PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 7, July 2017, Pages 2815–2826
http://dx.doi.org/10.1090/proc/13432
Article electronically published on December 8, 2016

BOUNDS FOR THE FIRST SEVERAL PRIME CHARACTER NONRESIDUES

PAUL POLLACK

(Communicated by Matthew A. Papanikolas)

Abstract. Let $\varepsilon > 0$. We prove that there are constants $m_0 = m_0(\varepsilon)$ and $\kappa = \kappa(\varepsilon) > 0$ for which the following holds: For every integer $m > m_0$ and every nontrivial Dirichlet character modulo m, there are more than m^κ primes $\ell \le m^{\frac{1}{4\sqrt{e}}+\varepsilon}$ with $\chi(\ell) \notin \{0,1\}$. The proof uses the fundamental lemma of the sieve, Norton's refinement of the Burgess bounds, and a result of Tenenbaum on the distribution of smooth numbers satisfying a coprimality condition. For quadratic characters, we demonstrate a somewhat weaker lower bound on the number of primes $\ell \le m^{\frac{1}{4}+\epsilon}$ with $\chi(\ell) = 1$.

1. Introduction

Let χ be a nonprincipal Dirichlet character. An integer n is called a χ-*nonresidue* if $\chi(n) \notin \{0,1\}$. Problems about character nonresidues go back to the beginnings of modern number theory. Indeed, one can read in Gauss's *Disquisitiones* that for primes $p \equiv 1 \pmod 8$ and $\chi(\cdot) = \left(\frac{p}{\cdot}\right)$, the smallest χ-nonresidue does not exceed $2\sqrt{p}+1$ [10, Article 129]. This was an auxiliary result required for Gauss's first proof of the quadratic reciprocity law.

In the early 20th century, I. M. Vinogradov initiated the study of how the quadratic residues and nonresidues modulo a prime p are distributed in the interval $[1, p-1]$. A particularly natural problem is to estimate the size of n_p, the smallest quadratic nonresidue modulo p. Vinogradov conjectured that $n_p \ll_\varepsilon p^\varepsilon$, for each $\varepsilon > 0$. By means of a novel estimate for character sums (independently discovered by Pólya), coupled with a clever sieving argument, he showed [24] that $n_p \ll_\varepsilon p^{\frac{1}{2\sqrt{e}}+\varepsilon}$. Burgess's character sum bounds [4], in conjunction with Vinogradov's methods, yield the sharper estimate

$$n_p \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}. \tag{1}$$

Fifty years of subsequent research has not led to any improvement in the exponent $\frac{1}{4\sqrt{e}}$. But generalizing (1), Norton showed that if χ is any nontrivial character modulo m, then the least χ-nonresidue is $O_\varepsilon(m^{1/4\sqrt{e}+\varepsilon})$. See [18, Theorem 1.30].

Since χ is completely multiplicative, the smallest χ-nonresidue is necessarily prime. In this note, we prove that there are actually many prime χ-nonresidues satisfying the Burgess–Norton upper bound.

Received by the editors August 24, 2015 and, in revised form, August 8, 2016.
2010 *Mathematics Subject Classification.* Primary 11A15; Secondary 11L40, 11N25.

Theorem 1.1. *For each $\varepsilon > 0$, there are numbers $m_0(\varepsilon)$ and $\kappa = \kappa(\varepsilon) > 0$ for which the following holds: For all $m > m_0$ and each nontrivial character $\chi \bmod m$, there are more than m^κ prime χ-nonresidues not exceeding $m^{\frac{1}{4\sqrt{e}}+\varepsilon}$.*

The problem of obtaining an upper bound on the first several prime character nonresidues was considered already by Vinogradov. In [24], he showed that for large p, there are at least $\frac{\log p}{7 \log\log p}$ prime quadratic nonresidues modulo p not exceeding

$$p^{\frac{1}{2}-\frac{1}{\log\log p}}.$$

For characters to prime moduli, a result resembling Theorem 1.1 was proved by Hudson in 1983 [15]. (See also Hudson's earlier investigations [12–14].) But even restricted to prime m, Theorem 1.1 improves on [15] in multiple respects. In [15], the exponent on p is $\frac{1}{4} + \varepsilon$ instead of $\frac{1}{4\sqrt{e}} + \varepsilon$, and the number of nonresidues produced is only $c_\varepsilon \frac{\log p}{\log\log p}$. Moreover, it is assumed in [15] that the order of χ is fixed. Stronger results than those of [15] were announced by Norton already in 1973 [17].[1] Unfortunately, a full account of Norton's work seems never to have appeared.

It becomes easier to produce small character nonresidues as the order of χ increases. This phenomenon was noticed by Vinogradov [25] and further investigated by Buhštab [3] and Davenport and Erdős [5]. To explain their results requires us to first recall the rudiments of the theory of smooth numbers. For each positive integer n, let $P^+(n)$ denote the largest prime factor of n, with the convention that $P^+(1) = 1$. A natural number n is called *y-smooth* (or *y-friable*) if $P^+(n) \le y$. For $x \ge y \ge 2$, we let $\Psi(x, y)$ be the count of y-smooth numbers up to x. We let ρ be Dickman's function, defined by

$$\rho(u) = 1 \text{ for } 0 \le u \le 1 \quad \text{and} \quad u\rho'(u) = -\rho(u-1) \quad \text{for } u > 1.$$

