

Moscow Journal

*of
Combinatorics
and
Number Theory*



Moscow Journal of Combinatorics and Number Theory. 2012. Vol. 2. Iss. 1. 88 p.

The journal was founded in 2010.

*Published by the Moscow Institute of Physics and Technology
with the support of Yandex and Microsoft.*

The aim of this journal is to publish original, high-quality research articles from a broad range of interests within combinatorics, number theory and allied areas. One volume of four issues is published annually.

Website of our journal

<http://mjcnt.phystech.edu>

E-mail

mjcnt@phystech.edu

Address of the Editorial Board

Moscow institute of physics
and technology (state university)
Faculty of Innovations
and High Technology,
Laboratory Korpus, k. 209,
9, Institutskii pereulok,
Dolgoprudny,
Moscow Region,
Russia,
141700

Адрес редакции

Московский физико-технический
институт (государственный университет)
Факультет инноваций
и высоких технологий
Лабораторный корпус, к. 209,
Институтский переулок, д. 9,
г. Долгопрудный,
Московская область,
Российская Федерация,
141700

URSS Publishers

56, Nakhimovsky Prospekt,
Moscow,
Russia,
117335

Издательство «УРСС»

Нахимовский пр-т, 56
Москва,
Российская Федерация,
117335

Журнал зарегистрирован в Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия 3 сентября 2010 г. Свидетельство ПИ № ФС77–41900.

Формат 70 × 100/16. Печ. л. 5.5. Зак. № ЖС-44.

Отпечатано в ООО «ЛЕНАНД».


117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISSN 2220–5438

© УРСС, 2012

SCIENTIFIC LITERATURE
AND TEXTBOOKS

E-mail: URSS@URSS.ru
Our catalogue on the Internet:
<http://URSS.ru>
Phone/fax: +7(499) 724 25 45,
+34 (625) 37 87 73



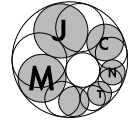
URSS

11995 ID 161043



9 785453 000296

All rights reserved. No part of this book may be used or reproduced in any manner whatsoever without written permission of the publisher.



On the maximum number of consecutive integers on which a character is constant

Enrique Treviño (Swarthmore)

Abstract: Let χ be a non-principal Dirichlet character to the prime modulus p . In 1963, Burgess showed that the maximum number of consecutive integers H for which χ remains constant is $O(p^{1/4} \log p)$. This is the best known asymptotic upper bound on this quantity. Recently, McGown proved an explicit version of Burgess's theorem, namely that $H < 7.06p^{1/4} \log p$ for $p \geq 5 \cdot 10^{18}$. Preobrazhenskaya, in the Legendre symbol case, showed that

$$H < \left(\frac{\pi}{\sqrt{6} \log 2} + o(1) \right) p^{1/4} \log p.$$

By improving an inequality of Burgess on character sums and using some ideas of Norton, we prove that $H < 1.55p^{1/4} \log p$ whenever $p \geq 2.5 \cdot 10^9$, and $H < 3.64p^{1/4} \log p$ for all p .

Keywords: character sums, Burgess inequality, consecutive non-residues, power residues

AMS Subject classification: 11L40, 11Y60

Received: 19.01.2012; **revised:** 02.02.2012

1. Introduction

Let χ be a non-principal Dirichlet character to the prime modulus p . In 1963, Burgess showed (see [2]) that the maximum number of consecutive integers for which χ remains constant is $O(p^{1/4} \log p)$. This is the best known asymptotic upper

bound on this quantity. Recently, McGown (see [9]) proved an explicit version of Burgess's theorem:

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

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

where the $o(1)$ terms depends only on p . Furthermore,

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

Stronger bounds were announced but not proven by Norton in 1973 (see [10]), namely that $H \leq 2.5p^{1/4} \log p$ for $p > e^{15} \approx 3.27 \times 10^6$ and $H < 4.1p^{1/4} \log p$, in general. Preobrazhenskaya in [12] showed that when the Dirichlet character is the Legendre symbol we have

$$H < \left(\frac{\pi}{\sqrt{6} \log 2} + o(1) \right) p^{1/4} \log p. \text{ } ^1)$$

The main ingredient in the proof of McGown is estimating

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

where p is a prime, χ is a non-principal character mod p , and $h \leq p$ is a positive integer. Burgess, using Weil's work on the Riemann Hypothesis for function fields (see [18]), showed in [3] that $S_\chi(h, w) < (4w)^{w+1} p h^w + 2wp^{1/2} h^{2w}$. McGown improved this estimate (see [9]) to

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

¹⁾ The proof by Preobrazhenskaya can be extended to any Dirichlet character of prime modulus and is almost as strong as the inequality we have in this paper. The constant provided by Preobrazhenskaya is approximately 1.8503.

