QUADRATIC NONRESIDUES BELOW THE BURGESS BOUND

WILLIAM D. BANKS AND VICTOR Z. GUO

Abstract. For any odd prime number \( p \), let \((\cdot|p)\) be the Legendre symbol, and let \( n_1(p) < n_2(p) < \cdots \) be the sequence of positive nonresidues modulo \( p \), i.e., \((n_k|p) = -1\) for each \( k \). In 1957, Burgess showed that the upper bound \( n_1(p) \ll \varepsilon p^{(4\sqrt{\varepsilon})^{-1}+\varepsilon} \) holds for any fixed \( \varepsilon > 0 \). In this paper, we prove that the stronger bound

\[
n_k(p) \ll p^{(4\sqrt{\varepsilon})^{-1} \exp \left( \sqrt{e^{-1} \log p \log \log p} \right)}
\]

holds for all odd primes \( p \), where the implied constant is absolute, provided that

\[
k \leq p^{(8\sqrt{\varepsilon})^{-1} \exp \left( \frac{1}{2} \sqrt{e^{-1} \log p \log \log p} - \frac{1}{2} \log \log p \right)}.
\]

For fixed \( \varepsilon \in (0, \frac{\pi-\pi}{2}) \), we also show that there is a number \( c = c(\varepsilon) > 0 \) such that for all odd primes \( p \) and either choice of \( \theta \in \{ \pm 1 \} \), there are \( \gg_{\varepsilon} y/(\log y)^{\varepsilon} \) natural numbers \( n \leq y \) with \((n|p) = \theta\) provided that

\[
y \geq p^{(4\sqrt{\varepsilon})^{-1} \exp \left( c(\log p)^{1-\varepsilon} \right)}.
\]

1. Introduction

For any odd prime \( p \), let \( n_1(p) \) denote the least positive quadratic nonresidue modulo \( p \); that is,

\[
n_1(p) := \min\{n \in \mathbb{N} : (n|p) = -1\},
\]

where \((\cdot|p)\) is the Legendre symbol. The first nontrivial bound on \( n_1(p) \) was given by Gauss [4, Article 129], who showed that \( n_1(p) < 2\sqrt{p} + 1 \) holds for every prime \( p \equiv 1 \pmod{8} \). Vinogradov [8] proved that the bound \( n_1(p) \ll_{\varepsilon} p^{(2\sqrt{\varepsilon})^{-1}+\varepsilon} \) holds for any \( \varepsilon > 0 \), and later, Burgess [1] extended this range by showing that the bound

\[
n_1(p) \ll_{\varepsilon} p^{(4\sqrt{\varepsilon})^{-1}+\varepsilon} \quad (1.1)
\]

holds for every fixed \( \varepsilon > 0 \); this result has not been improved since 1957.

The bound (1.1) implies that the inequality \( n_1(p) \leq p^{\frac{1}{4\sqrt{\varepsilon}} + f(p)} \) holds for all odd primes \( p \) with some function \( f \) such that \( f(p) \to 0 \) as \( p \to \infty \). Our aim in this note is to improve the bound (1.1) and to study quadratic nonresidues that lie below \( p^{(4\sqrt{\varepsilon})^{-1}+\varepsilon} \) for any fixed \( \varepsilon > 0 \). To this end, let \( n_1(p) < n_2(p) < \cdots \) be the sequence of positive nonresidues modulo \( p \).
Theorem 1. The bound

\[ n_k(p) \ll p^{(4\sqrt{7})^{-1}} \exp \left( \sqrt{e^{-1}} \log p \log \log p \right) \]  

holds for all odd primes \( p \) and all positive integers \( k \leq p^{(8\sqrt{7})^{-1}} \exp \left( \frac{1}{2} \sqrt{e^{-1}} \log p \log \log p - \frac{1}{2} \log \log p \right) \),

where the implied constant in (1.2) is absolute.

In a somewhat longer range, we establish the existence of many nonresidues.