The functions $\Psi(x, y)$ and $\rho(u)$ are intimately connected: it is known that $\Psi(x, y) \sim x\rho(u)$, where $u := \frac{\log x}{\log y}$, in a wide range of x and y. In fact, Hildebrand [11] has shown that this asymptotic formula holds whenever $x \to \infty$, as long as

$$y \ge \exp((\log\log x)^{5/3+\lambda})$$

for some fixed positive λ. For this estimate to be useful, one needs to understand the behavior of $\rho(u)$. It is not hard to show that ρ is strictly decreasing for $u > 1$ and that $\rho(u) \le 1/\Gamma(u+1)$. So for any $k > 1$, there is a unique $u_k > 1$ with $\rho(u_k) = \frac{1}{k}$. Buhštab and, independently, Davenport and Erdős (developing ideas implicit in [25]) showed that if $\chi \bmod p$ has order $k \ge 2$, then the least χ-nonresidue is $O_{\varepsilon,k}(p^{1/2u_k+\varepsilon})$. If in their argument Burgess's method (which was not available at the time) is used in place of the Pólya–Vinogradov inequality, then $1/2u_k$ may be replaced by $1/4u_k$ [26]. We prove the following:

Theorem 1.2. *Let $\varepsilon > 0$ and $k_0 \ge 2$. There are numbers $m_0(\varepsilon, k_0)$ and $\kappa = \kappa(\varepsilon, k_0) > 0$ for which the following holds: For all $m > m_0$ and each nontrivial character $\chi \bmod m$ of order $k \ge k_0$, there are more than m^κ prime χ-nonresidues not exceeding $m^{\frac{1}{4u_{k_0}}+\varepsilon}$.*

[1] Norton claims in [17]: *Let $\varepsilon > 0$ and $k_0 \ge 2$. If $m \ge 3$ and $[(\mathbf{Z}/m\mathbf{Z})^\times : (\mathbf{Z}/m\mathbf{Z})^{\times k}] \ge k_0$, then each of the smallest $\lfloor \log m/\log\log m \rfloor$ primes not dividing m that are kth power nonresidues modulo m is $\ll_{\varepsilon,k_0} n^{1/4u_{k_0}+\varepsilon}$.* Here u_{k_0} has the same meaning as in our introduction.

Remarks.

- It follows readily from the definition that $\rho(u) = 1 - \log u$ for $1 \le u \le 2$, and so $u_2 = e^{1/2} = 1.6487\ldots$ and $u_3 = e^{2/3} = 1.9477\ldots$. For $k > 3$, it does not seem that u_k has a simple closed form expression.
- Theorem 1.1 is the special case $k_0 = 2$ of Theorem 1.2.

One might compare Theorem 1.1 for the quadratic character modulo a prime p with a result of Banks–Garaev–Heath-Brown–Shparlinski [1]. They show that for each fixed $\varepsilon > 0$ and each $N \ge p^{1/4\sqrt{e}+\varepsilon}$, the proportion of quadratic nonresidues modulo p in $[1, N]$ is $\gg_\varepsilon 1$ for all primes $p > p_0(\varepsilon)$.

Our arguments use the ideas of Vinogradov and Davenport–Erdős but take advantage of modern developments in sieve methods and the theory of smooth numbers. A variant of the Burgess bounds developed by Norton also plays an important role. We note that an application of the sieve that is similar in spirit to ours appears in work of Bourgain and Lindenstrauss [2, Theorem 5.1].[2]

It is equally natural to ask for small prime character *residues*, i.e., primes ℓ with $\chi(\ell) = 1$. The most significant unconditional result in this direction is due to Linnik and A. I. Vinogradov [23]. They showed that if χ is the quadratic character modulo a prime p, then the smallest prime ℓ with $\chi(\ell) = 1$ satisfies $\ell \ll_\varepsilon p^{1/4+\varepsilon}$. More generally, Elliott [8] proved that when χ has order k, the least such ℓ is $O_{k,\varepsilon}(p^{\frac{k-1}{4}+\epsilon})$. As Elliott notes, this bound is only interesting for small values of k; otherwise, it is inferior to what follows from known forms of Linnik's theorem on primes in progressions. For extensions of the Linnik–Vinogradov method in a different direction, see [19, 20].

Our final result is a partial analogue of Theorem 1.1 for prime residues of quadratic characters. Regrettably, the number of primes produced falls short of a fixed power of m.

Theorem 1.3. *Let $\varepsilon > 0$ and let $A > 0$. There is an $m_0 = m_0(\varepsilon, A)$ with the following property: If $m > m_0$ and χ is a quadratic character modulo m, then there are at least $(\log m)^A$ primes $\ell \le m^{\frac{1}{4}+\varepsilon}$ with $\chi(\ell) = 1$.*

Results of the sort proven here have direct consequences for prime splitting in cyclic extensions of $\mathbf{Q}$. For example, Theorem 1.1 (respectively, Theorem 1.3) implies that there are more than $|\Delta|^\kappa$ inert (respectively, more than $(\log|\Delta|)^A$ split) primes $p \le |\Delta|^{\frac{1}{4\sqrt{e}}+\varepsilon}$ (respectively, $p \le |\Delta|^{\frac{1}{4}+\varepsilon}$) in the quadratic field of discriminant Δ as soon as $|\Delta|$ is large enough in terms of ε (and A).

2. Small prime nonresidues: Proofs of Theorems 1.1 and 1.2

2.1. **Preparation.** As might be expected, the Burgess bounds play the key role in our analysis. The following version is due to Norton (see [18, Theorem 1.6]).

