The least k-th power non-residue

Enrique Treviño

Department of Mathematics and Computer Science
Lake Forest College
Lake Forest, Illinois 60045, USA

Abstract

Let p be a prime number and let $k \geq 2$ be a divisor $p-1$. Norton proved that the least k-th power non-residue $\bmod p$ is at most $3.9p^{1/4}\log p$ unless $k = 2$ and $p \equiv 3 \pmod 4$, in which case the bound is $4.7p^{1/4}\log p$. By improving the upper bound in the Burgess inequality via a combinatorial idea, and by using some computing power, we improve the upper bounds to $0.9p^{1/4}\log p$ and $1.1p^{1/4}\log p$, respectively.

Contents

1. Introduction

Let p be a prime and let $k \geq 2$ be a divisor of $p-1$. Let $g(p,k)$ be the least k-th power non-residue $\bmod p$. The case $k = 2$, i.e., the question of how big the least quadratic non-residue is, has been studied extensively. Assuming the Generalized Riemann Hypothesis for Dirichlet L-functions, Ankeny [1]

showed that $g(p,2) \ll (\log p)^2$ and Bach [2] made this explicit by proving (under GRH) that $g(p,2) \leq 2(\log p)^2$. The best unconditional results (for $g(p,2)$) are due to Burgess [5], who, building on work by Vinogradov [19] and using Weil's bound for curves [20], showed that

$$g(p,k) \ll_{\varepsilon} p^{\frac{1}{4\sqrt{e}}+\varepsilon}.$$

For $k \geq 3$ we have better estimates. Let ρ be Dickman's function, i.e., a continuous function that satisfies $u\rho^{'}(u) + \rho(u-1) = 0$ and $\rho(u) = 1$ for $0 \leq u \leq 1$. Let α_k be the unique root of $\rho(\alpha) = \frac{1}{k}$. Wang Yuan [22], building on work of Vinogradov [19] and Buhštab [4], showed that, for real $\varepsilon > 0$,

$$g(p,k) \ll_{\varepsilon,k} p^{\frac{1}{4\alpha_k}+\varepsilon}.$$

It is worth noting that $\alpha_2 = \sqrt{e}$. Vinogradov showed that $\alpha_k \geq e^{\frac{k-1}{k}}$ and Buhštab proved, for $k \geq e^{33}$, that

$$\alpha_k > \frac{\log k}{\log\log k + 2}.$$

All of the work described so far has been of aymptotic nature. In terms of getting explicit bounds, Karl Norton [10], building on a technique of Burgess [7], was able to show that $g(p,k) \leq 3.9p^{1/4}\log p$ unless $k = 2$ and $p \equiv 3 \pmod 4$ for which he showed $g(p,k) \leq 4.7p^{1/4}\log p$. In this paper we will improve this result.

Let h and w be any positive integers, let $p \equiv 1 \bmod k$ be a prime, and let χ be a character $\bmod p$ of order k, that is, k is the smallest positive integer such that χ^k is the principal character. Define

$$S_w(p,h,\chi,k) := \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w}. \tag{1}$$

Norton's proof uses an inequality discovered by Burgess [6], namely that

$$S_w(p,h,\chi,k) < (4w)^{w+1}ph^w + 2wp^{1/2}h^{2w}.$$

Norton made some modifications to a clever argument of Burgess, to get an explicit lower bound for $S_w(p,h,\chi,k)$ depending on $g(p,k)$. This allowed him to get the above stated upper bound on $g(p,k)$.

Inspired by a paper of Booker [3] that deals with the quadratic case in the Burgess inequality, we improve the upper bound on (1) as follows:

Theorem 1.1. *Let p be a prime. Let w, h and k be integers such that $w \le 9h$, $h \le p$, $k \ge 2$ and $k \mid p-1$. Let χ be a character* $\bmod p$ *of order k. Then*

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} < \frac{(2w)!}{2^w w!} p h^w + (2w-1) p^{1/2} h^{2w}.$$

This upper bound was stated (but not proved) by Norton [11] and proved for quadratic characters by Booker [3]. With a more careful combinatorial analysis we improved the term $(4w)^{w+1}$ to

$$\frac{(2w)!}{2^w w!} \sim \sqrt{2} \left(\frac{2w}{e} \right)^w = o(w^w).$$

This improvement is the main result which allowed us to improve the upper bound on $g(p,k)$. This theorem has also allowed the author to get an explicit version of the Burgess inequality in [17] and to improve the best known explicit bound on the largest string on which a Dirichlet character $\bmod p$ is constant ([18]). We state our main result in the following theorem:

Theorem 1.2. *Let $p > 3$ be an odd prime. Let $k \ge 2$ be an integer such that $k \mid p-1$. Let $g(p,k)$ be the least k-th power non-residue* $\bmod p$*. Then*

$$g(p,k) < 0.9 p^{1/4} \log p,$$

unless $k = 2$ and $p \equiv 3 \pmod 4$, in which case

$$g(p,2) \le 1.1 p^{1/4} \log p.$$

A similar bound was announced but not proven by Norton (see [11]), namely that $g(p,k) \le 1.1 p^{1/4}(\log p + 4)$.

In section 2 we will prove our upper bound on $S_w(p,h,\chi,k)$, i.e., Theorem 1.1. In section 3 we will write down Norton's lower bound for $S_w(p,h,\chi,k)$ with some modifications. In the last section of this paper we combine the upper bound from section 2 with the lower bound from section 3 to prove Theorem 1.2.

2. Burgess–Booker upper bound

Definition 2.1. *Let $p > 2$ be a prime and let $l_1, l_2, \ldots, l_{2w}$ be fixed integers. Then define $q(x) \in \mathbb{F}_p(x)$ as follows:*

$$q(x) = (x+l_1)(x+l_2)\cdots(x+l_w)(x+l_{w+1})^{p-2}(x+l_{w+2})^{p-2}\cdots(x+l_{2w})^{p-2}.$$

Abusing notation, we will consider it as a rational function:

$$q(x) = \frac{(x+l_1)(x+l_2)\cdots(x+l_w)}{(x+l_{w+1})(x+l_{w+2})\cdots(x+l_{2w})}.$$

Note that if $k \mid p-1$, the polynomial form for $q(x)$ is a k-th power if and only if the rational form for $q(x)$ is a k-th power.

Definition 2.2. *Let p be a prime. Let w, h and k be integers such that $h \leq p$ and $k \mid p-1$. Let $[\mathbf{h}] = \{0, 1, 2, \ldots, h-1\}$. Let $q(x)$ be defined as in Definition 2.1. Then define $b_w(p,h,k)$ as follows:*

$$b_w(p,h,k) = \left| \left\{ (l_1, l_2, \ldots, l_{2w}) \in [\mathbf{h}]^{2w} \;\middle|\; q(x) \text{ is a } k\text{-th power } \in \mathbb{F}_p(x) \right\} \right|.$$

Lemma 2.1. *Let p be a prime. Let w, h and k be integers such that $h \leq p$, $k \geq 2$ and $k \mid p-1$. Let $b_w(p,h,k)$ be defined as in Definition 2.2. Then*

$$b_w(p,h,k) \leq \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!(k!)^d} \right)^2 \frac{h^{w-(k-2)d}}{(w-kd)!}.$$

Proof. Let $q(x)$ be defined as in Definition 2.1. One way of bounding how many $2w$-tuples make $q(x)$ a k-th power in $\mathbb{F}_p(x)$ is the following: given a tuple, we eliminate the terms from the numerator that appear also in the denominator. We do this until there are no more eliminations to be done. Let's say that the number of terms eliminated is t. Then t is an integer such that $0 \leq t \leq w$. Now for $q(x)$ to be a k-th power the numerator and the denominator must each be a k-th power.

Fix t. The number of ways of getting t eliminations is bounded above by

$$\binom{w}{t}^2 t! h^t. \tag{2}$$

The reason for this count is that we are picking t elements from the numerator to be matched up with t elements from the denominator. To pick the $2t$ factors that will be paired up we have $\binom{w}{t}^2$ ways of doing it. But now we have $t!$ ways of associating a one to one map between the t elements in the numerator and the t elements in the denominator. Once we have the t pairs, then there are at most h^t ways of picking the values for each pair, giving us the stated upper bound.

