On the second smallest prime non-residue

Kevin J. McGown[1]

Department of Mathematics, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093

Abstract

Let χ be a non-principal Dirichlet character modulo a prime p. Let $q_1 < q_2$ denote the two smallest prime non-residues of χ. We give explicit upper bounds on q_2 that improve upon all known results. We also provide a good upper estimate on the product $q_1 q_2$ which has an upcoming application to the study of norm-Euclidean Galois fields.

Keywords: Dirichlet character, non-residues, power residues
2010 MSC: Primary 11A15, 11N25; Secondary 11A05

1. Introduction and Summary

Let χ be a non-principal Dirichlet character modulo a prime p. We call a positive integer m a non-residue of χ if $\chi(m) \notin \{0, 1\}$, and denote by $q_1 < q_2 < \cdots < q_n$ the n smallest prime non-residues of χ. The question of putting an upper bound on q_1 is a classical problem which goes all the way back to the study of the least quadratic non-residue.

The literature on this problem is extensive and we will not review it here except to say that the work of Burgess in the 1960's significantly advanced existing knowledge on this matter. Burgess' famous character sum estimate (see [1]) implies that $q_n = O(p^{1/4+\varepsilon})$ for all n.[2] For the case of q_1, one can apply the "Vinogradov trick" (see [3, 4, 5]) to Burgess' result, which gives the stronger bound of $q_1 = O(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$ (see [1]).

Email address: kmcgown@ursinus.edu (Kevin J. McGown)

[1] *Current address:* Department of Mathematics and Computer Science, Ursinus College, 601 E. Main St., Collegeville, Pennsylvania 19426

[2] The O constant here depends upon ε and n; see [2] for more detail.

p_0	10^7	10^8	10^9	10^{10}	10^{11}	10^{12}
C	11.0421	8.2760	7.2906	6.8121	6.5496	6.3964

Table 1: Values of C for various choices of p_0

Making these results explicit with constants of a reasonable magnitude turns out to be difficult, and often times it is results of this nature that one requires in application. In this paper, we will restrict ourselves to the study of q_1 and q_2, and we will only be interested in bounds which are completely explicit and independent of the order of χ.[3]

The best known explicit bound on q_1 was given by Norton[4] (see [6]) by applying Burgess' method (see [1, 7]) with some modifications.

Theorem 1 (Norton). *Suppose that χ is a non-principal Dirichlet character modulo a prime p, and that q_1 is the smallest (prime) non-residue of χ. Then $q_1 < 4.7\,p^{1/4}\log p$, and moreover, the constant can be improved to* 3.9 *when the order of χ and $(p-1)/2$ have a common factor.*

We prove the following theorem, which can be viewed as a generalization of Norton's result but with a slightly larger constant.

Theorem 2. *Fix a real constant $p_0 \geq 10^7$. There exists an explicit constant C (see Table 1) such that if χ is a non-principal Dirichlet character modulo a prime $p \geq p_0$ and u is a prime with $u \geq e^2 \log p$, then there exists $n \in \mathbb{Z}^+$ with $(n,u) = 1$, $\chi(n) \neq 1$, and*

$$n < C\,p^{1/4}\log p\,.$$

Provided that q_1 is not too small, the above theorem immediately gives an explicit bound on q_2.

Corollary 1. *Fix a real constant $p_0 \geq 10^7$. Let χ be a non-principal Dirichlet character modulo a prime $p \geq p_0$. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. If $q_1 > e^2 \log p$, then*

$$q_2 < C\,p^{1/4}\log p\,,$$

[3]In Corollary 3 we do assume that χ has odd order, but we emphasize that none of our constants depend upon the order of χ.

[4]Recently, Treviño has improved upon this. See the comments in §6.

where the constant C is the same constant as in the statement of Theorem 2 (see Table 1).

Using a lemma of Hudson and an explicit result of the author on consecutive non-residues, we can remove the restriction on q_1 for a small price.

