NUMERICALLY EXPLICIT ESTIMATES FOR CHARACTER SUMS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Enrique Treviño

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 31, 2011

Examining Committee:

Carl Pomerance, Chair

Sergi Elizalde

Kannan Soundararajan

Andrew Yang

Brian W. Pogue, Ph.D.
Dean of Graduate Studies

Abstract

Character sums make their appearance in many number theory problems: showing that there are infinitely many primes in any coprime arithmetic progression, estimating the least quadratic non-residue, bounding the least primitive root, finding the size of the least inert prime in a real quadratic field, etc. In this thesis, we find numerically explicit estimates for character sums and give applications to some of these questions.

Granville, Mollin and Williams proved that the least inert prime q for a real quadratic field of discriminant D such that $D > 3705$ satisfies $q \leq \sqrt{D}/2$. Using a smoothed version of the Pólya–Vinogradov inequality (an explicit bound on character sums) and explicit estimates on the sum of primes, we improve the bound on q to $D^{0.45}$ for $D > 1596$.

Let χ be a non-principal Dirichlet character $\bmod p$ for a prime p. Using combinatorial methods, we improve an inequality of Burgess for the double sum

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

Using this inequality, we prove that for a prime p with $k \mid p-1$, the least k-th power non-residue $\bmod p$ is smaller than $0.9p^{1/4} \log p$ unless $k = 2$ and $p \equiv 3 \pmod 4$, in which case, the least k-th power non-residue is smaller than $1.1p^{1/4} \log p$. This

improves a result of Norton which has the coefficients 3.9 and 4.7 in the two cases, respectively. We also prove that the length H of the longest interval on which χ is constant is smaller than $3.64p^{1/4}\log p$ and if $p \geq 2.5 \cdot 10^9$, then $H \leq 1.55p^{1/4}\log p$. This improves a result of McGown which had for $p \geq 5 \cdot 10^{18}$ that $H \leq 7.06p^{1/4}\log p$, and for $p \geq 5 \cdot 10^{55}$ that $H \leq 7p^{1/4}\log p$.

The purpose of this thesis is to work out the best explicit estimates we can and to have them as tools for other mathematicians.

Acknowledgements

I would like to thank my advisor, Carl Pomerance, for his support on this project. Carl helped me every step of the way; suggesting problems, suggesting avenues of attack, steering my ideas into fruitful avenues, teaching me techniques and helping me improve my mathematical writing. Through it all, he has been very patient and very encouraging. I would not have been able to do this without him. Also, it has been a pleasure discussing mathematics with such a talented mathematician.

I would also like to thank Kannan Soundararajan, my external reviewer, who suggested the problem in Chapter 3 to Carl. That problem was a catalyst in my research; it was a very fun problem and, without it, I doubt I would have gained the momentum necessary to finish my thesis this year. I am grateful to him, Andrew Yang and Sergi Elizalde for their helpful comments on my dissertation.

I would like to express my gratitude to Andrew Granville, Hugh Montgomery and Robert Vaughan, who allowed me to look at unpublished manuscripts which helped me on my work on the Burgess inequality.

My friend, Paul Pollack, was very helpful in my preparations for the qualifying exams. He was also very encouraging about my work and pointed out useful references. He also pointed out work posted on the arXiv by Kevin McGown, which was what led me to work on Chapters 4 and 5.

Special thanks are owed to my friend and teacher David Cossio Ruiz. David prepared me for the Mathematical Olympiad when I was in High School and has been my role model when it comes to teaching. We have worked together preparing students for the Math Olympiad since 2002 and he has been a close friend since then.

On the non-mathematical side of my life, I would like to thank my father, Enrique Treviño Bazán, for being supportive of my unusual career path and teaching me to strive for excellence; my mother, Rosario López Álvarez, for all the love she's given me and for teaching me how to enjoy life; my sister, Maribel Treviño, for her support and her good TV show recommendations; and my uncle and aunt, Avelino López and Anthea Wesson, for treating me like their son.

I would also like to thank my friend Emmanuel Villaseñor. Even though he has no connection with the dissertation, due to my sudden marriage, there was no time for him to be the best man at my wedding, so I try to make reparations by including him here.

Finally, I would like to thank my beautiful wife, Yuliia Glushchenko. Yuliia has been very supportive and encouraging. I have been very happy throughout my graduate experience, and her love has been the main reason. I would also like to thank her for the delicious meals she cooks and the fun we've had salsa dancing.

Contents

List of Tables

Chapter 1

Introduction

Let n be a positive integer. For $q \in \{0, 1, 2, \ldots, n-1\}$, we call q a quadratic residue $\bmod n$ if there exists an integer x such that $x^2 \equiv q \pmod{n}$. Otherwise we call q a quadratic non-residue. Let $g(p)$ be the least quadratic non-residue $\bmod\ p$ for p prime. How big can $g(p)$ be?

- For the least quadratic non-residue to be greater than 2 we need 2 to be a quadratic residue; therefore $p \equiv \pm 1 \pmod{8}$, hence $p = 7$ is the first example.
- For the least quadratic non-residue to be greater than 3 we need 2 and 3 to be quadratic residues, therefore $p \equiv \pm 1 \pmod{8}$ and $p \equiv \pm 1 \pmod{12}$; therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least quadratic non-residue to be greater than 5 we need $2, 3$ and 5 to be quadratic residues, therefore $p \equiv \pm 1 \pmod{8}$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod{5}$; therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Note that the sizes of the primes are growing fast, suggesting that $g(p)$ is much smaller than p. The following heuristic suggests that $g(p) = O(\log p \log\log p)$ and that this is best possible up to a constant, i.e., $g(p) = \Omega(\log p \log\log p)$.

Let p_i be the i-th prime, i.e., $p_1 = 2, p_2 = 3, \ldots$. Then

- $\#\{p \le x \,|\, g(p) = 2\} \approx \frac{\pi(x)}{2}$,
- $\#\{p \le x \,|\, g(p) = 3\} \approx \frac{\pi(x)}{4}$ and hence
- $\#\{p \le x \,|\, g(p) = p_k\} \approx \frac{\pi(x)}{2^k}$.

Therefore, if $k = \frac{\log(\pi(x))}{\log 2} \sim \frac{\log x - \log\log x}{\log 2}$, one would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then one would not expect a prime with such a "large" least non-square. Therefore we want $k \approx C \log x$. Since $p_k \sim k \log k$, we have $g(x) \approx C \log x \log\log x$.

Ankeny showed [1] that $g(p) = O(\log^2 p)$ assuming the Extended Riemann Hypothesis (ERH). Bach was able to make this explicit in [2], proving that $g(p) \le 2\log^2 p$ assuming ERH. However, the best unconditional results are much worse. We know from work of Burgess and Vinogradov that for $\varepsilon > 0$, $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$. Explicitly, the best known result was due to Norton [31], who proved that

$$g(p) \le \begin{cases} 3.9 p^{1/4} \log p & \text{if } p \equiv 1 \pmod 4, \\ 4.7 p^{1/4} \log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

In Chapter 4, we prove

Theorem 1.1. *Let p be an odd prime. Then*

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 1.1p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The theorem (as well as Norton's result) actually goes a little further, bounding $g(p,k) :=$ the least k-th power non-residue. The technique used to bound $g(p)$ is to estimate character sums. While these estimates are interesting in their own right, they also are very useful to answer some questions from elementary number theory. Another example is bounding the least inert prime in a real quadratic field.

Let's give some background on character sums. For n a positive integer, a Dirichlet character $\chi \mod n$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ that satisfies that for any $a \in \mathbb{Z}$, $\chi(a+n) = \chi(a)$ (periodic), also for any $b \in \mathbb{Z}$ we have $\chi(ab) = \chi(a)\chi(b)$ (this property is called being totally multiplicative) and that $\chi(a) = 0$ if and only if $\gcd(a,n) > 1$. Dirichlet characters are very important in analytic number theory; one application is in the proof that there are infinitely many primes in any arithmetic progression $ax+b$ as long as $\gcd(a,b) = 1$. This proof depends on the fact that $L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0$ for any non-principal character χ (principal character mod q means $\chi(a) = 1$ for all integers a such that $\gcd(a,q) = 1$). From now on, Dirichlet characters will be referred to as characters.

Let χ be a character mod q and let M and N be non-negative reals with $N \geq 1$. Consider

$$S_\chi(M,N) = \sum_{M < n \leq M+N} \chi(n).$$

Notice that if $M = 0$ then $S_\chi(M, N)$ is the sum of χ evaluated at the first N integers and that by estimating this sum, using partial summation, we can estimate $L(1, \chi)$. Hence, bounds on $S_\chi(M, N)$ are important.

The first important upper bound on $S_\chi(M, N)$ came in 1918 in what we now call the Pólya–Vinogradov inequality (proven independently). The inequality states that there is a universal constant c such that for χ a non-principal Dirichlet character to the modulus q, $|S_\chi(M, N)| \leq c\sqrt{q}\log q$. Note that, surprisingly, the upper bound does not depend on N, it only depends on the modulus of the character. It is important to note that from the definition of a Dirichlet character it is easy to see that $|\chi(n)| = 1$ or $\chi(n) = 0$. From this it is trivial to see that $|S_\chi(M, N)| \leq N$. Now if N is small compared to $\sqrt{q}$ then Pólya–Vinogradov is not an improvement on the trivial bound.

A character with modulus n is induced (or not primitive) if it is the product of a character with a modulus which is a proper divisor of n with a principal character with modulus n; otherwise it is primitive. Mathematicians have worked out explicit estimates for the Pólya–Vinogradov inequality, i.e., finding an upper bound for the universal constant c. For example, Pomerance proved the following theorem in the case of primitive characters [36]

Theorem 1.2. *For χ a primitive character to the modulus $q > 1$, we have*

$$|S_\chi(M, N)| \leq \begin{cases} \dfrac{2}{\pi^2}\sqrt{q}\log q + \dfrac{4}{\pi^2}\sqrt{q}\log\log q + \dfrac{3}{2}\sqrt{q} & , \quad \chi(-1) = 1, \\ \dfrac{1}{2\pi}\sqrt{q}\log q + \dfrac{1}{\pi}\sqrt{q}\log\log q + \sqrt{q} & , \quad \chi(-1) = -1. \end{cases}$$

An immediate application of the Pólya–Vinogradov inequality is to put an upper bound on $g(p)$ with p prime. The reason we can do this is that the function that gives 1 if it is a quadratic residue, -1 if it is not a quadratic residue and 0 if the

number is not coprime to the modulus is a Dirichlet character mod p (this function is written $\left(\frac{\cdot}{p}\right)$ and it is called the Legendre symbol). If we show that the sum of these character values is small compared to the number of things we summed, it means that χ must have been -1 at some point, giving us a quadratic non-residue. Using the Pólya–Vinogradov inequality and a bit of sieving (known as the Vinogradov trick in this context) we can get that the least quadratic non-residue is bounded by $p^{\frac{1}{2\sqrt{e}}+\varepsilon}$ for large enough p depending on the choice of ε, a positive real number. As mentioned earlier, we conjecture that the least quadratic non-residue is much smaller than that.

Despite the Pólya–Vinogradov inequality not being able to yield a better result with respect to $g(p)$, the Pólya–Vinogradov inequality is relatively sharp. Indeed, there exist real numbers M and N such that $S_\chi(M,N) \gg \sqrt{q}$. In a sense, the inequality is only "off" by $\log q$. In this direction there are other nice results. For instance, Paley [34] showed that there exists an absolute constant c and infinitely many quadratic characters $\chi \pmod q$ such that $\max_{N,M} S(M,N) \geq c\sqrt{q}\log\log q$. Montgomery and Vaughan [28] proved that under GRH we have $S_\chi(M,N) \ll \sqrt{q}\log\log q$, hence making the Paley result best possible (up to a constant). This analysis works for quadratic characters, but what about characters of odd order? Work of Granville and Soundararajan [16] led to the following theorem of Goldmakher [14]:

Theorem 1.3. *For every primitive character $\chi \pmod q$ of odd order k,*

$$S_\chi(0,N) \ll_k \sqrt{q}(\log q)^{\Delta_k+o(1)}, \quad \textit{where } \Delta_k = \frac{k}{\pi}\sin\frac{\pi}{k}, \quad q\to\infty. \tag{1.1}$$

Moreover, under GRH

$$S_\chi(0,N) \ll_k \sqrt{q}(\log\log q)^{\Delta_k+o(1)}. \tag{1.2}$$

For both (1.1) and (1.2) the implicit constant depends only on k, and $o(1) \to 0$ as $q \to \infty$.

Furthermore, assuming GRH, for every odd integer $k \geq 3$, there exists an infinite family of characters $\chi \pmod q$ of order k satisfying

$$\max_N S_\chi(0,N) \gg_{\varepsilon,k} \sqrt{q}(\log\log q)^{\Delta_k - \varepsilon}.$$

As stated, the Pólya–Vinogradov inequality doesn't work well when N is small compared to $\sqrt{q}$. Allowing us to have N smaller would permit us to have a smaller upper bound for the quadratic non-residues. The best theorem in this direction is the Burgess bound [8].

Theorem 1.4. *Let χ be a primitive character* mod q*, where $q > 1$, r is a positive integer and $\varepsilon > 0$ is a real number. Let M and N be non-negative reals with $N \geq 1$. Then*

$$|S_\chi(M,N)| = \left|\sum_{M<n\leq M+N} \chi(n)\right| \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\varepsilon}$$

for $r = 1, 2, 3$ and for any $r \geq 1$ if q is cubefree, the implied constant depending only on ε and r.

Note that Pólya–Vinogradov works for any non-principal character while Burgess works for primitive characters and the modulus must be cubefree in the case $r > 3$. Norton [33] has extended it to all moduli by adding an extra term that depends on the number of prime powers in the factorization of q.

To illustrate the importance of the Burgess inequality, we'll sketch the proof that $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$. First, let $x = p^{\frac{1}{4}+\frac{1}{2r}}$ and $\varepsilon_1 < \frac{1}{4r^2}$, where r is a positive integer and p is prime. Let χ be a non-principal Dirichlet character mod p. Then by Theorem 1.4

we have

$$\left|\sum_{n\le x}\chi(n)\right| \ll x^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}+\varepsilon_1} = p^{\frac{1}{4}+\frac{1}{2r}+\left(\varepsilon_1-\frac{1}{4r^2}\right)} = o(x). \tag{1.3}$$

For $\delta > 0$, let $y = x^{\frac{1}{\sqrt{e}}+\delta}$ and assume that for all $n \le y$, $\chi(n) = 1$. Since $y^2 > x$, if $m \le x$ and $\chi(m) \ne 1$, then $m = qn$, where $\chi(q) = -1$, q is prime, and $q > y$. Using $\displaystyle\sum_{p\le x}\frac{1}{p} \sim \log\log p$ yields

$$\sum_{n\le x}\chi(n) \ge \sum_{n\le x}1 - 2\sum_{\substack{y<q\le x\\ \chi(q)\ne 1}}\sum_{n\le\frac{x}{q}}1 \gg x\left(1-2\sum_{\substack{y<q\le x\\ q \text{ prime}}}\frac{1}{q}\right) \gg_\delta x. \tag{1.4}$$

This idea is usually referred to as the Vinogradov trick. One can find a nice treatment of it in [9] or one can read the original in [44].

Combining (1.4) and (1.3) yields $g(p) \ll_\delta y$. Therefore, for $\varepsilon > 0$, we have $g(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.

Just like how it is useful to have explicit estimates for the Pólya–Vinogradov inequality, it is also useful to have explicit estimates for the Burgess inequality. In their analytic number theory book [22], Iwaniec and Kowalski give a sketch of a proof of the following explicit result:

Theorem 1.5. *Let χ be a primitive character* mod p*, where $p > 1$ is prime. Let r be a positive integer, and let M and N be non-negative reals with $N \ge 1$. Then*

$$|S_\chi(M,N)| = \left|\sum_{M<n\le M+N}\chi(n)\right| \le 30N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{r}}.$$

Iwaniec and Kowalski were not looking for the best possible constant. In Chapter 6, with an eye towards getting the best possible constant, we improve this to

Theorem 1.6. *Let p be a prime such that $p \geq 10^7$. Let χ be a non-principal Dirichlet character* mod p. *Let r be a positive integer, and let M and N be non-negative reals with $N \geq 1$. Then*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

If we restrict the range of N slightly in the Burgess inequality, there are stronger results due to Booker [4] and McGown [25]. Booker's result is stronger than McGown's but the proof is restricted to quadratic characters. In Chapter 6 we improve McGown's result, making it almost as strong as Booker's result.

Recently, in [23], Levin, Pomerance and Soundararajan considered a "smoothed" version of the Pólya–Vinogradov inequality. Instead of considering the sum of character values, they consider the sum of weighted character values

$$S_\chi^*(M,N) := \left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right|.$$

The theorem they prove is the following:

Theorem 1.7. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be real numbers with $0 < N \leq q$. Then*

$$\left|S_\chi^*(M,N)\right| = \left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$

The remarkable thing about this inequality is that it is very tight. Indeed, in Chapter 2, we prove:

Theorem 1.8. *Let χ be a primitive character to the modulus $q > 1$. Then, there*

exist integers M and N such that

$$\left|S_\chi^*(M,N)\right| > \frac{2}{\pi^2}\sqrt{q}.$$

This theorem shows us that the smoothed Pólya–Vinogradov inequality is best possible up to a constant.