Now, the number of ways in which the remaining parts of the the numerator can be a k-th power is

$$\frac{1}{d!}\binom{w-t}{k,k,k,\ldots,k}h^d = \frac{(w-t)!}{d!(k!)^d}h^d. \tag{3}$$

We divide by $d!$ because the multinomial associates an order to the groups being picked. We multiply by h^d because each group of size k has h options.

For the remaining parts of the denominator (of $q(x)$) we would have the same estimate with h replaced by $h-1$ (since we already eliminated the common terms). Since we are interested in an upper bound, to simplify calculations I will replace $h-1$ with h.

Combining (2) and (3) and summing over values of $t \equiv w \bmod k$ we arrive at the following upper bound for $b_w(p,h,k)$:

$$\sum_{\substack{0\le t\le w\\ t\equiv w \bmod k}} \left(\frac{(w-t)!}{d!(k!)^d}\right)^2 \binom{w}{t}^2 t!h^{t+2d} = \sum_{\substack{0\le t\le w\\ t\equiv w \bmod k}} \left(\frac{w!}{d!t!(k!)^d}\right)^2 t!h^{t+2d}. \tag{4}$$

Using that $t = w - dk$ we can change variables and reach the desired inequality. □

Definition 2.3. *Let w, h and k be positive integers such that $k \ge 2$. Then define $c_w(h,k)$ as follows:*

$$c_w(h,k) = \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!(k!)^d}\right)^2 \frac{h^{w-(k-2)d}}{(w-kd)!}.$$

Note that for any prime p with $k \mid p-1$, Lemma 2.1 implies that $b_w(p,h,k) \le c_w(h,k)$.

Lemma 2.2. *Let w, h and k be positive integers such that $k \ge 2$. Let $c_w(h,k)$ be defined as in Definition 2.3. If $w \le 9h$, then $c_w(h,k)$ is a decreasing function in k.*

Proof. Since k is an integer greater than or equal to 2, it is enough to show that $c_w(h,k) \le c_w(h,k-1)$ for all $k \ge 3$. From Definition 2.3 we have

$$c_w(h,k) = \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!(k!)^d}\right)^2 \frac{h^{w-(k-2)d}}{(w-kd)!}. \tag{5}$$

Now, we arrange the right hand side of (5) to look more like $c_w(h, k-1)$, getting:

$$\sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!((k-1)!)^d} \right)^2 \left(\frac{h^{w-(k-3)d}}{k^{2d}} \right) \left(\frac{1}{h^d (w-kd)!} \right)$$
$$= \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!((k-1)!)^d} \right)^2 \left(\frac{h^{w-(k-3)d}}{(w-(k-1)d)!} \right) \left(\frac{(w-(k-1)d)!}{k^{2d} h^d (w-kd)!} \right).$$

Now we use that $\frac{(w-(k-1)d)!}{(w-kd)!} \leq w^d$ to get the inequality

$$c_w(h,k) \leq \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!((k-1)!)^d} \right)^2 \left(\frac{h^{w-(k-3)d}}{(w-(k-1)d)!} \right) \left(\frac{w}{k^2 h} \right)^d \leq c_w(h, k-1).$$

The last step is true because $w \leq 9h$ and because $k \geq 3$. □

The following corollary is an obvious consequence:

Corollary 2.1. *Let w, h and k be positive integers such that $k \geq 2$. Let $c_w(h,k)$ be defined as in Definition 2.3. If $w \leq 9h$, then $c_w(h,k) \leq c_w(h,2)$.*

Now we will prove a combinatorial identity (and a corollary) that will be used later, but it is a cute result on its own.

Lemma 2.3. *Let w be a positive integer. Then*

$$\sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \frac{1}{(w-2d)!} \left(\frac{w!}{2^d d!} \right)^2 = \frac{(2w)!}{2^w w!}. \tag{6}$$

Proof. The proof will be done by counting the number of partitions of $\{1, 2, \ldots, 2w\}$ into w pairs in two ways. It is worth noting that the way to count the left hand side of (6) was done in Lemma 2.1 when $k = 2$, however we'll give a different exposition of the count below to perhaps make the combinatorics clearer.

Let's count the number of partitions. There are $2w-1$ choices to pair the number 1. Then pick the next lowest number not picked. There are $2w-3$ ways of choosing its partner. Then pick the next lowest number not

picked. There are $2w-5$ ways of choosing its partner. If we continue with this process, we get

$$(2w-1)(2w-3)\cdots(3)(1) = \frac{(2w)(2w-1)(2w-2)\cdots(2)(1)}{(2w)(2(w-1))\cdots(4)(2)} = \frac{(2w)!}{2^w w!}.$$

Notice that this is the right hand side of the equation.

Now, let's count the number of partitions differently. Consider the pairs as (i,j) with $0 < i < j \leq 2w$. Now let P be a partition of $\{1, 2, \ldots 2w\}$ into w pairs. Define $A(P)$, $B(P)$ and $C(P)$ in the following way:

- $A(P) = \{(i,j) \in P \,|\, 0 < i < j \leq w\}$
- $B(P) = \{(i,j) \in P \,|\, w < i < j \leq 2w\}$ and
- $C(P) = \{(i,j) \in P \,|\, 0 < i \leq w < j \leq 2w\}$

We can see by the construction that $A(P), B(P)$ and $C(P)$ are pairwise disjoint. We can also notice that $P = A(P) \cup B(P) \cup C(P)$. Let $|A(P)| = d$. Then the $w - 2d$ numbers $\leq w$ which are not in $A(P)$ must be paired with numbers $> w$. Therefore $|C(P)| = w - 2d$ and $|B(P)| = d$. Therefore a way of counting the number of partitions is by counting for each choice of d with $0 \leq d \leq \left\lfloor \frac{w}{2} \right\rfloor$ the number of ways of getting $A(P)$, $B(P)$ and $C(P)$. The number of ways of pairing up in this way is

$$\left(\frac{(2d)!}{2^d d!}\right)\left(\frac{(2d)!}{2^d d!}\right)\binom{w}{w-2d}^2 (w-2d)! = \frac{1}{(w-2d)!}\left(\frac{w!}{2^d d!}\right)^2$$

Once we sum over all d we get the left hand side of the equation, completing the proof. □

Corollary 2.2. *Let w be a positive integer. Then*

$$\sum_{d=0}^{\left\lfloor \frac{w}{2} \right\rfloor} \binom{w}{d}\binom{w-d}{d} 2^{w-2d} = \binom{2w}{w}.$$

Proof. Multiply both sides of equation (6) by $\frac{2^w}{w!}$. The right hand side of the equation becomes

$$\frac{(2w)!}{2^w w!}\left(\frac{2^w}{w!}\right) = \frac{(2w)!}{w!w!} = \binom{2w}{w}.$$

The left hand side becomes

$$\frac{2^w}{w!}\sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \frac{1}{(w-2d)!}\left(\frac{w!}{2^d d!}\right)^2 = \sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \frac{w! 2^{w-2d}}{d!d!(w-2d)!} = \sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \binom{w}{d}\binom{w-d}{d} 2^{w-2d}.$$

□

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Let $q(x)$ be defined as in Definition 2.1. Using that $|z|^2 = z\bar{z}$ and that $\bar{\chi}(n) = \chi(n)^{p-2}$ allows us to rewrite $S_w(p,h,\chi,k)$ in terms of $q(x)$ as follows:

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} = \sum_{\substack{l_1,\ldots l_{2w} \\ 0\le l_i \le h-1}} \sum_{x=1}^{p} \chi\left(q(x)\right).$$

If $q(x)$ is not a k-th power $\in \mathbb{F}_p(x)$ then using the Weil bound [14, Theorem 2C', page 43], we can bound the inner sum by $(r-1)\sqrt{p}$, where r is the number of distinct roots of $q(x)$ which do not have multiplicity a multiple of k. In particular, we can bound the inner sum by $(2w-1)\sqrt{p}$. Using Lemma 1 in [6], we have the better bound $(2w-2)\sqrt{p}+1$, but we shall not use it here. When $q(x)$ is a k-th power, then we use the trivial bound of p.