In [17], with the further restriction that $w \leq 9h$, the author improved the estimate to

$$S_\chi(h, w) < \frac{(2w)!}{2^w w!} p h^w + (2w - 1) p^{1/2} h^{2w}. \quad (1)$$

In this paper, with help from the upper bound (1) on $S_\chi(h, w)$ and an improvement on McGown's lower bound for $S_\chi(h, w)$, we are able to prove Norton's claim and go a little further.

THEOREM 1. *If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N + H]$, then*

$$H < \left\{ \frac{\pi}{2} \sqrt{\frac{e}{3}} + o(1) \right\} p^{1/4} \log p,$$

where the $o(1)$ terms depends only on p . Furthermore,

$$H \leq \begin{cases} 3.64p^{1/4} \log p, & \text{for all odd } p, \\ 1.55p^{1/4} \log p, & \text{for } p \geq 2.5 \cdot 10^9. \end{cases}$$

Remark 1. The constant

$$\frac{\pi}{2} \sqrt{\frac{e}{3}} = 1.49522 \dots$$

is

$$\frac{1}{2\sqrt{2e}} = 0.214441 \dots$$

times the size of McGown's asymptotic constant.

One reason we study this problem is that it is a generalization of the problem of finding the least k -th power non-residue mod p (the case $N = 0$) and it allows one to bound the maximum number of consecutive integers that belong to a given coset C_p/C_p^k , where $C_p = (\mathbb{Z}/p\mathbb{Z})$. Furthermore, McGown (see [8]) was able to use bounds on the least k -th power non-residue and the second least k -th power non-residue to put a bound on the size of the discriminant of a Norm-Euclidean Galois cubic field. Regarding the least k -th power non-residue, Norton proved that the least k -th power non-residue is bounded by $4.7p^{1/4} \log p$ in [11]. The author improved this to $1.1p^{1/4} \log p$ in [17].

Notation. Most of our notation is standard. A possible exception is our notation for $\prod_{p|n} p$ (the *algebraic radical* of n), written here as $\text{rad}(n)$ (some papers use the notation $\gamma(n)$). We write $\mu(n)$ for the Moebius function, (a, b) for the greatest common divisor of the integers a and b , and we write $\log x$ for the natural logarithm of x .

2. Some Lemmas

To prove Theorem 1 we will need a lower bound for $S_\chi(h, w)$. Before we can find a lower bound for $S_\chi(h, w)$ we need to prove four lemmas. The first lemma is an estimate on the number of squarefree numbers up to a real number X . The second lemma is an upper bound on the tail of the sum of $\mu(d)/d^2$. The third lemma is a nice result concerning $\mu(d)/d$. The first three lemmas will be used to prove the main lemma, which is an estimate which will be crucial in giving a lower bound for $S_\chi(h, w)$.

LEMMA 1. *For real $X \geq 1$, the number of squarefree integers in $[1, X]$ is at most $(2/3)X + 2$.*

PROOF. The number of squarefree numbers up to X is at most

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

LEMMA 2. *For real $X \geq 1$ and a a positive integer we have*

$$\left| \sum_{\substack{d > X \\ (d, a) = 1}} \frac{\mu(d)}{d^2} \right| < \frac{1}{X}, \quad (2)$$

PROOF. Note that for any positive integer d we have that $1/d^2$ is smaller than

$$\int_{d-1/2}^{d+1/2} dt/(t^2). \text{ Thus}$$

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

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 $1/(X - 1/2) - 1/(X + 4)^2$. This is smaller than $1/X$ once $X \geq 11$, proving the lemma for real $X \geq 11$.

To complete the proof for $X \geq 1$ we need to verify (2) for $X \leq 11$. To do this we use the fact that

$$\sum_{\substack{d \\ (d,a)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1},$$

which implies that

$$\sum_{\substack{d > X \\ (d,a)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1} - \sum_{\substack{d \leq X \\ (a,d)=1}} \frac{\mu(d)}{d^2} = \prod_{p|a} \left(1 - \frac{1}{p^2}\right) - \sum_{\substack{d \leq X \\ (a,d)=1}} \frac{\mu(d)}{d^2}.$$

Let $M = \prod_{p \leq 11} p = 2310$ and $m = (\text{rad}(a), M)$. Hence, for $d \leq X \leq 11$, we have