In Chapter 3 we use the smoothed Pólya–Vinogradov inequality to make an improvement on a theorem of Granville, Mollin and Williams. In [15], they prove that for any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$, i.e., the least inert prime in a real quadratic field of discriminant $D > 3705$ is less than $\sqrt{D}/2$. We improve this to:

Theorem 1.9. *For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$.*

The proof of the theorem consists of three parts: when D is small ($D \leq 2.6 \times 10^{17}$ for D odd and $D \leq 1.04 \times 10^{18}$ for D even), when D is huge ($D \geq 10^{24}$), and when D is neither small nor huge. To check D small we use the tables computed in [15]. The tables were created using a special computer called the Manitoba Scalable Sieving Unit (MSSU, see [24]). It ran for about 5 months. Recent developments in sieving machines (see [46]) suggests that a sieving machine could check up to about 10^{24}, which would allow us to improve the upper bound in the theorem to $D^{3/7}$ or better instead of $D^{0.45}$.

In Chapter 5 we tackle the problem of consecutive residues and non-residues of a Dirichlet character χ mod p. Let H be the largest integer such that there exists an

integer N such that $\chi(N+1) = \chi(N+2) = \ldots = \chi(N+H)$. The best asymptotic result is due to Burgess [7], where he shows that $H = O(p^{1/4} \log p)$. In a recent paper in the arXiv, McGown [26] proved that $H < 7.06p^{1/4} \log p$ whenever $p > 5 \cdot 10^{18}$ and $H < 7p^{1/4} \log p$ when $p > 5 \cdot 10^{55}$. We improve this to $H < 3p^{1/4} \log p$ for all odd p and $H < 1.55p^{1/4} \log p$ whenever $p > 2.5 \cdot 10^9$.

Overall, the purpose of the thesis is to get the best numerically explicit estimates we can on character sums. Chapter 3 is an example of an application of explicit character estimates, but there are others. For example, using the smoothed Pólya–Vinogradov inequality, Levin, Pomerance and Soundararajan [23] proved that for every prime $p > 3$ there is a primitive root t such that $\log_t x = x$, where $\log_t x$ is the discrete logarithm function to the base t for the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. Using an explicit estimate for the Burgess inequality, Booker [4] computed the class number of a 32-digit discriminant. Finally, using weaker estimates than the ones shown in Chapters 4, 5 and 6, McGown [25] showed that there are no norm-Euclidean Galois cubic fields of discriminant larger than 10^{140}. Using our estimates we would be able to improve that theorem.

1.1 Notation

Throughout the thesis we will have the following notation:

- ϕ refers to the Euler totient function, i.e., for a positive integer n, $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n.
- μ refers to the Moebius function, defined as follows: for n a positive integer, $\mu(n) = 1$, if $n = 1$ or if n is squarefree and has an even number of prime factors.

$\mu(n) = -1$ if n is squarefree and has an odd number of prime factors. Finally, $\mu(n) = 0$ if n is not squarefree, i.e., there is a prime p such that p^2 divides n .

- For n a positive integer, $\omega(n)$ will denote the number of distinct prime factors of n.

- For x a real number, $\lfloor x \rfloor$ is the floor function, i.e., the greatest integer less than or equal to x.

- For x a real number, $\{x\}$ is the fractional part of x, i.e., $\{x\} = x - \lfloor x \rfloor$.

- Throughout the thesis, p will represent a prime; this includes when we are considering sums. For example, $\sum_{p \leq x} p$ would be the sum of the prime numbers less than or equal to x.

- log refers to the natural logarithm, i.e., the logarithm base e.

- θ refers to the Chebyshev function, i.e., for x a positive real number, $\theta(x) = \sum_{p \leq x} \log p$.

- γ is the Euler–Mascheroni constant, i.e., $\gamma = \lim_{n \to \infty} \sum_{k=1}^{n} \frac{1}{k} - \log n$.

- For integers a and b, (a, b) will denote the greatest common divisor of a and b. Sometimes we will also denote this by $\gcd(a, b)$.

- We write $f = O(g)$ to mean that there is a constant C with $|f| \leq Cg$, for all values of the variables under consideration. This is usually denoted as big Oh notation or Landau O notation.

- Similarly, we use the Vinogradov symbol $\ll$, where $f \ll g$ if $|f| \leq Cg$ for some constant C, for all values of the variables under consideration. If we write $f \ll_k g$, it means that the constant C depends on k.
- We write $f = \Omega(g)$, if there is a constant C such that infinitely many positive integers n satisfy $|f(n)| \geq Cg(n)$. This differs from the computer science convention, where $f = \Omega(g)$ if $f \gg g$.
- We write $f = o(g)$ to mean that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Chapter 2

Smoothed Pólya–Vinogradov

Let χ be a non-principal Dirichlet character to the modulus q. It has been the interest of mathematicians to study the sum $\left|\sum_{n=M+1}^{M+N}\chi(n)\right|$. Pólya and Vinogradov, independently proved in 1918 that the sum is bounded above by $O(\sqrt{q}\log q)$. Assuming the Riemann Hypothesis for L-functions (GRH), Montgomery [28] showed that the sum is bounded by $O(\sqrt{q}\log\log q)$. This is best possible (up to a constant), because in 1932 Paley [34] proved that there are infinitely many quadratic characters χ such that there exists a constant $c>0$ that satisfy for some N the following inequality $\left|\sum_{n=1}^{N}\chi(n)\right| > c\sqrt{q}\log\log q$.

Recently, in [23], Levin, Pomerance and Soundararajan considered a "smoothed" version of the Pólya–Vinogradov inequality. Instead of considering the sum of the characters, they consider the weighted sum

$$S_\chi^*(M,N) := \left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right|.$$

The theorem they prove is the following:

Theorem 2.1. *Let χ be a primitive Dirichlet character to the modulus $q > 1$ and let M, N be real numbers with $0 < N \leq q$. Then*

$$\left|S_\chi^*(M,N)\right| = \left|\sum_{M\leq n\leq M+2N} \chi(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$

In section 2.1 we will give a proof of this theorem and several useful corollaries. The remarkable thing about this theorem is that it is not very hard to prove and it is a tight inequality, since one can show that $\left|S_\chi^*(M,N)\right| > c\sqrt{q}$ for some positive constant c. Indeed, in section 2.2 we will prove that $\left|S_\chi^*(M,N)\right| > \frac{2}{\pi^2}\sqrt{q}$. The proof was motivated by the proof in [29] that if $q > 1$ is a positive integer and χ is a primitive character mod q then $\max_{M,N}\left|\sum_{M<n\leq M+N}\chi(n)\right| \geq \frac{\sqrt{q}}{\pi}$.

2.1 Upper bound and corollaries

Proof of Theorem 2.1. We follow the proof in [23]. Let

$$H(t) = \max\{0, 1 - |t|\}.$$

We wish to estimate $|S_\chi^*(M,N)|$.

Using the identity (see Corollary 9.8 in [29])

$$\chi(n) = \frac{1}{\tau(\bar{\chi})}\sum_{j=1}^{q}\bar{\chi}(j)e(nj/q)$$

where $e(x) := e^{2\pi i x}$ and $\tau(\chi) = \sum_{a=1}^{q}\chi(a)e(a/q)$ is the Gauss sum, we can deduce

$$S_\chi^*(M,N) = \frac{1}{\tau(\bar{\chi})}\sum_{j=1}^{q}\bar{\chi}(j)\sum_{n\in\mathbb{Z}} e(nj/q)H\left(\frac{n-M}{N}-1\right).$$

The Fourier transform (see Appendix D in [29]) of H is

$$\widehat{H}(s) = \int_{-\infty}^{\infty} H(t)e(-st)dt = \frac{1-\cos 2\pi s}{2\pi^2 s^2} \text{ when } s\neq 0,\ \widehat{H}(0)=1,$$

which is nonnegative for s real. In general, if

$$f(t) = e(\alpha t)H(\beta t+\gamma), \tag{2.1}$$

with $\beta > 0$, then

$$\widehat{f}(s) = \frac{1}{\beta}e\left(\frac{s-\alpha}{\beta}\gamma\right)\widehat{H}\left(\frac{s-\alpha}{\beta}\right). \tag{2.2}$$

Using $\alpha = j/q$, $\beta = 1/N$ and $\gamma = -M/N-1$, then by Poisson summation (see Appendix D in [29]) we get

$$S_\chi^*(M,N) = \frac{N}{\tau(\bar{\chi})}\sum_{j=1}^{q}\bar{\chi}(j)\sum_{n\in\mathbb{Z}} e\left(-(M+N)\left(n-\frac{j}{q}\right)\right)\widehat{H}\left(\left(s-\frac{j}{q}\right)N\right). \tag{2.3}$$

Using that $\chi(q)=0$, that $\widehat{H}$ is nonnegative and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters we have

$$\left|S_\chi^*(M,N)\right| \leq \frac{N}{\sqrt{q}}\sum_{j=1}^{q-1}\sum_{n\in\mathbb{Z}}\widehat{H}\left(\left(n-\frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}}\sum_{k\in\mathbb{Z}/k\mathbb{Z}}\widehat{H}\left(\frac{kN}{q}\right).$$

Therefore

$$\left|S_\chi^*(M,N)\right| \le \frac{N}{\sqrt{q}}\left(\sum_{k\in\mathbb{Z}}\widehat{H}\left(\frac{kN}{q}\right)-\sum_{k\in\mathbb{Z}}\widehat{H}(kN)\right)$$
$$=\sqrt{q}\left(\sum_{k\in\mathbb{Z}}\frac{N}{q}\widehat{H}\left(\frac{kN}{q}\right)-\frac{N}{q}\sum_{k\in\mathbb{Z}}\widehat{H}(kN)\right)\le\sqrt{q}\left(\sum_{k\in\mathbb{Z}}\frac{N}{q}\widehat{H}\left(\frac{kN}{q}\right)-\frac{N}{q}\widehat{H}(0)\right).$$

Using $\alpha=\gamma=0$ and $\beta=\frac{q}{N}$ in (2.1) and (2.2) yields that the Fourier transform of $H\left(\frac{qt}{N}\right)$ is

$$\frac{1}{\beta}e\left(\frac{s-0}{\beta}\cdot(0)\right)\widehat{H}\left(\frac{s-0}{\beta}\right)=\frac{N}{q}\widehat{H}\left(\frac{sdN}{q}\right).$$

Therefore, by Poisson summation, we have

$$\left|S_\chi^*(M,N)\right|\le\sqrt{q}\sum_{l\in\mathbb{Z}}H\left(\frac{ql}{N}\right)-\frac{N}{\sqrt{q}}=\sqrt{q}H(0)-\frac{N}{\sqrt{q}}=\sqrt{q}-\frac{N}{\sqrt{q}}. \tag{2.4}$$

We used that $q\ge N$ which implies that for $l\neq 0$ and $l\in\mathbb{Z}$, $\left|\frac{ql}{N}\right|\ge\left|\frac{q}{N}\right|\ge 1$ which implies $H\left(\frac{ql}{N}\right)=0$. □

The following corollary, uses arithmetic information from the modulus q to give a better upper bound for some ranges of N.

Corollary 2.1. *Let χ be a primitive character to the modulus $q>1$, let M,N be real numbers with $0<N\le q$ and let m be a divisor of q such that $1\le m\le\frac{q}{N}$. Then*

$$\left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right|\le\frac{\phi(m)}{m}\sqrt{q}.$$

Proof. Following the proof of the previous theorem, we arrive at (2.3). From there, using that if $(n,m)>1$ then $\chi(n)=0$, that $\widehat{H}$ is nonnegative and that $|\tau(\bar{\chi})|=\sqrt{q}$

for primitive characters we have

$$\left|S_\chi^*(M,N)\right| \le \frac{N}{\sqrt{q}} \sum_{\substack{j=1\\(j,m)=1}}^{q} \sum_{n\in\mathbb{Z}} \widehat{H}\left(\left(n-\frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}} \sum_{\substack{k\in\mathbb{Z}\\(k,m)=1}} \widehat{H}\left(\frac{kN}{q}\right). \tag{2.5}$$

Using inclusion exclusion we get

$$\left|S_\chi^*(M,N)\right| \le \frac{N}{\sqrt{q}} \sum_{d|m} \mu(d) \sum_{k\in\mathbb{Z}} \widehat{H}\left(\frac{kdN}{q}\right) = \sqrt{q} \sum_{d|m} \frac{\mu(d)}{d} \sum_{k\in\mathbb{Z}} \frac{dN}{q} \widehat{H}\left(\frac{kdN}{q}\right).$$

Since the Fourier transform of $H\left(\frac{qt}{Nd}\right)$ is $\frac{dN}{q}\widehat{H}\left(\frac{sdN}{q}\right)$, then by Poisson summation

$$\left|S_\chi^*(M,N)\right| \le \sqrt{q} \sum_{d|m} \frac{\mu(d)}{d} \sum_{l\in\mathbb{Z}} H\left(\frac{ql}{Nd}\right) = \sqrt{q} \sum_{d|m} \frac{\mu(d)}{d} H(0) = \frac{\phi(m)}{m}\sqrt{q}.$$

We used that $q \ge mN$ which implies that for $l \ne 0$ and $l \in \mathbb{Z}$, $\left|\frac{ql}{Nd}\right| \ge \left|\frac{q}{Nm}\right| \ge 1$ which implies $H\left(\frac{ql}{Nd}\right) = 0$. □

The following corollary is a minor modification of Corollary 3 in [23], which was stated without proof.

Corollary 2.2. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be real numbers with $N > 0$. Then,*

$$\left|\sum_{M\le n\le M+2N} \chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| \le \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right). \tag{2.6}$$

In particular, $|S_\chi^*(M,N)| < \sqrt{q}$.

Proof. In the proof of Theorem 2.1, we only used that $N \le q$ in the last inequality

of (2.4). Therefore from (2.4) we have

$$|S_\chi^*(M,N)| \le \sqrt{q}\left(\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) - \frac{N}{q}\right).$$

To get the desired result we need only prove

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) \le \frac{N}{q} + \frac{q}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right).$$

Note that $H\left(\frac{ql}{N}\right) = 0$ for $|l| > \frac{N}{q}$. Also $H\left(\frac{ql}{N}\right) = H\left(\frac{-ql}{N}\right)$. Using these two facts together with $H(0) = 1$, we get

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) = 1 + 2\sum_{l\le\frac{N}{q}} H\left(\frac{ql}{N}\right) = 1 + 2\sum_{l\le\frac{N}{q}}\left(1-\frac{ql}{N}\right).$$

Therefore

$$\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) = 1 + 2\left\lfloor\frac{N}{q}\right\rfloor - \frac{2q}{N}\sum_{l\le\frac{N}{q}} l = 1 + 2\left\lfloor\frac{N}{q}\right\rfloor - \frac{q}{N}\left(\left\lfloor\frac{N}{q}\right\rfloor\right)\left(\left\lfloor\frac{N}{q}\right\rfloor + 1\right).$$

Letting $\theta = \frac{N}{q}$ and using that $\frac{N}{q} = \left\lfloor\frac{N}{q}\right\rfloor + \theta$, we get

$$\begin{aligned}\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{N}\right) &= 1 + \frac{2N}{q} - 2\theta + \frac{q}{N}\left(\frac{N^2}{q^2} + \frac{N}{q}(1-2\theta) - \theta(1-\theta)\right)\\ &= \frac{2N}{q} + 1 - 2\theta - \frac{N}{q} - (1-2\theta) + \frac{q}{N}\theta(1-\theta) = \frac{N}{q} + \frac{q}{N}\theta(1-\theta).\end{aligned}$$

Therefore (2.6) is true. Once we have (2.6), we can conclude that

$|S_\chi^*(M,N)| < \sqrt{q}$. Indeed, if $N \le q$, then

$$S_\chi^*(M,N) \le \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right) = \sqrt{q} - \frac{N}{\sqrt{q}} < \sqrt{q};$$

and if $N > q$, we have

$$S_\chi^*(M,N) \le \frac{q^{3/2}}{N}\left\{\frac{N}{q}\right\}\left(1-\left\{\frac{N}{q}\right\}\right) \le \frac{q^{3/2}}{4N} < \frac{\sqrt{q}}{4}.$$

□

Our last corollary is an inequality for general Dirichlet characters (as opposed to just primitive Dirichlet characters).

Corollary 2.3. *Let χ be a non-principal Dirichlet character to the modulus $q > 1$ and let M, N be real numbers with $N > 0$. Then,*

$$\left|\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| < \frac{4}{\sqrt{6}}\sqrt{q}.$$

Proof. In this proof, we follow the ideas used in [29] to extend the Pólya–Vinogradov inequality from primitive characters to general characters.