Using this analysis, we can now bound $S_w(p,h,\chi,k)$ by placing the bound $(2w-1)\sqrt{p}$ when $q(x)$ is not a k-th power and p otherwise. Combining this with $w \le 9h$ yields

$$S_w(p,h,\chi,k) \le (2w-1)h^{2w}\sqrt{p} + b_w(p,h,k)p \le (2w-1)h^{2w}\sqrt{p} + c_w(h,2)p. \tag{7}$$

Now, let's calculate $c_w(h,2)$:

$$c_w(h,2) = \sum_{d=0}^{\lfloor \frac{w}{2} \rfloor}\left(\frac{w!}{d!2^d}\right)^2 \frac{h^w}{(w-2d)!} = \frac{(2w)!}{2^w w!}h^w, \tag{8}$$

the last equality coming from Lemma 2.3.

Combining (7) and (8) we get the desired inequality. □

Remark 2.1. From the proof we could derive a better upper bound when $k > 2$, which is

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} < c_w(h,k)p + (2w-1)p^{1/2}h^{2w}. \tag{9}$$

3. Burgess–Norton lower bound

Let's start with a couple of lemmas that will be required in our lower bound estimate.

Lemma 3.1. *Let $x \geq 1$ be a real number. Then*

$$x \sum_{q \leq x} \frac{\phi(q)}{q} - \sum_{q \leq x} \phi(q) \geq \frac{3}{\pi^2} x^2 - x. \tag{10}$$

Proof. Let's estimate the sum.

$$\begin{aligned} x \sum_{q \leq x} \frac{\phi(q)}{q} - \sum_{q \leq x} \phi(q) &= \sum_{q \leq x} \left(\frac{x}{q} - 1 \right) \phi(q) = \sum_{q \leq x} \left(\frac{x}{q} - 1 \right) \sum_{d \mid q} \frac{\mu(d) q}{d} \\ &= \sum_{d \leq x} \frac{\mu(d)}{d} \sum_{q \leq \frac{x}{d}} (x - dq) = \sum_{d \leq x} \frac{\mu(d)}{d} \left(x \left\lfloor \frac{x}{d} \right\rfloor - \frac{d \lfloor \frac{x}{d} \rfloor \left(\lfloor \frac{x}{d} \rfloor + 1 \right)}{2} \right). \end{aligned}$$

Now, writing $\lfloor \frac{x}{d} \rfloor = \frac{x}{d} - \{ \frac{x}{d} \}$, we get

$$\begin{aligned} &\sum_{d \leq x} \frac{\mu(d)}{d} \left(\frac{x^2}{2d} - \frac{x}{2} + \frac{d \{ \frac{x}{d} \} \left(1 - \{ \frac{x}{d} \} \right)}{2} \right) \\ &= \frac{x^2}{2} \left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \sum_{d > x} \frac{\mu(d)}{d^2} \right) - \frac{x}{2} \sum_{d \leq x} \frac{\mu(d)}{d} + \frac{1}{2} \sum_{d \leq x} \mu(d) \left\{ \frac{x}{d} \right\} \left(1 - \left\{ \frac{x}{d} \right\} \right). \end{aligned}$$

Now, since $\displaystyle\sum_{d=1}^{\infty} \frac{\mu(d)}{d} = \frac{6}{\pi^2}$ and since $0 \leq \left\{ \frac{x}{d} \right\} \left(1 - \left\{ \frac{x}{d} \right\} \right) \leq \frac{1}{4}$, we have

$$x \sum_{q \leq x} \frac{\phi(q)}{q} - \sum_{q \leq x} \phi(q) \geq \frac{3}{\pi^2} x^2 - \frac{x^2}{2} \sum_{d > x} \frac{\mu(d)}{d^2} - \frac{x}{2} \sum_{d \leq x} \frac{\mu(d)}{d} - \frac{1}{8} \sum_{\substack{d \leq x \\ d \text{ squarefree}}} 1. \tag{11}$$

Claim 3.1. *For real $x \geq 1$,*

$$\left| \sum_{d > x} \frac{\mu(d)}{d^2} \right| \leq \frac{1}{x}.$$

Proof of the Claim: Note that for any positive integer d we have that $\frac{1}{d^2}$ is smaller than $\int_{d-1/2}^{d+1/2} \frac{dt}{t^2}$. Thus

$$\left|\sum_{d>x} \frac{\mu(d)}{d^2}\right| \leq \sum_{d>x} \int_{d-\frac{1}{2}}^{d+\frac{1}{2}} \frac{dt}{t^2} = \int_{x-\frac{1}{2}}^{\infty} \frac{dt}{t^2} = \frac{1}{x-\frac{1}{2}}.$$

To change $x - 1/2$ into x, note that there is at least one d missing in the interval $[x, x+4]$, since we only take squarefree d's in the sum. Thus the absolute value of the sum is smaller than $\frac{1}{x-\frac{1}{2}} - \frac{1}{(x+4)^2}$. This is smaller than $\frac{1}{x}$ once $x \geq 11$, proving the claim for real $x \geq 11$. To complete the proof for $x \geq 1$ we use the fact that $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$, which implies that $\sum_{d>x} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} - \sum_{d\leq x} \frac{\mu(d)}{d}$. One can now manually check the integer cases where $1 \leq x \leq 11$ and note that $\left|\sum_{d>x} \frac{\mu(d)}{d^2}\right| < \frac{1}{x+1}$, which implies the claim for real $x \leq 11$.

Claim 3.2. *For real $x \geq 1$, the number of squarefree integers in $[1, x]$ is at most $\frac{2}{3}x + 2$.*

Proof of the Claim: The number of squarefree numbers up to x is at most

$$\lfloor x \rfloor - \left\lfloor \frac{x}{4} \right\rfloor - \left\lfloor \frac{x}{9} \right\rfloor + \left\lfloor \frac{x}{36} \right\rfloor \leq \frac{2}{3}x + 2.$$

Claim 3.3. *For real $x \geq 1$,*

$$\left|\sum_{d\leq x} \frac{\mu(d)}{d}\right| \leq \frac{2}{3} + \frac{3}{x}.$$

Proof of the Claim: The proof here is a modified version of a proof of Hildebrand [9]. Let $e(n) = 1$ if $n = 1$ and $e(n) = 0$ otherwise. Let $S(x) = \sum_{n\leq x} e(n)$. Then $S(x) = 1$. However, we also have

$$S(x) = \sum_{n\leq x} \sum_{d|n} \mu(d) = \sum_{d\leq x} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = x \sum_{d\leq x} \frac{\mu(d)}{d} - \sum_{d\leq x} \mu(d) \left\{ \frac{x}{d} \right\}.$$

Therefore,

$$x\left|\sum_{d\le x}\frac{\mu(d)}{d}\right| \le \left|1+\sum_{d\le x}\mu(d)\left\{\frac{x}{d}\right\}\right| \le \frac{2}{3}x+3.$$

To prove the last inequality we used that the number of squarefree numbers up to x is at most $\frac{2}{3}x+2$, which was proven in the previous claim.

Combining Claims 3.1, 3.2 and 3.3 with (11) we have

$$x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q) \ge \frac{3}{\pi^2}x^2-\frac{11}{12}x-\frac{7}{4} \ge \frac{3}{\pi^2}x^2-x,$$

where the last inequality holds for $x \ge 21$.

