Functiones et Approximatio
46.2 (2012), 273–284
doi: 10.7169/facm/2012.46.2.10

ON THE CONSTANT IN BURGESS' BOUND FOR THE NUMBER OF CONSECUTIVE RESIDUES OR NON-RESIDUES

Kevin J. McGown

Abstract: We give an explicit version of a result due to D. Burgess. Let χ be a non-principal Dirichlet character modulo a prime p. We show that the maximum number of consecutive integers for which χ takes on a particular value is less than $\left\{\frac{\pi e\sqrt{6}}{3}+o(1)\right\}p^{1/4}\log p$, where the $o(1)$ term is given explicitly.

Keywords: Dirichlet character, consecutive non-residues, power residues.

1. Introduction

Let χ be a non-principal Dirichlet character to the prime modulus p. In 1963, D. Burgess showed (see [4]) that the maximum number of consecutive integers for which χ takes on any particular value is $O(p^{1/4}\log p)$. This still constitutes the best known asymptotic upper bound on this quantity. However, in some applications, one needs a more explicit result. Following the general lines of his original argument and making careful estimates throughout, we prove an explicit version of Burgess' theorem (see Theorem 4.1 and Corollary 4.3), thereby obtaining the following:

Theorem 1.1. *If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then*

$$H < \left\{\frac{\pi e\sqrt{6}}{3}+o(1)\right\}p^{1/4}\log p\,.$$

We note that the constant $(\pi e\sqrt{6})/3$ is approximately 6.97. As we have an explicit bound on the $o(1)$ term when p is large, we are able to obtain the following result which is more useful in applications:

2010 Mathematics Subject Classification: primary: 11A15, 11N25; secondary: 11L26, 11L40

Theorem 1.2. *If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then*

$$H < \begin{cases} 7.06\, p^{1/4} \log p\,, & \text{for } p \geqslant 5 \cdot 10^{18} \\ 7\, p^{1/4} \log p\,, & \text{for } p \geqslant 5 \cdot 10^{55} \end{cases} .$$

For the special case of $N = 0$, which amounts to giving a bound on the smallest non-residue of χ (i.e., the smallest n such that $\chi(n) \neq 1$), K. Norton proves a result analogous to Theorem 1.2 which holds for all p with a constant of 4.7 (see [10]). In addition, a result for arbitrary N, similar to the one given in Theorem 1.2 is stated, but not proved in [11]. R. Hudson (see [7]) cites a result slightly improving the one stated in [11] to appear in a future paper, but the present author cannot locate the purported proof. It seems a worthwhile endeavor to put down such a proof as it is possible that some authors avoid using the result in [11] due to the lack of proof (see, for example [8]), while others (see [7]) use the result for further derivations. To our knowledge, this is the first proof to appear in the literature which makes the constant in Burgess' theorem explicit.

It is perhaps useful here to comment briefly on the connection between Dirichlet characters and power residues. Fix an integer $k \geqslant 2$. We say that $n \in \mathbb{Z}$ is a k-th power residue modulo p if $(n, p) = 1$ and the equation $x^k \equiv n \pmod{p}$ is soluble in x. Suppose χ is any Dirichlet character modulo p of order $(k, p-1)$. One can easily show that $\chi(n) = 1$ if and only if n is a k-th power residue modulo p. Here we might as well assume $(k, p-1) > 1$, or else every integer is a k-th power residue modulo p and the only such χ is the principal character. If we denote by $C_p = (\mathbb{Z}/p\mathbb{Z})^\star$ the multiplicative group consisting of the integers modulo p and by C_p^k the subgroup of k-th powers modulo p, then the value of $\chi(n)$ determines to which coset of C_p/C_p^k the integer n belongs. In light of this, theorems 1.1 and 1.2 also give estimates (which are the best known) on the maximum number of consecutive integers that belong to a given coset of C_p/C_p^k.

We should also mention that Burgess' well-known character sum estimate (see [3]) gives a bound on the quantity (in the title of the paper) of $O(p^{1/4+\varepsilon})$. However, the constant associated to the O-symbol depends on ε and hence, although there are explicit versions of Burgess' character sum estimate available (see [9]), theorems 1.1 and 1.2 would not follow from this.