Proposition 2.1. *Let χ be a nontrivial character modulo m of order dividing k. Let r be a positive integer, and let $\epsilon > 0$. For all $x > 0$,*

$$\sum_{n \le x} \chi(n) \ll_{\epsilon,r} R_k(m)^{1/r} x^{1-\frac{1}{r}} m^{\frac{r+1}{4r^2}+\epsilon}.$$

[2] A special case of their result: *Given $\varepsilon > 0$, there is an $\alpha > 0$ such that $\sum_{p^\alpha \le \ell \le p^{1/4+\varepsilon}, \left(\frac{\ell}{p}\right)=-1} \frac{1}{\ell} > \frac{1}{2} - \varepsilon$, for all $p > p_0(\varepsilon)$.*

Here

$$R_k(m) = \min\left\{M(m)^{3/4}, Q(k)^{9/8}\right\},$$

where

$$M(m) = \prod_{p^e \| m,\ e \geq 3} p^e \qquad \text{and} \quad Q(k) = \prod_{p^e \| k,\ e \geq 2} p^e.$$

The factor of $R_k(m)^{1/r}$ *can be omitted if* $r \leq 3$.

Another crucial tool is a theorem of Tenenbaum concerning the distribution of smooth numbers satisfying a coprimality condition. For $x \geq y \geq 2$, let

$$\Psi_q(x,y) = \#\{n \leq x : \gcd(n,q) = 1, P^+(n) \leq y\}.$$

Proposition 2.2. *For positive integers* q *and real numbers* x, y *satisfying*

$$P^+(q) \leq y \leq x \quad \text{and} \quad \omega(q) \leq y^{1/\log(1+u)},$$

we have

$$\Psi_q(x,y) = \frac{\varphi(q)}{q}\Psi(x,y)\left(1 + O\left(\frac{\log(1+u)\log(1+\omega(q))}{\log y}\right)\right).$$

As before, u *denotes the ratio* $\log x/\log y$.

Proof. This is the main result of [21] in the case $c = 1$. □

Remark. If q' is the largest divisor of q supported on the primes not exceeding y, then $\Psi_q(x,y) = \Psi_{q'}(x,y)$. So the assumption in Proposition 2.2 that $P^+(q) \leq y$ does not entail any loss of generality.

Theorem 1.2 will be deduced from two variant results claiming weaker upper bounds.

Theorem 2.3. *Let* $\varepsilon > 0$ *and* $k_0 \geq 2$. *There are numbers* $m_0(\varepsilon, k_0)$ *and* $\kappa = \kappa(\varepsilon, k_0) > 0$ *for which the following holds: For all* $m > m_0$ *and each nontrivial character* χ *mod* m *of order* $k \geq k_0$, *there are more than* m^κ *prime* χ*-nonresidues not exceeding* $m^{\frac{1}{3uk_0}+\varepsilon}$.

Theorem 2.4. *Let* $\varepsilon > 0$ *and* $k_0 \geq 2$. *There are numbers* $m_0(\varepsilon, k_0)$ *and* $\kappa = \kappa(\varepsilon, k_0) > 0$ *for which the following holds: For all* $m > m_0$ *and each nontrivial character* χ *mod* m *of order* $k \geq k_0$, *there are more than* m^κ *prime* χ*-nonresidues not exceeding* $R_k(m)m^{\frac{1}{4uk_0}+\varepsilon}$. *Here* $R_k(m)$ *is as defined in Proposition* 2.1.

The proof of Theorem 2.4 is given in detail in the next section. We include only a brief remark about the proof of Theorem 2.3, which is almost entirely analogous (but slightly simpler). We then present the derivation of Theorem 1.2 from Theorems 2.3 and 2.4. We remind the reader that Theorem 1.1 is the special case $k_0 = 2$ of Theorem 1.2.

2.2. **Proof of Theorem 2.4.** We let χ be a nontrivial character modulo m of order $k \geq k_0$, where $k_0 \geq 2$ is fixed. With $\delta \in (0, \frac{1}{4})$, we set

$$x = R_k(m) \cdot m^{\frac{1}{4}+\delta}, \quad y = x^{\frac{1}{uk_0}+\delta}.$$

To prove Theorem 2.4, it suffices to show that for all large m (depending only on k_0 and δ), there are at least x^κ prime χ-nonresidues in $[1, y]$ for a certain constant $\kappa = \kappa(k_0, \delta) > 0$.

Let q be the product of the prime χ-nonresidues in $[1, y]$. Note that $\gcd(q, m) = 1$, from the definition of a χ-nonresidue. Our strategy is to estimate

$$\sum_{\substack{n\le x\\ \gcd(n,mq)=1}} (1+\chi(n)+\chi^2(n)+\cdots+\chi^{k-1}(n)) \tag{2}$$

in two different ways.

We first derive a lower bound on (2) under the assumption that there are not so many prime χ-nonresidues in $[1, y]$.