Theorem 2. Let \( \varepsilon \in (0, \xi] \) be fixed, where

\[ \xi := \frac{\pi - 2}{9\pi - 2} = 0.04344896 \ldots \]

There is a number \( c = c(\varepsilon) > 0 \) such that for all odd primes \( p \) and either either choice of \( \theta \in \{ \pm 1 \} \), we have

\[ \# \{ n \leq y : (n|p) = \theta \} \gg \frac{y}{(\log y)^{\varepsilon}} \quad (y \geq p^{(4\sqrt{7})^{-1}} \exp \left( c(\log p)^{1-\varepsilon} \right)), \]

where the constant implied by \( \gg \varepsilon \) depends only on \( \varepsilon \).

Acknowledgement. We thank Kannan Soundararajan, whose suggestion led to a significant sharpening of our Theorem 1.

2. Preliminaries

Throughout the paper, we use the symbols \( O \) and \( \ll \) with their standard meanings; any implied constants are absolute unless otherwise specified in the notation.

Throughout the paper, we denote

\[ \lambda := \frac{5\pi - 2}{9\pi - 2} = 0.52172448 \ldots, \quad \eta := \frac{1}{4} - \frac{1}{2\pi} = 0.09084505 \ldots. \]

The constant \( \eta \) appears in Granville and Soundararajan [5, Proposition 1], which is one of our principal tools. In view of the definition of \( \xi \) in Theorem 2, we note that the following relation holds:

\[ \xi = \eta(1 - \lambda) = 2\lambda - 1. \]  

(2.1)

In a series of papers, Burgess [2, 3] established several well known bounds on relatively short character sums of the form

\[ S_\chi(M, N) := \sum_{M < n \leq M+N} \chi(n) \quad (M, N \in \mathbb{Z}, \ N \geq 1). \]

Here, we use a slightly stronger estimate which holds for characters of prime conductor; see Iwaniec and Kowalski [7, Equation (12.58)].
Lemma 3. Let $\chi$ be a primitive Dirichlet character of prime conductor $p$. For any integer $r \geq 1$ we have

$$|S_\chi(M, N)| \leq 30N^{1-1/r}p^{(r+1)/4r^2}(\log p)^{1/r} \quad (M, N \in \mathbb{Z}, \ N \geq 1).$$

Proposition 4. Let $\chi$ be a primitive Dirichlet character of prime conductor $p$, and put

$$M_\chi(x) := \frac{1}{x} \sum_{n \leq x} \chi(n) \quad (x \geq 1).$$

Then, uniformly for $c \in [0, (\log p)^{1/3}]$ we have

$$M_\chi(x) \ll (\log p)^{-c^2} \quad (x \geq p^{1/4} \exp (c\sqrt{\log p \log \log p})).$$

Proof. We can assume that $c > 0$ else the result is trivial. Let $z := e^{c\sqrt{\log p \log \log p}}$. For any integer $N \geq p^{1/4}z$ we have by Lemma 3:

$$|M_\chi(N)| = N^{-1}|S_\chi(0, N)| \ll N^{-1/4}p^{(r+1)/4r^2}(\log p)^{1/r} \leq p^{1/4r^2}z^{-1/r}(\log p)^{1/r}$$

for any integer $r \geq 1$. We choose

$$r := \left\lceil \frac{1}{2c} \left( \frac{\log p}{\log \log p} \right)^{1/2} \right\rceil,$$

where $\lceil \cdot \rceil$ is the greatest integer function. Since $c \leq (\log p)^{1/3}$ it follows that

$$p^{1/4r^2}z^{-1/r}(\log p)^{1/r} = \exp \left( \frac{\log p}{4r^2} - \frac{c(\log p \log \log p)^{1/2}}{r} + \frac{\log \log p}{r} \right)$$

$$= \exp \left( -c^2 \log \log p + O \left( \frac{(\log \log p)^{3/2}}{(\log p)^{1/6}} \right) \right) \ll (\log p)^{-c^2}.$$

This implies the stated bound. \qed

3. Proof of Theorem 2

Our proof of Theorem 2 relies on ideas of Granville and Soundararajan [5,6]. We begin with a technical lemma.