The main idea behind Burgess' proof is to combine upper and lower bounds for the sum:

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

In Lemma 2.2 of §2 we give an upper bound for $S(\chi, h, r)$ in terms of r and h. In Proposition 3.3 of §3 we give a lower bound on $S(\chi, h, r)$ in terms of h and H, under some additional hypotheses on H. Combining these results, we obtain an upper bound on H in terms of r and h under the same hypotheses; this result is also given as part of Proposition 3.3. Then, in §4 we prove our main result (see Theorem 4.1) by invoking Proposition 3.3 with a careful choice of parameters.

Finally, by performing some simple numerical computations, we show that that the extra hypothesis on H can be dropped when p is large enough (see Corollary 4.3); theorems 1.1 and 1.2 will then follow immediately.

2. An Upper Bound on $S(\chi, h, r)$

The following character sum estimate was first given by A. Weil, as a consequence of his deep work on the Riemann hypothesis for function fields (see [15]). It is also proved as Theorem 2C' in [13] using an elementary method due to S. Stepanov (see [14]), which was later extended by both E. Bombieri (see [2]) and W. Schmidt (see [12]).

Lemma 2.1. *Let χ be a non-principal Dirichlet character to the prime modulus p, having order n. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with m distinct roots which is not an n-th power in $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ denotes the finite field with p elements. Then*

$$\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))\right| \leqslant (m-1)\, p^{1/2}\,.$$

The next lemma is a slight improvement over Lemma 2 in [3] which gives an upper bound on $S(\chi, h, r)$. The proof is not difficult if we grant ourselves Lemma 2.1.

Lemma 2.2. *Suppose χ is any non-principal Dirichlet character to the prime modulus p. If $r, h \in \mathbb{Z}^+$, then*

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

Proof. First we claim that we may assume, without loss of generality, that $r < h < p$. We commence by observing that $h = p$ implies $S(\chi, h, r) = 0$, in which case there is nothing to prove. We see that $h > p$ implies $S(\chi, h-p, r) = S(\chi, h, r)$, which allows us to inductively bring h into the range $0 < h < p$. Additionally, we notice that if $h \leqslant r$, then the theorem is trivial since in this case we would have $S(\chi, h, r) \leqslant h^{2r}p \leqslant (hr)^r p$. This establishes the claim.

Now, to begin the proof proper, we observe that

$$S(\chi, h, r) = \sum_{1\leqslant m_1,\ldots,m_{2r}\leqslant h}\ \sum_{x=0}^{p-1} \chi(x+m_1)\ldots\chi(x+m_r)\overline{\chi}(x+m_{r+1})\ldots\overline{\chi}(x+m_{2r})\,.$$

Define

$$\mathcal{M} := \{\mathbf{m} = (m_1, \ldots, m_{2r}) \mid 1 \leqslant m_1, \ldots, m_{2r} \leqslant h\}\,.$$

We can rewrite the above as

$$S(\chi, h, r) = \sum_{\mathbf{m}\in\mathcal{M}}\sum_{x\in\mathbb{F}_p} \chi(f_{\mathbf{m}}(x))\,,$$

where

$$f_{\mathbf{m}}(x) = (x+m_1)\dots(x+m_r)(x+m_{r+1})^{n-1}(x+m_{2r})^{n-1}\,,$$

and n denotes the order of χ. If $f_{\mathbf{m}}(x)$ is not an n-th power mod p, then by Lemma 2.1 we have

$$\left|\sum_{x\in\mathbb{F}_p}\chi(f_{\mathbf{m}}(x))\right| \leqslant (2r-1)\sqrt{p}\,.$$

Otherwise, we must settle for the trivial bound of p.