Corollary 2. *Let χ be a non-principal Dirichlet character modulo a prime $p \geq 10^{19}$. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. Then*

$$q_2 < 53\, p^{1/4} (\log p)^2 \,.$$

The value q_2 has not been as extensively studied as q_1, and it appears that prior to now, the best explicit bound was essentially $q_2 \leq c\, p^{2/5}$ for some absolute constant c (see [8, 9, 10, 11]). Corollary 2 constitutes an explicit bound on q_2 which even improves slightly on the best known O-bound of $p^{1/4+\varepsilon}$.

For the application the author has in mind to norm-Euclidean Galois fields (see [12]), the following corollary is more useful.

Corollary 3. *Let χ be a non-principal Dirichlet character modulo a prime $p \geq 10^{18}$ having odd order. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. Then*

$$q_1 q_2 < 24\, p^{1/2} (\log p)^2 \,.$$

2. Outline of the Proof

We will establish our results using a generalization of Burgess' method. The approach will be similar to a previous paper of the author (see [13]), but it will be sufficiently different as these results do not follow from the aforementioned ones or vice versa. The main idea behind Burgess' method is to combine upper and lower bounds for the following sum:

Definition 1. *If $h, r \in \mathbb{Z}^+$ and χ is a Dirichlet character modulo p, then we define*

$$S(\chi, h, r) := \sum_{x=0}^{p-1} \left| \sum_{m=1}^{h} \chi(x+m) \right|^{2r} .$$

We will use the following lemma, proven in [13], which is a slight improvement on Lemma 2 of [1].

Lemma 1. *Suppose χ is any non-principal Dirichlet character to the prime modulus p. If $r, h \in \mathbb{Z}^+$, then*

$$S(\chi, h, r) < \frac{1}{4}(4r)^r p h^r + (2r-1)p^{1/2}h^{2r}\,.$$

Apart from the use of Lemma 1, the proofs of Theorem 2 and Corollary 1 are completely self-contained; in particular, they do not rely on Theorem 1. However, the derivation of Corollary 2 will use Theorem 1.2 of [13], and the derivation of Corollary 3 will use Theorem 1 and an explicit version of the Pólya–Vinogradov inequality given in [14].

The meat of the proof of our results is to give a lower bound on $S(\chi, h, r)$, under some extra conditions on the involved parameters. In §3 we prove the following:

Proposition 1. *Let $h, r, u \in \mathbb{Z}^+$ with u prime and $h \le u$. Suppose that χ is a Dirichlet character modulo a prime $p \ge 5$ such that $\chi(n) = 1$ for all $n \in [1, H]$ satisfying $(n, u) = 1$. Assume $2h < H < (hp)^{1/2}$ and set $X := H/(2h) > 1$. Then*

$$S(\chi, h, r) \ge \frac{6}{\pi^2}(1-u^{-1})h(h-2)^{2r}X^2 f(X, u)\,.$$

For each fixed u we have $f(X, u) \to 1$ as $X \to \infty$; the function $f(X, u)$ is explicitly defined in Lemma 5.

Combining Lemma 1 and Proposition 1 with a careful choice of the parameters h and r gives our main result from which Theorem 2 follows:

Theorem 3. *Suppose that χ is a non-principal Dirichlet character modulo a prime $p \ge 10^7$, and that u is a prime with $u \ge e^2 \log p$. Suppose $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. Then*

$$H \le K g(p)\, p^{1/4} \log p\,,$$

where

$$K = \frac{\pi e}{\sqrt{2}} \approx 6.0385$$

and

$$g(p) = \sqrt{\frac{\left(1 + \frac{4}{3\log p}\right)}{\left(1 - \frac{1}{e^2 \log p}\right) f\left(\frac{K p^{1/4}}{2e^2}, 89\right)}}\,.$$

The function $g(p)$ is positive and decreasing for $p \geq 10^7$, with $g(p) \to 1$ as $p \to \infty$. The function $f(X, u)$ is defined in Lemma 5.

The proofs of Theorems 2 and 3 are carried out in §4. Finally in §5 we derive Corollaries 1, 2, and 3.

