \cdot h'(x_k) \leq \ell - 1. \]
It follows that
\[ \log n_\xi \leq \frac{\pi \sqrt{\ell}}{2(\sqrt{e} - 1)} \cdot h(k) + O(\ell^{3/2}). \]
If $3 \nmid k$, we may make the choice $\psi(n) := (\frac{n}{3})$, which yields
\[ n_\xi \ll \exp\left(\frac{\pi \sqrt{3}}{2(\sqrt{e} - 1)} \cdot h(k)\right) = \exp\left(\frac{\pi \sqrt{3}}{2(\sqrt{e} - 1)} \cdot \frac{\log k}{f(k)}\right). \]

We now shift our attention to Theorem 3. Here is a rough sketch of our argument. In [GL] it was shown that for any primitive odd characters $\xi \pmod{k}$ and $\psi \pmod{\ell}$, we have
\[ M(\xi \psi) \gtrsim \sqrt{\frac{k}{\pi}} \left| \sum_{n \leq N} \frac{\xi(n)}{n} \right| \quad (4) \]
for any small $N$. To make the inequality as tight as possible, one wishes to choose $N$ which maximizes the sum on the right-hand side. The natural choice $N = n_\xi$ would give $M(\xi \psi) \gtrsim \sqrt{\frac{k}{\pi}} \log n_\xi$, which is of the same shape as our claim but with a weaker constant. To do better, we employ a version of Vinogradov’s trick. For $n > n_\xi$ it is hard to predict the behavior of $\xi(n)$ in general; however, we know that $\xi(n) = 1$ for all $n_\xi$-smooth $n$, and there are many smooth numbers just a bit larger than $n_\xi$. Thus, taking $N$ to be slightly bigger than $n_\xi$ increases the size of the sum in (4). Optimizing the balance between the mysterious behavior of $\xi(n)$ and the well-understood behavior of smooth numbers, we settle on a choice of $N$ which gives the bound in Theorem 3.

Before making the above outline rigorous, we state a few preliminary results. The following two estimates, developed in [GL12] and [GL] to show that character sums can get large, significantly simplify our computations.

**Lemma 5** (see Lemma 2.2 of [GL12]). Let $\{a_n\}_{n \in \mathbb{Z}}$ be a sequence of complex numbers with $|a_n| \leq 1$ for all $n$, and let $x \geq 2$ be a real number. Then
\[ \max_{\theta \in [0, 1]} \left| \sum_{1 \leq |n| \leq x} \frac{a_n}{n} e(n\theta) \right| = \max_{\theta \in [0, 1]} \max_{1 \leq |n| \leq x} \left| \sum_{1 \leq |n| \leq N} \frac{a_n}{n} e(n\theta) \right| + O(1). \]

**Lemma 6** (see Lemma 2.1 of [GL]). If $\psi \pmod{m}$ is a primitive Dirichlet character, then
\[ \max_{\theta \in [0, 1]} \left| \sum_{n \in \mathbb{Z}} b_n \psi(n) e(n\theta) \right| \geq \frac{\sqrt{m}}{\phi(m)} \left| \sum_{(n, m) = 1} b_n \right| \]
for any set of complex numbers $\{b_n\}$ satisfying $\sum|b_n| < \infty$.

Next, in order to apply our version of Vinogradov’s trick, we shall require the following estimate. Given an integer $n \geq 2$, denote the largest prime factor of $n$ by $P^+(n)$.
Lemma 7. For any fixed $\alpha \in [1, 2]$ we have
\[
\sum_{\substack{n \leq y^\alpha \\ P^+(n) > y}} \frac{1}{n} = (\alpha \log \alpha - \alpha + 1) \log y + O(1).
\]

Proof. We have
\[
\sum_{\substack{n \leq y^\alpha \\ P^+(n) > y}} \frac{1}{n} = \sum_{y < n \leq y^\alpha} \frac{1}{n} - \sum_{y < n \leq y^\alpha} \frac{1}{n} = (\alpha - 1) \log y + O\left(\frac{1}{y}\right) - \sum_{y < n \leq y^\alpha} \frac{1}{n}.
\]

Thus it suffices to estimate the sum
\[
\sum_{y < n \leq y^\alpha} \frac{1}{n}.
\]

Applying partial summation and a change of variables, we obtain
\[
\sum_{y < n \leq y^\alpha} \frac{1}{n} = \Psi\left(y^\alpha, y\right) \frac{1}{\alpha y^\alpha - 1} + (\log y) \int_1^{\alpha} \frac{\Psi\left(y^\alpha u, y\right)}{y^\alpha} du,
\]
where $\Psi(x, y)$ denotes the number of $y$-smooth numbers up to $x$. When $x$ is not much larger than $y$, the quantity $\Psi(x, y)$ is well-understood. For example, for fixed $\alpha \in [1, 2]$ we have
\[
\Psi\left(y^\alpha, y\right) = 1 - \log \alpha + O\left(\frac{1}{\log y}\right)
\]
uniformly in $y \geq 2$. (See the excellent survey article \[Gra08\] for much more general results.) Employing this in \[5\] and simplifying yields
\[
\sum_{y < n \leq y^\alpha} \frac{1}{n} = (-\alpha \log \alpha + 2\alpha - 2) \log y + O(1).
\]

Combining this with our work above concludes the proof. \[\square\]

Having assembled all the ingredients, we can now prove Theorem \[3\].