It remains to count the number of exceptions – that is, the number of $\mathbf{m}\in\mathcal{M}$ such that $f_{\mathbf{m}}(x)$ is an n-th power mod p. A little care is required here – as an example, if $r=n=3$ and $p\geqslant 5$, then the vectors $\mathbf{m}=(1,2,3,1,2,3)$ and $\mathbf{m}=(1,1,1,2,2,2)$ are both exceptions, but the way in which they arise is slightly different; as r gets larger compared to n, the situation only gets worse. In light of this difficulty, we will actually count (as Burgess does in [4]) the number of $\mathbf{m}=(m_1,\dots,m_{2r})\in\mathcal{M}$ such that each m_j is repeated at least once.

We let u denote the number of distinct m_j (so that $u\leqslant r<h$) and denote by $1=j_1<j_2<\dots<j_u\leqslant 2r$ the indices corresponding to the first occurrence of each of the u values among the m_j. The number of ways to choose the j_k is bounded by $\binom{2r-1}{u-1}$, and there are at most h choices for each m_{j_k} while the remaining m_j are restricted to at most u values. In light of all this, we find that the number of exceptions is bounded above by

$$\sum_{u=1}^{r}\binom{2r-1}{u-1}h^u u^{2r-u} \leqslant (hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1}\left(\frac{u}{h}\right)^{r-u} \leqslant (hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1}.$$

Finally, to complete the proof, we observe

$$(hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1} = (hr)^r 2^{2r-2} = \frac{1}{4}(4rh)^r. \qquad \blacksquare$$

3. A Lower Bound on $S(\chi,h,r)$

In obtaining the desired lower bound, the idea is to locate a large number of intervals on which χ is constant. The next two lemmas will be useful in accomplishing this end. The following lemma makes the error term in Lemma 3 of [4] explicit and improves the main constant from $1-\pi^2/12\approx 0.178$ to $3/\pi^2\approx 0.304$.

Lemma 3.1. *Let $X\geqslant 7$. If $a,b\in\mathbb{Z}$ are coprime with $a\geqslant 1$, then there are at least*

$$X^2\left(\frac{3}{\pi^2}-\frac{\log X}{2X}-\frac{1}{X}-\frac{1}{2X^2}\right)$$

distinct numbers of the form

$$\frac{at+b}{q}$$

where $0\leqslant t<q\leqslant X$.

Proof. As in [4], we observe that $\#\{q^{-1}(at+b) \mid 0 \leqslant t < q \leqslant X\}$ is bounded below by

$$\sum_{q \leqslant X} \sum_{\substack{0 \leqslant t < q \\ (at+b,q)=1}} 1 = \sum_{q \leqslant X} \sum_{0 \leqslant t < q} \sum_{m \mid (at+b,q)} \mu(m)$$

Writing $q = rm$ allows us to rewrite the sum above as

$$\sum_{m \leqslant X} \mu(m) \sum_{r \leqslant X/m} \sum_{\substack{0 \leqslant t < rm \\ at \equiv -b \quad (m)}} 1.$$

Since $(a,b) = 1$, the congruence $at \equiv -b \pmod{m}$ has a solution if and only if $(m,a) = 1$. Therefore we can rewrite our sum in the following way:

$$\sum_{\substack{m \leqslant X \\ (m,a)=1}} \mu(m) \sum_{r \leqslant X/m} \sum_{\substack{0 \leqslant t < rm \\ at \equiv -b \quad (m)}} 1 = \sum_{\substack{m \leqslant X \\ (m,a)=1}} \mu(m) \sum_{r \leqslant X/m} r.$$

A careful lower estimate of the sum on the right-hand side above will give the desired result. Using the identity

$$\sum_{r \leqslant Y} r = \frac{Y^2}{2} + \frac{Y}{2}\theta_Y, \qquad \theta_Y \in [-1,1],$$

which holds for $Y > 0$, we obtain

$$\sum_{\substack{m \leqslant X \\ (m,a)=1}} \mu(m) \sum_{r \leqslant X/m} r = \frac{X^2}{2} \sum_{\substack{m \leqslant X \\ (m,a)=1}} \frac{\mu(m)}{m^2} + \frac{X}{2} \sum_{\substack{m \leqslant X \\ (m,a)=1}} \frac{\mu(m)}{m}\theta_{X/m}. \tag{3.1}$$