For $x \le 3$, the right hand side of (10) is negative, while the left hand side is positive, therefore the inequality is true for $x \le 3$. Now, for the integers $3 \le x \le 21$ we can manually check that

$$x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q) \ge \frac{3}{\pi^2}(x+1)^2-(x+1).$$

Since the right hand side of (10) is increasing for $x \ge 3$, we have a proof for all real $x \le 21$. □

Lemma 3.2. *Let $x \ge 1$ be a real number. Then*

$$2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q) \ge \frac{9}{\pi^2}x^2-x\left(\frac{\log x}{3}+3\right). \tag{12}$$

Proof. Doing the estimates the same way as in Lemma 3.1, we get

$$\begin{aligned}2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q) &= \frac{9}{\pi^2}x^2-\frac{3x^2}{2}\sum_{d>x}\frac{\mu(d)}{d}\\ &\quad-\frac{x}{2}\sum_{d\le x}\frac{\mu(d)}{d}-x\sum_{d\le x}\frac{\mu(d)}{d}\left\{\frac{x}{d}\right\}+\frac{1}{2}\sum_{d\le x}\left\{\frac{x}{d}\right\}\left(1-\left\{\frac{x}{d}\right\}\right)\mu(d).\end{aligned} \tag{13}$$

Claim 3.4. *For real $x \ge 1$,*

$$x\sum_{d\le x}\frac{\mu(d)}{d}\left\{\frac{x}{d}\right\}-\frac{1}{2}\sum_{d\le x}\left\{\frac{x}{d}\right\}\left(1-\left\{\frac{x}{d}\right\}\right)\mu(d) \le \frac{1}{3}x\log x+\frac{11}{10}x+\frac{3}{2}.$$

Proof of the Claim: We have

$$x\sum_{d\le x}\frac{\mu(d)}{d}\left\{\frac{x}{d}\right\}-\frac{1}{2}\sum_{d\le x}\left\{\frac{x}{d}\right\}\left(1-\left\{\frac{x}{d}\right\}\right)\mu(d)$$
$$=\sum_{d\le x}\mu(d)\left\{\frac{x}{d}\right\}\left(\frac{x}{d}-\frac{1-\left\{\frac{x}{d}\right\}}{2}\right). \quad (14)$$

Note, that all factors except $\mu(d)$ are positive, which implies that we can bound (14) by

$$\sum_{\substack{d\le x\\ \mu(d)=1}}\left\{\frac{x}{d}\right\}\left(\frac{x}{d}-\frac{1-\left\{\frac{x}{d}\right\}}{2}\right)\le x\sum_{\substack{d\le x\\ \mu(d)=1}}\frac{1}{d}. \quad (15)$$

Note that $\log x\le\sum_{d\le x}\frac{1}{d}\le\log x+1$. Now, let's bound the sum over squarefree numbers:

$$\sum_{\substack{d\le x\\ d \text{ squarefree}}}\frac{1}{d}\le\sum_{d\le x}\frac{1}{d}-\frac{1}{4}\sum_{d\le\frac{x}{4}}\frac{1}{d}-\frac{1}{9}\sum_{d\le\frac{x}{9}}\frac{1}{d}+\frac{1}{36}\sum_{d\le\frac{x}{36}}\frac{1}{d}$$
$$\le\frac{2}{3}\log x+1+\frac{1}{36}+\frac{\log 4}{4}+\frac{\log 9}{9}-\frac{\log 36}{36}\le\frac{2}{3}\log x+\frac{23}{15}.$$

However,

$$\sum_{\substack{d\le x\\ d \text{ squarefree}}}\frac{1}{d}=\sum_{\substack{d\le x\\ \mu(d)=1}}\frac{1}{d}+\sum_{\substack{d\le x\\ \mu(d)=-1}}\frac{1}{d}\le\frac{2}{3}\log x+\frac{23}{15}, \quad (16)$$

and

$$\sum_{d\le x}\frac{\mu(d)}{d}=\sum_{\substack{d\le x\\ \mu(d)=1}}\frac{1}{d}-\sum_{\substack{d\le x\\ \mu(d)=-1}}\frac{1}{d}\le\frac{2}{3}+\frac{3}{x}. \quad (17)$$

The last inequality being true because of Claim 3.3. Adding (16) and (17), dividing by 2, and using (14) and (15) we get our claim.

Now, using the results of Claims 3.1, 3.3 and 3.4 in (13) yields

$$2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q)$$
$$\ge\frac{9}{\pi^2}x^2-x\left(\frac{\log x}{3}+\frac{3}{2}+\frac{1}{3}+\frac{11}{10}\right)-3\ge\frac{9}{\pi^2}x^2-x\left(\frac{\log x}{3}+3\right),$$

where the last inequality is true for $x\ge 45$.

For $x\le 3$, the right hand side of (12) is negative, while the left hand side is positive, therefore the inequality is true for $x\le 3$. Now, for the integers $3\le x\le 45$ we can manually check that

$$2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q)\ge\frac{9}{\pi^2}(x+1)^2-(x+1)\left(\frac{\log(x+1)}{3}+3\right).$$

Since the right hand side of (12) is increasing for $x\ge 3$, we have a proof for all real $x\le 45$. □

To prove a lower bound on $S_w(p,h,k)$ we will need an upper bound on $g(p,k)$. The next lemma is an elementary bound on $g(p,k)$ proven for $k=2$ in [12] (Lemma 1).

Lemma 3.3. *Let $g(p,k)$ be the least k-th power non-residue* $\bmod p$. *Then*

$$g(p,k)<\sqrt{p}+\frac{1}{2}.$$

Proof. The following proof is very similar to the one in [12] but the argument goes all the back to Western and Miller (see [21]) and Norton [10]. Let $q=g(p,k)$ and $r=\left\lceil\frac{p}{q}\right\rceil$. Note that $p<rq<p+q$, therefore rq is a k-th power $\bmod p$. Since q is a k-th power non-residue $\bmod p$, then r is also a k-th power non-residue $\bmod p$. By the minimality of q, $r\ge q$. Therefore $1+p/q>r\ge q$. Since p is an integer and $p>q^2-q$, then

$$p\ge q^2-q+1>\left(q-\frac{1}{2}\right)^2,$$

and the lemma follows. □

We now have the ingredients to prove the lower bound on $S_w(p,h,k)$.

Theorem 3.1. *Let $p \geq 5$ be a prime. Let χ be a character* $\bmod p$ *of order k. Assume that $\chi(a) = 1$ for all $1 \leq a < H$. Let h and w be positive integers such that $4 \leq h \leq H$. Let $X = H/h$ and let $A = \frac{3}{\pi^2}$. Then*

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} \geq 2h^{2w-1}AH^2 \left(1 - \frac{1}{2AX}\right).$$

Furthermore, if -1 is a k-th power $\bmod p$*, then*

$$S_w(p,h,\chi,k) \geq 3h^{2w-1}AH^2 \left(1 - \frac{\frac{\log X}{3} + 3}{3AX} - \frac{1}{3AX^2} + \frac{1}{3AX^2h}\right).$$

Proof. We follow the proof in [10] with some minor modifications. The idea is to find long intervals where χ is constant (either 1 or -1), making the inner sum as big as possible in a segment.

For each pair of integers t, q with

$$0 \leq t < q \leq X \text{ and } \gcd(t,q) = 1, \tag{18}$$

define $I(q,t)$ to be the closed interval

$$I(q,t) = \left[\frac{tp - H}{q}, \frac{tp + H}{q}\right].$$

Claim 3.5. *The intervals $I(q,t)$ are disjoint.*

Proof of the Claim: Let's assume that $I(q_1,t_1)$ and $I(q_2,t_2)$ contain a common element s, so that $|s - \frac{t_i p}{q_i}| \leq \frac{H}{q_i}$ for $i = 1, 2$. Thus, $|\frac{t_1 p}{q_1} - \frac{t_2 p}{q_2}| \leq \frac{H}{q_1} + \frac{H}{q_2}$. By Lemma 3.3, $H \leq g(p,k) < \sqrt{p} + 1/2$. Using that $h \geq 4$ and $p \geq 2$, we get

$$|t_1q_2 - t_2q_1| \leq \frac{(q_1+q_2)H}{p} \leq \frac{2HX}{p} = \frac{2H^2}{hp} < \frac{2p + 2\sqrt{p} + 1/2}{4p} < 1.$$

Now, since $|t_1q_2 - t_2q_1| < 1$ and t_1, t_2, q_1, q_2 are integers, we have $t_1q_2 = t_2q_1$. But $\gcd(q_1,t_1) = 1$ and $\gcd(q_2,t_2) = 1$, therefore $t_1 = t_2$ and $q_1 = q_2$ proving the claim.