Lemma 2.5. *There are constants $\eta = \eta(\delta, k_0) > 0$, $\kappa = \kappa(\delta, k_0) > 0$, and $m_0 = m_0(\delta, k_0)$ with the following property: If $m > m_0$ and $\omega(q) \le x^\kappa$, then*

$$\sum_{\substack{n\le x\\ \gcd(n,mq)=1}} (1+\chi(n)+\cdots+\chi(n)^{k-1}) \ge \left(1+\frac{2k}{3}\eta\right)\frac{\varphi(mq)}{mq}x.$$

Proof. Observe that

$$\begin{aligned}\sum_{\substack{n\le x\\ \gcd(n,mq)=1}} (1+\chi(n)+\cdots+\chi(n)^{k-1}) &= k \sum_{\substack{n\le x\\ \gcd(n,q)=1,\ \chi(n)=1}} 1\\ &\ge k \sum_{\substack{n\le x\\ \gcd(n,mq)=1\\ p\mid n\Rightarrow p\le y}} 1\\ &= k\cdot\Psi_{mq}(x,y).\end{aligned}$$

We estimate $\Psi_{mq}(x, y)$ using Proposition 2.2 and the succeeding remark. We have $u \asymp_{k_0} 1$ or, equivalently, $\log y \asymp_{k_0} \log x$. So if κ is sufficiently small in terms of k_0 and $\omega(q) \le x^\kappa$, Proposition 2.2 gives

$$\begin{aligned}\Psi_{mq}(x,y) &= \left(\Psi(x,y)\prod_{\substack{p\mid mq\\ p\le y}}\left(1-\frac{1}{p}\right)\right)\left(1+O_{k_0}\left(\frac{\log(1+x^\kappa)}{\log x}\right)\right)\\ &\ge \Psi(x,y)\frac{\varphi(mq)}{mq}\left(1+O_{k_0}\left(\frac{\log(1+x^\kappa)}{\log x}\right)\right).\end{aligned}$$

Now the result of Hildebrand quoted in the introduction (or a much more elementary theorem) shows that $\Psi(x, y) = \Psi(x, x^{\frac{1}{u_{k_0}}+\delta}) \ge (\frac{1}{k_0}+\eta)x$ for a certain $\eta = \eta(k_0, \delta) > 0$ and all large x. So if κ is fixed sufficiently small, depending on k_0 and δ, and x is sufficiently large, then

$$\Psi_{mq}(x,y) > \left(\frac{1}{k_0}+\frac{2}{3}\eta\right)\frac{\varphi(mq)}{mq}x.$$

Hence,

$$\sum_{\substack{n\le x\\ \gcd(n,q)=1}} (1+\chi(n)+\cdots+\chi(n)^{k-1}) \ge \left(\frac{k}{k_0}+\frac{2k}{3}\eta\right)\frac{\varphi(mq)}{mq}x \ge \left(1+\frac{2k}{3}\eta\right)\frac{\varphi(mq)}{mq}x.$$

□

We turn next to an upper bound.

Lemma 2.6. *Let $\beta > 0$. There are numbers $\eta' = \eta'(\delta) > 0$, $\kappa' = \kappa'(\delta, \beta) > 0$ and $m_0 = m_0(\delta, \beta)$ with the following property: If $m > m_0$ and $\omega(q) \le x^{\kappa'}$, then*

$$\sum_{\substack{n \le x \\ \gcd(n, mq) = 1}} (1 + \chi(n) + \chi(n)^2 + \cdots + \chi(n)^{k-1}) \le (1 + \beta) \frac{\varphi(mq)}{mq} x + O_\delta(k x^{1-\eta'}).$$

Proof. We let $\mathcal{A} = \{n \le x : \gcd(n, m) = 1,\ \chi(n) = 1\}$ and observe that

$$\sum_{\substack{n \le x \\ \gcd(n, mq) = 1}} (1 + \chi(n) + \chi(n)^2 + \cdots + \chi(n)^{k-1}) = k \sum_{\substack{n \in \mathcal{A} \\ \gcd(n, q) = 1}} 1. \tag{3}$$

We apply the fundamental lemma of the sieve to estimate the right-hand sum. (The precise form of the fundamental lemma is not so important, but we have in mind [7, Theorem 4.1, p. 29].) Let $d \in [1, x]$ be a squarefree integer dividing q. Then

$$\sum_{\substack{n \in \mathcal{A} \\ d \mid n}} 1 = \frac{1}{k} \sum_{\substack{n \le x \\ \gcd(n, m) = 1,\ d \mid n}} (1 + \chi(n) + \cdots + \chi(n)^{k-1}).$$

For each $j = 0, 1, 2, \ldots, k-1$,

$$\sum_{\substack{n \le x \\ \gcd(n, m) = 1,\ d \mid n}} \chi^j(n) = \chi^j(d) \sum_{\substack{e \le x/d \\ \gcd(e, m) = 1}} \chi^j(e).$$

When $j = 0$, the right-hand side is $\frac{x}{d} \frac{\varphi(m)}{m} + O_\epsilon(m^\epsilon)$ by a straightforward inclusion-exclusion. For $j \in \{1, 2, \ldots, k-1\}$, Proposition 2.1 gives

$$\begin{aligned} \sum_{\substack{e \le x/d \\ \gcd(e, m) = 1}} \chi^j(e) = \sum_{e \le x/d} \chi^j(e) \sum_{\substack{f \mid e \\ f \mid m}} \mu(f) &= \sum_{f \mid m} \mu(f) \chi^j(f) \sum_{g \le x/df} \chi^j(g) \\ &\ll_{\epsilon, r} R_k(m)^{1/r} x^{1 - \frac{1}{r}} d^{-1 + \frac{1}{r}} m^{\frac{r+1}{4r^2} + \epsilon} \sum_{f \mid m} f^{-1 + \frac{1}{r}} \\ &\ll_\epsilon R_k(m)^{1/r} x^{1 - \frac{1}{r}} d^{-1 + \frac{1}{r}} m^{\frac{r+1}{4r^2} + 2\epsilon}; \end{aligned}$$

here $r \ge 2$ and $\epsilon > 0$ are parameters to be chosen. (We used in the last step that the sum on f has only $O_\epsilon(m^\epsilon)$ terms, each of which is $O(1)$.) Assembling the preceding estimates,

$$\sum_{\substack{n \in \mathcal{A} \\ d \mid n}} 1 = \frac{x}{dk} \frac{\varphi(m)}{m} + r(d), \quad \text{where} \quad r(d) \ll_{\epsilon, r} R_k(m)^{1/r} x^{1 - \frac{1}{r}} d^{-1 + \frac{1}{r}} m^{\frac{r+1}{4r^2} + 2\epsilon}.$$