Proof of Theorem \[3\]. Let $\chi := \xi \psi$ and let $q := k\ell$, so that $\chi \pmod{q}$ is an even primitive character. In this case, Pólya’s Fourier expansion reads
\[
S_\chi(q\alpha) = -\frac{\tau(\chi)}{2\pi i} \sum_{1 \leq |n| \leq q} \frac{\overline{\chi(n)}}{n} e(-n\alpha) + O(\log q),
\]
where $\tau(\chi)$ is the Gauss sum. It follows that
\[
M(\chi) = \frac{\sqrt{q}}{2\pi} \max_\alpha \left| \sum_{1 \leq |n| \leq q} \frac{\overline{\chi(n)}}{n} e(-n\alpha) \right| + O(\sqrt{q}). \quad (6)
\]
Pick any \( N \leq q \). Lemmas 5 and 6 imply
\[
\max_\alpha \left| \sum_{1 \leq |n| \leq N} \frac{\overline{\chi}(n)}{n} e(-n\alpha) \right| \geq \max_\alpha \left| \sum_{1 \leq |n| \leq N} \frac{\overline{\chi}(n)}{n} e(-n\alpha) \right| + O(1)
\]
\[
\geq \frac{\sqrt{\ell}}{\varphi(\ell)} \left| \sum_{1 \leq |n| \leq N} \frac{\overline{\xi}(n)}{n} \right| + O(1).
\]
Plugging this into (6) gives
\[
M(\chi) \geq \frac{\sqrt{k}}{\pi} \cdot \frac{\ell}{\varphi(\ell)} \left| \sum_{n \leq N} \frac{\xi(n)}{n} \right| + O(\sqrt{q}).
\]
(7)

It remains to choose \( N \) to maximize the sum on the right hand side.

Write \( N = y^\alpha \), where \( y \leq n_\xi \) and \( \alpha \in [1, 2] \) will be determined later (note that \( y^\alpha \leq q \)).

We are trying to find a lower bound on the magnitude of
\[
\sum_{n \leq y^\alpha} \frac{\xi(n)}{n} = \sum_{n \leq y^\alpha} \frac{1}{n} + \sum_{n \leq y^\alpha} \frac{\xi(n) - 1}{n}.
\]
(8)

Now, \( \xi(n) = 1 \) whenever \( P^+(n) \leq y \), so we have
\[
\left| \sum_{n \leq y^\alpha} \frac{\xi(n) - 1}{n} \right| \leq 2 \sum_{n \leq y^\alpha} \frac{1}{n}.
\]
(9)

Combining (8) and (9) gives
\[
\left| \sum_{n \leq y^\alpha} \frac{\xi(n)}{n} \right| \geq \sum_{n \leq y^\alpha} \frac{1}{n} - 2 \sum_{n \leq y^\alpha} \frac{1}{n}.
\]

Getting rid of the coprimality restrictions by standard arguments and applying Lemma 7 yields
\[
\left| \sum_{n \leq y^\alpha} \frac{\xi(n)}{n} \right| \geq \frac{\varphi(\ell)}{\ell} (-2\alpha \log \alpha + 3\alpha - 2) \log y + O(\log \ell \log \log \ell).
\]

Substituting this into (7) gives the lower bound
\[
M(\chi) \geq \frac{\sqrt{k}}{\pi} (-2\alpha \log \alpha + 3\alpha - 2) \log y + O(\sqrt{q}).
\]
The right side is maximized when \( \alpha = \sqrt{e} \) and \( y = n_\xi \). Making these choices and rearranging the inequality concludes the proof of Theorem 3.
\( \square \)
3. Heuristics and Conjecture 4

Let $\chi(n) := \xi(n) \left( \frac{n}{3} \right)$, where $\xi(m)$ is an odd primitive character with $3 \nmid k$. Our inequality (7) implies

$$M(\chi) \geq \sqrt{k} \cdot \frac{3}{2} \left| \sum_{n \leq k \atop (n,3) = 1} \frac{\xi(n)}{n} \right| + O(\sqrt{k})$$

$$\approx \frac{\sqrt{k}}{\pi} \sum_{n \leq k} \frac{\xi(n)}{n} + O(\sqrt{k}).$$

Pick any $y \leq k$ and $0 = u_0 < u_1 < \cdots < u_\ell = \log k \log y$. Then we can write

$$\sum_{n \leq k} \frac{\xi(n)}{n} = \sum_{y^{u_0} \leq n < y^{u_1}} \frac{\xi(n)}{n} + \sum_{y^{u_1} \leq n < y^{u_2}} \frac{\xi(n)}{n} + \cdots + \sum_{y^{u_{\ell-1}} \leq n < y^{u_\ell}} \frac{\xi(n)}{n}.$$