Claim 3.6. *Each $I(q,t) \subset [-H, -H + p)$.*

Proof of the Claim: Since $t \geq 0$ and $p \geq 2$, we have $\frac{tp-H}{p} \geq \frac{-H}{p} \geq -H$. Now, since $t < q$, we have $t \leq q-1$, therefore

$$\frac{tp+H}{q} \leq \frac{(q-1)p+H}{q} = p - \frac{p-H}{q} \leq p - \frac{p-H}{X} = p - \frac{(p-H)h}{H}.$$

In the inequalities we used $q \leq X$ and that $X = H/h$. To finish proving the claim we will use that $h \geq 4$:

$$\frac{tp+H}{q} \leq p - \frac{(p-H)h}{H} \leq p - \frac{4(p-H)}{H} < p - H.$$

The last inequality is true because $H < \sqrt{p}+1/2$ and $4 \leq h \leq p$ and therefore $H^2 + 4H < p + 5\sqrt{p} + 3 < 4p$, which is true for $p \geq 5$. Therefore, we have proved the claim.

Using the periodicity of χ and Claims 3.5 and 3.6 we have the following:

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} = \sum_{-H \leq m < -H+p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w}$$

$$\geq \sum_{q,t} \sum_{m \in I(q,t)} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} = \sum_{q,t} \sum_{m \in I(q,t)} \left| \sum_{l=0}^{h-1} \chi(q(m+l)-tp) \right|^{2w}. \quad (19)$$

The sum is over all pairs (q,t) satisfying (18). Note that $\chi(q) = 1$ because $0 < q \leq X < H$. The last equality in (19) comes from $\chi(m+l) = \chi(q)\chi(m+l) = \chi(q(m+l)) = \chi(q(m+l)-tp)$ (it is only needed that $\chi(q) \neq 0$, for (19) to be true).

For q, t satisfying (18), let $J(q,t)$ and $K(q,t)$ be defined as follows:

$$J(q,t) = \left[\frac{tp-H}{q}, \frac{tp}{q} - h + 1 \right)$$

and

$$K(q,t) = \left(\frac{tp}{q}, \frac{tp+H}{q} - h + 1 \right].$$

If $m \in J(q,t)$, then for $0 \leq l \leq h-1$ we have $0 < tp - q(m+l) \leq H$, therefore $\chi(q(m+l)-tp)) = \chi(-1)\chi(tp-q(m+l)) = \chi(-1)$.

Similarly, if $m \in K(q,t)$, then for $0 \leq l \leq h-1$ we have $0 < q(m+l) - tp \leq H$ and hence $\chi(q(m+l)-tp) = \chi(1) = 1$.

Since each of $J(q,t)$, $K(q,t)$ contains at least $\frac{H}{q}-h$ integers (note that $q \leq X = \frac{H}{h}$ and hence $\frac{H}{q} \geq h$) then we can place a lower bound on $S_w(p,h,\chi,k)$ as follows:

$$S_w(p,h,\chi,k) \geq 2\sum_{q,t}\left(\frac{hX}{q}-h\right)h^{2w}$$

$$= 2h^{2w+1}\left(X\sum_{1\leq q\leq X}\frac{\phi(q)}{q}-\sum_{1\leq q\leq X}\phi(q)\right) \geq 2AX^2h^{2w+1}\left(1-\frac{1}{2AX}\right). \quad (20)$$

The last inequality being Lemma 3.1. Once we make the substitution of $X = \frac{H}{h}$ we get the desired inequality.

If -1 is a k-th power $\bmod\ p$, we can improve (20). Instead of using $J(q,t)$ and $K(q,t)$, we simply consider the interval

$$L(q,t) = \left[\frac{tp-H}{q}, \frac{tp+H}{q}-h+1\right].$$

If $m \in L(q,t)$, then for $0 \leq l \leq h-1$, we have $-H \leq q(m+l)-tp \leq H$, and hence $\chi(q(m+l)-tp) = 1$ unless $q(m+l) = tp$. Since $q > t \geq 0$, then $0 \leq m+l = \frac{t}{q}p < p$. But $p \mid q(m+l)$ implies that $m+l = 0$, and so $t = 0$. Because of the coprimality condition, $t = 0$ implies $q = 1$. In this latter case, we omit those values of m for which there is an l with $m+l = 0$, and we get

$$S_w(p,h,\chi,k) \geq \sum_{-H\leq m\leq -h} h^{2w} + \sum_{1\leq m\leq H-h+1} h^{2w} + \sum_{\substack{q,t\\ q>1}}\sum_{m\in L(q,t)} h^{2w}$$

$$\geq (2(H-h)+1)\,h^{2w} + \sum_{1<q\leq X}\sum_{\substack{0\leq t<q\\ \gcd(t,q)=1}}\left(\frac{2H}{q}-h\right)h^{2w}.$$

From this and $X = \frac{H}{h}$, it follows that if -1 is a k-th power $\bmod p$, then

$$S_w(p,h,\chi,k) \geq h^{2w+1}\left(2X\sum_{1\leq q\leq X}\frac{\phi(q)}{q}-\sum_{1\leq q\leq X}\phi(q)-1+\frac{1}{h}\right)$$

$$\geq 3AX^2h^{2w+1}\left(1-\frac{\frac{\log x}{3}+3}{3AX}-\frac{1}{3AX^2}+\frac{1}{3AX^2h}\right).$$

The last inequality comes from Lemma 3.2. Once we make the substitution of $X = \frac{H}{h}$ we get the desired inequality. □

4. Main theorem

Before we prove our main theorem, we need a lemma:

Lemma 4.1. *Let p be a prime. Let $k > 1$ be an integer such that $k \mid p-1$. If $d = \gcd\left(k, \frac{p-1}{2}\right)$ and $d \geq 2$, then -1 is a d-th power* $\bmod p$ *and furthermore $g(p,k) \leq g(p,d)$.*

Proof. Let r be a primitive root $\bmod p$. Then $r^{\frac{p-1}{2}} \equiv -1 \bmod p$. Since $d \mid \frac{p-1}{2}$, then -1 is a d-th power $\bmod p$. Now note that if $a < g(p,k)$, then a is a k-th power $\bmod p$ and hence a d-th power $\bmod p$ since $d \mid k$, therefore $g(p,d) \geq g(p,k)$. □

Note that $d \geq 2$ unless $k = 2$ and $p \equiv 3 \pmod 4$.

The following theorem will deal with the large cases of our main theorem. The main theorem will be split into cases after proving this theorem.

Theorem 4.1. *Let p be an odd prime. Let $k \geq 2$ be an integer such that $k \mid p-1$ and let $p \geq p_0$. Then*

$$g(p,k) < \beta(p_0) p^{1/4} \log p,$$

unless $k = 2$ and $p \equiv 3 \pmod 4$, in which case

$$g(p,2) \leq \alpha(p_0) p^{1/4} \log p,$$

where $\beta(p_0)$ and $\alpha(p_0)$ are constants depending only on p_0 described in Table 1.

We remark that from the proof, one can show that $\alpha(p_0) \to \sqrt{\frac{e}{8A}} = \frac{\pi}{2}\sqrt{\frac{e}{6}} = 1.05728\ldots$ and $\beta(p_0) \to \sqrt{\frac{e}{12A}} = \frac{\pi}{6}\sqrt{e} = 0.863268\ldots$ as $p_0 \to \infty$.

Proof. Let χ be a character $\bmod p$ of order k. Assume that $\chi(a) = 1$ for all $1 \leq a < H$. Let h and w be positive integers such that $4 \leq h \leq H$. Let $X = H/h$ and let $A = \frac{3}{\pi^2}$. Then by Theorem 3.1

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} \geq 2h^{2w-1} A H^2 \left(1 - \frac{1}{2AX}\right).$$

If $w \leq 9h$, we have from Theorem 1.1

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} < \frac{(2w)!}{2^w w!} p h^w + (2w-1) p^{1/2} h^{2w}. \quad (21)$$

p_0	$\beta(p_0)$	$\alpha(p_0)$
10^7	1.27188	1.46048
10^8	1.18098	1.39566
10^9	1.12507	1.35024
10^{10}	1.08759	1.31654
10^{12}	1.04060	1.26945
10^{15}	1.00115	1.22520
10^{20}	0.96549	1.18242
10^{30}	0.93104	1.14029
10^{40}	0.91397	1.11938
10^{50}	0.90377	1.10689
10^{60}	0.89699	1.09858

Table 1: Upper bound for the least k-th power non-residue mod p for $p \geq p_0$.