By the fundamental lemma, for any choices of real parameters $z \ge 2$ and $v \ge 1$ with $z^{2v} < x$,

$$\begin{aligned} \sum_{\substack{n \in \mathcal{A} \\ \gcd(n, q) = 1}} 1 \le \sum_{\substack{n \in \mathcal{A} \\ p \mid \gcd(n, q) \Rightarrow p \ge z}} 1 &= \left(\frac{x}{k} \frac{\varphi(m)}{m} \prod_{\substack{p \mid q \\ p < z}} \left(1 - \frac{1}{p}\right) \right) \left(1 + O(v^{-v})\right) \\ &\quad + O_{\epsilon, r}\left(R_k(m)^{1/r} x^{1 - \frac{1}{r}} m^{\frac{r+1}{4r^2} + 2\epsilon} \sum_{\substack{d < z^{2v} \\ d \mid q}} \mu^2(d) 3^{\omega(d)} d^{-1 + \frac{1}{r}} \right). \end{aligned}$$

We now make a choice of parameters. Let $r = \lceil \frac{1}{2\delta} \rceil$ (so that $\delta \geq \frac{1}{2r}$). Since $x = R_k(m) \cdot m^{1/4+\delta}$, we have

$$R_k(m)^{1/r} x^{1-\frac{1}{r}} m^{\frac{r+1}{4r^2}} = x \cdot m^{-\frac{1}{4r}-\delta/r} m^{\frac{r+1}{4r^2}} = x \cdot m^{\frac{1}{r}(\frac{1}{4r}-\delta)} \leq x \cdot m^{-\frac{\delta}{4r^2}}.$$

We take $\epsilon = \frac{\delta}{16r^2}$, so that

$$m^{2\epsilon} = m^{\frac{\delta}{8r^2}}.$$

Since $r \geq 2$ and $3^{\omega(d)} \ll d^{1/2}$, each term in the sum on d is $O(1)$. Putting it all together, the O-term above is

$$\ll_\delta x \cdot m^{-\frac{\delta}{4r^2}} \cdot m^{\frac{\delta}{8r^2}} \cdot z^{2v}.$$

Since $x = R_k(m) \cdot m^{1/4+\delta} \leq m^{3/4} \cdot m^{1/4+\delta} < m^2$, this upper bound is $\ll_\delta x^{1-\frac{\delta}{16r^2}} z^{2v}$. Taking $z = x^{\frac{\delta}{64r^2 v}}$ gives a final upper bound on the O-term of

$$\ll_\delta x^{1-\eta'}, \quad \text{where} \quad \eta' = \frac{\delta}{32r^2}.$$

Turning attention to the main term, we fix v large enough that the factor $1 + O(v^{-v})$ is smaller than $1 + \frac{1}{2}\beta$. Then our main term above does not exceed

$$\frac{x}{k}\frac{\varphi(mq)}{mq}\left(1+\frac{1}{2}\beta\right)\prod_{\substack{p|q\\ p\geq z}}\left(1-\frac{1}{p}\right)^{-1} \leq \frac{x}{k}\frac{\varphi(mq)}{mq}\left(1+\frac{1}{2}\beta\right)\exp\left(2\sum_{\substack{p|q\\ p\geq z}}\frac{1}{p}\right)$$
$$\leq \frac{x}{k}\frac{\varphi(mq)}{mq}\left(1+\frac{1}{2}\beta\right)\exp(2\omega(q)z^{-1}).$$

Take $\kappa' = \frac{\delta}{128r^2 v}$. Under the assumption that $\omega(q) \leq x^{\kappa'}$, we have $2\omega(q)z^{-1} \leq 2x^{-\delta/128r^2 v}$ and $\exp(2\omega(q)z^{-1}) = 1 + O(x^{-\delta/128r^2 v})$. So once x (or equivalently, m) is large enough, our main term is smaller than $\frac{x}{k}\frac{\varphi(mq)}{mq}(1+\beta)$. So we have shown that for large m,

$$\sum_{\substack{n\in\mathcal{A}\\ \gcd(n,q)=1}} 1 \leq \frac{x}{k}\frac{\varphi(mq)}{mq}(1+\beta) + O_\delta(x^{1-\eta'}).$$

Recalling (3) finishes the proof. □

Completion of the proof of Theorem 2.4. We keep the notation from earlier in this section. Let η, κ be as specified in Lemma 2.5. With $\beta = \eta/2$, choose η' and κ' as in Lemma 2.6. If m is large and we assume that

$$\omega(q) \leq x^{\kappa''}, \quad \text{where} \quad \kappa'' = \min\{\kappa, \kappa'\},$$

then these lemmas imply that

$$\left(1+\frac{2k}{3}\eta\right)\frac{\varphi(mq)}{mq}x \leq \left(1+\frac{1}{2}\eta\right)\frac{\varphi(mq)}{mq}x + O_\delta(kx^{1-\eta'}).$$