$(d, a) = (d, m)$. We also have that $p \mid \frac{M}{m}$ implies $p \nmid a$. Since $(1 - 1/p^2) < 1$, then

$$\prod_{p \nmid a} \left(1 - \frac{1}{p^2}\right) - \sum_{\substack{d \leq X \\ (a,d)=1}} \frac{\mu(d)}{d^2} \leq \prod_{p \mid \frac{M}{m}} \left(1 - \frac{1}{p^2}\right) - \sum_{\substack{d \leq X \\ (d,m)=1}} \frac{\mu(d)}{d^2}. \quad (3)$$

Now, using that $p \mid a$ implies $p \mid m$ and that $(1 - 1/p^2)^{-1} > 1$ yields

$$\frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1} - \sum_{\substack{d \leq X \\ (a,d)=1}} \frac{\mu(d)}{d^2} \geq \frac{6}{\pi^2} \prod_{p|m} \left(1 - \frac{1}{p^2}\right)^{-1} - \sum_{\substack{d \leq X \\ (m,d)=1}} \frac{\mu(d)}{d^2}. \quad (4)$$

One can now manually check that the right hand side of (3) is less than $1/(X + 1)$ and that the right hand side of (4) is greater than $-1/(X + 1)$ for integer $X \in [1, 11]$ and the 32 possible values of m . This shows that

$$\left| \sum_{\substack{d > X \\ (d,a)=1}} \frac{\mu(d)}{d^2} \right| < \frac{1}{X + 1}$$

for all integers $X \in [1, 11]$. Since this is true for all integers $X \in [1, 11]$, then we have (2) for any real $X \in [1, 11]$. \square

Tao in an expository article [15] proved the following lemma²⁾. We give a different proof inspired by the online lecture notes of Hildebrand [6].

LEMMA 3. *For $X \geq 1$ a real number and a a positive integer:*

$$\left| \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} \right| \leq 1. \tag{5}$$

PROOF. Let

$$e_a(n) := \begin{cases} 1, & \text{if } \text{rad}(n) \mid \text{rad}(a), \\ 0, & \text{otherwise.} \end{cases}$$

Now consider the sum

$$S_a(X) := \sum_{n \leq X} e_a(n).$$

First note that if $S_a(X) = \lfloor X \rfloor$, then the only term summed in (5) is $d = 1$, showing that the sum is 1. Therefore we may assume that $S_a(X) < \lfloor X \rfloor$. Now,

$$S_a(X) = \sum_{n \leq X} e_a(n) = \sum_{n \leq X} \sum_{\substack{d \mid n \\ (d,a)=1}} \mu(d) = \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\lfloor \frac{X}{d} \right\rfloor.$$

Therefore

$$\begin{aligned} \left| X \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} \right| &= \left| S_a(X) + \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \right| = \\ &= \left| \sum_{\substack{d \leq X \\ \text{rad}(d) \mid \text{rad}(a)}} 1 + \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \right|. \end{aligned} \tag{6}$$

²⁾ Generalizations of this inequality can be found in [5] and [14].

Note that the conditions $\text{rad}(d) \mid \text{rad}(a)$ and $(d, a) = 1$ overlap only when $d = 1$. Therefore the right hand side of (6) is $\leq \lfloor X \rfloor + 1$. Now, note that since $S_a(X) < \lfloor X \rfloor$, there is a prime $j \leq X$ such that $(j, a) = 1$. Since $\mu(j) = -1$, we can conclude that the right hand side of (6) is $\leq \lfloor X \rfloor$. This concludes the proof of (5). \square

The following is the main lemma of the section:

LEMMA 4. *For a and b coprime integers and $X \geq 1$ a real number, we have*

$$\sum_{q \leq X} \sum_{\substack{0 \leq t < q \\ \gcd(at+b, q) = 1}} \left(\frac{X}{q} - 1 \right) \geq \frac{3}{\pi^2} X^2 - \frac{13}{12} X - \frac{1}{4}.$$

PROOF. Start by using inclusion-exclusion to get the sum equal to

$$\sum_{q \leq X} \sum_{0 \leq t < q} \sum_{d \mid \gcd(at+b, q)} \mu(d) \left(\frac{X}{q} - 1 \right).$$

Writing $q = rd$ and exchanging summation gives us

$$\sum_{d \leq X} \sum_{r \leq \frac{X}{d}} \sum_{\substack{0 \leq t < rd \\ at \equiv -b \pmod{d}}} \mu(d) \left(\frac{X}{rd} - 1 \right).$$