Combining these two we get that

$$2AH^2\left(1-\frac{1}{2AX}\right) < \frac{(2w)!}{2^w w!}ph^{1-w} + (2w-1)p^{1/2}h = f(w,h), \tag{22}$$

is true for all positive integers h and w satisfying $4 \leq h \leq H$ and $w \leq 9h$.

Note that if we want to have H as small as possible, then we want to minimize $f(w,h)$, because the left hand side is approximately $2AH^2$, so H is approximately $\sqrt{f(w,h)/(2A)}$, where A is a constant. To minimize $f(w,h)$ one can use simple techniques from Calculus to figure out the best asymptotic choices of w and h. Below we have chosen h and w to match the optimal asymptotic choice and to simplify some of the difficulties that come from dealing with the fact that h and w are integers.

Let

$$h = \left\lfloor \left(\frac{(2w)!}{2^w w!}\frac{w-1}{2w-1}\right)^{\frac{1}{w}} p^{\frac{1}{2w}} \right\rfloor + 1 \tag{23}$$

and

$$w = \left\lfloor \frac{\log p}{4} \right\rfloor + 1. \tag{24}$$

Then

$$f(w,h) = h\sqrt{p}\left(\frac{(2w)!}{2^w w!}\frac{\sqrt{p}}{h^w} + 2w - 1\right) < h\sqrt{p}\left(2w+1+\frac{1}{w-1}\right)$$
$$< \left(\frac{(2w)!}{2^w w!}\frac{w-1}{2w-1}\right)^{\frac{1}{w}}\left(2w+1+\frac{1}{w-1}\right)p^{\frac{1}{2}+\frac{1}{2w}} + p^{\frac{1}{2}}\left(2w+1+\frac{1}{w-1}\right)$$
$$< \left(2w+1+\frac{1}{w-1}\right)\sqrt{p}\left(e^2\left(\frac{(2w)!}{2^w w!}\frac{w-1}{2w-1}\right)^{\frac{1}{w}} + 1\right). \quad (25)$$

The last inequality is true because $p^{\frac{1}{2w}} < e^2$.

Note the following explicit inequalities on Stirling's formula [13] which will help us deal with the above expression:

$$\left(\frac{n}{e}\right)^n \sqrt{2\pi n}\, e^{\frac{1}{12n+1}} < n! < \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\, e^{\frac{1}{12n}}.$$

Hence

$$\left(\frac{(2w)!}{2^w w!}\right)^{\frac{1}{w}} < \left(\left(\frac{2w}{e}\right)^w \sqrt{2}\, e^{\frac{1}{24w}-\frac{1}{12w+1}}\right)^{\frac{1}{w}} = \left(\frac{2w}{e}\right) 2^{\frac{1}{2w}}\, e^{\frac{1}{24w^2}-\frac{1}{12w^2+w}}. \quad (26)$$

Combining (26) with (25) and using that $\frac{w-1}{2w-1} < \frac{1}{2}$ we get

$$f(w,h) < \left(2w+1+\frac{1}{w-1}\right)\sqrt{p}\left(2we\, 2^{-\frac{1}{2w}}\, e^{\frac{1}{24w^2}-\frac{1}{12w^2+w}} + 1\right)$$
$$< \left(2w+1+\frac{1}{w-1}\right)(2we+1)\sqrt{p}.$$

Now, the right hand side is increasing in w, so we may just use an upper bound for w which would be $\frac{\log p}{4} + 1$. Using this upper bound yields

$$f(w,h) < \left(\frac{e}{4}\log^2 p + \frac{5e+1}{2}\log p + 8e + 3 + \frac{8e+4}{\log p}\right)\sqrt{p}$$
$$= \left(\frac{e}{4} + \frac{5e+1}{2\log p} + \frac{8e+3}{\log^2 p} + \frac{8e+4}{\log^3 p}\right)\sqrt{p}\log^2 p = K(p)\sqrt{p}\log^2 p, \quad (27)$$

where $K(p)$ depends on p and goes to $\frac{e}{4}$ as $p \to \infty$.

Also note

$$h < 2we + 1 < \frac{e}{2}\log p + (2e+1) = \left(\frac{e}{2} + \frac{2e+1}{\log p}\right)\log p.$$

Assume $p \geq p_0$ and $H \geq \alpha(p_0)\, p^{1/4}\log p$. We have $\alpha(p_0) \geq \sqrt{\frac{e}{8A}}$, hence

$$X = \frac{H}{h} \geq \frac{\alpha(p_0)p^{1/4}\log p}{\left(\frac{e}{2} + \frac{2e+1}{\log p}\right)\log p} \geq \frac{\sqrt{\frac{e}{8A}}}{\left(\frac{e}{2} + \frac{2e+1}{\log p}\right)}p^{1/4}.$$

Let $X(p_0)$ be defined as

$$X(p_0) = \frac{\sqrt{\frac{e}{8A}}}{\left(\frac{e}{2} + \frac{2e+1}{\log p_0}\right)}p_0^{1/4},$$

and let

$$\alpha(p_0) = \sqrt{\frac{K(p_0)}{2A\left(1 - \frac{1}{2AX(p_0)}\right)}}.$$

The left hand side of (22) can therefore be bounded from below for $p \geq p_0$:

$$2AH^2\left(1 - \frac{1}{2AX}\right) \geq 2A\left(\alpha(p_0)\right)^2\sqrt{p}\log^2 p\left(1 - \frac{1}{2AX(p_0)}\right)$$

$$\geq K(p_0)\sqrt{p}\log^2 p \geq K(p)\sqrt{p}\log^2 p > f(w,h),$$

giving us a contradiction, proving that $H < \alpha(p_0)p^{1/4}\log p$, that is

$$g(p,k) \leq \alpha(p_0)p^{1/4}\log p.$$

Now, if -1 is a k-th power mod p we can do better, since by the second part of Theorem 3.1 we have

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w}$$

$$\geq 3h^{2w-1}AH^2\left(1 - \frac{\frac{\log X}{3}+3}{3AX} - \frac{1}{3AX^2} + \frac{1}{3AX^2h}\right).$$

Combining this with (21) we get

$$3AH^2\left(1-\frac{\frac{\log X}{3}+3}{3AX}-\frac{1}{3AX^2}+\frac{1}{3AX^2h}\right)<f(w,h). \tag{28}$$

Assume $p\geq p_0$ and $H\geq \beta(p_0)\,p^{1/4}\log p\geq \sqrt{\frac{e}{12A}}p^{1/4}\log p$, then we can work just as before. Let

$$X(p_0)=\frac{\sqrt{\frac{e}{12A}}}{\left(\frac{e}{2}+\frac{2e+1}{\log p_0}\right)}p_0^{1/4},$$

and let

$$\beta(p_0)\geq\sqrt{\frac{K(p_0)}{3A\left(1-\frac{\frac{\log(X(p_0))}{3}+3}{3AX(p_0)}-\frac{1}{3AX(p_0)^2}+\frac{1}{3AX(p_0)^2h}\right)}}.$$

The left hand side of (28) can therefore be bounded from below for $p\geq p_0$:

$$\begin{aligned}
&3AH^2\left(1-\frac{\frac{\log X}{3}+3}{3AX}-\frac{1}{3AX^2}+\frac{1}{3AX^2h}\right)\\
&\geq 3A\left(\beta(p_0)\right)^2\sqrt{p}\log^2 p\left(1-\frac{\frac{\log(X(p_0))}{3}+3}{3AX(p_0)}-\frac{1}{3AX(p_0)^2}+\frac{1}{3AX(p_0)^2h}\right)\\
&\geq K(p_0)\sqrt{p}\log^2 p\geq K(p)\sqrt{p}\log^2 p>f(w,h),
\end{aligned}$$

giving us a contradiction, proving that $H<\beta(p_0)p^{1/4}\log p$, that is

$$g(p,k)\leq\beta(p_0)p^{1/4}\log p.$$

If $\gcd\left(k,\frac{p-1}{2}\right)=d>1$, then Lemma 4.1 implies that -1 is a d-th power and

$$g(p,k)\leq g(p,d)\leq\beta(p_0)p^{1/4}\log p.$$

Note that we do need $d>1$ as the last inequality is only true for $d\geq 2$.