3. Proof of Proposition 1

The idea is to locate a large number of disjoint intervals on which χ is "almost constant." For the remainder of this section p will denote a prime with $p \geq 5$, and h, H will denote positive integers. The following are the intervals that will be of interest to us:

Definition 2. *For integers with $0 \leq t < q$, we define the intervals*

$$\mathcal{I}(q,t) = \left(\frac{pt}{q}, \frac{pt+H}{q}\right], \quad \mathcal{I}(q,t)^\star = \left(\frac{pt}{q}, \frac{pt+H}{q} - h\right],$$
$$\mathcal{J}(q,t) = \left[\frac{pt-H}{q}, \frac{pt}{q}\right), \quad \mathcal{J}(q,t)^\star = \left[\frac{pt-H}{q}, \frac{pt}{q} - h\right).$$

We note that the intervals $\mathcal{I}(q,t)^\star$, $\mathcal{J}(q,t)^\star$ might be empty. In fact, they are non-empty exactly when $h < H/q$, which will always be the case whenever we employ them.

Lemma 2. *Let $X > 1$ be a real number and suppose $2XH < p$. Then the intervals $\mathcal{I}(q,t), \mathcal{J}(q,t)$ where $0 \leq t < q \leq X$ with $(t,q) = 1$ are disjoint subintervals of $(0, p-H)$, except for $\mathcal{J}(1,0) = [-H, 0)$.*

Proof. The fact that $\mathcal{I}(q,t), \mathcal{J}(q,t) \subseteq (0, p-H)$ except for $\mathcal{J}(1,0)$ follows easily from the fact that $2XH < p$. Indeed,

$$\frac{pt+H}{q} = \frac{pt}{q} + \frac{H}{q} < \frac{p(X-1)}{X} + \frac{p}{2X} = p - \frac{p}{2X} < p - H,$$

and, in addition, $(pt-H)/q > 0$ follows from $H < p$ provided $t \neq 0$.

If $\mathcal{I}(q_1, t_1)$ and $\mathcal{I}(q_2, t_2)$ intersect, then we have:

$$pt_1/q_1 \leq (H + pt_2)/q_2$$
$$pt_2/q_2 \leq (H + pt_1)/q_1$$

It follows that

$$|t_1q_2 - t_2q_1| \leq \frac{XH}{p} < 1\,;$$

whence $t_1q_2 = t_2q_1$ which implies $t_1 = t_2$, $q_1 = q_2$. (When $t_1 = t_2 = 0$, the condition $(q_1, t_1) = (q_2, t_2) = 1$ forces $q_1 = q_2 = 1$, so the argument goes through in this case as well.) An similar argument shows that $\mathcal{J}(q_1, t_1)$ and $\mathcal{J}(q_2, t_2)$ cannot intersect.

If $\mathcal{I}(q_1, t_1)$ and $\mathcal{J}(q_2, t_2)$ intersect, then we have:

$$\begin{array}{rcl} pt_1/q_1 & \leq & pt_2/q_2 \\ (pt_2 - H)/q_2 & \leq & (pt_1 + H)/q_1 \end{array}$$

It follows that

$$|t_1q_2 - t_2q_1| \leq \frac{(q_1+q_2)H}{p} \leq \frac{2XH}{p} < 1\,,$$

and as before this implies $t_1 = t_2$, $q_1 = q_2$. But it is plain that this is impossible. ■

Lemma 3. *Let $h, u \in \mathbb{Z}^+$ with u prime and $h \leq u$. Suppose that χ is a Dirichlet character modulo p such that $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. If $z \in \mathcal{I}(q,t)^\star \cup \mathcal{J}(q,t)^\star$ and $(q, u) = 1$, then*

$$\left|\sum_{m=0}^{h-1} \chi(z+m)\right| \geq h - 2\,.$$

Proof. We note that by hypothesis $\mathcal{I}(q,t)^\star \cup \mathcal{J}(q,t)^\star \neq \emptyset$ and hence $h < H/q$. First suppose $z \in \mathcal{I}(q,t)^\star$. We will show that the values $\chi(z+n)$ for $n = 0, \ldots, h-1$ are all equal except for possibly one value of n. This will immediately give the result upon application of the triangle inequality.