Let χ be induced by a primitive character χ^* of modulus $d > 1$. This is possible since χ is non-principal. In the case that χ is primitive, then $\chi^* = \chi$. Letting χ_0 be the principal character mod q, we have that $\chi = \chi^*\chi_0$. Therefore $\chi(n) = \chi^*(n)$ for n an integer coprime to q, and $\chi(n) = 0$ otherwise.

Let r be the product of primes that divide q but not d. Then when $(n,r) > 1$, we have $\chi(n) = 0$. If $(n,r) = 1$, then $\chi(n) = \chi^*(n)$. Therefore

$$\sum_{M\le n\le M+2N}\chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)=\sum_{\substack{M\le n\le M+2N\\(n,r)=1}}\chi^*(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)$$
$$=\sum_{M\le n\le M+2N}\chi^*(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\sum_{k|(n,r)}\mu(k)$$
$$=\sum_{k|r}\mu(k)\sum_{\substack{M\le n\le M+2N\\k|n}}\chi^*(n)\left(1-\left|\frac{n-M}{N}-1\right|\right).$$

Now, writing $n=km$ and using that χ^* is totally multiplicative we get

$$\sum_{k|r}\mu(k)\chi^*(k)\sum_{\frac{M}{k}\le m\le\frac{M+2N}{k}}\chi^*(m)\left(1-\left|\frac{m-\frac{M}{k}}{\frac{N}{k}}-1\right|\right)=\sum_{k|r}\mu(k)\chi^*(k)S_{\chi^*}\left(\frac{M}{k},\frac{N}{k}\right).$$

By Corollary 2.2, $|S_{\chi^*}(M/k,N/k)|<\sqrt{d}$. Hence, taking absolute value we have

$$|S^*_\chi(M,N)|<\sum_{k|r}\sqrt{d}=2^{\omega(r)}\sqrt{d}\le 2^{\omega(r)}\sqrt{\frac{q}{r}}. \tag{2.7}$$

Since 2^ω is a multiplicative function, and for $p\ge 5$, $2<\sqrt{p}$, we have

$$\frac{2^{\omega(r)}}{\sqrt{r}}=\prod_{p|r}\frac{2}{\sqrt{p}}\le\frac{2}{\sqrt{2}}\times\frac{2}{\sqrt{3}}=\frac{4}{\sqrt{6}}. \tag{2.8}$$

Combining (2.7) with (2.8) yields the desired result. □

2.2 Lower bound

Let's start with a lemma that will be used in the proof of the lower bound.

2.2 Lower bound

Lemma 2.1. *Let $N \in \mathbb{N}$ and $\alpha \in \mathbb{R}$ such that $e(\alpha) \neq 1$, then*

$$\sum_{n=0}^{N} n \cdot e(\alpha n) = \frac{Ne\left((N+1)\,\alpha\right) - (N+1)e\left(N\alpha\right) + 1}{\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2}$$

Proof. For $x \in \mathbb{R}$, we have $\displaystyle\sum_{n=0}^{N} x^n = \frac{x^{N+1}-1}{x-1}$, by differentiating both sides and multiplying by x we get

$$\sum_{n=0}^{N} n \cdot x^n = x\frac{(N+1)x^N(x-1) - (x^{N+1}-1)}{(x-1)^2} = x\frac{Nx^{N+1} - (N+1)x^N + 1}{(x-1)^2}.$$

Therefore, by making the substitution $x = e(\alpha)$ we get

$$S(N) := \sum_{n=0}^{N} n \cdot e(\alpha n) = e(\alpha)\frac{Ne\left((N+1)\alpha\right) - (N+1)e\left(N\alpha\right) + 1}{(e(\alpha)-1)^2}.$$

Using that $(e(\alpha)-1)^2 = e(\alpha)\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2$ yields the lemma. □

Theorem 2.2. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be positive integers. Then*

$$S_2(N) := \max_{1 \leq M \leq q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin\frac{\pi N}{q}\right)^2}{\left(\sin\frac{\pi}{q}\right)^2} \tag{2.9}$$

Proof. Let

$$S_3(N) := \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right),$$

and note that

$$|S_3(N)| \leq \sum_{M=1}^{q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right|$$
$$\leq q \max_{1\leq M\leq q} \left| \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| = qS_2(N).$$

Therefore we can focus on $S_3(N)$.

$$S_3(N) = \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \sum_{n=M}^{M+2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right)$$
$$= \sum_{n=0}^{2N} \sum_{M=1}^{q} e\left(\frac{M}{q}\right) \chi(n+M) \left(1 - \left|\frac{n}{N} - 1\right|\right).$$

Now we can do a change of variable, to go from M to $L-n$:

$$S_3(N) = \sum_{n=0}^{2N} \sum_{L=1}^{q} e\left(\frac{L-n}{q}\right) \chi(L) \left(1 - \left|\frac{n}{N} - 1\right|\right)$$
$$= \sum_{n=0}^{2N} e\left(-\frac{n}{q}\right) \left(1 - \left|\frac{n}{N} - 1\right|\right) \sum_{L=1}^{q} e\left(\frac{L}{q}\right) \chi(L).$$

Therefore,

$$S_3(N) = \tau(\chi) \sum_{n=0}^{2N} e\left(-\frac{n}{q}\right) \left(1 - \left|\frac{n}{N} - 1\right|\right) = \tau(\chi) S_4(N).$$

Now it's time to work on $S_4(N)$:

$$S_4(N) = \sum_{n=0}^{2N} e\left(-\frac{n}{q}\right) \left(1 - \left|\frac{n}{N} - 1\right|\right) = \sum_{n=0}^{N} e\left(-\frac{n}{q}\right) \frac{n}{N} + \sum_{n=N+1}^{2n} e\left(-\frac{n}{q}\right) \left(2 - \frac{n}{N}\right).$$

By making the change of variable $m = 2N - n$, we get

$$S_4(N) = \frac{1}{N}\sum_{n=0}^{N} e\left(-\frac{n}{q}\right) n \; + \; \frac{e\left(-\frac{2N}{q}\right)}{N}\sum_{m=0}^{N-1} e\left(\frac{m}{q}\right) m.$$

Using Lemma 2.1 with $\alpha = -\frac{1}{q}$ we get

$$S_4(N) = \frac{1}{N}\frac{Ne\left((N+1)\alpha\right) - (N+1)e\left(N\alpha\right) + 1}{\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2} + \frac{e\left(2N\alpha\right)}{N}\frac{(N-1)e\left(-N\alpha\right) - Ne\left(-(N-1)\alpha\right) + 1}{\left(e\left(-\frac{\alpha}{2}\right) - e\left(\frac{\alpha}{2}\right)\right)^2}.$$

Therefore, by taking common denominator and multiplying out we get that $S_4(N)$ equals

$$\frac{Ne\left((N+1)\alpha\right) - (N+1)e\left(N\alpha\right) + 1 + (N-1)e(N\alpha) - Ne((N+1)\alpha) + e(2N\alpha)}{N\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2},$$

which equals

$$\frac{e(2N\alpha) - 2e(N\alpha) + 1}{N\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2} = \frac{e(N\alpha)}{N}\frac{\left(e\left(\frac{N\alpha}{2}\right) - e\left(-\frac{N\alpha}{2}\right)\right)^2}{\left(e\left(\frac{\alpha}{2}\right) - e\left(-\frac{\alpha}{2}\right)\right)^2} = \frac{e(N\alpha)}{N}\frac{(\sin N\pi\alpha)^2}{(\sin \pi\alpha)^2}. \quad (2.10)$$

From earlier we know, $qS_2(N) \geq |S_3(N)| = |\tau(\chi)||S_4(N)|$. Using $|\tau(\chi)| = \sqrt{q}$, that $|e(x)| = 1$ and (2.10) yields the theorem. □

Corollary 2.4. *Let χ be a primitive character to the modulus $q > 1$ and let M, N be positive integers. Then*

$$\max_{M,N}\left|\sum_{n=M}^{M+2N} \chi(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| \geq \frac{2}{\pi^2}\sqrt{q}.$$

Proof. If q is even, let $N = \frac{q}{2}$. Therefore (2.9) becomes

$$S_2(N) \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin \frac{\pi N}{q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2} = \frac{2}{q\sqrt{q}} \frac{1}{\left(\sin \frac{\pi}{q}\right)^2} \geq \frac{2}{\pi^2}\sqrt{q}.$$

The last inequality comes from $\frac{1}{\sin x} \geq \frac{1}{x}$.

If q is odd, let $N = \frac{q-1}{2}$, now we get

$$S_2(N) \geq \frac{1}{N\sqrt{q}} \frac{\left(\sin \frac{\pi N}{q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2} = \frac{2}{(q-1)\sqrt{q}} \frac{\left(\cos \frac{\pi}{2q}\right)^2}{\left(\sin \frac{\pi}{q}\right)^2}.$$

From this and $\sin \frac{\pi}{q} = 2 \sin \frac{\pi}{2q} \cos \frac{\pi}{2q}$ we get

$$S_2(N) \geq \frac{2}{4(q-1)\sqrt{q}} \frac{1}{\left(\sin \frac{\pi}{2q}\right)^2} \geq \frac{2}{\pi^2} \frac{q}{q-1}\sqrt{q} > \frac{2}{\pi^2}\sqrt{q}.$$

□

Remark 2.1. If we consider $N = \frac{q}{3}$ for $3 \mid q$, $N = \frac{q-1}{3}$ for $q \equiv 1 \pmod 3$ and $N = \frac{q-2}{3}$ for $q \equiv 2 \pmod 3$ then we can improve the constant from $\frac{2}{\pi^2} = 0.202642\ldots$ to $\frac{9}{4\pi^2} = 0.227973\ldots$. With N around $\frac{2q}{5}$ the constant improves a bit more to $\frac{5(5+\sqrt{5})}{16\pi^2} = 0.229115\ldots$. The optimal value for N under this technique is around $N = .371q$ where the constant is 0.230651.

Chapter 3

The least inert prime in a real quadratic field

In [15], Granville, Mollin and Williams prove the following theorem:

Theorem 3.1. *For any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$.*

Their proof consists of three parts. They verify the truth of the conjecture up to fairly large values of D computationally. They show using analytic methods that there are no counterexamples for $D > 10^{32}$ and they complete the proof using analytic methods combined with computation (what I'll refer to as the hybrid case).

Note that D is a fundamental discriminant if and only if either D is squarefree, $D \neq 1$, and $D \equiv 1 \pmod 4$ or $D = 4L$ with L squarefree and $L \equiv 2, 3 \pmod 4$. Since $(D/2) = -1$ for $D \equiv 5 \pmod 8$, we need only consider values of D such that $D = L \equiv 1 \pmod 8$ or $D = 4L$ with $L \equiv 2, 3 \pmod 4$.

For the computational aspect, they used the Manitoba Scalable Sieving Unit, a

very powerful sieving machine (see [24] for more details). They ran the machine for a period of 5 months to produce three tables. From these tables the relevant information is the following:

If

(a) $L \equiv 1 \pmod 8$ with $(L/q) = 0$ or 1 for all odd $q \leq 257$,

(b) $L \equiv 2 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \leq 283$, or

(c) $L \equiv 3 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \leq 277$

then $L > 2.6 \times 10^{17}$.

From (a) we see that if D is odd and $D < 2.6 \times 10^{17}$ then there exists $q \leq 257$ for which $(D/q) = -1$, verifying the theorem for $D > 4(257)^2 = 264196$. From (b) and (c) we see that if D is even and $D = 4L < 4 \times 2.6 \times 10^{17} = 1.04 \times 10^{18}$ then there exists a $q \leq 283$ for which $(D/q) = -1$, verifying the theorem for $D > 4(283)^2 = 320356$. Running a simple loop over all fundamental discriminants below 320356 we find that if we let

$$S = \{D| \text{ the least prime } p \text{ such that } (D/p) = -1 \text{ satisfies } p > \sqrt{D}/2\},$$

then

$$\begin{aligned} S = \{&5, 8, 12, 13, 17, 24, 28, 33, 40, 57, 60, 73, 76, 88, 97, 105, 120, 124, \\ &129, 136, 145, 156, 184, 204, 249, 280, 316, 345, 364, 385, 424, 456, \\ &520, 561, 609, 616, 924, 940, 984, 1065, 1596, 2044, 3705\}. \end{aligned}$$

We point out that in [15] they failed to mention that 120 and 561 are in S and

they incorrectly claim $2244 \in S$ (note that 2244 is not a fundamental discriminant since $2244/4 = 561 \equiv 1 \pmod 4$). Theorem 3.1 was first conjectured in Chapter 6 of [27] with a slightly different wording, focusing on the radicand instead of on the fundamental discriminant. When [15] translated radicands to discriminants there were mistakes; changing 561 to 2244 (this accounts for claiming $2244 \in S$ while neglecting that $561 \in S$) and we suspect that since $60 \in S$ they thought that the radicand 30 was already accounted for, therefore not including 120 in S.

For the analytical methods in the proof, i.e., to show that $D > 10^{32}$ works, the main tool in the paper is the Pólya–Vinogradov inequality. The Pólya–Vinogradov inequality states that there exists an absolute universal constant c such that for every character χ to the modulus q we have the inequality $\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \leq c\sqrt{q}\log q$. This is the aspect on which we have been able to make some improvements, by using the Smoothed Pólya–Vinogradov inequality.

To complete the proof, i.e., show that when $D \leq 10^{32}$, $D > 2.6 \times 10^{17}$ works in the odd case and $D > 1.04 \times 10^{18}$ works in the even case. The authors combined the Pólya–Vinogradov inequality with computation. This aspect of their proof would not be needed if one uses the Smoothed Pólya–Vinogradov, however it is needed in our case to be able to improve their theorem.

In this paper we will prove

Theorem 3.2. *For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$.*

Note, that by using the tables provided in [15] the only even values of $D < 1.04\times10^{18}$ that can contradict the theorem satisfy $D < 283^{1/.45} < 280812$ and the only odd values of $D < 2.6 \times 10^{17}$ that can contradict the theorem satisfy $D < 257^{1/.45} <$

226677. Checking over all these values we find that the set of counterexamples $S^{'}$ is

$$S^{'} = \{8, 12, 24, 28, 33, 40, 60, 105, 120, 156, 184, 204, 280, 364, 456, 520, 1596\}.$$

This set is sparser than S because for $D < 2^{20} = 1048576$, $\sqrt{D}/2$ is smaller than $D^{0.45}$.

The chapter is divided as follows: In section 3.1, we prove a slightly better smoothed Pólya–Vinogradov inequality, one that uses a little more information about the modulus of the character. This inequality will be key in our proof of Theorem 3.2. In section 3.2, we will prove many technical lemmas that will be used in the proof of the main theorem. In section 3.3 we prove the theorem for $D > 10^{24}$ and in the last section (section 3.4) we close the gap proving the theorem for $D > 10^{18}$ when D is even and $D > 10^{17}$ when D is odd.

3.1 Smoothed Pólya–Vinogradov

Theorem 3.3. *Let χ be a primitive character to the modulus $q > 1$, let M, N be real numbers with $0 < N \leq q$. Then*

$$\left|S_{\chi}^{*}(M,N)\right| = \left|\sum_{M \leq n \leq M+2N} \chi(n)\left(1 - \left|\frac{n-M}{N} - 1\right|\right)\right| \leq \frac{\phi(q)}{q}\sqrt{q} + 2^{(\omega(q)-1)}\frac{N}{\sqrt{q}}.$$

Remark 3.1. This theorem is similar to Corollary 2.1. Both use arithmetic properties of q to improve the upper bound. In the ranges we will require of N, this inequality will be more useful to us.