Let $\zeta(s)$ denote the Riemann zeta function. When $s > 1$, we have

$$\sum_{\substack{m=1 \\ (m,a)=1}}^{\infty} \mu(m) m^{-s} = \zeta(s)^{-1} \prod_{p \mid a} (1 - p^{-s})^{-1} \geqslant \zeta(s)^{-1},$$

and the tail of the series is bounded in absolute value by

$$\sum_{m > X} m^{-s} \leqslant \frac{1}{X^s} + \frac{1}{(s-1)} \cdot \frac{1}{X^{s-1}};$$

therefore

$$\sum_{\substack{m \leqslant X \\ (m,a)=1}} \mu(m) m^{-s} \geqslant \zeta(s)^{-1} - \frac{1}{X^s} - \frac{1}{(s-1)} \cdot \frac{1}{X^{s-1}}.$$

Setting $s = 2$ gives

$$\sum_{\substack{m \leqslant X \\ (m,a)=1}} \frac{\mu(m)}{m^2} \geqslant \zeta(2)^{-1} - \frac{1}{X^2} - \frac{1}{X}\,.$$

Now we deal with the second sum on the right-hand side of (3.1); we have

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

Summarizing, we have shown

$$\begin{aligned} \left| \sum_{\substack{m \leqslant X \\ (m,a)=1}} \mu(m) \sum_{r \leqslant X/m} r \right| &\geqslant \frac{X^2}{2}\left(\frac{1}{\zeta(2)} - \frac{1}{X^2} - \frac{1}{X}\right) - \frac{X}{2}(1 + \log X) \\ &= X^2 \left(\frac{1}{2\zeta(2)} - \frac{\log X}{2X} - \frac{1}{X} - \frac{1}{2X^2}\right). \end{aligned}$$

In light of the fact that $\zeta(2) = \pi^2/6$, we have arrived at the desired conclusion. The reader may worry why we failed to use the hypothesis that $X \geqslant 7$. This hypothesis is not necessary for the truth of the conclusion, but we include it nonetheless to ensure that our estimate gives a positive number. ■

Finally we will require Dirichlet's Theorem in Diophantine approximation; see, for example, Theorem 1 in Chapter 1 of [5].

Lemma 3.2. *Let θ, $A \in \mathbb{R}$ with $A > 1$. Then there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1$ such that*

$$0 < a < A, \qquad |a\theta - b| \leqslant A^{-1}.$$

We are now ready to give our lower bound on $S(\chi, h, r)$.

Proposition 3.3. *Let $h, r \in \mathbb{Z}^+$. Suppose χ is a non-principal Dirichlet character to the prime modulus p which is constant on $(N, N + H]$ and such that*

$$14h \leqslant H \leqslant (2h-1)^{1/3} p^{1/3}\,.$$

If we set $X := H/(2h) \geqslant 7$, then

$$S(\chi, h, r) \geqslant \left(\frac{3}{\pi^2}\right) X^2 h^{2r+1} f(X)\,,$$

where

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

and therefore

$$H < \frac{2\pi h}{\sqrt{3f(X)}} p^{1/4} \left[\frac{1}{4h} \left(\frac{4r}{h} \right)^r p^{1/2} + \left(\frac{2r-1}{h} \right) \right]^{1/2} .$$

Note: $f(X)$ is positive and increasing on $[7,\infty)$ and $f(X) \to 1$ as $X \to \infty$.

Proof. Following the argument given in [4], we define the real interval

$$I(q,t) := \left(\frac{N+pt}{q}, \frac{N+H+pt}{q} \right] ,$$

for $0 \leqslant t < q \leqslant X$. We take note of two important properities of $I(q,t)$, which we will use later. First, the length of $I(q,t)$ is $H/q \geqslant H/X = 2h$. Second, χ is constant on $I(q,t)$; this is because for any $z \in I(q,t)$ we have $\chi(qz - pt) = \zeta$ and hence $\chi(z) = \overline{\chi}(q)\zeta$. We are interested in locating a large number of non-overlapping intervals of this form.