For $n = 0, \ldots, h-1$, we have $z + n \in \mathcal{I}(q,t)$ and hence $q(z+n) - pt \in (0, H]$. Provided u does not divide $q(z+n) - pt$, we have

$$\chi(z+n) = \overline{\chi}(q)\chi(q(z+n)) = \overline{\chi}(q)\chi(q(z+n) - pt) = \overline{\chi}(q)\,.$$

But if u divides $q(z+n) - pt$ for two distinct values of n, say n_1 and n_2, we find that u divides $q(n_1 - n_2)$. Since $(u, q) = 1$, we conclude that u divides $n_1 - n_2$ and hence $|n_1 - n_2| \geq u$. This leads to $h \leq u \leq |n_1 - n_2| \leq h - 1$, a contradiction. The proof for $z \in \mathcal{J}(q,t)^\star$ is similar. ■

Lemma 4. *Suppose that $X > 1$ is a real number and $u \in \mathbb{Z}^+$ is prime. Then*

$$\sum_{\substack{n \le X \\ (n,u)=1}} n = \frac{(1-u^{-1})}{2} X^2 + \theta_{X,u} X \,,$$

where the sum is taken over positive integers and $\theta_{X,u}$ denotes a real number, depending on X and u, that belongs to the interval $(-1,1)$.

Proof. For any $Y > 0$ we have

$$\sum_{n \le Y} n = \frac{\lfloor Y \rfloor (\lfloor Y \rfloor + 1)}{2} \,.$$

Upon an application of the obvious inequality $Y - 1 < \lfloor Y \rfloor \le Y$, we obtain the identity

$$\sum_{n \le Y} n = \frac{Y^2}{2} + \frac{Y}{2}\theta_Y \,,$$

where $\theta_Y \in (-1, 1]$. Now we write

$$\begin{aligned} \sum_{\substack{n \le X \\ (n,u)=1}} n &= \sum_{n \le X} n - u \sum_{n \le X/u} n \\ &= \frac{X^2}{2}(1-u^{-1}) + \frac{X}{2}(\theta_X - \theta_{X/u}) \,, \end{aligned}$$

and observe that

$$-2 < \theta_X - \theta_{X/u} < 2 \,.$$

The result follows. ■

Lemma 5. *Suppose $X > 1$ and $u \in \mathbb{Z}^+$ is prime. Then*

$$\sum_{\substack{1 \le q \le X \\ (q,u)=1}} \phi(q) \ \ge \ \frac{3}{\pi^2}(1-u^{-1}) X^2 f(X,u) \,,$$

where

$$f(X,u) = 1 - \frac{\pi^2}{3}\left(\frac{1}{2X^2} + \frac{1}{2X} + \frac{1}{1-u^{-1}} \cdot \frac{1+\log X}{X} \right) \,.$$

Proof. First we observe:

$$\begin{aligned}\sum_{\substack{1\le q\le X\\(q,u)=1}} \phi(q) &= \sum_{\substack{1\le q\le X\\(q,u)=1}} \sum_{m|q} \frac{q}{m}\,\mu(m)\\ &= \sum_{\substack{1\le m\le X\\(m,u)=1}} \mu(m) \sum_{\substack{1\le r\le X/m\\(r,u)=1}} r\end{aligned}$$

Applying Lemma 4 to the above gives:

$$\sum_{\substack{1\le q\le X\\(q,u)=1}} \phi(q) \quad =$$

$$\frac{X^2}{2}\left(1-u^{-1}\right)\left(\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m^2}\right) + \; X\left(\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m}\,\theta_{X/m,u}\right)$$