Proof. The proof is very similar to the proof of Theorem 2.1. Let

$$H(t) = \max\{0, 1 - |t|\}.$$

We wish to estimate $|S_\chi^*(M,N)|$. Following the same strategy as in the proof of Theorem 2.1 and using that if $(n,q) > 1$ then $\chi(n) = 0$, we have from (2.5)

$$\left|S_\chi^*(M,N)\right| \leq \frac{N}{\sqrt{q}} \sum_{\substack{j=1 \\ (j,q)=1}}^{q} \sum_{n\in\mathbb{Z}} \widehat{H}\left(\left(n - \frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}} \sum_{\substack{k\in\mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Using inclusion exclusion we get

$$\left|S_\chi^*(M,N)\right| \leq \frac{N}{\sqrt{q}} \sum_{d|q} \mu(d) \sum_{k\in\mathbb{Z}} \widehat{H}\left(\frac{kdN}{q}\right) = \sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} \sum_{k\in\mathbb{Z}} \frac{dN}{q} \widehat{H}\left(\frac{kdN}{q}\right).$$

Since the Fourier transform of $H\left(\frac{qt}{Nd}\right)$ is $\frac{dN}{q}\widehat{H}\left(\frac{sdN}{q}\right)$, then by Poisson summation

$$\begin{aligned}
\left|S_\chi^*(M,N)\right| &\leq \sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} \sum_{l\in\mathbb{Z}} H\left(\frac{ql}{Nd}\right) = \sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} \left(1 + 2 \sum_{1\leq l\leq \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right)\right) \\
&= \sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} + 2\sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} \sum_{1\leq l\leq \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right) \\
&= \frac{\phi(q)}{q}\sqrt{q} + 2\sqrt{q} \sum_{d|q} \frac{\mu(d)}{d} \sum_{1\leq l\leq \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right). \quad (3.1)
\end{aligned}$$

Note that for the last inner sum to be nonzero, $d \geq \frac{q}{N}$. Let's calculate the inner sum:

$$\sum_{1\leq l\leq \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right) = \left\lfloor \frac{Nd}{q} \right\rfloor \left(1 - \frac{q}{2Nd}\left(\left\lfloor \frac{Nd}{q} \right\rfloor + 1\right)\right).$$

Replacing $\left\lfloor \frac{Nd}{q} \right\rfloor$ with $\frac{Nd}{q} - \left\{ \frac{Nd}{q} \right\}$ and multiplying through, we get:

$$\sum_{1 \le l \le \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right) = \frac{Nd}{2q} - \frac{1}{2} + \frac{q}{2Nd} \left\{ \frac{Nd}{q} \right\} \left(1 - \left\{ \frac{Nd}{q} \right\}\right). \tag{3.2}$$

Now,

$$\frac{q}{2Nd} \left\{ \frac{Nd}{q} \right\} \left(1 - \left\{ \frac{Nd}{q} \right\}\right) \le \frac{q}{8Nd} \le \frac{1}{8}. \tag{3.3}$$

The last inequality follows from $d \ge \frac{q}{N}$. Combining (3.2) with (3.3) we get

$$0 \le \sum_{l \le \frac{Nd}{q}} \left(1 - \frac{ql}{Nd}\right) < \frac{Nd}{2q}. \tag{3.4}$$

From (3.1) and (3.4) we get

$$\begin{aligned} \left|S_\chi^*(M,N)\right| &< \frac{\phi(q)}{q}\sqrt{q} + 2\sqrt{q} \sum_{\substack{d \mid q \\ \mu(d)=1}} \frac{1}{d} \left(\frac{Nd}{2q}\right) \\ &\le \frac{\phi(q)}{q}\sqrt{q} + \frac{N}{\sqrt{q}} \sum_{\substack{d \mid q \\ \mu(d)=1}} 1 = \frac{\phi(q)}{q}\sqrt{q} + 2^{(\omega(q)-1)} \frac{N}{\sqrt{q}}. \end{aligned}$$

□

3.2 Useful lemmas

We start by calculating a sum that pops up when dealing with the smoothed Pólya–Vinogradov inequality.

Lemma 3.1. *If x is a positive real number, then*

$$\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)=x-\frac{\|x\|^2}{x},$$

where $\|x\|$ is the distance of x to the nearest integer.

Proof. Let's work on the sum:

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\sum_{n\le x}\frac{n}{x}+\sum_{x<n\le 2x}\left(2-\frac{n}{x}\right)=\frac{2}{x}\sum_{n\le x}n-\frac{1}{x}\sum_{n\le 2x}n+2\lfloor 2x\rfloor-2\lfloor x\rfloor\\&=\frac{2}{x}\frac{\lfloor x\rfloor(\lfloor x\rfloor+1)}{2}-\frac{1}{x}\frac{\lfloor 2x\rfloor(\lfloor 2x\rfloor+1)}{2}+2\lfloor 2x\rfloor-2\lfloor x\rfloor\\&=\frac{\lfloor 2x\rfloor}{2x}\left(2x+\{2x\}-1\right)-\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right).\quad(3.5)\end{aligned}$$

Case 1: $\|x\|=\{x\}$. Then $\lfloor 2x\rfloor=2\lfloor x\rfloor$ and $\{2x\}=2\{x\}$. Using this and equation (3.5) we get

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\frac{\lfloor x\rfloor}{x}\left(2x+2\{x\}-1-x-\{x\}+1\right)\\&=\frac{\lfloor x\rfloor}{x}\left(x+\{x\}\right)=\frac{x^2-\{x\}^2}{x}=x-\frac{\|x\|^2}{x}.\end{aligned}$$

Case 2: $\|x\|=1-\{x\}$. Then $\lfloor 2x\rfloor=2\lfloor x\rfloor+1$ and $\{2x\}=2\{x\}-1$. Using this and equation (3.5) we get

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\frac{2\lfloor x\rfloor+1}{2x}\left(2x+2\{x\}-2\right)-\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right)\\&=\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right)+\frac{1}{2x}\left(2x+2\{x\}-2\right)=\frac{x+\{x\}-1}{x}\left(\lfloor x\rfloor+1\right)\\&=\frac{(x+(\{x\}-1))(x-(\{x\}-1))}{x}=\frac{x^2-(1-\{x\})^2}{x}=x-\frac{\|x\|^2}{x}.\end{aligned}$$

□

In the proof of the main theorem, we will need to consider the same sum but sieving out the numbers n that satisfy $\gcd(n, D) > 1$. Therefore we prove the following result.

Lemma 3.2. *Let N be a positive real number and let D be a positive integer. Then*

$$\sum_{\substack{n\leq 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) \geq \frac{\phi(D)}{D}N - 2^{(\omega(D)-2)}.$$

Proof. Using Lemma 3.1,

$$\begin{aligned}\sum_{\substack{n\leq 2N\\(n,D)=1}} \left(1-\left|\frac{n}{N}-1\right|\right) &= \sum_{d|D}\mu(d)\sum_{n\leq \frac{2N}{d}}\left(1-\left|\frac{nd}{N}-1\right|\right) = \sum_{d|D}\mu(d)\left(\frac{N}{d}-\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}\right)\\ &= \sum_{d|D}\frac{\mu(d)}{d}N - \sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}} = \frac{\phi(D)}{D}N - \sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}. \quad (3.6)\end{aligned}$$

Now, since $\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}$ is nonnegative, we can bound the sum by summing over d such that $\mu(d) = 1$. Also, if $d \geq 2N$ then $\|N/d\| = N/d$, so we can split it in two sums.

$$\begin{aligned}\sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}} &= \sum_{\substack{d\leq 2N\\d|D}}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}} + \sum_{\substack{d>2N\\d|D}}\mu(d)\frac{N}{d} \leq \sum_{\substack{d\leq 2N\\d|D,\ \mu(d)=1}}\frac{d}{4N} + \sum_{\substack{d>2N\\d|D,\ \mu(d)=1}}\frac{N}{d}\\ &\leq \sum_{\substack{d\leq 2N\\d|D,\ \mu(d)=1}}\frac{1}{2} + \sum_{\substack{d>2N\\d|D,\ \mu(d)=1}}\frac{1}{2} = \sum_{\substack{d|D\\\mu(d)=1}}\frac{1}{2} = 2^{(\omega(D)-2)}. \quad (3.7)\end{aligned}$$

Combining (3.6) and (3.7) we get the lemma.

□

The previous lemma has $2^{\omega(D)}$ in its error term, therefore it is useful to have

explicit bounds on $2^{\omega(D)}$. We find such estimates in the following lemma.

Lemma 3.3. *Let D be a positive integer. Then $2^{\omega(D)} < 4.8618\, D^{1/4}$. If $D > 7.43 \times 10^{12}$ then $2^{\omega(D)} < 2.4817\, D^{1/4}$. If $D > 3.05 \times 10^{14}$, then $2^{\omega(D)} < 1.9615\, D^{1/4}$. If $D > 1.31 \times 10^{16}$ then $2^{\omega(D)} < 1.532\, D^{1/4}$. Finally, if $D > 3.26 \times 10^{19}$, then $2^{\omega(D)} < D^{1/4}$.*

Proof. Since 2^{ω} is multiplicative, we have

$$\frac{2^{\omega(D)}}{D^{1/4}} = \prod_{p|D} \frac{2}{p^{1/4}}.$$

Since 13 is the last prime p with $p^{\frac{1}{4}} < 2$, then

$$\prod_{p|D} \frac{2}{p^{1/4}} \leq \prod_{p \leq 13} \frac{2}{p^{1/4}} \leq 4.8618.$$

Let p_i be the i-th prime. Let $k \geq 6$ be an integer. Assume that

$$D \geq M(k) := \prod_{i=1}^{k} p_i.$$

We will show that

$$\frac{2^{\omega(D)}}{D^{1/4}} \leq \prod_{i=1}^{k} \frac{2}{p_i} := F(k). \tag{3.8}$$

This will yield the lemma, since $7.43 \times 10^{12} > M(12)$ and $F(12) > 2.4817$. The other claims in the lemma coming from using $k = 13$, $k = 14$ and $k = 16$, respectively.

Let's prove (3.8). We will do it in two cases, when $\omega(D) \leq k$ and when $\omega(D) > k$. In the first case, we have

$$\frac{2^{\omega(D)}}{D^{1/4}} \leq \frac{2^k}{M(k)^{1/4}} = F(k).$$

In the second case we have $\omega(D) > k$. Let $\omega(D) = r$. Since $M(r)$ is the smallest number with r distinct prime factors, we have that $D \geq M(r)$. Therefore

$$\frac{2^{\omega(D)}}{D^{1/4}} \leq \frac{2^{\omega(M(r))}}{M(r)^{1/4}} = \left(\prod_{i=1}^{k} \frac{2}{p_i^{1/4}}\right)\left(\prod_{i=k+1}^{r} \frac{2}{p_i^{1/4}}\right) \leq \left(\prod_{i=1}^{k} \frac{2}{p_i^{1/4}}\right).$$

The last inequality is true since $p_7^{1/4} > 2$, and $k + i \geq 7$ for $i = 1, 2, \ldots, r - k$. □

The proof of the main theorem also requires explicit estimates for the sum of primes. The following lemma (which is also of independent interest), gives lower and upper bounds on the sum of primes up to x.

Lemma 3.4. *For x a positive real number. If $x \geq a$ then there exist c_1 and c_2 depending on a such that*

$$\frac{x^2}{2\log x} + \frac{c_1 x^2}{\log^2 x} \leq \sum_{p \leq x} p \leq \frac{x^2}{2\log x} + \frac{c_2 x^2}{\log^2 x}.$$

The following table gives us c_1 and c_2 for various values of a:

a	c_1	c_2
315437	0.205448	0.330479
468577	0.211358	0.325931
486377	0.212903	0.325538
644123	0.214289	0.322610
678407	0.214930	0.322327
758231	0.215540	0.321505
758711	0.215938	0.321490
10544111	0.239817	0.292511

Table 3.1: Bounds for the sum of primes.

Proof. To estimate the sum, we will use the very good estimates of $\theta(x)$ which can be found in Schoenfeld [40] and for the largest a we use an estimate of Dusart [11]. Let $x \geq a$, now let k_1 and k_2 satisfy

$$x - k_2 \frac{x}{\log x} \leq \theta(x) \leq x + k_1 \frac{x}{\log x}.$$

Table 3.2 has the values of k_1 and k_2 for different a and it also has a column for a constant C which will pop up later in the proof.

For $x \geq a$	$\theta(x) \leq x + k_1 \frac{x}{\log x}$	$\theta(x) \geq x - k_2 \frac{x}{\log x}$	$\int_a^x \frac{t}{\log^3 t}\, dt \leq C \frac{x^2}{\log^2 x}$
a	k_1	k_2	C
315437	0.0201384	1/29	0.0371582
468577	0.0201384	1/35	0.0360657
486377	0.0201384	1/37	0.0359661
644123	0.0201384	1/39	0.0352334
678407	0.0201384	1/40	0.0351014
758231	0.0201384	1/41	0.0348216
758711	0.0201384	0.0239922	0.0348201
10544111	0.006788	0.006788	0.0293063

Table 3.2: Bounds for $\theta(x)$.

Now, let's work with the sum of primes using partial summation:

$$\sum_{p \leq x} p = \sum_{p \leq x} \log p \frac{p}{\log p} = \theta(x) \frac{x}{\log x} - \int_2^x \theta(t) \left(\frac{1}{\log t} - \frac{1}{\log^2 t} \right) dt.$$

Then we can expand and get

$$\begin{aligned} \sum_{p \leq x} p &= \frac{\theta(x)x}{\log x} - \int_2^x \frac{\theta(t)}{\log t}\, dt + \int_2^x \frac{\theta(t)}{\log^2 t}\, dt \\ &= \frac{\theta(x)x}{\log x} - \int_2^a \frac{\theta(t)}{\log t}\, dt + \int_2^a \frac{\theta(t)}{\log^2 t}\, dt - \int_a^x \frac{\theta(t)}{\log t}\, dt + \int_a^x \frac{\theta(t)}{\log^2 t}\, dt. \quad (3.9) \end{aligned}$$

Now using this equation, we will work out an upper bound and then a lower bound. Let's proceed with the upper bound.

First we have for $x \geq a$

$$\frac{\theta(x)x}{\log x} \leq \frac{x^2}{\log x} + \frac{k_1 x^2}{\log^2 x}. \tag{3.10}$$

Then we have

$$-\int_a^x \frac{\theta(t)}{\log t}\,dt \leq -\int_a^x \frac{t - \frac{k_2 t}{\log t}}{\log t}\,dt = -\int_a^x \frac{t}{\log t}\,dt + k_2 \int_a^x \frac{t}{\log^2 t}\,dt. \tag{3.11}$$

We also have

$$\int_a^x \frac{\theta(t)}{\log^2 t}\,dt \leq \int_a^x \frac{t}{\log^2 t}\,dt + k_1 \int_a^x \frac{t}{\log^3 t}\,dt. \tag{3.12}$$

By using partial integration we get

$$\int_a^x \frac{t}{\log t}\,dt = \frac{x^2}{2\log x} - \frac{a^2}{2\log a} + \int_a^x \frac{t}{2\log^2 t}\,dt, \tag{3.13}$$

and

$$\int_a^x \frac{t}{\log^2 t}\,dt = \frac{x^2}{2\log^2 x} - \frac{a^2}{2\log^2 a} + \int_a^x \frac{t}{\log^3 t}\,dt. \tag{3.14}$$

Using (3.10), (3.11) and (3.12) on (3.9) yields

$$\sum_{p \leq x} p \leq \frac{x^2}{\log x} + \frac{k_1 x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \int_a^x \frac{t}{\log t}\,dt + (1 + k_2)\int_a^x \frac{t}{\log^2 t}\,dt + k_1 \int_a^x \frac{t}{\log^3 t}\,dt.$$

Now, using (3.13) we get

$$\sum_{p\le x} p \le \frac{x^2}{\log x} + \frac{k_1 x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \frac{x^2}{2\log x} + \frac{a^2}{2\log a} - \int_a^x \frac{t}{2\log^2 t}\,dt + (1+k_2)\int_a^x \frac{t}{\log^2 t}\,dt + k_1\int_a^x \frac{t}{\log^3 t}\,dt.$$

By simplifying and then using (3.14) we get that the right hand side equals

$$\frac{x^2}{2\log x} + \frac{k_1 x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} + \left(\frac{1}{2}+k_2\right)\left(\frac{x^2}{2\log^2 x} - \frac{a^2}{2\log^2 a} + \int_a^x \frac{t}{\log^3 t}\,dt\right) + k_1\int_a^x \frac{t}{\log^3 t}\,dt.$$

By rearranging further we get that this equals

$$\frac{x^2}{2\log x} + \left(\frac{1}{4}+k_1+\frac{k_2}{2}\right)\frac{x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2}+k_2\right)\frac{a^2}{2\log^2 a} + \left(\frac{1}{2}+k_1+k_2\right)\int_a^x \frac{t}{\log^3 t}\,dt.$$

Now, $\int_2^a \frac{\theta(t)}{\log t}\,dt$, $\int_2^a \frac{\theta(t)}{\log^2 t}\,dt$ and $\int_2^a \frac{t}{\log^3 t}\,dt$ are constant. Also, $\int_a^x \frac{t}{\log^3 t}\,dt = o\left(x^2/(\log^2 x)\right)$ and hence, we can then find a constant C (see Table 3.2) such that

$$\frac{\int_a^x \frac{t}{\log^3 t}\,dt}{\frac{x^2}{\log^2 x}} \le C.$$

Therefore, for $x \ge a$, we have

$$\sum_{p\le x} p \le \frac{x^2}{2\log x} + \left(\frac{1}{4}+k_1+\frac{k_2}{2}+\left(\frac{1}{2}+k_1+k_2\right)C + A\right)\frac{x^2}{\log^2 x},$$

where

$$A = \max\left\{0, \frac{\int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \int_2^a \frac{\theta(t)}{\log t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2}+k_2\right)\frac{a^2}{2\log^2 a}}{\frac{a^2}{\log^2 a}}\right\}.$$

We can now plug it into a calculator and get the third column in Table 3.1. This completes our work for the upper bound.