Rearranging,

$$k\eta\frac{\varphi(mq)}{mq}x \ll \frac{4k-3}{6}\eta \cdot \frac{\varphi(mq)}{mq}x \ll_\delta kx^{1-\eta'},$$

and so

$$\frac{mq}{\varphi(mq)} \gg_{k_0,\delta} x^{\eta'}.$$

Noting that $m < x^4$ and $q \le y^{\omega(q)} \le x^{\omega(q)}$, we see that for large x,

$$\frac{mq}{\varphi(mq)} \ll \log\log(mq+2) \ll \log\log x + \log(\omega(q)+2) \ll \log x.$$

Comparing with the above lower bound, we see that x, and hence m, is bounded. Turning it around, for m large enough, there are at least $x^{\kappa''}$ prime χ-nonresidues in $[1, y]$. □

Sketch of the proof of Theorem 2.3. The proof of Theorem 2.3 is quite similar, except that now we take $x = m^{1/3+\delta}$. With this choice of x, we can apply the Burgess bounds with $r = 3$, which allows us to omit the factor of $R_k(m)$ in the resulting estimates. □

2.3. **Deduction of Theorem 1.2.** Let $\varepsilon > 0$ and $k_0 \ge 2$ be fixed. Let χ be a nonprincipal character mod m of order k, where $k \ge k_0$. We would like to show that as long as m is large enough there must be at least m^κ prime χ-nonresidues not exceeding $x^{1/4u_{k_0}+\varepsilon}$, for a certain $\kappa = \kappa(\varepsilon, k_0) > 0$. Let k_1 be the smallest positive integer with $3u_{k_1} > 4u_{k_0}$. If $k \ge k_1$, apply Theorem 2.3: We find that for large m, there are at least m^{κ_0} prime χ-nonresidues

$$\le m^{\frac{1}{3u_{k_1}}+\varepsilon} \le m^{\frac{1}{4u_{k_0}}+\varepsilon},$$

where $\kappa_0 = \kappa(\varepsilon, k_1)$ in the notation of Theorem 2.3. Suppose instead that $k_0 \le k < k_1$. Then $R_k(m)$ is bounded in terms of k_0. Theorem 2.4 thus shows that for large m, there are at least m^{κ_1} prime χ-nonresidues

$$\le R_k(m) m^{\frac{1}{4u_{k_0}}+\varepsilon/2} \le m^{\frac{1}{4u_{k_0}}+\varepsilon},$$

where $\kappa_1 = \kappa(\varepsilon/2, k_0)$ in the notation of Theorem 2.4. Theorem 1.2 follows with $\kappa = \min\{\kappa_0, \kappa_1\}$.

Remark. By a minor modification of our proof, one can establish the following more general result. Theorem 1.2 corresponds to the case $H = \ker\chi$.

Theorem 2.7. *Let $\varepsilon > 0$ and $k_0 \ge 2$. There are numbers $m_0(\varepsilon, k_0)$ and $\kappa = \kappa(\varepsilon, k_0) > 0$ for which the following holds: For all $m > m_0$ and every proper subgroup H of $G = (\mathbf{Z}/m\mathbf{Z})^\times$ of index $k \ge k_0$, there are more than m^κ primes ℓ not exceeding $m^{\frac{1}{4u_{k_0}}+\varepsilon}$ with $\ell \nmid m$ and $\ell \bmod m \notin H$.*

This strengthens [18, Theorem 1.20], where the bound $O_{k_0,\epsilon}(m^{\frac{1}{4u_{k_0}}+\varepsilon})$ is established for the first such prime ℓ.

The main idea in the proof of the generalization is to replace $1 + \chi(n) + \cdots + \chi(n)^{k-1}$ with $\sum_{\chi \in \widehat{G/H}} \chi(n)$, where $\widehat{G/H}$ denotes the group of characters χ mod m with $\ker\chi \supset H$. We leave the remaining details to the reader.

3. Small prime residues of quadratic characters: Proof of Theorem 1.3

The next proposition is a variant of [23, Theorem 2]. Given a character χ, we let $r_\chi(n) = \sum_{d|n} \chi(d)$. Since χ will be clear from context, we will suppress the subscript.

Proposition 3.1. *For each $\epsilon > 0$, there is a constant $\eta = \eta(\epsilon) > 0$ for which the following holds: If χ is a quadratic character modulo m and $x \geq m^{1/4+\epsilon}$, then*

$$\sum_{n\leq x} r(n) = L(1,\chi)x + O_\epsilon(x^{1-\eta}).$$

Proof. With $\upsilon = \frac{1/4+\epsilon/2}{1/4+\epsilon}$, put $y = x^\upsilon$, so that $y \geq m^{\frac{1}{4}+\frac{1}{2}\epsilon}$. Put $z = x/y$. By Dirichlet's hyperbola method,

$$\sum_{n\leq x} r(n) = \sum_{d\leq y}\chi(d)\sum_{e\leq x/d} 1 + \sum_{e\leq z}\sum_{d\leq x/e}\chi(d) - \sum_{d\leq y}\chi(d)\sum_{e\leq z} 1. \tag{4}$$