Lemma 5. Let $g$ be a completely multiplicative function such that $-1 \leq g(n) \leq 1$ for all $n \in \mathbb{N}$. Let $x$ be large, and suppose that $g(p) = 1$ for all $p \leq y := \exp ((\log x)^{1/3})$. Then, uniformly for $1/\sqrt{e} \leq \alpha \leq 1$, we have

$$1 - \tau(\alpha) + O\left((\log x)^{-\xi}\right) \leq M_g(x^\alpha) \leq 1 - \tau(\alpha) + \frac{1}{2} \tau(\alpha)^2 + O\left((\log x)^{-\xi}\right),$$

where

$$\tau(\alpha) := \sum_{p \leq x^\alpha} \frac{1 - g(p)}{p}.$$
Proof. Let \( \vartheta \) be the Chebyshev function \( \vartheta(u) := \sum_{p \leq u} \log p \), and define
\[
X(t) := \frac{1}{\vartheta(y^t)} \sum_{p \leq y^t} g(p) \log p.
\]

Put \( u_\alpha := (\log x^\alpha)/\log y = \alpha(\log x)^{1-\lambda} \). Using [5, Proposition 1] and taking into account (2.1), we derive the estimate
\[
M_\alpha(x^\alpha) = \sigma(u_\alpha) + O((\log x)^{-\xi}) \quad (1/\sqrt{e} \leq \alpha \leq 1),
\tag{3.1}
\]
where \( \sigma \) is the unique solution to the integral equation
\[
u \sigma(u) = \sigma \ast X(u) = \int_0^u \sigma(u - t)X(t) \, dt \quad \text{for} \quad u > 1,
\]
with the initial condition \( \sigma(u) = 1 \) for \( 0 \leq u \leq 1 \).

Moreover, using [5, Proposition 3.6] we see that
\[
1 - I_1(u_\alpha; X) \leq \sigma(u_\alpha) \leq 1 - I_1(u_\alpha; X) + I_2(u_\alpha; X),
\]
where
\[
I_1(u; X) := \int_1^u \frac{1 - X(t)}{t} \, dt,
\]
\[
I_2(u; X) := \int_1^u \int_{(t_1 + t_2 \leq u)} \frac{1 - X(t_1) - X(t_2)}{t_1 t_2} \, dt_1 \, dt_2.
\]

Removing the condition \( t_1 + t_2 \leq u \) we derive that \( I_2(u; X) \leq I_1(u; X)^2 \); hence, in view of the trivial bound \( \tau(\alpha) \ll \log \log x \) it suffices to establish the uniform estimate
\[
I_1(u_\alpha; X) = \tau(\alpha) + O((\log y)^{-1}) \quad (1/\sqrt{e} \leq \alpha \leq 1). \tag{3.2}
\]

For this, put \( S(v) := \sum_{p \leq v} (1 - g(p)) \log p \), and note that
\[
\tau(\alpha) = \int_y^{x^\alpha} \frac{dS(v)}{v \log v} = \left[ \frac{S(v)}{v \log v} \right]_y^{x^\alpha} + \int_y^{x^\alpha} \frac{S(v)(\log v + 1)}{(v \log v)^2} \, dv
\]
\[
= \int_y^{x^\alpha} \frac{S(v)}{v^2 \log v} \, dv + O((\log y)^{-1}),
\]
where we have used the bound \( S(v) \ll v \). Making the change of variables \( v = y^t, \, dv = y^t \log y \, dt \), and taking into account that \( S(y^t) = \vartheta(y^t)(1 - X(t)) \), we have
\[
\tau(\alpha) = \int_1^{\alpha} \frac{\vartheta(y^t)}{y^t} \frac{1 - X(t)}{t} \, dt + O((\log y)^{-1}).
\]

The estimate (3.2) now follows from the Prime Number Theorem in the form \( \vartheta(y^t) = y^t + O(y^t/\log y^t) \). \qed