By Lemma 3.2, there exists coprime $a, b \in \mathbb{Z}$ such that $1 \leqslant a \leqslant H$ and

$$|aNp^{-1} - b| \leqslant 1/H . \tag{3.2}$$

One shows that if $I(q_1,t_1)$ and $I(q_2,t_2)$ overlap, then

$$|Np^{-1}(q_1 - q_2) + t_2 q_1 - t_1 q_2| < p^{-1} X H . \tag{3.3}$$

Equations (3.2) and (3.3) yield

$$\left| \frac{b}{a}(q_1 - q_2) + t_2 q_1 - t_1 q_2 \right| < \frac{XH}{p} + \frac{|q_1 - q_2|}{Ha} \leqslant \frac{XH}{p} + \frac{X}{Ha} = \frac{H^2 a + p}{2ahp} .$$

But since $a \leqslant H$ and $H^3 \leqslant (2h-1)p$ by hypothesis, we have

$$\frac{H^2 a + p}{2ahp} \leqslant \frac{H^3 + p}{2ahp} \leqslant \frac{1}{a} .$$

Hence

$$\left| \frac{b}{a}(q_1 - q_2) + t_2 q_1 - t_1 q_2 \right| < \frac{1}{a} ,$$

and it follows that $I(q_1,t_1)$ and $I(q_2,t_2)$ can only overlap if

$$\frac{at_1 + b}{q_1} = \frac{at_2 + b}{q_2} .$$

Invoking Lemma 3.1, we find that there will be at least $(3/\pi^2) X^2 f(X)$ disjoint intervals $I(q,t)$ of the given form.

Having located the desired intervals, we are ready to give a lower estimate for $S(\chi, h, r)$. Let $z(q,t)$ denote the smallest integer in $I(q,t)$. Since $I(q,t)$ has length at least $2h$, the integers $z(q,t) + n + m$, for $n = 0, \ldots, h-1$ and $m = 1, \ldots, h$ are distinct elements of $I(q,t)$. Moreover, as q,t run through the values selected by Lemma 3.1, the $I(q,t)$ are disjoint. Now, using the fact that χ is constant on each $I(q,t)$, one obtains the following bound for $S(\chi,h,r)$:

$$\begin{aligned}\sum_{x=0}^{p-1}\left|\sum_{m=1}^{h}\chi(x+m)\right|^{2r} &\geqslant \sum_{q,t}\sum_{n=0}^{h-1}\left|\sum_{m=1}^{h}\chi(z(q,t)+n+m)\right|^{2r}\\ &=\sum_{q,t}\sum_{n=0}^{h-1}h^{2r}\\ &=h^{2r+1}\sum_{q,t}1\\ &\geqslant\left(\frac{3}{\pi^2}\right)X^2h^{2r+1}f(X).\end{aligned}$$

Now we combine this lower bound on $S(\chi,h,r)$ with the upper bound given in Lemma 2.2 to obtain

$$\left(\frac{3}{\pi^2}\right)\left(\frac{H}{2h}\right)^2 h^{2r+1}f(X)<\frac{1}{4}(4r)^r p h^r+(2r-1)p^{1/2}h^{2r}\,,$$

which implies

$$H^2<\frac{4\pi^2h^2}{3f(X)}p^{1/2}\left[\frac{1}{4h}\left(\frac{4r}{h}\right)^r p^{1/2}+\left(\frac{2r-1}{h}\right)\right].$$

(We have used the fact that $f(X)>0$ for $X\geqslant 7$ in order to divide both sides by $f(X)$ and preserve the inequality.) Taking the square root of both sides yields the result. ■

4. The Main Result

Theorem 4.1. *Suppose χ is a non-principal Dirichlet character to the prime modulus $p\geqslant 5\cdot 10^4$ which is constant on $(N,N+H]$. If $H\leqslant(2e^2\log p-3)^{1/3}p^{1/3}$, then*

$$H<C\,g(p)\cdot p^{1/4}\log p\,,$$

where

$$C=\frac{\pi e\sqrt{6}}{3}\approx 6.97266$$

and $g(p)\to 1$ as $p\to\infty$. In fact,

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

where $f(X)$ is defined in Proposition 3.3. Note that $g(p)$ is positive and decreasing for $p\geqslant 5\cdot 10^4$.