By Proposition 2.1 (with $k = 2$, so that $R_k(m)^{1/r} = 1$), there is an $\eta_0 = \eta_0(\epsilon) > 0$ with $\sum_{d\leq T}\chi(d) \ll_\epsilon T^{1-\eta_0}$ for all $T \geq y$. Thus, the second double sum on the right of (4) is $\ll_\delta x^{1-\eta_0}\sum_{e\leq z} e^{\eta_0-1} \ll_\delta x(z/x)^{\eta_0} = xy^{-\eta_0}$. Similarly, the third double sum is $\ll_\epsilon zy^{1-\eta_0} = xy^{-\eta_0}$. Finally,

$$\begin{aligned}\sum_{d\leq y}\chi(d)\sum_{e\leq x/d} 1 = \sum_{d\leq y}\chi(d)\left(\frac{x}{d} + O(1)\right) &= xL(1,\chi) - x\sum_{d>y}\frac{\chi(d)}{d} + O(y)\\ &= xL(1,\chi) + O_\epsilon(xy^{-\eta_0}) + O(y).\end{aligned}$$

(Here the sum on $d > y$ has been handled by partial summation.) Collecting our estimates and keeping in mind that $y = x^\upsilon$, we obtain the theorem with η defined by $1 - \eta = \max\{\upsilon, 1 - \upsilon\eta_0\}$. □

Proof of Theorem 1.3. Let $\varepsilon \in (0, \frac{1}{4})$ and let χ be a quadratic character modulo m. Let

$$x = m^{\frac{1}{4}+\varepsilon},$$

and let q be the product of the primes $\ell \leq x$ with $\chi(\ell) = 1$. We suppose that $\omega(q) \leq (\log m)^A$, and we show that this implies that m is bounded by a constant depending on ε and A. Throughout this proof, we suppress any dependence on ε and A in our O-notation.

By Proposition 3.1,

$$\sum_{n\leq x} r(n) = L(1,\chi)\cdot x + O(x^{1-\eta}). \tag{5}$$

We can estimate the sum in a second way. Observe that

$$r(n) = \prod_{\ell^e \| n}(1 + \chi(\ell) + \cdots + \chi(\ell^e)) \geq 0. \tag{6}$$

Hence, if the subset $\mathcal{S}$ of $[1, x]$ is chosen to contain the support of $r(n)$ on $[1, x]$, then

$$0 \leq \sum_{n\leq x} r(n) \leq \#\mathcal{S}\cdot\left(\max_{n\in\mathcal{S}} r(n)\right).$$

Examining the expression in (6) for $r(n)$, we see that $\mathcal{S}$ can be chosen as the set of $n \leq x$ where every prime that appears to the first power in the factorization of n divides mq. For each $n \in \mathcal{S}$, we can write $n = n_1n_2$, where n_1 is a squarefree divisor of mq and n_2 is squarefull. The number of elements of $\mathcal{S}$ with $n_2 > x^{1/2}$ is $O(x^{3/4})$. For the remaining elements of $\mathcal{S}$, we have $n_1 \leq x/n_2$ and n_1 is a squarefree product of primes dividing mq. There is a bijection

$$\iota\colon \{\text{squarefree divisors of } mq\} \to \{\text{squarefrees composed of the first } \omega(mq) \text{ primes}\}$$

with $\iota(r) \le r$ for all r. Hence, given n_2, the number of choices for n_1 is at most the number of integers in $[1, x/n_2]$ supported on the product of the first $\omega(mq)$ primes. By our assumption on $\omega(q)$, those primes all belong to the interval $[1, (\log x)^{A+1}]$ once x is large. Hence, given n_2, the number of possible values of n_1 is at most

$$\Psi(x/n_2, (\log x)^{A+1}).$$

For fixed $\theta \ge 1$, a classical theorem of de Bruijn [6] asserts that $\Psi(X, (\log X)^\theta) = X^{1-\frac{1}{\theta}+o(1)}$, as $X \to \infty$. Since $x/n_2 \ge x^{1/2}$, we deduce that

$$\Psi(x/n_2, (\log x)^{A+1}) \le (x/n_2)^{1-\frac{1}{A+2}}$$

if x is large. Summing on squarefull $n_2 \le x^{1/4}$, we see that the number of elements of $\mathcal{S}$ arising in this way is $O(x^{1-\frac{1}{A+2}})$. Hence,

$$\#\mathcal{S} \ll x^{3/4} + x^{1-\frac{1}{A+2}} \ll x^{1-\eta'}, \quad \text{where} \quad \eta' = \min\left\{\frac{1}{4}, \frac{1}{A+2}\right\}.$$

Since $r(n) \le \tau(n) \ll x^{\eta'/2}$ for $n \le x$,

$$\sum_{n \le x} r(n) \ll \#\mathcal{S} \cdot x^{\eta'/2} \ll x^{1-\eta'/2}. \tag{7}$$

Comparing (5) and (7) gives

$$L(1, \chi) \ll x^{-\min\{\eta'/2, \eta\}}.$$

But for large x, this contradicts Siegel's theorem [16, Theorem 11.14, p. 372]. □

Remark. Any improvement on Siegel's lower bound for $L(1, \chi)$ would boost the number of ℓ's produced in Theorem 1.3. Substantial improvements of this kind would have other closely related implications. For example, a simple modification of an argument of Wolke [27] shows that for any quadratic character χ mod m,

$$\sum_{\substack{\ell \le m \\ \chi(\ell)=1}} \frac{1}{\ell} \ge \frac{1}{2} \log\left(\frac{\varphi(m)}{m} L(1, \chi) \log m\right) + O(1),$$

where the $O(1)$ constant is absolute. (Here is the short proof: By Proposition 3.1, $\frac{1}{m}\sum_{n \le m} r(n) \gg L(1, \chi)$. On the other hand, [22, Theorem 5, p. 308] yields $\frac{1}{m}\sum_{n \le m} r(n) \ll \frac{1}{\log m}\sum_{n \le m} \frac{r(n)}{n} \ll \frac{1}{\log m} \cdot \frac{m}{\varphi(m)} \cdot \exp\left(2\sum_{\ell \le m,\ \chi(\ell)=1} \frac{1}{\ell}\right)$.)