The next statement is a variant of [6, Proposition 7.1].
Let $x$ be large, and let $f$ be a completely multiplicative function such that $-1 \leq f(n) \leq 1$ for all $n \in \mathbb{N}$. Then, uniformly for $1/\sqrt{e} \leq \alpha \leq 1$, we have

$$|M_f(x^\alpha)| \leq \max \{|\delta_1|, \frac{1}{2} + 2(\log \alpha)^2\} + O\left(\max \{|M_f(x)|, (\log x)^{-\varepsilon}\}\right),$$

where

$$\delta_1 := 1 - 2 \log(1 + \sqrt{e}) + 4 \int_{1}^{\sqrt{e}} \frac{\log u}{u+1} \, du = -0.656999 \ldots.$$

**Proof.** We follow the proof of [6, Proposition 7.1] closely, making use of the work in [5]. Let $y := \exp((\log x)^{\lambda})$, and let $g$ be the completely multiplicative function defined by

$$g(p) := \begin{cases} 
1 & \text{if } p \leq y, \\
 f(p) & \text{if } p > y.
\end{cases}$$

Using [5, Proposition 4.4] (with $S = [-1, 1]$ and $\varphi = \pi/2$) and taking into account (2.1), we derive the estimate

$$M_f(x^\alpha) = \Theta(f, y) M_g(x^\alpha) + O((\log x)^{-\varepsilon}),$$

where

$$\Theta(f, y) := \prod_{p \leq y} \left(1 - \frac{1}{p}\right) \left(1 - \frac{f(p)}{p}\right)^{-1}.$$

Since $|M_g(x^\alpha)| \leq 1$, we obtain (3.3) whenever $\Theta(f, y) \leq \frac{1}{2}$; thus, we can assume without loss of generality that $\Theta(f, y) \in [\frac{1}{2}, 1]$, and it suffices to show that

$$|M_g(x^\alpha)| \leq \max \{|\delta_1|, \frac{1}{2} + 2(\log \alpha)^2\} + O(B)$$

holds uniformly for $1/\sqrt{e} \leq \alpha \leq 1$, where

$$B := \max \{|M_f(x)|, (\log x)^{-\varepsilon}\}.$$

Applying Lemma 5 with $\alpha = 1$, we have

$$\tau(1) \geq 1 + O(B).$$

Further, by Mertens’ theorem we have for $1/\sqrt{e} \leq \alpha \leq 1$:

$$\tau(1) - \tau(\alpha) = \sum_{x^\alpha < p \leq x} \frac{1 - g(p)}{p} \leq \sum_{x^\alpha < p \leq x} \frac{2}{p} = 2 \log \alpha + O\left((\log x)^{-1}\right).$$

Consequently,

$$\tau(\alpha) \geq 1 - 2 \log \alpha + O(B).$$

Using [5, Theorem 5.1] together with (3.1), if $\tau(\alpha) \geq 1$ we have

$$|M_g(x^\alpha)| \leq |\delta_1| + O((\log x)^{-\varepsilon}) = |\delta_1| + O(B).$$
On the other hand, if \( 1 - 2 \log \alpha + O(B) \leq \tau(\alpha) \leq 1 \) we can apply Lemma 5 again to conclude that
\[
\left| M_p(x^\alpha) \right| \leq 1 - \tau(\alpha) + \frac{1}{2} \tau(\alpha)^2 + O(B) \leq \frac{1}{2} + 2(\log \alpha)^2 + O(B).
\]
Putting these estimates together, we obtain (3.4), which finishes the proof. \( \square \)

**Proof of Theorem 2.** Let \( \chi := \langle \cdot | p \rangle \) and let \( \varepsilon \in (0, \xi] \) and \( \theta \in \{ \pm 1 \} \) be fixed. Since
\[
\# \{ n \leq y : \chi(n) = \theta \} = \frac{1}{2} y \left( 1 + \theta M_x(y) + O(p^{-1}) \right),
\]
the result is easily proved for \( y > p \) (e.g., using Proposition 4). Thus, we can assume \( y \leq p \) in what follows. Moreover, it suffices to prove the theorem for all sufficiently large primes \( p \) (depending on \( \varepsilon \)).