Before launching the proof of Theorem 4.1, we will establish the following:

Lemma 4.2. *Let $p \geqslant 3$ be an integer. Suppose that $A, B > 0$ are real numbers such that $h = \lfloor A \log p \rfloor$ and $r = \lfloor B \log p \rfloor$ are positive integers with $2r + 1 \leqslant h$. Then*

$$A \geqslant 4B \cdot \exp\left(\frac{1}{2B}\right) \qquad \Longrightarrow \qquad \frac{1}{2h}\left(\frac{4r}{h}\right)^r \leqslant \frac{1}{Ap^{1/2}\log p}.$$

Proof. By convexity, $\log t \geqslant (2\log 2)(t-1)$ for all $t \in [1/2, 1]$ and thus

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

This implies

$$\frac{1}{2} \leqslant \left(\frac{h}{h+1}\right)^{r+1}$$

and therefore

$$\frac{1}{2h}\left(\frac{4r}{h}\right)^r \leqslant \frac{1}{h+1}\left(\frac{4r}{h+1}\right)^r \leqslant \frac{1}{A\log p}\left(\frac{4B}{A}\right)^r.$$

Hence to obtain the desired implication, is suffices to show

$$\left(\frac{4B}{A}\right)^r \leqslant p^{-1/2}.$$

Taking logarithms, this is equivalent to

$$r\log\left(\frac{4B}{A}\right) \leqslant -\frac{1}{2}\log p,$$

which follows from inequality

$$B\log\left(\frac{4B}{A}\right) \leqslant -\frac{1}{2},$$

which is true by hypothesis. ■

Proof of Theorem 4.1. We will suppose $H \geqslant Cp^{1/4}\log p$, or else there is nothing to prove. Set $h = \lfloor A\log p \rfloor$ and $r = \lfloor B \log p \rfloor$, where $A := e^2$ and $B := 1/4$. The constants A and B were chosen as to minimize the quantity AB subject to the constraint $A \geqslant 4B\exp\left(\frac{1}{2B}\right)$. One easily checks that $14h \leqslant Cp^{1/4}\log p$ for our choices of h and C, provided $p \geqslant 5 \cdot 10^4$ and hence $14h \leqslant H$. Also, we note that $H \leqslant (2h-1)^{1/3}p^{1/3}$ by hypothesis. We apply Proposition 3.3 and adopt all notation relevant to its statement. This gives:

$$H < \frac{2\pi h}{\sqrt{3f(X)}}p^{1/4}\left[\frac{1}{4h}\left(\frac{4r}{h}\right)^r p^{1/2} + \left(\frac{2r-1}{h}\right)\right]^{1/2} \tag{4.1}$$

In order for the quantity inside the square brackets above to remain bounded as p gets large, and moreover be as small as possible, we would like

$$\frac{1}{4h}\left(\frac{4r}{h}\right)^r p^{1/2} \to 0\,.$$

As the constants A and B were chosen to satisfy the conditions of Lemma 4.2 (the condition above was precisely the motivation for the lemma), we have

$$\frac{1}{2h}\left(\frac{4r}{h}\right)^r \leqslant \frac{1}{Ap^{1/2}\log p}\,.$$

To give a clean bound on the the quantity $(2r-1)/h$ we notice that $2r \leqslant h+1$ implies

$$\frac{2r-1}{h} \leqslant \frac{2r}{h+1} \leqslant \frac{2B}{A}\,.$$

Thus inequality (4.1) becomes

$$\begin{aligned} H &< \frac{2\pi A}{\sqrt{3f(X)}}\,p^{1/4}\log p\left[\frac{1}{2A\log p}+\frac{2B}{A}\right]^{1/2} \\ &= p^{1/4}\log p\left[\frac{8\pi^2 AB}{3f(X)}\left(1+\frac{1}{4B\log p}\right)\right]^{1/2}. \end{aligned}$$