Since $\gcd(a, b) = 1$, the congruence $at \equiv -b \pmod{d}$ has a solution if and only if $\gcd(d, a) = 1$. Note that in such a case, there are r values of t such that $0 \leq t < rd$ and $at \equiv -b \pmod{d}$. Therefore the sum becomes

$$\sum_{\substack{d \leq X \\ \gcd(d, a) = 1}} \mu(d) \sum_{r \leq \frac{X}{d}} \sum_{\substack{0 \leq t < rd \\ at \equiv -b \pmod{d}}} \left(\frac{X}{rd} - 1 \right) = \sum_{\substack{d \leq X \\ \gcd(d, a) = 1}} \frac{\mu(d)}{d} \sum_{r \leq \frac{X}{d}} (X - rd). \quad (7)$$

Writing

$$\frac{X}{d} = \left\lfloor \frac{X}{d} \right\rfloor + \left\{ \frac{X}{d} \right\}$$

we evaluate the inside sum of (7) as

$$\sum_{r \leq (X/d)} (X - rd) = X \left\lfloor \frac{X}{d} \right\rfloor - \frac{d \lfloor X/d \rfloor (\lfloor X/d \rfloor + 1)}{2} = \frac{X^2}{2d} - \frac{X}{2} + \frac{d \{X/d\} (1 - \{X/d\})}{2}.$$

Therefore (7) becomes

$$\sum_{\substack{d \leq X \\ \gcd(d,a)=1}} \frac{\mu(d)}{d} \left(\frac{X^2}{2d} - \frac{X}{2} + \frac{d\{X/d\}(1-\{X/d\})}{2} \right) = \frac{X^2}{2} \sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{\mu(d)}{d^2} - \frac{X^2}{2} \sum_{\substack{d > X \\ (d,a)=1}} \frac{\mu(d)}{d^2} - \frac{X}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} + \frac{1}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \left(1 - \left\{ \frac{X}{d} \right\} \right). \quad (8)$$

Now,

$$\sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2} \right)^{-1} \geq \frac{6}{\pi^2}. \quad (9)$$

Using Lemma 1 we get

$$\frac{1}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \left(1 - \left\{ \frac{X}{d} \right\} \right) \geq -\frac{1}{8} \sum_{\substack{d \leq X \\ d \text{ squarefree}}} 1 \geq -\frac{1}{12}x - \frac{1}{4}. \quad (10)$$

Combining (9), (10), Lemma 2 and Lemma 3 with (8) yields the proof. □

3. Lower bound for $S_\chi(h, w)$

Now we are ready to find a lower bound for $S_\chi(h, w)$. The proposition we shall prove improves Proposition 3.3 in [9] by a factor of 4 and it also has a smaller error term (saving a $\log X$). Another improvement is that the proposition has a less demanding condition for H , namely that $H \leq (h/2)^{2/3} \cdot p^{1/3}$ instead of $H \leq (2h - 1)^{1/3} \cdot p^{1/3}$.

Throughout, let $A = (3/\pi^2)$.

PROPOSITION 1. *Let h and w be positive integers. Let χ be a non-principal Dirichlet character to the prime modulus p which is constant on $(N, N + H]$ and such that*

$$4h \leq H \leq \left(\frac{h}{2} \right)^{2/3} p^{1/3}.$$

Let $X := H/h$, then $X \geq 4$ and

$$S_\chi(h, w) \geq \left(\frac{3}{\pi^2} \right) X^2 h^{2w+1} g(X) = AH^2 h^{2w-1} g(X),$$

where

$$g(X) = 1 - \left(\frac{13}{12AX} + \frac{1}{4AX^2} \right).$$

PROOF. The proof follows McGown's treatment of the method of Burgess with some modifications inspired by the work of Norton.

By Dirichlet's Theorem in Diophantine approximation (see Theorem 7 on p. 101 of [4]), there exist coprime integers a and b satisfying $1 \leq a \leq \lfloor 2H/h \rfloor$ and

$$\left| a \frac{N}{p} - b \right| \leq \frac{1}{\lfloor \frac{2H}{h} \rfloor + 1} \leq \frac{h}{2H}. \quad (11)$$

Let's define the real interval:

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

for integers $0 \leq t < q \leq X$ and $\gcd(at + b, q) = 1$.

The reason $I(q, t)$ is important, is that χ is constant inside the interval. Indeed, if $m \in I(q, t)$, then $\chi(qm - pt) = \chi(N + i)$ for some i such that $0 < i \leq H$. Therefore $\chi(m) = \bar{\chi}(q)\chi(N + i)$. We will show that the $I(q, t)$ are disjoint and that $I(q, t) \subseteq (0, p)$.