Let \( \alpha \in \left[ \frac{1}{\sqrt[4]{e}}, 1 \right] \) and put \( x := y^{1/\alpha} \). Note that \( \log p = \log x = \log y \) since \( p^{(4\sqrt[4]{e})^{-1}} \leq y \leq p \). Applying Proposition 4, the bound \( M_{x}(x) \ll (\log x)^{-\varepsilon} \) holds provided that
\[
x \geq p^{1/4} \exp \left( \varepsilon^{-1/2} \sqrt{\log p \log \log p} \right),
\]
which we assume for the moment. Since \( \varepsilon \leq \xi \), Proposition 6 yields the bound
\[
\left| M_{x}(y) \right| = \left| M_{x}(x^{\alpha}) \right| \leq 1 - (2\sqrt{e} - 1) c_1 (\log p)^{-\varepsilon} + O_{\varepsilon} (\log x)^{-2\varepsilon}).
\]
In particular, for some sufficiently large \( c_2 > 0 \) (depending on \( \varepsilon \)) the bound
\[
\left| M_{x}(y) \right| = \left| M_{x}(x^{\alpha}) \right| \leq 1 - c_2 (\log y)^{-\varepsilon}
\]
holds. In view of (3.5) we obtain the stated result.

To verify (3.6), observe that \( \alpha^{-1} \geq \sqrt{e} - c_3 (\log p)^{-\varepsilon} \) with some number \( c_3 > 0 \) that depends only on \( \varepsilon \). If \( c > 0 \) and \( y \geq p^{(4\sqrt[4]{e})^{-1} e^{(\log p)^{1-\varepsilon}}} \), then
\[
\log x = \alpha^{-1} \log y \geq \left( \frac{1}{4\sqrt{e}} \log p + c (\log p)^{1-\varepsilon} \right) \left( \sqrt{e} - c_3 (\log p)^{-\varepsilon} \right)
\]
\[
= \frac{1}{4} \log p + \left( c \sqrt{e} - \frac{c_3}{4\sqrt{e}} - cc_3 (\log p)^{-\varepsilon} \right) (\log p)^{1-\varepsilon}.
\]
Hence, if \( c \) and \( p \) are large enough, depending only on \( \varepsilon \), then
\[
\log x \geq \frac{1}{4} \log p + \varepsilon^{-1/2} \sqrt{\log p \log \log p}
\]
as required. \( \square \)

### 4. Proof of Theorem 1

Let \( C > 0 \) be a fixed (absolute) constant to be determined below. Put
\[
E := p^{(4\sqrt[4]{e})^{-1}} \exp \left( \sqrt{e^{-1} \log p \log \log p} \right) \quad \text{and} \quad B := E^{1/2} (\log p)^{1/2}.
\]
Let $N := n_1(p)$ and $M := n_k(p)$, where $k$ is a positive integer such that
\[ k \leq CE^{1/2} (\log p)^{-1/2}. \tag{4.1} \]

To prove the theorem we need to show that $M \ll E$.

**Case 1:** $N \leq B$. If the interval $[1, 2k]$ contains at least $k$ nonresidues, then
\[ M \leq 2k \ll E^{1/2} (\log p)^{-1/2} \ll E \]
and we are done. If the interval $[1, 2k]$ contains fewer than $k$ nonresidues, then $[1, 2k]$ contains at least $k$ residues $m_1, \ldots, m_k$. Therefore, $Nm_1, \ldots, Nm_k$ are all nonresidues in $[1, 2kB]$, and we have (using (4.1) and the definition of $B$)
\[ M \leq 2kB \ll E. \]

**Case 2:** $N > B$. Applying Theorem 2 with $\varepsilon := \xi$, $y := B^{5/2}$ and $\theta := -1$, there is an absolute constant $c_1 > 0$ such that
\[ \# \{ n \leq B^{5/2} : (n|p) = -1 \} \gg \frac{B^{5/2}}{(\log B)^{\varepsilon}} \]
provided that
\[ B^{5/2} \geq p^{(4\sqrt{\pi})^{-1}} \exp \left( c_1 (\log p)^{1-\varepsilon} \right). \]