Now we use the bounds:

$$\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m^2} \ge \frac{6}{\pi^2} - \frac{1}{X^2} - \frac{1}{X}\,,$$

$$\left|\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m}\,\theta_{X/m,u}\right| \le \sum_{1\le m\le X} \frac{1}{m} \le 1+\log X$$

The result follows from an application of the triangle inequality and some rearrangement. ■

Proof of Proposition 1. We will employ the intervals $\mathcal{I}(q,t)^\star$ and $\mathcal{J}(q,t)^\star$ from Definition 2 where $0 \le t < q \le X$. We begin by noting that $H/q \ge H/X = 2h$. If we let $z = z(q,t)$ be the smallest integer in $\mathcal{I}(q,t)^\star$, then it follows that $\mathcal{I}(q,t)^\star$ contains the integer points z, $z+1$, …, $z+h-1$; this is because the length of the interval is $H/q - h \ge h$. A similar statement is true for $\mathcal{J}(q,t)^\star$. Hence $\mathcal{I}(q,t)^\star$ and $\mathcal{J}(q,t)^\star$ both contain at least h integer points.

Using Lemma 2 and Lemma 3 we have:

$$\begin{aligned}
S(\chi, h, r) &= \sum_{x=0}^{p-1} \left| \sum_{m=0}^{h-1} \chi(x+m) \right|^{2r} \\
&\geq \sum_{\substack{0 \leq t < q \leq X \\ (q,u)=(q,t)=1}} \sum_{z \in \mathcal{I}(q,t)^\star \cup \mathcal{J}(q,t)^\star} \left| \sum_{m=0}^{h-1} \chi(z+m) \right|^{2r} \\
&\geq \sum_{\substack{0 \leq t < q \leq X \\ (q,tu)=1}} 2h(h-2)^{2r} \\
&= 2h(h-2)^{2r} \sum_{\substack{1 \leq q \leq X \\ (q,u)=1}} \phi(q)
\end{aligned}$$

Now the result follows from Lemma 5. ■

4. Proofs of the Theorems

Before launching the proof of Theorem 3, we establish the following simple convexity result:

Lemma 6. *Suppose $h, r \geq 1$. We have the following implications:*

$$\begin{aligned}
h \geq 6r+5 &\implies \frac{1}{2h}\left(\frac{4r}{h-2}\right)^r \leq \frac{1}{h+1}\left(\frac{4r}{h+1}\right)^r \\
h \geq 16r+2 &\implies \left(\frac{h}{h-2}\right)^r < \frac{7}{6} \\
h \geq 2r-1 &\implies \frac{2r-1}{h} \leq \frac{2r}{h+1}
\end{aligned}$$

Proof. By the convexity of the logarithm, we have $\log t \geq (2\log 2)(t-1)$ for all $t \in [1/2, 1]$. Applying this, together with the hypothesis that $6(r+1) \leq h+1$, we get

$$\log\left(\frac{h-2}{h+1}\right) \geq -\frac{6\log 2}{h+1} \geq -\frac{\log 2}{r+1}.$$

This yields

$$\frac{1}{2} \leq \left(\frac{h-2}{h+1}\right)^{r+1},$$

and first implication follows. For the proof of the second implication, we observe (again by convexity) that $\log t \leq t-1$ for all t and hence

$$r \log\left(\frac{h}{h-2}\right) \leq \frac{2r}{h-2} \leq \frac{1}{8};$$

this leads to

$$\left(\frac{h}{h-2}\right)^{r} \leq \exp\left(\frac{1}{8}\right) < \frac{7}{6}.$$

The third implication is trivial. ■

Proof of Theorem 3. Before beginning the proof proper, we show that we may reduce to the case where

$$H \leq (e^2 \log p - 1)^{1/2} p^{1/2}. \tag{1}$$

Assume we can prove the result when (1) holds. If (1) fails to hold, then we set $H_0 = \lfloor (e^2 \log p - 1)^{1/2} p^{1/2} \rfloor$, and note that we still have $\chi(n) = 1$ for all $n \in [1, H_0]$ with $(n, u) = 1$ for this smaller value H_0. Applying the result for this new interval gives a contradiction since $Kg(p)p^{1/4} \log p < (e^2 \log p - 1)^{1/2} p^{1/2} - 1$ for $p \geq 10^7$.