It is time to work on the lower bound. We proceed in the same way. In fact, every time a k_1 appears in the previous inequalities, it may be replaced by $-k_2$ and viceversa. One would also replace the $\leq$ symbol with $\geq$. After doing this, we reach the following inequality:

$$\sum_{p\leq x} p \geq \frac{x^2}{2\log x} + \left(\frac{1}{4} - k_2 - \frac{k_1}{2}\right)\frac{x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{4} - \frac{k_1}{2}\right)\frac{a^2}{\log^2 a} + \left(\frac{1}{2} - k_1 - k_2\right)\int_a^x \frac{t}{\log^3 t}\,dt.$$

Working with the constant in the lower bound is a bit trickier than in the upper bound because we have to consider whether $\left(\frac{1}{2} - k_1 - k_2\right)$ is positive or negative. In the case it is negative, we replace the integral with C, in the case it is positive we replace it with 0. Note that the expression is positive when $x \geq 599$ and it is negative when $x < 599$.

Therefore, we have two cases, for $x \geq a$ with $a < 599$ we have

$$\sum_{p\leq x} p \leq \frac{x^2}{2\log x} + \left(\frac{1}{4} - k_2 - \frac{k_1}{2} + \left(\frac{1}{2} - k_1 - k_2\right)C + A\right)\frac{x^2}{\log^2 x},$$

and for $a \geq 599$ we have

$$\sum_{p\leq x} p \leq \frac{x^2}{2\log x} + \left(\frac{1}{4} - k_2 - \frac{k_1}{2} + A\right)\frac{x^2}{\log^2 x},$$

where

$$A = \min\left\{0, \frac{\int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \int_2^a \frac{\theta(t)}{\log t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2} - k_1\right)\frac{a^2}{2\log^2 a}}{\frac{a^2}{\log^2 a}}\right\}.$$

After plugging the numbers in the calculator we get the desired results, completing the lemma. □

Corollary 3.1. *For x, y real numbers such that $x > y$. For $y \geq a$, there exist c_1 and c_2 depending on a such that*

$$\frac{1}{2}\left(\frac{x^2}{\log x} - \frac{y^2}{\log y}\right) + \frac{c_1 x^2}{\log^2 x} - \frac{c_2 y^2}{\log^2 y} \leq \sum_{y<p\leq x} p \leq \frac{1}{2}\left(\frac{x^2}{\log x} - \frac{y^2}{\log y}\right) + \frac{c_2 x^2}{\log^2 x} - \frac{c_1 y^2}{\log^2 y}.$$

The values of c_1 and c_2 can be found in the table for Lemma 3.4.

Proof. It easily follows from the lemma once we write $\sum_{y<p\leq x} p = \sum_{p\leq x} p - \sum_{p\leq y} p$. □

Using the estimates on the sum of primes, we can then use these to estimate the sum which comes up in the proof of the main theorem. We do this in the following lemma.

Lemma 3.5. *Let $B \geq 315487$ and N be positive real numbers. For $n \leq \frac{2N}{B}$ a natural number we have the following inequality:*

$$\sum_{B<p\leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{n\log B}.$$

Proof. If $n \leq \frac{N}{B}$ then

$$\sum_{B<p\leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{B<p\leq \frac{N}{n}} \frac{np}{N} + \sum_{\frac{N}{n}<p\leq \frac{2N}{n}} \left(2 - \frac{np}{N}\right), \tag{3.15}$$

and if $n > \frac{N}{B}$ then

$$\sum_{B<p\leq\frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{B<p\leq\frac{2N}{n}} \left(2 - \frac{np}{N}\right) \leq \sum_{\frac{N}{n}<p\leq\frac{2N}{n}} \left(2 - \frac{np}{N}\right). \tag{3.16}$$

Since both sums require the bounding of $\sum_{\frac{N}{n}<p\leq\frac{2N}{n}} \left(2 - \frac{np}{N}\right)$, we'll estimate this first.

Dusart [11, Theorem 14, p.22] proved that for $x > 1$, $\pi(2x) - \pi(x) \leq \frac{x}{\log x}$. Combining that with Corollary 3.1 yields

$$\begin{aligned}
\sum_{\frac{N}{n}<p\leq\frac{2N}{n}} \left(2 - \frac{np}{N}\right) &= 2\left(\pi\left(\frac{2N}{n}\right) - \pi\left(\frac{N}{n}\right)\right) - \frac{n}{N}\sum_{\frac{N}{n}<p\leq\frac{2N}{n}} p \\
&\leq \frac{2N}{n\log\frac{N}{n}} - \frac{n}{N}\left(\frac{2N^2}{n^2\log\left(\frac{2N}{n}\right)} - \frac{N^2}{2n^2\log\left(\frac{N}{n}\right)} + \frac{4c_1N^2}{n^2\log^2\left(\frac{2N}{n}\right)} - \frac{c_2N^2}{n^2\log^2\left(\frac{N}{n}\right)}\right) \\
&= \frac{2N}{n\log\left(\frac{N}{n}\right)} - \frac{2N}{n\log\left(\frac{2N}{n}\right)} + \frac{N}{2n\log\left(\frac{N}{n}\right)} - \frac{4c_1N}{n\log^2\left(\frac{2N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)},
\end{aligned} \tag{3.17}$$

where c_1 and c_2 come from Table 3.1 in Lemma 3.4. Since

$$\frac{2N}{n\log\left(\frac{N}{n}\right)} - \frac{2N}{n\log\left(\frac{2N}{n}\right)} = \frac{(\log 4)N}{n\log\left(\frac{N}{n}\right)\log\left(\frac{2N}{n}\right)},$$

then (3.17) becomes

$$\frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{(\log 4)N}{n\log\left(\frac{N}{n}\right)\log\left(\frac{2N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)} - \frac{4c_1N}{n\log^2\left(\frac{2N}{n}\right)},$$

which equals

$$\frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)} f(N,n), \tag{3.18}$$

where

$$f(N,n) = c_2 + (\log 4)\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right) - 4c_1\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right)^2.$$

Since $\log x/\log 2x$ is an increasing function for $x > 0$ and $\frac{\log x}{\log 2x} < 1$, then we can bound $f(N,n)$ by replacing the fraction with 1 in the positive term and by picking the smallest possible value of $\frac{N}{n}$ in the negative part. Since $n \leq \frac{2N}{B}$, then we have that $\frac{N}{n} \geq \frac{B}{2}$. Therefore

$$f(N,n) \leq c_2 + \log 4 - 4c_1\left(\frac{\log\left(\frac{B}{2}\right)}{\log B}\right)^2.$$

Using Lemma 3.4, for $B \geq 315487$, we have $c_1 = 0.205448$ and $c_2 = .330479$ and together with $\frac{N}{n} \geq \frac{B}{2}$ we get that $f(N,n) \leq 1$ yielding

$$\sum_{\frac{N}{n} < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}. \tag{3.19}$$

To complete the estimate we care about, we must now bound $\frac{n}{N}\sum_{B < p \leq \frac{N}{n}} p$. We can do this by using Corollary 3.1:

$$\begin{aligned}\frac{n}{N}\sum_{B < p \leq \frac{N}{n}} p &\leq \frac{n}{N}\left(\frac{N^2}{2n^2\log\left(\frac{N}{n}\right)} - \frac{B^2}{2\log B} + \frac{c_2N^2}{n^2\log^2\left(\frac{N}{n}\right)} - \frac{c_1B^2}{\log^2 B}\right) \\ &= \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1nB^2}{N\log^2 B} - \frac{nB^2}{2N\log B}. \end{aligned} \tag{3.20}$$

Now, for $n \leq \frac{N}{B}$, by (3.15) and using the estimates of (3.19) and (3.20) we have

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{n\log\left(\frac{N}{n}\right)} + \frac{(1+c_2)N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1nB^2}{N\log^2 B} - \frac{nB^2}{2N\log B}.$$

We want to prove this is $\leq \frac{N}{n \log B}$. We note that $\frac{N}{n \log B} - \frac{N}{n \log\left(\frac{N}{n}\right)} = \frac{N \log\left(\frac{N}{nB}\right)}{n \log B \log\left(\frac{N}{n}\right)}$, so what we want is

$$\frac{N \log\left(\frac{N}{nB}\right)}{n \log B \log\left(\frac{N}{n}\right)} + \frac{c_1 n B^2}{N \log^2 B} + \frac{nB^2}{2N \log B} \geq \frac{(1+c_2)N}{n \log^2\left(\frac{N}{n}\right)}.$$

After making the substition of $\frac{N}{n} = Bk$ we have that we want

$$\frac{Bk \log k}{\log B \log Bk} + \frac{c_1 B}{k \log^2 B} + \frac{B}{2k \log B} \geq \frac{(1+c_2)Bk}{\log^2 Bk}.$$

We can divide the whole inequality by B and multiply by $\log^2 Bk$, so we get

$$k \log k \frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k \log B} \geq (1+c_2)k.$$

For $k \geq 4$, using that for $B \geq 315487$, $c_2 = 0.330479$ we have

$$k \log k \frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k \log B} \geq k \log k \geq (1+c_2)k.$$

And for $1 \leq k < 4$ using that $B \geq 315487$ we have

$$k \log k \frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k \log B} \geq k \log k + \frac{c_1}{k} + \frac{\log 315487}{2k} \geq (1+c_2)k.$$

This completes the proof of the lemma when $n \leq \frac{N}{B}$.

For $n > \frac{N}{B}$, using (3.16) and (3.19) we have

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{2n \log\left(\frac{N}{n}\right)} + \frac{N}{n \log^2\left(\frac{N}{n}\right)}.$$

Now using that $\frac{N}{B} < n \leq \frac{2N}{B}$ we have that $\frac{B}{2} \leq \frac{N}{n} \leq B$. Using this we have

$$\frac{N}{n \log B} - \frac{N}{2n \log\left(\frac{N}{n}\right)} = \frac{N \log\left(\frac{N^2}{n^2 B}\right)}{2n \log B \log\left(\frac{N}{n}\right)} \geq \frac{N \log\left(\frac{B}{4}\right)}{2n \log B \log B}. \tag{3.21}$$

and

$$\frac{N}{n \log^2\left(\frac{N}{n}\right)} \leq \frac{N}{n \log^2\left(\frac{B}{2}\right)} \tag{3.22}$$

For $B \geq 73$ we have $\log(B/4) \log^2(B/2) \geq 2 \log^2 B$ and hence from combining the inequalities (3.21) and (3.22) we get

$$\frac{N}{n \log B} - \frac{N}{2n \log\left(\frac{N}{n}\right)} \geq \frac{N}{n \log^2\left(\frac{N}{n}\right)},$$

completing the proof that for $n > \frac{N}{B}$

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{n \log B}.$$

□

During the proof of the main theorem, one of the problems that arises comes from bounding

$$\frac{D}{\phi(D)} \sum_{\substack{n \leq x \\ (n,D)=1}} \frac{1}{n}.$$

The difficulty is that when D has many prime factors $\frac{D}{\phi(D)}$ is big while the other factor is small. And if D has few prime factors we have the opposite situation. The following lemma allows us to simplify this situation by showing that we can reduce it to considering D having many small prime factors.

Lemma 3.6. *Let $M = \prod_{p \le x} p$. For a positive integer D, let k be the positive integer that satisfies that $(D, M) = M/k$. Then*

$$\sum_{\substack{n \le x \\ (n,D)=1}} \frac{1}{n} \le \frac{k}{\phi(k)}.$$

Proof. Note that if $n \le x$ and $(n, D) = 1$ then any prime p that divides n also divides k. Therefore

$$\sum_{\substack{n \le x \\ (n,D)=1}} \frac{1}{n} \le \prod_{p|k} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \prod_{p|k} \frac{p}{p-1} = \prod_{p|k} \frac{p}{\phi(p)} = \frac{k}{\phi(k)}.$$

□

The following lemma combines Lemmas 3.5 and 3.6 to give us the result we need in the proof of the main theorem.

Lemma 3.7. *For B and N positive real numbers and D a positive integer. Let $M = \prod_{p \le \frac{2N}{B}} p$ and k be a positive integer such that $(D, M) = \frac{M}{k}$. Then, we have*

$$\sum_{B < p \le 2N} \sum_{\substack{n \le \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \le \frac{k}{\phi(k)} \frac{N}{\log B}.$$

Proof. Exchanging order of summation we get:

$$\sum_{B < p \le 2N} \sum_{\substack{n \le \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{\substack{n \le \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

The inner sum can be dealt with using Lemma 3.5 and then we will use

Lemma 3.6 for the outer sum:

$$\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right) \leq \sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \frac{N}{n\log B} \leq \frac{k}{\phi(k)}\frac{N}{\log B}.$$

□

Finally, we end the section with an explicit estimate concerning the ratio $\frac{D}{\phi(D)}$ that will be needed in the proof of the main theorem.

Lemma 3.8. *For D a positive integer greater than $6\cdot 10^{12}$ we have*

$$\frac{D}{\phi(D)} < 2\log\log D.$$

Proof. Rosser and Schoenfeld [38] proved that for $D > 223092870$ the following inequality is true:

$$\frac{D}{\phi(D)} \leq e^{\gamma}\log\log D + \frac{2.5}{\log\log D}.$$

Therefore, $D/\phi(D) \leq 2\log\log D$ for $D > 6\cdot 10^{12}$. □

3.3 Proof of the theorem when $D > 10^{24}$

Theorem 3.4. *For D a fundamental discriminant larger than 10^{24} there exists a prime $p \leq D^{0.45}$ such that $\left(\frac{D}{p}\right) = -1$*

Proof. Assume to the contrary that no such p exists. Let $\chi(p) = \left(\frac{D}{p}\right)$. Since D is a fundamental discriminant, χ is a primitive character mod D.

3.3 Proof of the theorem when $D > 10^{24}$

Consider

$$S_\chi(N) = \sum_{n \le 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right).$$

By Theorem 3.3, we have

$$|S_\chi(N)| \le \frac{\phi(D)}{D}\sqrt{D} + 2^{(\omega(D)-1)}\frac{N}{\sqrt{D}}. \tag{3.23}$$

However, using our assumption that $\chi(p) \neq -1$ for $p \le D^{0.45} = B$ we can calculate $S_\chi(N)$ by separating the sum into $\chi(n) = 1, 0$ and -1. To account for $\chi(n) = 0$ we sum over the numbers relatively prime to D. The following is true when $B^2 > 2N$:

$$S_\chi(N) = \sum_{\substack{n \le 2N \\ (n,D)=1}} \left(1 - \left|\frac{n}{N} - 1\right|\right) - 2 \sum_{\substack{B < p \le 2N \\ \chi(p) = -1}} \sum_{\substack{n \le \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right). \tag{3.24}$$

Using Lemma 3.2 and (3.23), (3.24) we get

$$\frac{\phi(D)}{D}\sqrt{D} + 2^{(\omega(D)-1)}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N - 2^{(\omega(D)-2)} - 2 \sum_{\substack{n \le \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right). \tag{3.25}$$

Now, letting $N = c\sqrt{D}$ for some constant c we get that the inequality in (3.25) is equivalent to

$$0 \ge c - 1 - 2^{\omega(D)}\left(\frac{c}{2} + \frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}}\frac{D}{\phi(D)} \sum_{\substack{n \le \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \tag{3.26}$$

Now, using Lemma 3.7 we get that if $M = \prod_{p \leq \frac{2N}{B}} p$ and $(D, M) = \frac{M}{k}$ then

$$\sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{\log B} \frac{k}{\phi(k)} = \frac{c\sqrt{D}}{\log B} \frac{k}{\phi(k)}.$$

Therefore (3.26) becomes

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2c}{\log B} \frac{D}{\phi(D)} \frac{k}{\phi(k)} \tag{3.27}$$

Now, since

$$\frac{D}{\phi(D)} \frac{k}{\phi(k)} = \prod_{p \leq \frac{2N}{B}} \frac{p}{p-1} \times \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1} \leq e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1},$$

then (3.27) becomes

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2c}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1}. \tag{3.28}$$

Now, let's pick $c = 8$. Now, D has at most 19 primes bigger than $\frac{2N}{B} = 16D^{0.05}$ dividing it. We have that $\frac{2N}{B} > 253$ and the product of $\frac{p}{p-1}$ for the first 19 primes bigger than 253 is smaller than 1.0642. We also have that for $D > 3.26 \times 10^{19}$, $2^{\omega(D)} < D^{1/4}$. Also, for $D > 10^{13}$ we have $\frac{D}{\phi(D)} < 2 \log\log D$ (Lemma 3.8). Combining these facts with (3.28) we get the inequality:

$$0 \geq 7 - 8.5 \frac{\log\log D}{D^{1/4}} - \frac{16}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) 1.0642. \tag{3.29}$$

If we let $B = D^{.45}$, then $\frac{2N}{B} = 16D^{.05}$ and the right hand side of (3.29) is $0.028836\ldots$ at $D = 10^{24}$. Since as D increases, the right hand side increases and at $D = 10^{24}$ it is already positive, we have arrived at a contradiction for all $D \geq 10^{24}$.

□

Remark 3.2. This proof with a few modifications would yield that for D a fundamental discriminant larger than 10^{16}, there exists a prime $p \leq \sqrt{D}/2$ such that $\left(\frac{D}{p}\right) = -1$. This gives us a proof of Theorem 3.1 without the need of the hybrid case.