First, let's show that the $I(q, t)$ are disjoint. If $I(q_1, t_1)$ and $I(q_2, t_2)$ overlap then either

$$\frac{N + pt_1}{q_1} \leq \frac{N + pt_2}{q_2} < \frac{N + H + pt_1}{q_1} \quad \text{or} \quad \frac{N + pt_2}{q_2} \leq \frac{N + pt_1}{q_1} < \frac{N + H + pt_2}{q_2}.$$

In the first case, multiply all by $q_1 q_2$ and then subtract $Nq_2 + pt_1 q_2$. This yields

$$0 \leq N(q_1 - q_2) + p(t_2 q_1 - t_1 q_2) < Hq_2.$$

Analogously, for the second case, we get

$$-Hq_1 < N(q_1 - q_2) + p(t_2 q_1 + t_1 q_2) \leq 0.$$

Therefore,

$$\left| \frac{N(q_1 - q_2)}{p} + t_2 q_1 - t_1 q_2 \right| < \frac{\max\{q_1, q_2\}H}{p} \leq \frac{XH}{p}. \quad (12)$$

Therefore, combining (11) and (12), we get

$$\begin{aligned} \left| \frac{b}{a}(q_1 - q_2) + t_2q_1 - t_1q_2 \right| &= \left| \left(\frac{N}{p} + \left(\frac{b}{a} - \frac{N}{p} \right) \right) (q_1 - q_2) + t_2q_1 - t_1q_2 \right| \leq \\ &\leq \left| \frac{N}{p}(q_1 - q_2) + t_2q_1 - t_1q_2 \right| + \left| \left(\frac{b}{a} - \frac{N}{p} \right) (q_1 - q_2) \right| < \\ &< \frac{XH}{p} + \frac{h|q_1 - q_2|}{2aH} \leq \frac{XH}{p} + \frac{Xh}{2aH} = X \frac{2aH^2 + hp}{2aHp} = \frac{2aH^2 + hp}{2ahp}. \end{aligned}$$

Since $a \leq (2H/h)$ and $H^3 \leq (h^2p/4)$ by hypothesis, then

$$\frac{2H^2a + ph}{2ahp} \leq \frac{\frac{4H^3}{h} + ph}{2ahp} \leq \frac{2ph}{2ahp} = \frac{1}{a}.$$

Therefore

$$\left| \frac{b}{a}(q_1 - q_2) + t_2q_1 - t_1q_2 \right| < \frac{1}{a},$$

implying that

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

However, since $\gcd(at_1 + b, q_1) = 1$ and $\gcd(at_2 + b, q_2) = 1$, then $q_1 = q_2$ and therefore $t_1 = t_2$. We have now proved that the $I(q, t)$ are disjoint.

Since $\chi(p) = 0$, we can assume without loss of generality that $N + H < p$. Now let's prove that $I(q, t) \subseteq (0, p)$. If $m \in I(q, t)$, then $m > ((N + pt)/q) \geq 0$. Also,

$$m \leq \frac{N + H + pt}{q} < \frac{p(t + 1)}{q} \leq p.$$

Since the $I(q, t)$ are disjoint and they are contained in $(0, p)$, we have

$$\begin{aligned} S_\chi(h, w) &= \sum_{m=0}^{p-1} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} \geq \sum_{q,t} \sum_{m \in I(q,t)} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} \geq \\ &\geq h^{2w} \sum_{q,t} \left(\frac{H}{q} - h \right) = h^{2w+1} \sum_{q \leq X} \sum_{\substack{0 \leq t < q \\ \gcd(at+b,q)=1}} \left(\frac{X}{q} - 1 \right). \end{aligned}$$

The last inequality is true since there are at least $(H/q) - h$ subsets of h consecutive integers in $I(q, t)$, and when there are h consecutive integers $m, m+1, \dots, m+h-1$, we have

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

To finish the proof of the Proposition we use Lemma 4. □

4. Proof of the main theorem

PROOF OF THEOREM 1. Let h and w be positive integers, and let $A = 3/\pi^2$. Assume that

$$4h \leq H \leq \left(\frac{h}{2}\right)^{2/3} p^{1/3}.$$

Then by Proposition 1 and (1) we have (for $w \leq 9h$):

$$AH^2 h^{2w-1} g(X) \leq S_\chi(h, w) < \frac{(2w)!}{2^w w!} p h^w + (2w-1) p^{1/2} h^{2w}.$$