Since $\gcd\left(k,\frac{p-1}{2}\right)=1$ if and only if $k=2$ and $p\equiv 3\pmod 4$, we conclude the statement of the theorem. The values of the table for $\alpha(p_0)$ and $\beta(p_0)$ were computed by plugging in the respective values of p_0. □

We have proved the main theorem for $p \geq 10^{60}$. To complete the proof we'll do it in four cases:

- when $k = 2$ and $p \equiv 1 \pmod 4$ with $p \leq 10^{25}$,
- when $k = 2$ and $p \equiv 1 \pmod 4$ or $k \geq 3$, where $10^{25} < p < 10^{60}$,
- when $k \geq 3$ with $p \leq 10^{25}$, and
- when $k = 2$ and $p \equiv 3 \pmod 4$ with $p < 10^{60}$.

To deal with the case where $k = 2$ and $p \equiv 1 \pmod 4$ we first show that either p is a $(g(p,2)-1)$-pseudosquare or $g(p,2) = 2$. Let's recall what a pseudosquare is:

Definition 4.1. *A positive integer n is called a q-pseudosquare if $n \equiv 1 \pmod 8$ is not a square and for all odd primes $r \leq q$, we have $\left(\frac{n}{r}\right) = 1$, where $\left(\frac{n}{r}\right)$ is the Legendre symbol.*

Lemma 4.2. *For p a prime satisfying $p \equiv 1 \pmod 4$ then either p is a $(g(p,2)-1)$-pseudosquare or $g(p,2) = 2$.*

Proof. If $p \equiv 5 \pmod 8$ then 2 is not a square $\bmod p$, and hence $g(p,2) = 2$. Therefore, we may assume that $p \equiv 1 \pmod 8$. Note that by the definition of $g(p,2)$, we have that $\left(\frac{r}{p}\right) = 1$ for all odd primes $r < g(p,2)$. Now, since $p \equiv 1 \pmod 8$, by quadratic reciprocity we have

$$\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = 1.$$

Therefore p is a $(g(p,2)-1)$-pseudosquare. □

Proposition 4.1. *Let p be a prime such that $p \equiv 1 \pmod 4$ and $p \leq 10^{25}$. Then*

$$g(p,2) \leq 0.9p^{1/4} \log p.$$

Proof. If $p \equiv 5 \pmod 8$, then $g(p,2) = 2$ and hence $g(p,2) \leq 0.9p^{1/4} \log p$ as long as $p \geq 5$, which is true. Therefore, we may assume $p \equiv 1 \pmod 8$. We know from Lemma 4.2 that p is a $(g(p,2)-1)$-pseudosquare. In [15], it was shown that for $q \geq 379$, 379-pseudosquares are greater than 10^{25}. Therefore if $g(p,2) \geq 379$, then $p \geq 10^{25}$.

w	h	p	w	h	p	w	h	p
16	76	$[10^{25}, 10^{27}]$	17	85	$[10^{27}, 10^{29}]$	17	99	$[10^{29}, 10^{31}]$
18	106	$[10^{31}, 10^{33}]$	18	121	$[10^{33}, 10^{35}]$	21	116	$[10^{35}, 10^{38}]$
22	131	$[10^{38}, 10^{41}]$	25	134	$[10^{41}, 10^{44}]$	29	132	$[10^{44}, 10^{47}]$
30	141	$[10^{47}, 10^{50}]$	31	159	$[10^{50}, 10^{54}]$	34	168	$[10^{54}, 10^{58}]$
34	180	$[10^{58}, 10^{60}]$						

Table 2: Values of h and w chosen to prove that $g(p,2) \leq 0.9p^{1/4}\log p$ whenever $p \equiv 1 \pmod 4$ and $10^{25} \leq p \leq 10^{60}$. As an example on how to read the table: when $w = 16$ and $h = 76$, then $\gamma(p, w, h) < 0.9$ for all $p \in [10^{25}, 10^{27}]$.

Since the solution to $0.9p^{1/4}\log p = 379$ is below 900000, then we need only check up to 900000 for the cases where $g(p,2) \leq 379$. A simple loop in the computer confirms that for all these cases we have $g(p,2) \leq 0.9p^{1/4}\log p$, completing the proof of the proposition. □

Proposition 4.2. *Let p be prime such that $10^{25} < p < 10^{60}$. If $p \equiv 1 \pmod 4$ and $k = 2$ or if $k \geq 3$, then $g(p,k) \leq 0.9p^{1/4}\log p$.*

Proof. To deal with this gap, we'll choose particular w's and h's in $f(w,h)$ (see (22)) instead of the values of h and w chosen in Theorem 4.1.

Let $A = \frac{3}{\pi^2}$ as before

$$X(p) = \frac{\sqrt{\frac{e}{12A}}}{h}p^{1/4}.$$

Let $\gamma(p,w,h)$ be defined in the following way:

$$\gamma(p,w,h) = \sqrt{\frac{f(w,h)}{3A\sqrt{p}\log^2 p\left(1 - \frac{\frac{\log(X(p))}{3}+3}{3A(X(p))} - \frac{1}{3A(X(p))^2} + \frac{1}{3A(X(p))^2 h}\right)}}.$$

Then by similar arguments as in Theorem 4.1, we have that $g(p,k)$ is less than $\gamma(p,h,w)p^{1/4}\log p$. Hence, all we want is for $\gamma(p,h,w)$ to be less than or equal to 0.9. We'll attack this by picking particular h's and w's in different intervals. To check whether $\gamma(p,h,w) \leq 0.9$, we need only check the endpoints of the intervals since $\gamma(p,h,w)$ is concave up. Table 2 completes the proof. □

Remark 4.1. The method can also yield $g(p,2) \leq 0.87p^{1/4}\log p$ when $p \equiv 1 \pmod 4$. However, it would require a much longer table to fill up the intervals all the way up to 10^{310}. It is also worth noting that if we started at 10^7 instead of 10^{25} (i.e., if we didn't have the result on pseudosquares), then the inequality we would get would be $g(p,2) \leq 0.93p^{1/4}\log p$, which is not much worse. Thus, the main ingredient in the improvement over Norton is not computational power, but improving the upper bound on the Burgess inequality.

Proposition 4.3. *Let $p \leq 10^{25}$ be a prime, and let $k \geq 3$ be an integer. Then*

$$g(p,k) \leq 0.9p^{1/4}\log p.$$

Proof. Note that an upper bound for the least k-th power non-residue is the least primitive root $\bmod p$, since a primitive root cannot be a k-th power. Running a loop where we check the least primitive root over primes up to 10^5 reveals that the only examples where the primitive root is greater than $0.9p^{1/4}\log p$ are $p = 2, 3, 7$ and 191. For $p = 2$, it doesn't make sense to define k-th power non-residue. For $p = 3$ it only makes sense when $k = 2$, but $k \geq 3$. For $p = 7$ it makes sense for $k = 2$ and $k = 3$. Since $k \geq 3$, we are left with the $k = 3$ case. For $k = 3$, the least cubic non-residue is $2 < (0.9)7^{1/4}\log 7$. To check what happens with $p = 191$, I ran a program looping over the possible k's (divisors of 190) and found that the least k-th power non-residue is 2 for all $k \mid p-1$ with $k \geq 3$. Therefore, for $k \geq 3$ and $p \leq 10^5$, $g(p,k) \leq 0.9p^{1/4}\log p$. Therefore we are now in the case where $10^5 \leq p \leq 10^{25}$.