3.4 Proof the theorem when $D \leq 10^{24}$

Theorem 3.5. *For D a fundamental discriminant such that $1596 < D \leq 10^{24}$, there exists a prime p such that $p < D^{0.45}$ and $\left(\frac{D}{p}\right) = -1$.*

Proof. Assume to the contrary that no such p exists. Following the same steps as in the proof for the infinite case we reach (3.26):

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}} \frac{D}{\phi(D)} \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right)$$

From the proof of Lemma 3.5 we can get tighter inequalities for the inner sum in the double sum above. If we combine (3.18) and (3.20) we get:

For $n \leq \frac{N}{B}$

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{n \log\left(\frac{N}{n}\right)} + \frac{(f(N,n) + c_2)N}{n \log^2\left(\frac{N}{n}\right)} - \frac{c_1 n B^2}{N \log^2 B} - \frac{nB^2}{2N \log B} = g_1(N, n, B, c_1, c_2),$$

where c_1 and c_2 come from Table 3.1 in Lemma 3.4 and

$$f(N,n) = c_2 + (\log 4)\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right) - 4c_1\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right)^2. \tag{3.30}$$

Now, for $n > \frac{N}{B}$, using (3.18) we get

$$\sum_{B<p\leq\frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)} f(N,n) = g_2(N,n,B,c_1,c_2).$$

Something that will be important later on in the proof is that $f(N,n)$ is decreasing whenever $n < N/6.09$, therefore let's prove it now:

Claim 3.1. *For a fixed integer n, if we let $c_1 = 0.239818$, then for $N > 6.09n$, $f(N,n)$ is a decreasing function.*

Proof of the Claim: First note that if we let $x = \frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}$, then $f(N,n) = c_2 + (\log 4)x - 4c_1x^2$. We note that the maximum occurs when $x_0 = \frac{\log 4}{8c_1} = 0.722576\ldots$. For $N > 6.09n$ we have $x > x_0$ because x increases as N increases. Since $f(N,n)$ is decreasing once $x > x_0$, then as N grows, $f(N,n)$ decreases.

Now, let $c = 7.8$, $c_1 = 0.239818$ and $c_2 = 0.29251$. Notice that $N = c\sqrt{D}$ depends only on D and $B = D^{0.45}$ also depends only on D. Now define

$$g(n,D) = \frac{1}{\sqrt{D}} \begin{cases} g_1(N,n,B,c_1,c_2) & : \quad n \leq \frac{N}{B}; \\ g_2(N,n,B,c_1,c_2) & : \quad n > \frac{N}{B}. \end{cases}$$

Therefore for $B \geq 10544111$, (3.26) becomes

$$0 \geq 7.8 - 1 - 2^{\omega(D)}\,(4.15)\,\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n \leq (15.6)D^{1/20} \\ (n,D)=1}} g(n,D). \tag{3.31}$$

Now, let $M = \prod_{p \leq 41} p$ and let $m = \gcd(D, M)$. Note that since m is squarefree and 41 is the 13th prime, then there are 2^{13} possible values of m. Now, let's define a function $A(D, m, \omega, u)$ in the following way

$$A(D,m,\omega,u) = 6.8 - 2^{\omega}\,(4.15)\,\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n \leq u \\ (n,m)=1}} g(n,D).$$

Claim 3.2. *Let m be a fixed positive integer. Let U be a fixed real number. Let $M = \prod_{p \leq 41} p$. Let $D \leq U$ be a positive integer such that $(D, M) = m$. Now let $u = \lfloor (15.6)U^{1/20} \rfloor$. Let ω be the maximum number of distinct primes a number below U can have. If $D \geq 4.05 \times 10^{15}$ then $0 \geq A(D, m, \omega, u)$.*

Proof of the Claim: Let $D \leq U$. We have $\omega(D) \leq \omega$. We also have $u \geq \lfloor (15.6)D^{1/20} \rfloor$. Now, $D \geq 4.05 \times 10^{15} > 10544111^{1/0.45}$, therefore $B > 10544111$ and hence we have (3.31). Since $m \mid D$, if $(n, D) = 1$ then $(n, m) = 1$. Also note that $g(n, D) \geq 0$. Combining this with (3.31) we have

$$\begin{aligned} 0 \geq 6.8 - 2^{\omega(D)}(4.15)\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n \leq (15.6)D^{1/20} \\ (n,D)=1}} g(n,D) \\ \geq 6.8 - 2^{\omega}(4.15)\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n \leq u \\ (n,m)=1}} g(n,D) = A(D,m,\omega,u). \end{aligned}$$

For example, when $D \leq 10^{24}$, we would have $U = 10^{24}$. Since any $D \leq 10^{24}$ has at most 18 distinct prime factors, $\omega = 18$. Now, $u = \lfloor (15.6)D^{1/20} \rfloor = \lfloor 247.243 \rfloor = 247$. Once we fix an m, we get that if $D \geq 4.05 \times 10^{15}$ then $0 \geq A(D, m, 18, 247)$.

Therefore to reach a contradiction we must find values of D for which $A(D, m, 18, 247) > 0$.

Once U and m are fixed, it seems that $A(D, m, \omega, u)$ is increasing with D. The only cause for uncertainty comes from the factor $\frac{D}{\phi(D)}$ and from $g(n, D)$. Let's deal with this. Let p_i be the i-th prime. Note $p_{13} = 41$. Since we want to maximize $\frac{D}{\phi(D)}$ (to make $A(D, m, \omega, u)$ as small as possible), then we do is consider the product of the smallest primes bigger than 41 and consider $D_v(m) = m \times \prod_{13<i\leq v} p_i$. Since we also have to deal with $g(n, D)$, what we will do is make it as big as possible in a range. Let's analyze the value of $g(n, D)$:

If $n \leq \frac{N}{B}$, then

$$\begin{aligned} g(n, D) &= \frac{1}{\sqrt{D}} \left(\frac{N}{n \log\left(\frac{N}{n}\right)} + \frac{(f(N, n) + c_2)N}{n \log^2\left(\frac{N}{n}\right)} - \frac{c_1 n B^2}{N \log^2 B} - \frac{nB^2}{2N \log B} \right) \\ &= \frac{c}{n \log\left(\frac{c\sqrt{D}}{n}\right)} + \frac{(f(N, n) + c_2)c}{n \log^2\left(\frac{c\sqrt{D}}{n}\right)} - \frac{c_1 n}{cD^{1/10} \log^2\left(D^{.45}\right)} - \frac{n}{2cD^{1/10} \log\left(D^{.45}\right)} \\ &= H_1(n, D) - H_2(n, D), \end{aligned}$$

where $H_1(n, D)$ consists of the two positive terms and $H_2(n, D)$ consists of the two terms being substracted. Now, $f(N, n)$ is decreasing for $N > 6.09n$. Since $n \leq u = 247$ we have that $N > 6.09n$. Therefore $f(N, n)$ is decreasing, showing that $H_1(n, D)$ is decreasing. $H_2(n, D)$ is also a decreasing function, making $-H_2(n, D)$ an increasing function.

Now, for $n > \frac{N}{B}$, we have

$$g(n,D) = \frac{1}{\sqrt{D}}\left(\frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}f(N,n)\right)$$
$$= \frac{c}{2n\log\left(\frac{c\sqrt{D}}{n}\right)} + \frac{cf(N,n)}{n\log^2\left(\frac{c\sqrt{D}}{n}\right)} = H_3(n,D).$$

Again, because $f(N,n)$ is decreasing, the right hand side is decreasing.

All of this allows us to get the following claim:

Claim 3.3. *If D, D_1, D_2 are positive reals such that $D \in [D_1, D_2)$, then*

$$g(n,D) \leq G(n,D_1,D_2) := \begin{cases} H_1(n,D_1) - H_2(n,D_2) & n \leq cD_1^{0.05}; \\ H_3(n,D_1) & n > cD_2^{0.05}; \\ \max\left\{H_1(n,D_1) - H_2(n,D_2), H_3(n,D_1)\right\} & \text{otherwise.} \end{cases}$$

Proof of the Claim: If $n \leq cD_1^{0.05}$, then for any $D \in [D_1, D_2)$ we have $n \leq \frac{N}{B}$, therefore $g(n,D) = H_1(n,D) - H_2(n,D)$. But, since both H_1 and H_2 are decreasing functions, we have $g(n,D) \leq H_1(n,D_1) - H_2(n,D_2)$.

If $n > cD_2^{0.05}$, then for any $D \in [D_1, D_2)$ we have $n > \frac{N}{B}$, therefore $g(n,D) = H_3(n,D)$. Since H_3 is decreasing we have $g(n,D) \leq H_3(n,D_1)$.

For the few values of n such that $cD_1^{0.05} < n \leq cD_2^{0.05}$, we just take the maximum, so we have $g(n,D) \leq \max\left\{H_1(n,D_1) - H_2(n,D_2), H_3(n,D_1)\right\}$.

Now, let's define a function similar to A called A_2 so that we can take this into account.

$$A_2(D,m,\omega,u,D_1,D_2) = 6.8 - \frac{2^\omega\,(4.15)}{\sqrt{D_1}}\frac{D}{\phi(D)} - \frac{2D}{\phi(D)}\sum_{\substack{n\leq u \\ (n,m)=1}} G(n,D_1,D_2). \quad (3.32)$$

Claim 3.4. *Let D be a positive integer. Let m be defined the same way as in Claim 3.2. Let v be an integer ≥ 13 such that $D_v(m) \geq 4.05 \times 10^{15}$. Let D_1 and D_2 be real numbers such that $[D_1, D_2) \subseteq [D_v(m), D_{v+1}(m))$. Let $\omega = \omega(m) + v - 13$. Let $u = \lfloor (15.6) D_2^{0.05} \rfloor$. Then, if $D \in [D_1, D_2)$, we have $0 \geq A_2(D_v(m), m, \omega, u, D_1, D_2)$.*

Proof of the Claim: Since $m | D$ and $D < D_{v+1}(m)$ then $\omega(D) < \omega(m) + v + 1 - 13 \leq \omega(m) + v - 13 = \omega$. We also have

$$\frac{D}{\phi(D)} = \frac{m}{\phi(m)} \prod_{\substack{p > p_{13} \\ p | D}} \frac{p}{p-1} \leq \frac{m}{\phi(m)} \prod_{13 < i \leq v} \frac{p_i}{p_i - 1} = \frac{D_v(m)}{\phi(D_v(m))}.$$

From Claim 3.3, we have $g(n, D) \leq G(n, D_1, D_2)$. Also, from Claim 3.2 using $U = D_2$ and because $\omega(D) \leq \omega$, we have for $D \geq 4.05 \times 10^{15}$, the inequality $0 \geq A(D, m, \omega, u)$.

Therefore, we have

$$\begin{aligned} 0 \geq A(D, m, \omega, u) &= 6.8 - \frac{2^{\omega}(4.15)}{\sqrt{D}} \frac{D}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n \leq u \\ (n,m)=1}} g(n, D) \\ &\geq 6.8 - \frac{2^{\omega}(4.15)}{\sqrt{D_1}} \frac{D_v(m)}{\phi(D_v(m))} - \frac{2D_v(m)}{\phi(D_v(m))} \sum_{\substack{n \leq u \\ (n,m)=1}} G(n, D_1, D_2) \\ &= A_2(D_v(m), m, \omega, u, D_1, D_2). \end{aligned}$$

What this allows us to do is just check $A_2(D, m, \omega, u, D_1, D_2)$ for some numbers and cover a whole interval. Our implementation will run by checking $A_2(D_v(m), m, \omega, u, D_v(m), D_{v+1}(m))$, where $\omega = \omega(m) + v - 13$ and $u = \lfloor (15.6) D_{v+1}(m) \rfloor$. The process is then to find for each m the first v such that

$A_2(D_v(m), m, \omega, u, D_v(m), D_{v+1}(m)) > 0$ and
$A_2(D_{v+i}(m), m, \omega, u, D_{v+i}(m), D_{v+i+1}(m)) > 0$ for all positive integers i while $D_{v+i}(m) \leq 10^{24}$. We will denote this $D_v(m)$ by $K(m)$. Now, we find the maximum $K(m)$ among the 2^{13} possible m's. We denote this maximum by K and we note that for all $D \geq K$ with $D \leq 10^{24}$ we have $A(D, m, \omega, u) > 0$, giving us a contradiction, yielding the desired theorem for $D \geq K$.

Since the odd cases are easier than the even ones (because $D/\phi(D)$ is smaller when D is odd), we split the process in dealing with the odd D's first and then with the even D's. After running a loop that computes $K(m)$ for every odd m and finds the maximum value K, we find that $K = 21853026051351495 < 2.2 \times 10^{16}$. This implies that for all $D \geq 2.2 \times 10^{16}$, odd fundamental discriminants, the theorem is true. Since we had already dealt with the case $D \leq 2.6 \times 10^{17}$, this finishes the proof for odd D.

Now let's consider the case where D is even. In this case our goal is to prove it for all $D \geq 1.04 \times 10^{18}$, since we have computational tables proving the smaller D. Just as in the case for odd m, we run a loop that computes $K(m)$ for every even m and then find the maximum among this, which we call K. In this case, $K = 1707159924755154870 < 1.71 \times 10^{18}$. Note that K is slightly larger than our desired outcome since it doesn't lead us all the way down to 1.04×10^{18}. This forces us to work a little harder to reach the theorem.

To get rid of this new obstacle we use the fact that in Claim 3.4 we have more flexibility than we've been using. We need not have $D_1 = D_v(m)$ and $D_2 = D_{v+1}(m)$ as we have been using so far, we could pick values in between. First of all, I found all the m values that have $D(m, U) > 1.04 \times 10^{18}$. There are only twelve values of

m. By the nature of the process the twelve counterexamples are of the form $D_v(m)$. Seven of the examples have $v = 20$ and the other five have $v = 19$. Therefore what we can do is consider $D_1 = 32D_{v-1}(m)$ and $D_2 = D_v(m)$. After evaluating $A(D_v(m), m, \omega, u, D_1, D_2)$ for these twelve m's, we find that all of them are greater than zero. Finishing the proof for even values.

Combining the result for even and odd values yields the theorem. □

As an extra note, this naive algorithm runs in around 15 minutes on a Pentium(R) Dual-Core CPU E5300 @ 2.60GHz. The coding involved in this proof is in the appendix.

Remark 3.3. With the same techniques we can prove that for D a fundamental discriminant satisfying $D > 10^{24}$, there exists a prime p such that $p \leq D^{3/7}$ and the Kronecker symbol $(D/p) = -1$. Computations on pseudosquares (see [42] and [46]) suggest that sieving machines can check for the values below 10^{24} (such as MSSU computed the values under 10^{18}).

Chapter 4

The least k-th power non-residue

Let p be a prime and let k be an integer with $k \mid p-1$ and $k > 1$. Let $g(p,k)$ be the least k-th power non residue $\bmod p$. Karl Norton [31], 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 $g(p,k) \leq 4.7p^{1/4}\log p$.

Let h and w be any positive integers, 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

$$S_w(p,h,\chi,k) := \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w}. \tag{4.1}$$

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 [4] that deals with the quadratic case in the Burgess inequality, we improve the upper bound on (4.1); allowing us to improve the upper bound on $g(p,k)$.

In section 4.1 we will prove our upper bound on $S_w(p,h,\chi,k)$. In section 4.2 we will write down Norton's lower bound for (4.1) with some modifications. In the last section of this chapter we combine the upper bound from section 4.1 with the lower bound from section 4.2 to prove our main theorem.

Theorem 4.1. *Let $p>3$ be an odd prime. Let $k\geq 2$ be an integer such that $k \mid p-1$. Let $g(p,k)$ be the least k-th power non-residue* $\bmod p$. *Then*

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

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

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

A similar bound was announced but not proven by Norton (see [32]), namely that $g(p,k)\leq 1.1p^{1/4}(\log p+4)$.

4.1 Burgess–Booker upper bound

Definition 4.1. 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, and this is the key reason I treat the simpler-looking rational form. I was motivated to look at it this way by the exposition by Iwaniec and Kowalski (see [22]) of the Burgess inequality.

Definition 4.2. 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 4.1. 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 4.1. *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 4.2. 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 4.1. 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

$$\binom{w}{t}^2 t! h^t. \tag{4.2}$$

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, let's calculate the number of ways in which the remaining parts of the the numerator can be a k-th power. First notice that if $t \not\equiv w \pmod{k}$, then the remaining parts of the numerator cannot be a kth power. Therefore, we should assume $t \equiv w \bmod k$. Now, notice that we have h options for the first term. Now we must select the $k-1$ terms that join it to create the k-th power. There are $\binom{w-t-1}{k-1}$ ways of choosing this. Then we pick an element that hasn't been picked. This element has h choices. Now we pick its $k-1$ partners. We have $\binom{w-t-k-1}{k-1}$ ways of doing this. We keep going until we're finished. If we let $d = (w-t)/k$, then the number of ways is

$$\begin{aligned} h^d \binom{w-t-1}{k-1}\binom{w-t-k-1}{k-1}\cdots\binom{k-1}{k-1} &= \frac{(w-t)!}{(w-t)(w-t-k)\cdots(k)}\frac{h^d}{((k-1)!)^d} \\ &= \frac{(w-t)!}{k^d(1\cdot 2\cdots d)((k-1)!)^d}h^d = \frac{(w-t)!}{d!(k!)^d}h^d. \end{aligned} \tag{4.3}$$

Alternatively, we could have reached this formula by picking d groups of size k using the multinomial $\binom{w-t}{k,k,k,\ldots,k}$ and then dividing by $d!$ since the multinomial

associates an order to the groups being picked. Each group of size k has h options giving us the same count as in (4.3).