Now we begin the proof. First, we may assume $H \geq Kp^{1/4} \log p$, or else there is nothing to prove. We set $h = \lfloor A \log p \rfloor$, $r = \lfloor B \log p \rfloor$ with $A = e^2$, $B = 1/4$ and verify that r, h satisfy all three conditions in Lemma 6. The constants A and B were chosen to minimize the quantity AB subject to the constraint $A \geq 4B \exp(1/(2B))$.

One verifies that $Kp^{1/4} > 28e^2$ for $p \geq 10^7$ and hence $H > 28h$. We set $X := H/(2h)$ and observe that we have the a priori lower bound

$$X = \frac{H}{2h} \geq \frac{Kp^{1/4} \log p}{2e^2 \log p} = \frac{Kp^{1/4}}{2e^2},$$

and, in particular, $X > 14$ from the previous sentence. Since $p \geq 10^5$ and $e^2 \log(10^5) \approx 85.1$, we know $u \geq 89$ and hence $f(X, u) \geq f(X, 89)$. For notational convenience, we will write $f(X) := f(X, 89)$.

Combining Lemma 1 and Proposition 1, we obtain

$$\frac{6}{\pi^2}\left(1-u^{-1}\right)h(h-2)^{2r}\left(\frac{H}{2h}\right)^2 f(X) \;\le\; \frac{1}{4}(4r)^r p h^r + (2r-1)p^{1/2}h^{2r}\,.$$

Rearranging the above and applying Lemma 6 gives

$$\begin{aligned}
&\frac{6}{\pi^2}\left(1-u^{-1}\right)H^2 f(X) \\
&\qquad \le 4h^2 p^{1/2}\left[\frac{1}{4h}\left(\frac{4r}{h-2}\right)^r\left(\frac{h}{h-2}\right)^r p^{1/2} + \frac{2r-1}{h}\left(\frac{h}{h-2}\right)^{2r}\right] \\
&\qquad \le 4h^2 p^{1/2}\left[\frac{1}{h+1}\left(\frac{4r}{h+1}\right)^r p^{1/2} + \frac{3r}{h+1}\right]. \qquad (2)
\end{aligned}$$

Plugging in our choices of r, h and using the fact that

$$A \ge 4B\exp\left(\frac{1}{2B}\right) \implies \left(\frac{4B}{A}\right)^r \le p^{-1/2}$$

we obtain

$$\begin{aligned}
\frac{6}{\pi^2}\left(1-u^{-1}\right)H^2 f(X) \;&\le\; 4A^2(\log p)^2 p^{1/2}\left[\frac{1}{A\log p}\left(\frac{4B}{A}\right)^r p^{1/2} + \frac{3B}{A}\right] \\
&\le\; 4A^2 p^{1/2}(\log p)^2\left(\frac{1}{A\log p} + \frac{3B}{A}\right) \\
&=\; 12ABp^{1/2}(\log p)^2\left(1 + \frac{1}{3B\log p}\right). \qquad (3)
\end{aligned}$$

Plugging in our choices of A and B yields: [5]

$$\frac{6}{\pi^2}\left(1-u^{-1}\right)H^2 f(X) \le 3e^2 p^{1/2}(\log p)^2\left(1+\frac{4}{3\log p}\right) \qquad (4)$$

As $f(X)$ is increasing and positive for $X \ge 14$, the result now follows upon solving (4) for H. ■

[5] At this point our choices of A and B are properly motivated – the condition $A \ge 4B\exp(1/(2B))$ was to ensure that the quantity in the square brackets of (2) remains bounded as $p \to \infty$, and we wanted to minimize AB so that the constant appearing in (3) was as small as possible.