Therefore,

$$AH^2 g(X) < f(w, h), \tag{13}$$

where

$$f(w, h) = \frac{(2w)!}{2^w w!} p h^{1-w} + (2w-1) p^{1/2} h.$$

Using techniques from Calculus and an explicit version of Stirling's formula (such as the one in [13]) we can choose optimal w and h to make $f(w, h)$ as small as possible. For the details of this computation see [17] or [16]. For large p , good choices for h and w are

$$h = \left\lfloor \left(\frac{e}{2} + \frac{2e+1}{\log p} \right) \log p \right\rfloor,$$

and

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

From there one can obtain

$$f(w, h) < \left(\frac{e}{4} + \frac{5e+1}{2 \log p} + \frac{8e+3}{\log^2 p} + \frac{8e+4}{\log^3 p} \right) \sqrt{p} \log^2 p = K(p) \sqrt{p} \log^2 p. \tag{14}$$

Assume that

$$p \geq p_0 \quad \text{and} \quad H \geq C(p_0) p^{1/4} \log p.$$

We may assume

$$C(p_0) \geq \pi \sqrt{\frac{e}{12}},$$

hence

$$X = \frac{H}{h} \geq \frac{C(p_0) p^{1/4} \log p}{\left(\frac{e}{2} + \frac{2e+1}{\log p}\right) \log p} \geq \frac{\pi \sqrt{\frac{e}{12}}}{\left(\frac{e}{2} + \frac{2e+1}{\log p}\right)} p^{1/4}.$$

Let $X(p_0)$ be defined as

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

Note that since

$$H \geq \pi \sqrt{\frac{e}{12}} p^{1/4} \log p \quad \text{and} \quad h < \left(\frac{e}{2} + \frac{2e+1}{\log p}\right) \log p,$$

then $H \geq 4h$ as long as $p \geq 1500$. Now let

$$C(p_0) = \sqrt{\frac{K(p_0)}{A g(X(p_0))}},$$

with $K(p)$ introduced in (14).

The left hand side of (13) can therefore be bounded from below for $p \geq p_0$:

$$\begin{aligned} AH^2 g(X) &\geq A (C(p_0))^2 \sqrt{p} \log^2 p g(X(p_0)) \geq \\ &\geq K(p_0) \sqrt{p} \log^2 p \geq K(p) \sqrt{p} \log^2 p > f(w, h), \end{aligned}$$

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

$$H \leq \left(\frac{h}{2}\right)^{2/3} p^{1/3}.$$

Note that if $H > (h/2)^{2/3} \cdot p^{1/3}$, then χ is constant on a subset of H of cardinality at most $(h/2)^{2/3} \cdot p^{1/3}$. Therefore, $H < C(p_0)p^{1/4} \log p$ whenever

$$\left(\frac{h}{2}\right)^{2/3} p^{1/3} \geq C(p_0)p^{1/4} \log p.$$

For $p \geq 10^{10}$ we have that

$$C(p_0)p^{1/4} \log p < \left(\frac{h}{2}\right)^{2/3} p^{1/3},$$

which implies that for $p \geq 10^{10}$, $H < C(p_0)p^{1/4} \log p$.

It is not hard to see that

$$C(p_0) = \pi \sqrt{\frac{e}{12}} + o(1),$$

thus proving the first assertion in the Theorem.

Table 1 shows values of $C(p_0)$ for different values of p_0 .

We have been able to attack the problem with asymptotic choices for h and w , but we can fix the values of h and w and improve the bounds.

From Table 1 we have established that $H < 1.55p^{1/4} \log p$ when $p \geq 10^{64}$. Therefore to finish the proof of the theorem, we need to deal with the interval $2.5 \cdot 10^9 < p < 10^{64}$.

Let

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

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

$$\gamma(p, w, h) = \sqrt{\frac{f(w, h)}{A\sqrt{p} \log^2 p g(X(p))}}.$$

Table 1

Upper bound H on the number of consecutive residues with equal character value.

For $p \geq p_0$, $H < C(p_0)p^{1/4} \log p$

| | | | | | | | | | | |
|----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| p_0 | 10^{10} | 10^{12} | 10^{15} | 10^{18} | 10^{20} | 10^{30} | 10^{40} | 10^{50} | 10^{60} | 10^{64} |
| $C(p_0)$ | 1.86591 | 1.79646 | 1.73289 | 1.69225 | 1.6722 | 1.6126 | 1.58304 | 1.56537 | 1.55362 | 1.54995 |