Now it is plain that the asymptotic constant in the above expression is directly proportional to $\sqrt{AB}$, which motivates our choices of A and B. Plugging in the values of A and B, we obtain:

$$\begin{aligned} H &< p^{1/4}\log p\left[\frac{2\pi^2 e^2}{3f(X)}\left(1+\frac{1}{\log p}\right)\right]^{1/2} \\ &= \frac{e\pi\sqrt{6}}{3}p^{1/4}\log p\left[\frac{1}{f(X)}\left(1+\frac{1}{\log p}\right)\right]^{1/2} \end{aligned}$$

Finally, we note that we have an a priori lower bound on X; namely

$$X = \frac{H}{2h} \geqslant \frac{Cp^{1/4}\log p}{2A\log p} = \frac{C\,p^{1/4}}{2e^2}.$$

In light of the fact that $f(X)$ is increasing, this gives

$$f(X)^{-1} \leqslant f\left(\frac{C\,p^{1/4}}{2e^2}\right)^{-1},$$

and the result follows. ■

Corollary 4.3. *If χ is a non-principal Dirichlet character to the prime modulus $p \geqslant 5\cdot 10^{18}$ which is constant on $(N, N+H]$, then*

$$H < C\,g(p)\cdot p^{1/4}\log p,$$

where C and $g(p)$ are as in Theorem 4.1.

Proof. In order to apply Theorem 4.1, which will give the result, it suffices to show that $H \leqslant (2e^2 \log p - 3)^{1/3} p^{1/3}$. By way of contradiction, suppose $H > (2e^2 \log p - 3)^{1/3} p^{1/3}$. In this case we set $H = \lfloor (2e^2 \log p - 3)^{1/3} p^{1/3} \rfloor$, and note that χ is clearly still constant on $(N, N+H]$ for smaller H. We invoke Theorem 4.1 to conclude that $H < Cg(p)p^{1/4} \log p$ where $Cg(p) \leqslant Cg(5 \cdot 10^{18}) < 7.06$. Using the fact that $p \geqslant 5 \cdot 10^{18}$, we have

$$H < 7.06 p^{1/4} \log p < (2e^2 \log p - 3)^{1/3} p^{1/3} - 1 < H,$$

which is a contradiction. ■

It remains to derive theorems 1.1 and 1.2. Theorem 1.1 follows immediately from Corollary 4.3, and Theorem 1.2 follows immediately as well in light of the facts that $Cg(5 \cdot 10^{18}) < 7.06$ and $Cg(5 \cdot 10^{55}) < 7$.

Remark. It would be highly desirable to prove a form of Theorem 1.2 with a reasonable constant when $p < 10^{20}$. For small p the best result appears to be due to A. Brauer, using elementary methods. In [1], he shows that $H \leqslant \sqrt{2p} + 2$ for all p.

Acknowledgement. The author would like to thank Professor H. M. Stark for his helpful suggestions.

References

[1] A. Brauer, *Über die Verteilung der Potenzreste*, Math. Z. **35** (1932), no. 1, 39–50.

[2] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, pp. 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974.

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

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

[5] J.W.S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45. Cambridge University Press, New York, 1957.

[6] H. Davenport, *Multiplicative number theory*, Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer–Verlag, New York, 2000.

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

[8] P. Hummel, *On consecutive quadratic non-residues: a conjecture of Issai Schur*, J. Number Theory **103** (2003), no. 2, 257–266.

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[10] K.K. Norton, *Numbers with small prime factors, and the least kth power non-residue*, Memoirs of the American Mathematical Society, 106. American Mathematical Society, Providence, R.I. 1971.

[11] K.K. Norton, *Bounds for sequences of consecutive power residues. I*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 213–220. Amer. Math. Soc., Providence, R.I., 1973.

[12] W.M. Schmidt, *Zur Methode von Stepanov*, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, IV. Acta Arith. **24** (1973), 347–367.

[13] W.M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin–New York, 1976.

[14] S.A. Stepanov, *Elementary method in the theory of congruences for a prime modulus*, Acta Arith. **17** (1970), 231–247.

[15] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **34** (1948), 204–207.

Address: Kevin J. McGown: Department of Mathematics, Oregon State University, 368 Kidder Hall, Covallis, Oregon, USA, 97331.

E-mail: mcgownk@math.oregonstate.edu

Received: 24 March 2011