For the remaining parts of the denominator we would have the same estimate with h replaced by $h-1$ (since we already eliminated the common terms). Despite being able to replace it by $h-1$, I will consider it as h to simplify computations.

Combining (4.2) and (4.3) and summing over values of $t \equiv w \bmod k$ we arrive at the following upper bound for $b_w(p,h,k)$:

$$\sum_{\substack{0\le t\le w\\ t\equiv w \bmod k}} \left(\frac{(w-t)!}{d!(k!)^d}\right)^2 \binom{w}{t}^2 t!h^{t+2d} \quad = \quad \sum_{\substack{0\le t\le w\\ t\equiv w \bmod k}} \left(\frac{w!}{d!t!(k!)^d}\right)^2 t!h^{t+2d}. \quad (4.4)$$

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

□

Definition 4.3. 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 4.1 implies that $b_w(p,h,k) \le c_w(h,k)$.

Lemma 4.2. *Let w, h and k be positive integers such that $k \ge 2$. Let $c_w(h,k)$ be defined as in Definition 4.3. 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

$c_w(h,k) \leq c_w(h,k-1)$ for all $k \geq 3$. From Definition 4.3 we have

$$c_w(h,k) = \sum_{d=0}^{\lfloor \frac{w}{k} \rfloor} \left(\frac{w!}{d!(k!)^d} \right)^2 \frac{h^{w-(k-2)d}}{(w-kd)!}. \tag{4.5}$$

Now, we arrange the right hand side of (4.5) 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

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

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

The following corollary is an obvious consequence:

Corollary 4.1. *Let w, h and k be positive integers such that $k \geq 2$. Let $c_w(h,k)$ be defined as in Definition 4.3. 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 4.3. *Let w be a positive integer. Then*

$$\sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \frac{1}{(w-2d)!} \left(\frac{w!}{2^d d!} \right)^2 = \frac{(2w)!}{2^w w!}. \tag{4.6}$$

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 (4.6) was done in Lemma 4.1 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 4.2. *Let w be a positive integer. Then*

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

Proof. Multiply both sides of equation (4.6) 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

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

□

Theorem 4.2. *Let p be a prime. Let w, h and k be integers such that $w \leq 9h$, $h \leq p$, $k \geq 2$ and $k \mid p-1$. Let χ be a character $\pmod p$ of order k. Then*

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

Proof. Let $q(x)$ be defined as in Definition 4.1. 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:

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

If $q(x)$ is not a k-th power $\in \mathbb{F}_p(x)$ then using the Weil bound [39, 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 $(2w-1)\sqrt{p}$. When $q(x)$ is a k-th power, then we use the trivial bound for 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

$$S_w(p,h,\chi,k) \le (2w-1)h^{2w}\sqrt{p} + b_w(p,h,k)p \le (2w-1)h^{2w}\sqrt{p} + c_w(h,2)p. \quad (4.7)$$

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

$$c_w(h,2) = \sum_{d=0}^{\lfloor \frac{w}{2} \rfloor} \left(\frac{w!}{d!2^d} \right)^2 \frac{h^w}{(w-2d)!} = \frac{(2w)!}{2^w w!} h^w, \quad (4.8)$$

the last equality coming from Lemma 4.3.

Combining (4.7) and (4.8) we get the desired inequality.

□

Remark 4.1. From the proof we could derive a better upper bound when $k > 2$,

which is

$$S_w(p,h,\chi,k)=\sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w}<c_w(h,k)ph^w+(2w-1)p^{1/2}h^{2w}. \tag{4.9}$$

4.2 Burgess–Norton lower bound

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

Lemma 4.4. *Let $x\geq 1$ be a real number. Then*

$$x\sum_{q\leq x}\frac{\phi(q)}{q}-\sum_{q\leq x}\phi(q)\geq\frac{3}{\pi^2}x^2-x. \tag{4.10}$$

Proof. Let's estimate the sum.

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

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

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

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

$$x \sum_{q \le x} \frac{\phi(q)}{q} - \sum_{q \le x} \phi(q) \ge \frac{3}{\pi^2} x^2 - \frac{x^2}{2} \sum_{d>x} \frac{\mu(d)}{d^2} - \frac{x}{2} \sum_{d \le x} \frac{\mu(d)}{d} - \frac{1}{8} \sum_{\substack{d \le x \\ d \text{ squarefree}}} 1. \quad (4.11)$$

Claim 4.1. *For real $x \ge 1$,*

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

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

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

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 $x \ge 11$, proving the claim for real $x \ge 11$. To complete the proof for $x \ge 1$ we use the fact that $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$, which implies that $\sum_{d>x} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} - \sum_{d \le x} \frac{\mu(d)}{d}$. One can now manually check the integer cases where $1 \le x \le 11$ and note that $\left| \sum_{d>x} \frac{\mu(d)}{d^2} \right| < \frac{1}{x+1}$, which implies the claim for real $x \le 11$.

Claim 4.2. *For real $x \ge 1$, 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 4.3. *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 [19]. 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

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

Therefore,

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

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 4.1, 4.2 and 4.3 with (4.11) we have

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

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

For $x \leq 3$, the right hand side of (4.10) is negative, while the left hand side is positive, therefore the inequality is true for $x \leq 3$. Now, for the integers $3 \leq x \leq 21$

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 (4.10) is increasing for $x\ge 3$, we have a proof for all real $x\le 21$. □

Lemma 4.5. *Let $x\ge 1$ be a real number. Then*

$$2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q)\ge\frac{9}{\pi^2}x^2-x\left(\frac{\log x}{3}+3\right). \tag{4.12}$$

Proof. Doing the estimates the same way as in Lemma 4.5, we get

$$\begin{aligned}&2x\sum_{q\le x}\frac{\phi(q)}{q}-\sum_{q\le x}\phi(q)\\&=\frac{9}{\pi^2}x^2-\frac{3x^2}{2}\sum_{d>x}\frac{\mu(d)}{d}-\frac{x}{2}\sum_{d\le x}\frac{\mu(d)}{d}-x\sum_{d\le x}\frac{\mu(d)}{d}\left\{\frac{x}{d}\right\}+\frac{1}{2}\sum_{d\le x}\left\{\frac{x}{d}\right\}\left(1-\left\{\frac{x}{d}\right\}\right)\mu(d).\end{aligned} \tag{4.13}$$

Claim 4.4. *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

$$x\sum_{d\le x}\frac{\mu(d)}{d}\left\{\frac{x}{d}\right\}-\frac{1}{2}\sum_{d\le x}\left\{\frac{x}{d}\right\}\left(1-\left\{\frac{x}{d}\right\}\right)\mu(d)=\sum_{d\le x}\mu(d)\left\{\frac{x}{d}\right\}\left(\frac{x}{d}-\frac{1-\left\{\frac{x}{d}\right\}}{2}\right). \tag{4.14}$$

Note, that all factors except $\mu(d)$ are positive, which implies that we can bound (4.14)

by

$$\sum_{\substack{d\le x\\ \mu(d)=1}} \left\{\frac{x}{d}\right\}\left(\frac{x}{d}-\frac{1-\left\{\frac{x}{d}\right\}}{2}\right) \le x \sum_{\substack{d\le x\\ \mu(d)=1}} \frac{1}{d}. \tag{4.15}$$

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:

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

However,

$$\sum_{\substack{d\le x\\ d \text{ squarefree}}} \frac{1}{d} = \sum_{\substack{d\le x\\ \mu(d)=1}} \frac{1}{d} + \sum_{\substack{d\le x\\ \mu(d)=-1}} \frac{1}{d} \le \frac{2}{3}\log x + \frac{23}{15}, \tag{4.16}$$

and

$$\sum_{d\le x}\frac{\mu(d)}{d} = \sum_{\substack{d\le x\\ \mu(d)=1}} \frac{1}{d} - \sum_{\substack{d\le x\\ \mu(d)=-1}} \frac{1}{d} \le \frac{2}{3} + \frac{3}{x}. \tag{4.17}$$

The last inequality being true because of Claim 4.3. Adding (4.16) and (4.17), dividing by 2, and using (4.14) and (4.15) we get our claim.

Now, using the results of Claims 4.1, 4.3 and 4.4 in (4.13) 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 we get for $x \ge 45$.

For $x \le 3$, the right hand side of (4.12) 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 (4.12) is increasing for $x\ge 3$, we have a proof for all real $x\le 45$.

□

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

Theorem 4.3. *Let p be a prime. Let χ be a character $\pmod p$ of order k. Assume that $\chi(a)=1$ for all $1\le a<H$. Let h and w be positive integers such that $4\le h\le H$. Let $X=H/h$ and let $A=\frac{3}{\pi^2}$. Then*

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

Furthermore, if -1 is a k-th power, then

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

Proof. We follow the proof in [31] 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.

Claim 4.5. *If $\chi(a)=1$ for all $1\le a<H$, then $H<\sqrt{p}+1$.*

Proof of the Claim: We use an argument that was mentioned by Western and Miller (see [45]) and by Norton [31]. Assume that $H\ge\sqrt{p}+1$. Let $q=g(p,k)$. Note that

$q \geq H$. Let $r = \left\lceil \frac{p}{q} \right\rceil$. Note that $p < rq < p + q$, therefore rq is a k-th power $\bmod p$.

Since $q \geq \sqrt{p} + 1$, then

$$r = \left\lceil \frac{p}{q} \right\rceil \leq \left\lceil \frac{p}{\sqrt{p}+1} \right\rceil \leq \lceil \sqrt{p} \rceil < \sqrt{p} + 1 \leq q.$$

Therefore, $r < q$, which means r is a k-th power. Since r and rq are k-th powers, then q must be a k-th power. But this is a contradiction. Therefore $q < \sqrt{p} + 1$ and hence $H < \sqrt{p} + 1$.

For each pair of integers t, q with

$$0 \leq t < q \leq X \text{ and } \gcd(t, q) = 1, \tag{4.18}$$

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

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

Claim 4.6. *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, $|\frac{t_1 p}{q_1} - \frac{t_2 p}{q_2}| \leq \frac{H}{q_1} + \frac{H}{q_2}$. This leads to

$$|t_1 q_2 - t_2 q_1| \leq \frac{(q_1 + q_2)H}{p} \leq \frac{2HX}{p} = \frac{2H^2}{hp} < 1.$$

The last inequality comes from $H < \sqrt{p} + 1$, $h \geq 4$ and $p \geq 2$.

Now, since $|t_1 q_2 - t_2 q_1| < 1$ and t_1, t_2, q_1, q_2 are integers, we have $t_1 q_2 = t_2 q_1$. 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 4.7. *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 $H < \sqrt{p}+1$ and $4 \leq h \leq p$ and therefore $H^2 + 4H < p + 6\sqrt{p} + 1 < 4p$, which is true for $p \geq 5$. Therefore, we have proved the claim.

Using the periodicity of χ and Claims 4.6 and 4.7 we have the following:

$$\begin{aligned} S_w(p,h,\chi,k) &= \sum_{m=1}^{p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} = \sum_{-H \leq m < -H+p} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} \\ &\geq \sum_{q,t} \sum_{m \in I(q,t)} \left| \sum_{l=0}^{h-1} \chi(m+l) \right|^{2w} = \sum_{q,t} \sum_{m \in I(q,t)} \left| \sum_{l=0}^{h-1} \chi(q(m+l)-tp) \right|^{2w}. \quad (4.19) \end{aligned}$$

The sum is over all pairs (q,t) satisfying (4.18). Note that $\chi(q) = 1$ because $0 < q \leq X < H$. The last equality in (4.19) 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 (4.19) to be true).

For q, t satisfying (4.18), 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:

$$\begin{aligned} S_w(p,h,\chi,k) &\geq 2\sum_{q,t}\left(\frac{hX}{q} - h\right)h^{2w} \\ &= 2h^{2w+1}\left(X\sum_{1\leq q\leq X}\frac{\phi(q)}{q} - \sum_{1\leq q\leq X}\phi(q)\right) \geq 2AX^2h^{2w+1}\left(1 - \frac{1}{2AX}\right). \quad (4.20) \end{aligned}$$

The last inequality being Lemma 4.4. Once we make the substitution of $X = \frac{H}{h}$ we get the desired inequality.

If -1 is a k-th power $\pmod p$, we can improve (4.20). 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

$$\begin{aligned} S_w(p,h,\chi,k) &\geq \sum_{-H\leq m\leq -h} h^{2w} + \sum_{1\leq m\leq H-h+1} h^{2w} + \sum_{\substack{q,t\\ q>1}} \sum_{m\in L(q,t)} h^{2w} \\ &\geq (2(H-h)+1)\,h^{2w} + \sum_{1<q\leq X} \sum_{\substack{0\leq t<q\\ \gcd(t,q)=1}} \left(\frac{2H}{q}-h\right) h^{2w}. \end{aligned}$$

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

$$\begin{aligned} S_w(p,h,\chi,k) &\geq h^{2w+1}\left(2X\sum_{1\leq q\leq X}\frac{\phi(q)}{q} - \sum_{1\leq q\leq X}\phi(q) - 1 + \frac{1}{h}\right) \\ &\geq 3AX^2h^{2w+1}\left(1-\frac{\frac{\log x}{3}+3}{3AX}-\frac{1}{3AX^2}+\frac{1}{3AX^2h}\right). \end{aligned}$$

The last inequality being Lemma 4.5. Once we make the substitution of $X=\frac{H}{h}$ we get the desired inequality. □

4.3 Main theorem

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

Lemma 4.6. *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 and furthermore $g(p,k)\leq g(p,d)$.*

Proof. Let r be a primitive root $\pmod p$. Then $r^{\frac{p-1}{2}}\equiv -1 \pmod p$. Since $d\,|\,\frac{p-1}{2}$,

then -1 is a d-th power. Now note that if $a < g(p,k)$, then a is a k-th power and hence a d-th power 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 4.4. *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 4.1.

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 4.1: Upper bound for the least k-th power non-residue.

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 $\pmod p$ of order k. Assume that $\chi(a) = 1$ for all $1 \le a < H$. Let h and w be positive integers such that $4 \le h \le H$. Let $X = H/h$ and let $A = \frac{3}{\pi^2}$. Then by Theorem 4.3

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

If $w \le 9h$, we have from Theorem 4.2

$$S_w(p,h,\chi,k) = \sum_{m=1}^{p}\left|\sum_{l=0}^{h-1}\chi(m+l)\right|^{2w} < \frac{(2w)!}{2^w w!}ph^w + (2w-1)p^{1/2}h^{2w}. \tag{4.21}$$

Combining these two we get that

$$2AH^2\left(1-\frac{1}{2AX}\right) < \frac{(2w)!}{2^w w!}ph^{1-w} + (2w-1)p^{1/2}h = f(w,h), \tag{4.22}$$

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

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.

Because $f(w,h)$ as a function of h is simpler than $f(w,h)$ as a function of w, we will first fix w and find the optimal h. Since $\frac{\partial f}{\partial h}(w,h) = \frac{(2w)!}{2^w w!}p(1-w)h^{-w} + (2w-1)\sqrt{p}$, then the optimal h is an integer close to

$$h_w = \left(\left(\frac{(2w)!}{2^w(w)!}\right)\frac{w-1}{2w-1}\right)^{\frac{1}{w}} p^{\frac{1}{2w}}.$$

Now fixing $h = h_w$, we can look for the optimal w by taking the derivative of $f(w,h)$ with respect to w. Let's first simplify $f(w,h)$ as follows

$$f(w,h) = \frac{(2w)!}{2^w w!}\left(\frac{h}{h^w}\right)p + (2w-1)h\sqrt{p} = h\sqrt{p}\left(2w+1+\frac{1}{w-1}\right). \tag{4.23}$$

Therefore

$$\frac{\partial f}{\partial w}(w,h) = h'\left(2w+1+\frac{1}{w-1}\right)\sqrt{p} + h\left(2-\frac{1}{(w-1)^2}\right)\sqrt{p}. \tag{4.24}$$

Since we are looking for w as a function of p, and h is a complicated function, to help us find the optimal value of w, we will first calculate an approximation for h by using Stirling's formula:

$$\begin{aligned} h &= \left(\frac{(2w)!}{2^w w!}\left(\frac{w-1}{2w-1}\right)\right)^{\frac{1}{w}} p^{\frac{1}{2w}} = \left(\frac{(2w)!}{2^w w!}\left(\frac{1}{2}\right)\right)^{\frac{1}{w}} p^{\frac{1}{2w}}\left(1+O\left(\frac{1}{w}\right)\right) \\ &= \left(\left(\frac{2w}{e}\right)^w \frac{\sqrt{2}}{2}\right)^{\frac{1}{w}} p^{\frac{1}{2w}}\left(1+O\left(\frac{1}{w}\right)\right)^2 = \frac{2w}{e}\left(\frac{p}{2}\right)^{\frac{1}{2w}}\left(1+O\left(\frac{1}{w}\right)\right). \end{aligned} \tag{4.25}$$

Therefore

$$\begin{aligned} h' &= \left(\left(\frac{2w}{e}\right)\left(\frac{-\log\frac{p}{2}}{2w^2}\right)\left(\frac{p}{2}\right)^{\frac{1}{2w}} + \frac{2}{e}\left(\frac{p}{2}\right)^{\frac{1}{2w}}\right)\left(1+O\left(\frac{1}{w}\right)\right) \\ &= h\left(\frac{-\log\frac{p}{2}}{2w^2}+\frac{1}{w}\right)\left(1+O\left(\frac{1}{w}\right)\right). \end{aligned} \tag{4.26}$$

Letting $\frac{\partial f}{\partial w}(w,h) = 0$, by substituting h and h' from (4.25), (4.26) on (4.24) we find that we want

$$\frac{-\log p}{w} + 4 + O\left(\frac{\log p}{w^2}\right) + O\left(\frac{1}{w}\right) = 0,$$

Yielding that the optimal value of w is asymptotic to $\frac{\log p}{4}$.