Table 2

As an example on how to read the table: when $w = 10$ and $h = 62$, then $\gamma(p, w, h) < 1.55$ for all $p \in [10^{18}, 10^{19}]$. It is also worth noting that the inequalities $4h \leq 1.55p^{1/4} \log p < h^{2/3}p^{1/3}$ and $w \leq 9h$ are also verified for each choice of w and h

| w | h | p | w | h | p | w | h | p |
|-----|-----|-----------------------------|-----|-----|------------------------------|-----|-----|------------------------------|
| 6 | 26 | $[2.5 \cdot 10^9, 10^{10}]$ | 6 | 28 | $[10^{10}, 4 \cdot 10^{10}]$ | 7 | 28 | $[4 \cdot 10^{10}, 10^{11}]$ |
| 7 | 32 | $[10^{11}, 10^{12}]$ | 7 | 37 | $[10^{12}, 10^{13}]$ | 8 | 41 | $[10^{13}, 10^{14}]$ |
| 8 | 44 | $[10^{14}, 10^{15}]$ | 9 | 45 | $[10^{15}, 10^{16}]$ | 9 | 51 | $[10^{16}, 10^{17}]$ |
| 9 | 59 | $[10^{17}, 10^{18}]$ | 10 | 62 | $[10^{18}, 10^{19}]$ | 11 | 63 | $[10^{19}, 10^{20}]$ |
| 11 | 71 | $[10^{20}, 10^{21}]$ | 12 | 72 | $[10^{21}, 10^{23}]$ | 13 | 79 | $[10^{23}, 10^{25}]$ |
| 15 | 82 | $[10^{25}, 10^{27}]$ | 15 | 96 | $[10^{27}, 10^{29}]$ | 17 | 97 | $[10^{29}, 10^{31}]$ |
| 18 | 105 | $[10^{31}, 10^{33}]$ | 18 | 119 | $[10^{33}, 10^{35}]$ | 19 | 127 | $[10^{35}, 10^{37}]$ |
| 20 | 135 | $[10^{37}, 10^{39}]$ | 20 | 149 | $[10^{39}, 10^{41}]$ | 22 | 150 | $[10^{41}, 10^{43}]$ |
| 23 | 158 | $[10^{43}, 10^{46}]$ | 25 | 166 | $[10^{46}, 10^{49}]$ | 27 | 174 | $[10^{49}, 10^{52}]$ |
| 29 | 183 | $[10^{52}, 10^{55}]$ | 31 | 191 | $[10^{55}, 10^{58}]$ | 33 | 200 | $[10^{58}, 10^{62}]$ |
| 33 | 215 | $[10^{62}, 10^{64}]$ | | | | | | |

Then by similar arguments as before we have $H < \gamma(p, h, w)p^{1/4} \log p$ whenever h and w are picked such that

$$4h \leq \gamma(p, h, w)p^{1/4} \log p < \left(\frac{h}{2}\right)^{2/3} p^{1/3}$$

and $w \leq 9h$. Hence, all we want is for $\gamma(p, h, w)$ to be at most 1.55, and for $4h \leq 1.55p^{1/4} \log p < h^{2/3}p^{1/3}$. By picking w 's and h 's as in the Table 2, we complete the proof for $p > 2.5 \cdot 10^9$ (noticing that with h and w fixed, $\gamma(p, w, h)$ is concave up, allowing us to just check the endpoints of the intervals).

Let's now prove that for all p we have $H < 3.64p^{1/4} \log p$. It is true for $p = 2$ since $3.64 \cdot 2^{1/4} \log 2 > 1$. Now, for $1.9 \leq p \leq 3 \cdot 10^6$, it is true because of the following inequality of Brauer [1] (established with elementary methods):

$$H < \sqrt{2p} + 2 < 3.64p^{1/4} \log p.$$

Assume $p > 1.9 \cdot 10^6$. We're going to show that in this case, in fact $H < 3p^{1/4} \log p$. Note that we have a restriction on h since we want $H < (h/2)^{2/3} \cdot p^{1/3}$ to be able to use our machinery. If $h = 94$, then for $p \geq 1.9 \cdot 10^6$ we have

$$\left(\frac{h}{2}\right)^{2/3} p^{1/3} > 3p^{1/4} \log p > 4h_0.$$

Using $w = 2$, we have $\gamma(p, w, h) < 3$ whenever $p \in [3 \cdot 10^6, 10^8]$. Now picking $w = 3$ we get $\gamma(p, w, h) < 3$ whenever $p \in [10^8, 10^{11}]$. But, for $p > 2.5 \cdot 10^9$, we can use the bound of $H < 1.55p^{1/4} \log p$, completing the proof. \square