Proof of Theorem 2. Suppose $p \geq 10^7$. Let n_0 denote the smallest $n \in \mathbb{Z}^+$ such that $(n, u) = 1$ and $\chi(n) \neq 1$. Set $H := n_0 - 1$ so that $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. We apply Theorem 3 to find $H \leq Kg(p_0)\, p^{1/4} \log p$ when $p \geq p_0 \geq 10^7$. Therefore

$$n_0 \leq Kg(p_0)\, p^{1/4} \log p + 1\,,$$

for $p \geq p_0 \geq 10^7$. Computation of the table of constants is routine; for each value of p_0, we compute (being careful to round up) the quantity

$$Kg(p_0) + \frac{1}{p_0^{1/4} \log p_0}\,. \quad \blacksquare$$

5. Proofs of the Corollaries

Proof of Corollary 1. Apply Theorem 2 with $u = q_1$ and observe that the smallest $n \in \mathbb{Z}^+$ with $(n, q_1) = 1$ and $\chi(n) \neq 1$ is equal to q_2. $\blacksquare$

The following is a lemma due to Hudson (see [11]) that will allow us to prove Corollary 2. The proof is brief and so we include it for the sake of completeness.

Lemma 7 (Hudson). *Let χ be a non-principal Dirichlet character modulo a prime $p \geq 5$. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ, and that $q_1 \neq 2$ or $q_2 \neq 3$. Let S denote the maximal number of consecutive integers for which χ takes the same value. Then $q_2 \leq Sq_1 + 1$.*

Proof. Let $t \in \mathbb{Z}^+$ be maximal such that $1 + tq_1 < q_2$. (This is always possible unless $q_1 = 2$ and $q_2 = 3$.) Then the $t + 1$ integers

$$1,\, 1 + q_1,\, \ldots,\, 1 + tq_1 \tag{5}$$

are residues with respect to χ. Let x be denote the unique inverse of q_1 modulo p in the interval $(0, p)$. Multiplying (5) by x allows us to see that the $t + 1$ consecutive integers

$$x,\, x + 1,\, \ldots,\, x + t$$

take on the same character value; hence $t + 1 \leq S$. By the maximality of t, we conclude that $q_2 \leq (t + 1)q_1 + 1 \leq Sq_1 + 1$. $\blacksquare$

We note that the above Lemma can be improved if $\chi(-1) = 1$ (see [11]) but we will not require this. The other result we we use in the proof of Corollary 2 is the following, which is a special case of Theorem 1.2 of [13].

Theorem 4. *If χ is any non-principal Dirichlet character to the prime modulus $p \geq 10^{19}$ which is constant on $(N, N+H]$, then $H < 7.1\, p^{1/4} \log p$.*

Proof of Corollary 2. If $q_1 > e^2 \log p$, then we apply Corollary 1 and we are done. Hence we may assume that $q_1 \leq e^2 \log p$. If $q_2 = 3$, then we are clearly done, so we may also assume $q_2 \neq 3$. In this case, we combine Lemma 7 and Theorem 4 to conclude that $q_2 \leq (7.1\, p^{1/4} \log p)(e^2 \log p) + 1 < 53\, p^{1/4} (\log p)^2$. ■

In order to prove Corollary 3, we will use the following result which gives a weak bound on q_2, but requires no extra hypotheses on q_1.

Lemma 8. *Let χ be a non-principal Dirichlet character modulo $m \geq 10^{15}$. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. Then*

$$q_2 < 2\, m^{1/2} \log m\,.$$

Proof. Using the explicit version of the Pólya–Vinogradov inequality proven in [14], we find

$$\begin{aligned}
\left| \sum_{\substack{n<x \\ (n,q_1)=1}} \chi(n) \right| &= \left| \sum_{n<x} \chi(n) - \chi(q_1) \sum_{n<x/q_1} \chi(n) \right| \\
&\leq \left| \sum_{n<x} \chi(n) \right| + \left| \sum_{n<x/q_1} \chi(n) \right| \\
&\leq 2 \left(\frac{1}{3 \log 3}\, m^{1/2} \log m + 6.5\, m^{1/2} \right) .
\end{aligned}$$