Acknowledgments

This work was motivated in part by observations made on `MathOverflow` by "GH from MO" [9]. The author is also grateful to "Lucia" for pointing out there the work of Bourgain–Lindenstrauss. He thanks Enrique Treviño and the referee for useful feedback. This research was supported by NSF award DMS-1402268.

References

[1] W. D. Banks, M. Z. Garaev, D. R. Heath-Brown, and I. E. Shparlinski, *Density of non-residues in Burgess-type intervals and applications*, Bull. Lond. Math. Soc. **40** (2008), no. 1, 88–96, DOI 10.1112/blms/bdm111. MR2409181

[2] Jean Bourgain and Elon Lindenstrauss, *Entropy of quantum limits*, Comm. Math. Phys. **233** (2003), no. 1, 153–171, DOI 10.1007/s00220-002-0770-8. MR1957735

[3] A. A. Buhštab, *On those numbers in an arithmetic progression all prime factors of which are small in order of magnitude* (Russian), Doklady Akad. Nauk SSSR (N.S.) **67** (1949), 5–8. MR0030995

[4] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112. MR0093504

[5] H. Davenport and P. Erdös, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), 252–265. MR0055368

[6] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free prime factors $> y$. II*, Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math. **28** (1966), 239–247. MR0205945

[7] Harold G. Diamond and H. Halberstam, *A higher-dimensional sieve method,* with an appendix ("Procedures for computing sieve functions") by William F. Galway, Cambridge Tracts in Mathematics, vol. 177, Cambridge University Press, Cambridge, 2008. MR2458547

[8] P. D. T. A. Elliott, *The least prime $k-$*th*-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210. MR0281686

[9] GH from MO (`http://mathoverflow.net/users/11919/gh-from-mo`), *Given a prime p how many primes $\ell < p$ of a given quadratic character mod p?*, MathOverflow, URL: `http://mathoverflow.net/q/52393` (version: 2014-09-03).

[10] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, translated and with a preface by Arthur A. Clarke; revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse, Springer-Verlag, New York, 1986. MR837656

[11] Adolf Hildebrand, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, J. Number Theory **22** (1986), no. 3, 289–307, DOI 10.1016/0022-314X(86)90013-2. MR831874

[12] Richard H. Hudson, *Prime k-th power non-residues*, Acta Arith. **23** (1973), 89–106. MR0321849

[13] Richard H. Hudson, *A note on the second smallest prime kth power nonresidue*, Proc. Amer. Math. Soc. **46** (1974), 343–346. MR0364139

[14] Richard H. Hudson, *Power residues and nonresidues in arithmetic progressions*, Trans. Amer. Math. Soc. **194** (1974), 277–289. MR0374002

[15] Richard H. Hudson, *A note on prime kth power nonresidues*, Manuscripta Math. **42** (1983), no. 2-3, 285–288, DOI 10.1007/BF01169590. MR701210

[16] 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. MR2378655

[17] K. K. Norton, *Estimates for prime kth power nonresidues*, Notices Amer. Math. Soc. **21** (1974), January, 74T-A12.

[18] Karl K. Norton, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78. MR1623353

[19] Paul Pollack, *Prime splitting in abelian number fields and linear combinations of Dirichlet characters*, Int. J. Number Theory **10** (2014), no. 4, 885–903, DOI 10.1142/S1793042114500055. MR3208865

[20] Paul Pollack, *The smallest prime that splits completely in an abelian number field*, Proc. Amer. Math. Soc. **142** (2014), no. 6, 1925–1934, DOI 10.1090/S0002-9939-2014-12199-X. MR3182011

[21] G. Tenenbaum, *Cribler les entiers sans grand facteur premier* (French, with English and French summaries), Philos. Trans. Roy. Soc. London Ser. A **345** (1993), no. 1676, 377–384, DOI 10.1098/rsta.1993.0136. MR1253499

[22] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas. MR1342300

[23] A. I. Vinogradov and Ju. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue* (Russian), Dokl. Akad. Nauk SSSR **168** (1966), 259–261. MR0209223

[24] I. M. Vinogradov, *On the distribution of quadratic residues and nonresidues*, J. Phys.-Mat. ob-va Permsk Univ. **2** (1919), 1–16 (Russian).

[25] J. M. Vinogradov, *On the bound of the least non-residue of nth powers*, Trans. Amer. Math. Soc. **29** (1927), no. 1, 218–226, DOI 10.2307/1989287. MR1501385

[26] Wang Yuan, *Estimation and application of character sums* (Chinese), Shuxue Jinzhan **7** (1964), 78–83. MR0229588

[27] D. Wolke, *A note on the least prime quadratic residue* (mod p), Acta Arith. **16** (1969/1970), 85–87. MR0245536

Department of Mathematics, Boyd Graduate Studies Building, University of Georgia, Athens, Georgia 30602

E-mail address: pollack@uga.edu