Remark 2. As mentioned earlier, Norton announced (but didn't give details) that he could prove $H < 4.1p^{1/4} \log p$ for all odd p and $H < 2.5p^{1/4} \log p$ for $p > e^{15} \approx 3.27 \times 10^6$. In Theorem 1 we prove something slightly better than his first claim, but it is hard to judge with his second claim (as our better bound kicks in later). To fill the gap, we will now show that $H < 2.4p^{1/4} \log p$ for $p > e^{15}$ (a slightly stronger claim than Norton's). Note that we need only fill in the gap $e^{15} < p \leq 2.5 \times 10^9$. For $h \geq 67$ we have $4h < 2.4p^{1/4} \log p < (h/2)^{2/3} \cdot p^{1/3}$ whenever $p > e^{15}$. Therefore we have $H < \gamma(p, w, 67)p^{1/4} \log p$ for $p > e^{15}$. We note that $\gamma(p, 2, 67) < 2.4$ when $p \in (e^{15}, 10^{7.5})$ and $\gamma(p, 3, 67) < 2.4$ when $p \in [10^{7.5}, 2.5 \cdot 10^9]$, completing the proof of our claim.

Remark 3. If we're looking for the maximum number of consecutive non-residues for which χ remains constant, then we can do a little better than $H < 3.64p^{1/4} \log p$. In fact we can prove $H < 3p^{1/4} \log p$ for all odd p . Let's prove it. It is true for $p = 3$ and for $p = 5$ since in both cases we have $3p^{1/4} \log p > p$. Now, for $7 \leq p \leq 2 \cdot 10^6$, it is true because of the following inequality of Hudson [7]³⁾:

$$H < p^{1/2} + 2^{2/3} p^{1/3} + 2^{1/3} p^{1/6} + 1 < 3p^{1/4} \log p.$$

We can conclude by noting that for $p > 1.9 \cdot 10^6$, $H < 3p^{1/4} \log p$.

³⁾ This inequality was done using elementary methods that build on the work of Brauer [1]. The inequality uses a clever construction that is able to use information on $g(p, k)$ to bound the number of consecutive non-residues for which χ remains constant. However, it does not appear to extend to include the case of the maximum number of consecutive residues.

Acknowledgements. I would like to thank Carl Pomerance for his useful comments regarding this paper and his encouragement. I would also like to thank Paul Pollack who directed me to McGown's work. Finally, I thank the anonymous referee for his helpful comments. This research was partially supported by Swarthmore research grant 24176.

Bibliography

1. **A. Brauer**, *Über die Verteilung der Potenzreste*, Math. Z. **35** (1932), № 1, 39–50.
2. **D. A. Burgess**, *A note on the distribution of residues and non-residues*, J. London Math. Soc. **38** (1963), 253–256.
3. **D. A. Burgess**, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192.
4. **P. Erdős and János Surányi**, *Topics in the theory of numbers*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003, Translated from the second Hungarian edition by Barry Guiduli.
5. **A. Granville and K. Soundararajan**, *Large character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. **20** (2007), № 2, 357–384 (electronic).
6. **A. Hildebrand**, *Introduction to Analytic Number Theory Lecture Notes*, 2005.
7. **R. H. Hudson**, *On the distribution of k -th power nonresidues*, Duke Math. J. **39** (1972), 85–88.
8. **K. J. McGown**, *Norm-Euclidean cyclic fields of prime degree*, Int. J. Number Theory (to appear).
9. **K. J. McGown**, *On the constant in Burgess' bound for the number of consecutive residues or non-residues*, Funct. Approx. Comment. Math. (to appear).
10. **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), Amer. Math. Soc., Providence, R.I., 1973, pp. 213–220.
11. **K. K. Norton**, *Numbers with small prime factors, and the least k th power non-residue*, Memoirs of the American Mathematical Society, No. 106, American Mathematical Society, Providence, R.I., 1971.
12. **T. A. Preobrazhenskaya**, *An estimate for the number of consecutive quadrature residues*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. (2009), № 1, 24–28.
13. **H. Robbins**, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.
14. **M. Skalba**, *On Euler-von Mangoldt's equation*, Colloq. Math. **69** (1995), № 1, 143–145.
15. **T. Tao**, *A remark on partial sums involving the Möbius function*, Bull. Aust. Math. Soc. **81** (2010), № 2, 343–349.

16. **E. Treviño**, *Numerically explicit estimates for character sums*, 2011, Thesis (Ph.D.)–Dartmouth College.
17. **E. Treviño**, *The least k -th power non-residue*, Submitted,
<http://www.swarthmore.edu/NatSci/etrevin1/LeastNonResidue.pdf>, 2011.
18. **A. Weil**, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

ENRIQUE TREVIÑO

Department of Mathematics and Statistics,
Swarthmore College,
Swarthmore, Pennsylvania 19081, USA
etrevin1@swarthmore.edu