If $\chi(n) = 1$ for all $n \leq x$ with $(n, q_1) = 1$, then

$$\left| \sum_{\substack{n<x \\ (n,q_1)=1}} \chi(n) \right| \geq (1 - q_1^{-1})x - 1\,.$$

Thus for $1 < x < q_2$, we have

$$(1 - q_1^{-1})x - 1 \leq 2 \left(\frac{1}{3 \log 3}\, m^{1/2} \log m + 6.5\, m^{1/2} \right) .$$

Using the fact that $q_1 \geq 2$ and letting x approach q_2 from the left, we obtain

$$q_2 \leq 4 \left(\frac{1}{3 \log 3} \, m^{1/2} \log m + 6.5 \, m^{1/2} \right) + 2 \,,$$

and the result follows. ■

Proof of Corollary 3. If $q_1 < e^2 \log p$, we use Lemma 8 to obtain $q_2 < 2\, p^{1/2} \log p$ and hence $q_1 q_2 < 2e^2 p^{1/2} (\log p)^2 < 15\, p^{1/2} (\log p)^2$. If $q_1 \geq e^2 \log p$, then we apply Theorem 1 (using the fact that χ has odd order) and Corollary 1 to find $q_1 q_2 \leq C' \, p^{1/2} (\log p)^2$ with $C' = (3.9)(6.1536) < 24$. ■

6. Additional Comments

After the submission of this manuscript, Treviño gave improvements to Theorem 1, Lemma 1, and Theorem 4 (see [15, 16]). Plugging in these improved results would lead to better constants in the results of this paper, but we have chosen to leave our results as originally stated. The interested reader can follow the arguments to obtain the improved constants.

The author would like to thank the referee for helpful suggestions which improved the quality of this paper.

References

[1] D. A. Burgess, On character sums and primitive roots, Proc. London Math. Soc. (3) 12 (1962) 179–192.

[2] R. H. Hudson, A note on prime kth power nonresidues, Manuscripta Math. 42 (1983) 285–288.

[3] I. M. Vinogradov, Sur la distribution des residus et des non-residus des puissances, J. Phys. Math. Soc. Perm. 1 (1918) 94–96.

[4] I. M. Vinogradov, On a general theorem concerning the distribution of the residues and non-residues of powers, Trans. Amer. Math. Soc. 29 (1927) 209–217.

[5] I. M. Vinogradov, On the bound of the least non-residue of nth powers, Trans. Amer. Math. Soc. 29 (1927) 218–226.

[6] K. K. Norton, Numbers with small prime factors, and the least kth power non-residue, Memoirs of the American Mathematical Society, No. 106, American Mathematical Society, Providence, R.I., 1971.

[7] D. A. Burgess, A note on the distribution of residues and non-residues, J. London Math. Soc. 38 (1963) 253–256.

[8] A. Brauer, Über den kleinsten quadratischen Nichtrest, Math. Z. 33 (1931) 161–176.

[9] A. Brauer, On the non-existence of the Euclidean algorithm in certain quadratic number fields, Amer. J. Math. 62 (1940) 697–716.

[10] C. T. Whyburn, The second smallest quadratic non-residue, Duke Math. J. 32 (1965) 519–528.

[11] R. H. Hudson, Prime k-th power non-residues, Acta Arith. 23 (1973) 89–106.

[12] K. J. McGown, Norm-Euclidean cyclic fields of prime degree, Int. J. Number Theory 8 (2012) 227–254.

[13] K. J. McGown, On the constant in Burgess' bound for the number of consecutive residues or non-residues, Funct. Approx. Comment. Math. 46 (2012) 273–284.

[14] G. Bachman, L. Rachakonda, On a problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality, Ramanujan J. 5 (2001) 65–71.

[15] E. Treviño, On the maximum number of consecutive integers on which a character is constant, Mosc. J. Comb. Number Theory 2 (2012) 56–72.

[16] E. Treviño, The Burgess inequality and the least k-th power non-residue (to appear).