Now, suppose $\xi(n) = 1$ for all $y$-smooth integers $n$. The proportion of $n \in [y^{u_j-1}, y^{u_j})$ which are $y$-smooth is roughly $\rho(u_j)$, where $\rho$ is the Dickman-de Bruijn function. If $n_\xi$ is large, then $\xi$ should behave randomly on those $n$ which are not $n_\xi$-smooth. We are therefore led to guess that, when $y = n_\xi$,

$$\sum_{y^{u_j-1} \leq n < y^{u_j}} \frac{\xi(n)}{n} \approx \rho(u_j) \left( \log y^{u_j} - \log y^{u_j-1} \right).$$

This would imply

$$\sum_{n \leq k} \frac{\xi(n)}{n} \approx (\log n_\xi) \sum_{j \leq \ell} (u_j - u_{j-1}) \rho(u_j) \approx (\log n_\xi) \int_0^{\log k \log n_\xi} \rho(u) du.$$

Since we presumably have $n_\xi \ll k^{o(1)}$, we see that

$$\sum_{n \leq k} \frac{\xi(n)}{n} \approx (\log n_\xi) \int_0^\infty \rho(u) du = e^\gamma \log n_\xi.$$

Substituting this into our initial inequality, we are led to the statement of Conjecture 4.

$$\log n_\xi \leq \left( \frac{\pi}{e^\gamma + o(1)} \right) \frac{M(\chi)}{\sqrt{k}}.$$

Applying the conjectured bound (3) to the even character $\chi \pmod{3k}$ would yield

$$n_\xi \ll (\log k)^{1+o(1)}.$$
Theorem 8. Suppose $\chi \pmod{q}$ is a primitive even character, and let $n_\chi$ denote its least nonresidue. Then either $n_\chi \ll \exp\left((\log q)^{5/6+\epsilon}\right)$, or $M(\chi) \leq \sqrt{q(\log q)^{2/3+o(1)}}$.

Proof. Suppose $n_\chi \geq \exp\left((\log q)^{5/6+\epsilon}\right)$. Then

$$D(\chi, \chi_0; q)^2 = \sum_{p \leq q} \frac{1 - \text{Re} \chi(p)}{p} = \sum_{n_\chi \leq p \leq q} \frac{1 - \text{Re} \chi(p)}{p} \leq \sum_{n_\chi \leq p \leq q} \frac{2}{p} \leq \left(\frac{1}{3} - 2\epsilon\right) \log \log q + o(1). \tag{10}$$

In Lemma 3.3 of [BGS13], Balog, Granville and Soundararajan show that for all $\psi$ other than the most pretentious character,

$$D(\chi(n), \psi(n)n^t; q)^2 \geq \left(\frac{1}{3} + o(1)\right) \log \log q$$

for all $t$. It follows that $\chi$ is most pretentious to the trivial character. If $\chi$ is even, then Theorem 2.9 of [Gol12] implies that

$$M(\chi) \ll \sqrt{q(\log q)^{2/3+o(1)}}. \quad \square$$

References

[Ank52] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55 (1952), 65–72.
[BGS13] Antal Balog, Andrew Granville, and Kannan Soundararajan, *Multiplicative functions in arithmetic progressions*, Ann. Math. Qué. 37 (2013), no. 1, 3–30.
[Bob] Jonathan Bober, *Averages of character sums*, in preparation.
[Gol10] Leo Goldmakher, *Character sums to smooth moduli are small*, Canad. J. Math. 62 (2010), no. 5, 1099–1115.
[Gol12] Leo Goldmakher, *Multiplicative mimicry and improvements to the Pólya-Vinogradov inequality*, Algebra Number Theory 6 (2012), no. 1, 123–163.
[GL12] Leo Goldmakher and Youness Lamzouri, *Lower bounds on odd order character sums*, Int. Math. Res. Not. IMRN 21 (2012), 5006–5013.
[GL] Leo Goldmakher and Youness Lamzouri, *Large even order character sums*, Proc. Amer. Math. Soc., to appear.
[Gra08] Andrew Granville, *Smooth numbers: computational number theory and beyond*, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008.
[GS07] Andrew Granville and K. Soundararajan, *Large character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. 20 (2007), no. 2, 357–384.
[Hil86] Adolf Hildebrand, *A note on Burgess’ character sum estimate*, C. R. Math. Rep. Acad. Sci. Canada VIII (1986), no. 1, 35–37.
[Hil88] Adolf Hildebrand, *Large values of character sums*, J. Number Theory 29 (1988), no. 3, 271–296.
[Ste72] P. J. Stephens, *Optimizing the size of $L(1, \chi)$*, Proc. London Math. Soc. (3) 24 (1972), 1–14.