Since $B^{5/2} > E^{5/4}$ the latter inequality is easily satisfied for all large $p$; thus, if $p$ is large enough, then the $k$-th nonresidue $M = n_k(p)$ satisfies
\[ N \leq M \leq B^{5/2} < N^{5/2}. \]

Let $x \in (M, N^3)$, and note that $\log x = \log p = \log N$. Following an idea of Vinogradov, we see that the inequality $x < N^3$ implies that every nonresidue $n \leq x$ can be uniquely represented in the form $n = qm$, where $q$ is a prime nonresidue, and $m$ is a positive integer residue not exceeding $x/q$; this leads to the lower bound
\[ \sum_{n \leq x} (n|p) \geq x - 2 \sum_{\substack{n \leq x \\ N \leq q \leq x \\ (q|p) = -1}} \frac{x}{q} + O(1). \]

Since $M = n_k(p)$, there are at most $k$ prime nonresidues in $[N, M]$; thus,
\[ \sum_{n \leq x} (n|p) \geq x - \frac{2kx}{N} - 2 \sum_{M < q \leq x} \frac{x}{q} + O(1). \]

Recalling that $N > B = E^{1/2} (\log p)^{1/2}$ and using (4.1) together with the Prime Number Theorem, we derive the lower bound
\[ \sum_{n \leq x} (n|p) \geq x \left( 1 - \frac{2C}{\log p} - 2 \log \frac{\log x}{\log M} \right) + O \left( \frac{x}{(\log x)^{100}} \right). \]
Now let $x := e^{-3C} M^{\sqrt{e}}$. Since $-2 \log(1 - t) \geq 2t$ for all $t \in [0, \frac{1}{2}]$, for any sufficiently large $p$ (depending on the choice of $C$) we have

$$1 - 2 \log \frac{\log x}{\log M} = -2 \log \left(1 - \frac{3C}{\sqrt{e} \log M}\right) \geq \frac{6C}{\sqrt{e} \log M},$$

and thus

$$\frac{1}{x} \sum_{n \leq x} (n|p) \geq \frac{6C}{\sqrt{e} \log M} - \frac{2C}{\log p} + O\left(\frac{1}{(\log x)^{10}}\right).$$

Since $M \leq B^{5/2} \leq p$ for all large $p$, it follows that

$$\frac{1}{x} \sum_{n \leq x} (n|p) \geq \frac{C}{\log p}$$

if $p$ is large enough (depending on $C$). On the other hand, using Proposition 4 with $c = 1$, we see that there is an absolute constant $C_0 > 0$ such that

$$\frac{1}{x} \sum_{n \leq x} (n|p) \leq \frac{C_0}{\log p}$$

whenever $x \geq p^{1/4} e^{\log p \log \log p}$. If $C$ is initially chosen so that $C > C_0$, then these two bounds are incompatible unless

$$e^{-3C} M^{\sqrt{e}} \leq p^{1/4} \exp\left(\sqrt{\log p \log \log p}\right).$$

The theorem follows.

References

[1] D. A. Burgess, “The distribution of quadratic residues and non-residues.” Mathematika 4 (1957), 106–112.
[2] D. A. Burgess, “On character sums and $L$-series.” Proc. London Math. Soc. (3) 12 (1962), 193–206.
[3] D. A. Burgess, “On character sums and $L$-series. II.” Proc. London Math. Soc. (3) 13 (1963), 524–536.
[4] C. F. Gauss, Disquisitiones Arithmeticae. Leipzig, Fleischer, 1801.
[5] A. Granville and K. Soundararajan, “The spectrum of multiplicative functions.” Ann. of Math. (2) 153 (2001), no. 2, 407–470.
[6] A. Granville and K. Soundararajan, “Large character sums: Burgess’s theorem and zeros of $L$-functions.” Preprint, 2015. arXiv:1501.01804
[7] H. Iwaniec and E. Kowalski, Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.
[8] I. M. Vinogradov, “On the distribution of residues and nonresidues of powers.” J. Physico-Mathematical Soc. of Perm 1 (1918), 94–96.