Let's recall (9):

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} < c_w(h,k)ph^w + (2w-1)p^{1/2}h^{2w}.$$

Since $c_w(h,k)$ is decreasing on k and $k \geq 3$, we can replace $c_w(h,k)$ by $c_w(h,3)$. Let $f_2(w,h)$ be defined as

$$\begin{aligned} f_2(w,h) &:= h\sqrt{p}\left(2w - 1 + c_w(h,3)\frac{\sqrt{p}}{h^w}\right) \\ &= h\sqrt{p}\left(2w - 1 + \sum_{d=0}^{\lfloor \frac{w}{3} \rfloor}\left(\left(\frac{w!}{d!(3!)^d}\right)^2\left(\frac{\sqrt{p}}{h^{d+w}(w-3d)!}\right)\right)\right). \end{aligned}$$

w	h	p
3	12	$[10^5, 10^7]$
4	16	$[10^7, 10^9]$
6	21	$[10^9, 10^{12}]$
8	37	$[10^{12}, 10^{18}]$
12	47	$[10^{18}, 10^{25}]$

Table 3: Values of h and w chosen to prove that $g(p,k) \leq 0.9p^{1/4}\log p$ whenever $k \geq 3$ and $10^5 \leq p \leq 10^{25}$. As an example on how to read the table: when $w = 6$ and $h = 21$, then $\gamma_2(p, w, h) < 0.9$ for all $p \in [10^9, 10^{12}]$.

Then by Theorem 3.1 combined with (9), we have that the inequality (28) becomes

$$3AH^2\left(1 - \frac{\frac{\log X}{3}+3}{3AX} - \frac{1}{3AX^2} + \frac{1}{3AX^2h}\right) < f_2(w,h),$$

where A is the constant we've been using, $H \leq g(p,k)$ and $X = \frac{H}{h}$. Now, let

$$X(p) = \frac{\sqrt{\frac{e}{12A}}}{h}p^{1/4}.$$

Let $\gamma_2(p,w,h)$ be defined in the following way:

$$\gamma_2(p,w,h) = \sqrt{\frac{f_2(w,h)}{3A\sqrt{p}\log^2 p\left(1 - \frac{\frac{\log(X(p))}{3}+3}{3A(X(p))} - \frac{1}{3A(X(p))^2} + \frac{1}{3A(X(p))^2h}\right)}}.$$

Then by similar arguments as in Theorem 4.1, we have that $g(p,k)$ is less than $\gamma_2(p,h,w)p^{1/4}\log p$. Hence, all we want is for $\gamma_2(p,h,w)$ to be less than or equal to 0.9. We'll attack this by picking particular h's and w's in different intervals. Table 3 completes the proof of the interval $10^5 \leq p \leq 10^{25}$. □

Proposition 4.4. *Let $p > 3$ be a prime such that $p \equiv 3 \pmod 4$ and $p < 10^{60}$. Then*

$$g(p,2) \leq 1.1p^{1/4}\log p.$$

Proof. Running a loop over primes $p \equiv 3 \pmod 4$ up to 10^7 reveals that there is only one counter example, $p = 3$. Hence for $3 < p \leq 10^7$, $g(p,2) \leq 1.1p^{1/4}\log p$.

w	h	p	w	h	p	w	h	p
4	21	$[10^7, 10^{7.6}]$	5	21	$[10^{7.6}, 10^8]$	5	24	$[10^8, 10^9]$
6	25	$[10^9, 10^{10}]$	7	27	$[10^{10}, 10^{11}]$	7	34	$[10^{11}, 10^{12}]$
8	35	$[10^{12}, 10^{13}]$	9	36	$[10^{13}, 10^{14}]$	8	44	$[10^{14}, 10^{15}]$
8	55	$[10^{15}, 10^{16}]$	9	56	$[10^{16}, 10^{17}]$	9	64	$[10^{17}, 10^{18}]$
10	64	$[10^{18}, 10^{19}]$	12	60	$[10^{19}, 10^{21}]$	13	67	$[10^{21}, 10^{23}]$
14	75	$[10^{23}, 10^{25}]$	16	77	$[10^{25}, 10^{27}]$	17	85	$[10^{27}, 10^{29}]$
18	93	$[10^{29}, 10^{31}]$	19	100	$[10^{31}, 10^{33}]$	20	108	$[10^{33}, 10^{36}]$
21	121	$[10^{36}, 10^{39}]$	24	125	$[10^{39}, 10^{42}]$	25	140	$[10^{42}, 10^{45}]$
27	148	$[10^{45}, 10^{48}]$	28	163	$[10^{48}, 10^{51}]$	29	177	$[10^{51}, 10^{54}]$
30	192	$[10^{54}, 10^{58}]$	31	200	$[10^{58}, 10^{60}]$			

Table 4: Values of h and w chosen to prove that $g(p,2) \leq 1.1p^{1/4}\log p$ whenever $p \equiv 3 \pmod 4$ and $10^7 \leq p \leq 10^{60}$. As an example on how to read the table: when $w = 10$ and $h = 64$, then $\gamma_3(p,w,h) < 1.1$ for all $p \in [10^{18}, 10^{19}]$.

Therefore we are now in the case where $10^7 < p < 10^{60}$. To deal with this gap, we'll follow the same strategy as in Proposition 4.1, which is to choose particular w's and h's in $f(w,h)$ and fill up gaps.

As in the proof of Proposition 4.1, let A be the constant we've been using and let

$$X(p) = \frac{\sqrt{\frac{e}{8A}}}{h}p^{1/4}.$$

Let $\gamma_3(p,w,h)$ be defined in the following way:

$$\gamma_3(p,w,h) = \sqrt{\frac{f(w,h)}{2A\sqrt{p}\log^2 p\left(1 - \frac{1}{2AX(p)}\right)}}.$$

Then by similar arguments as in Theorem 4.1, we have that $g(p,2)$ is less than $\gamma_3(p,h,w)p^{1/4}\log p$. Hence, all we want is for $\gamma_3(p,h,w)$ to be less than or equal to 1.1. We'll attack this by picking particular h's and w's in different intervals. To check whether $\gamma_3(p,h,w) \leq 1.1$, we need only check the endpoints of the intervals, since $\gamma_3(p,h,w)$ is concave up. Table 4 completes the proof. □

Combining Propositions (4.1), (4.2), (4.3) and (4.4) yields Theorem 1.2.

5. Acknowledgements

I would like to thank my advisor Carl Pomerance for his guidance. He has been the driving force of my research. I would also like to thank Paul Pollack for pointing out Hildebrand's lecture notes and commenting on a draft of this paper. Finally, I'd like to thank the anonymous referee for his excellent suggestions that improved this paper.

6. Bibliography

[1] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[2] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[3] A. R. Booker. Quadratic class numbers and character sums. *Math. Comp.*, 75(255):1481–1492 (electronic), 2006.

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

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

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

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

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

[9] A. Hildebrand. Introduction to Analytic Number Theory Lecture Notes. 2005.

[10] 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.*

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

[12] P. Pollack and E. Treviño. The primes that Euclid forgot. *Amer. Math. Monthly*, 121:433-437, 2014.

[13] H. Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955.

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

[15] J. P. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 331–339. 2010.

[16] E. Treviño. *Numerically explicit estimates for character sums.* 2011. Thesis (Ph.D.)–Dartmouth College.

[17] E. Treviño. The Burgess inequality and the least k-th power non-residue. Submitted.

[18] E. Treviño. On the maximum number of consecutive integers on which a character is constant. *Moscow Journal of Combinatorics and Number Theory* 2012, vol.2, iss. 1, pp. 56-72.

[19] I. M. Vinogradov. *Selected works.* Springer-Verlag, Berlin, 1985. With a biography by K. K. Mardzhanishvili, Translated from the Russian by Naidu Psv [P. S. V. Naidu], Translation edited by Yu. A. Bakhturin.

[20] André Weil. Sur les courbes algébriques et les variétés qui s'en déduisent *Actualités Sci. Ind., no. 1041 (1945), Deuxième Partie, §IV.*

[21] A. E. Western and J. C. P. Miller. *Tables of indices and primitive roots.* Royal Society Mathematical Tables, Vol. 9. Published for the Royal Society at the Cambridge University Press, London, 1968.

[22] W. Yuan. Estimation and application of character sums. *Shuxue Jinzhan*, 7:78–83, 1964.