Let

$$h = \left\lfloor \left(\frac{(2w)!}{2^w w!} \frac{w-1}{2w-1} \right)^{\frac{1}{w}} p^{\frac{1}{2w}} \right\rfloor + 1 \tag{4.27}$$

and

$$w = \left\lfloor \frac{\log p}{4} \right\rfloor + 1. \tag{4.28}$$

Then

$$\begin{aligned} f(w,h) = h\sqrt{p}\left(\frac{(2w)!}{2^w w!} \frac{\sqrt{p}}{h^w} + 2w - 1 \right) &< h\sqrt{p}\left(2w + 1 + \frac{1}{w-1} \right) \\ < \left(\frac{(2w)!}{2^w w!} \frac{w-1}{2w-1} \right)^{\frac{1}{w}} \left(2w + 1 + \frac{1}{w-1} \right) p^{\frac{1}{2}+\frac{1}{2w}} &+ p^{\frac{1}{2}} \left(2w + 1 + \frac{1}{w-1} \right) \\ < \left(2w + 1 + \frac{1}{w-1} \right) \sqrt{p} \left(e^2 \left(\frac{(2w)!}{2^w w!} \frac{w-1}{2w-1} \right)^{\frac{1}{w}} + 1 \right). \end{aligned} \tag{4.29}$$

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

Note the following explicit inequalities on Stirling's formula [37] 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

$$\left(\frac{(2w)!}{2^w w!} \right)^{\frac{1}{w}} < \left(\left(\frac{2w}{e} \right)^w \sqrt{2}\, e^{\frac{1}{24w} - \frac{1}{12w+1}} \right)^{\frac{1}{w}} = \left(\frac{2w}{e} \right) 2^{\frac{1}{2w}}\, e^{\frac{1}{24w^2} - \frac{1}{12w^2+w}}. \tag{4.30}$$

Combining (4.30) with (4.29) 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

$$f(w,h) < \left(\frac{e}{4}\log^2 p+\frac{5e+1}{2}\log p+8e+3+\frac{8e+4}{\log p}\right)\sqrt{p}$$
$$= \left(\frac{e}{4}+\frac{5e+1}{2\log p}+\frac{8e+3}{\log^2 p}+\frac{8e+4}{\log^3 p}\right)\sqrt{p}\log^2 p = K(p)\sqrt{p}\log^2 p, \quad (4.31)$$

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

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

Now let

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

The left hand side of (4.22) 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 we can do better, since by the second part of Theorem 4.3 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 (4.21) we get

$$3AH^2\left(1 - \frac{\frac{\log X}{3}+3}{3AX} - \frac{1}{3AX^2} + \frac{1}{3AX^2h}\right) < f(w,h). \tag{4.32}$$

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 and let

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

Now 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 (4.32) 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 4.6 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 4.4. 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 4.7. *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 mod 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*

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

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 4.7 that p is a $(g(p,2)-1)$-pseudosquare. In [42], it was shown that for $q \geq 379$, 379-pseudosquares are greater than 10^{25}. Therefore if $g(p,2) \geq 379$, then $p \geq 10^{25}$.

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 (4.23))instead of the values of h and w chosen in Theorem 4.4.

Let A be the constant we've been using and let

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

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 4.4, we have $g(p,k) < \gamma(p,h,w)p^{1/4}\log p$. 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 $\gamma(p,h,w) \leq 0.9$,

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 4.2: 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 $p \in [10^{25}, 10^{27}]$.

we need only check the endpoints of the intervals since $\gamma(p, h, w)$ is concave up. Table 4.2 completes the proof.

□

Remark 4.2. 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. Showing us that 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 (4.9):

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

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

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

Then by Theorem 4.3 combined with (4.9), we have that the inequality (4.32) becomes

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

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 4.3: 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 $p \in [10^9, 10^{12}]$.

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:

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

Then by similar arguments as in Theorem 4.4, we have $g(p,k) < \gamma_2(p,h,w)p^{1/4}\log p$. 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 4.3 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 $3 < p \leq 10^7$, $g(p, 2) \leq 1.1p^{1/4} \log p$.

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 4.4, we have $g(p, 2) < \gamma_3(p, h, w)p^{1/4} \log p$. 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 4.4 completes the proof.

□

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

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 4.4: 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 $p \in [10^{18}, 10^{19}]$.

Chapter 5

On consecutive residues and non-residues

Let χ be a non-principal Dirichlet character to the prime modulus p. In 1963, Burgess showed (see [7]) 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 [26]) proved an explicit version of Burgess's theorem:

Theorem 5.1. *If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then*

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

Furthermore,

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

A similar bound was announced but not proven by Norton (see [32]), 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.

The main ingredient in the proof is estimating

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

where p is a prime, χ is a non-principal character $\bmod\ p$ of order k, and h is a positive integer.

In this chapter, with help from our upper bound on $S_w(p,h,\chi,k)$ (Theorem 4.2) and an improvement on McGown's lower bound, we are able to prove Norton's claim and go a little further.

Theorem 5.2. *If χ is any non-principal Dirichlet character to the prime modulus p which is constant on $(N, N+H]$, then*

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

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 5.1. The constant $\frac{\pi}{2}\sqrt{\frac{e}{3}} = 1.49522\ldots$ is $\frac{1}{2\sqrt{2e}} = 0.214441\ldots$ times the size of McGown's asymptotic constant.

5.1 Lower bound for $S_w(p, h, \chi, k)$

To prove Theorem 5.2 we will need a lower bound for $S_w(p, h, \chi, k)$. The proposition we shall prove improves Proposition 3.3 in [26] by a factor of 4 and it also has a smaller error term (saving a $\log X$). It also has a less demanding condition for H.

Throughout, let $A = \frac{3}{\pi^2}$.

Proposition 5.1. *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

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

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 [12]), there exist coprime integers a and b satisfying $1 \leq a \leq \left\lfloor \frac{2H}{h} \right\rfloor$ and

$$\left| a\frac{N}{p} - b \right| \leq \frac{1}{\left\lfloor \frac{2H}{h} \right\rfloor + 1} \leq \frac{h}{2H}. \tag{5.1}$$

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 $\chi(m) = \bar{\chi}(q)\chi(N+i)$. As in our proof of Theorem 4.3, 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 $\frac{N+pt_1}{q_1} \leq \frac{N_p t_2}{q_2} < \frac{N+H+pt_1}{q_1}$ or $\frac{N+pt_2}{q_2} \leq \frac{N_p t_1}{q_1} < \frac{N+H+pt_2}{q_2}$.

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,

$$\left| \frac{N(q_1 - q_2)}{p} + t_2 q_1 - t_1 q_2 \right| < \frac{\max\{q_1, q_2\} H}{p} \leq \frac{XH}{p}. \tag{5.2}$$

Therefore, combining (5.1) and (5.2), we get

$$\left| \frac{b}{a}(q_1 - q_2) + t_2 q_1 - t_1 q_2 \right| = \left| \left(\frac{N}{p} + \left(\frac{b}{a} - \frac{N}{p} \right) \right)(q_1 - q_2) + t_2 q_1 - t_1 q_2 \right|$$

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

Since $a \leq \frac{2H}{h}$ and $H^3 \leq \frac{h^2p}{4}$ 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 $m > \frac{N+pt}{q} \geq 0$. 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

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

The last inequality is true since there are at least $\frac{H}{q}-h$ subsets of h consecutive

integers in $I(q,t)$, and when there are h consecutive integers $m, m+1, \ldots m+h-1$, we have

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

To finish the proof of the Proposition, we need to prove the following claim:

Claim 5.1. *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 of the Claim: 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

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

Since $\gcd(a,b) = 1$, the congruence $at \equiv -b \bmod d$ 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 $at \equiv -b \bmod d$. Therefore the sum becomes

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

The inside of the sum was evaluated in the proof of Lemma 4.4 and writing $\frac{X}{d} =$

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

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

$$\frac{X^2}{2} \sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{\mu(d)}{d^2} - \frac{X^2}{2} \sum_{\substack{d > X \\ (d,a)=1}} \frac{\mu(d)}{d^2} - \frac{X}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} + \frac{1}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \left(1 - \left\{ \frac{X}{d} \right\} \right). \tag{5.3}$$

Now,

$$\sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{p \mid a} \left(1 - \frac{1}{p^2} \right)^{-1} \geq \frac{6}{\pi^2}. \tag{5.4}$$

Using Claim 4.1 we can get

$$\sum_{\substack{d > X \\ (d,a)=1}} \frac{\mu(d)}{d^2} \leq \sum_{\substack{d > X \\ d \text{ squarefree}}} \frac{1}{d^2} < \frac{1}{X}. \tag{5.5}$$

Tao in an expository article [43] proved the following inequality [1]

$$\left| \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} \right| \leq 1. \tag{5.6}$$

We include a short proof of (5.6) similar to the proof of Claim 4.3. Let

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

[1] Generalizations of this inequality can be found in [16] and [41].

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 (5.6) 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

$$\left| X \sum_{\substack{d \leq X \\ (d,a)=1}} \frac{\mu(d)}{d} \right| = \left| S_a(X) + \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \right| = \left| \sum_{\substack{d \leq X \\ \mathrm{rad}(d) \mid \mathrm{rad}(a)}} 1 + \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \right|. \tag{5.7}$$

Note that the conditions $\mathrm{rad}(d) \mid \mathrm{rad}(a)$ and $(d, a) = 1$ overlap only when $d = 1$. Therefore the right hand side of (5.7) 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 (5.7) is $\leq \lfloor X \rfloor$. This concludes the proof of (5.6).

We also have from Claim 4.3 that

$$\frac{1}{2} \sum_{\substack{d \leq X \\ (d,a)=1}} \mu(d) \left\{ \frac{X}{d} \right\} \left(1 - \left\{ \frac{X}{d} \right\} \right) \leq \frac{1}{8} \sum_{\substack{d \leq X \\ d \text{ squarefree}}} 1 \leq \frac{1}{12} x + \frac{1}{4}. \tag{5.8}$$

Combining (5.4), (5.5), (5.6) and (5.8) with (5.3) proves Claim 5.1. □

5.2 Proof of the main theorem

Proof of Theorem 5.2. Let h and w be positive integers. Assume $4h \leq H \leq \left(\frac{h}{2}\right)^{2/3} p^{1/3}$. Then by Proposition 5.1 and Theorem 4.2 we have (for $w \leq 9h$):

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

Therefore,

$$AH^2 g(X) < f(w, h), \tag{5.9}$$

where $f(w, h)$ is defined as in (4.22). We have already dealt with bounding $f(w, h)$ in Theorem 4.4 by choosing optimal h and w. The choices for h and w can be found in (4.27) and (4.28), respectively. From there one can obtain (4.31), a bound for $f(w, h)$ which we repeat below:

$$f(w, h) < \left(\frac{e}{4} + \frac{5e+1}{2\log p} + \frac{8e+3}{\log^2 p} + \frac{8e+4}{\log^3 p}\right) \sqrt{p} \log^2 p = K(p) \sqrt{p} \log^2 p. \tag{5.10}$$

Also recall

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

Following the same approach as in Theorem 4.4, let's assume $p \geq p_0$ and $H \geq C(p_0)\, p^{1/4} \log p$. We may assume $C(p_0) \geq \pi \sqrt{\frac{e}{12}}$, hence

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

5.2 Proof of the main theorem

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 $H \geq \pi\sqrt{\frac{e}{12}} p^{1/4} \log p$ and $h < \left(\frac{e}{2} + \frac{2e+1}{\log p}\right) \log p$, 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 (5.10).

The left hand side of (5.9) can therefore be bounded from below for $p \geq p_0$:

$$AH^2 g(X) \geq A\left(C(p_0)\right)^2 \sqrt{p} \log^2 p \; g(X(p_0))$$

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

giving us a contradiction, proving that $H < C(p_0)p^{1/4}\log p$ whenever $H \leq \left(\frac{h}{2}\right)^{2/3} p^{1/3}$.

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.

For $p \geq 1.1 \cdot 10^{10}$ 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 $p \geq 1.1 \cdot 10^{10}$, $H < C(p_0)p^{1/4}\log p$.

Table 5.1 shows values of $C(p_0)$ for different values of p_0.

Just as in the proof of Propositions 4.1, 4.4 and 4.3, we can fix the values of h and w and improve the bounds.

For $p \geq 2.5 \cdot 10^9$, we have $1.55p^{1/4}\log p < \left(\frac{h}{2}\right)^{2/3} p^{1/3}$, and from the table, 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 $2.5 \cdot 10^9 < p < 10^{64}$.

p_0	$C(p_0)$
1.1×10^{10}	1.86409
10^{12}	1.79646
10^{15}	1.73289
10^{18}	1.69225
10^{20}	1.6722
10^{30}	1.6126
10^{40}	1.58304
10^{50}	1.56537
10^{60}	1.55362
10^{64}	1.54995

Table 5.1: Upper bound H on the number of consecutive residues with equal character value. For $p \geq p_0$, $H < C(p_0)p^{1/4}\log p$.

As in the proof of Proposition 4.1, let

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

Let $\gamma_4(p, w, h)$ be defined in the following way:

$$\gamma_4(p, w, h) = \sqrt{\frac{f(w, h)}{A\sqrt{p}\log^2 p\, g(X(p))}}.$$

Then by similar arguments as in Theorem 4.4, we have $H < \gamma_4(p, h, w)p^{1/4}\log p$. Hence, all we want is for $\gamma_4(p, h, w)$ to be at most 1.55 and for $1.55p^{1/4}\log p < h^{2/3}p^{1/3}$. By picking w's and h's as in the Table 5.2, we complete the proof for $p > 2.5 \cdot 10^9$ (noticing that with h and w fixed, $\gamma_4(p, w, h)$ is concave up, allowing us to just check the endpoints of the intervals).

Let's now prove that for all odd p we have $H < 4p^{1/4}\log p$. It is obviously true for $p = 2$ since $4 \cdot 2^{1/4}\log 2 > 2$. Now, for $1.9 \leq p \leq 3 \cdot 10^6$, it is true because of the

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	$[10^{62}, 10^{64}]$						

Table 5.2: As an example on how to read the table: when $w = 10$ and $h = 62$, then $\gamma_4(p, w, h) < 1.55$ for all $p \in [10^{18}, 10^{19}]$. It is also worth noting that the inequality $1.55p^{1/4} \log p < h^{2/3}p^{1/3}$ is also verified for each choice of w and h.

following inequality of Brauer [5] (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 $H < \left(\frac{h}{2}\right)^{2/3} p^{1/3}$ to be able to use our machinery. If $h = 94$, then for $p \geq 1.9 \cdot 10^6$ we have $\left(\frac{h}{2}\right)^{2/3} p^{1/3} > 3p^{1/4} \log p$. Using $w = 2$, we have $\gamma_4(p, w, h) < 3$ whenever $p \in [3 \cdot 10^6, 10^8]$. Now picking $w = 3$ we get $\gamma_4(p, w, h) < 3$ 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. □

Remark 5.2. 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 5.2 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, I 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 $2.4p^{1/4}\log p < \left(\frac{h}{2}\right)^{2/3} p^{1/3}$ whenever $p > e^{15}$. Therefore we have $H < \gamma_4(p, w, 67)p^{1/4}\log p$ for $p > e^{15}$. We note that $\gamma_4(p, 2, 67) < 2.4$ when $p \in (e^{15}, 10^{7.5})$ and $\gamma_4(p, 3, 67) < 2.4$ when $p \in [10^{7.5}, 2.5 \cdot 10^9]$, completing the proof of our claim.

Remark 5.3. 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 [21][2] :

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

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

[2]This inequality was done using elementary methods that build on the work of Brauer [5]. 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

Chapter 6

Burgess

Let χ be a character mod q. In Chapter 1 we defined $S_\chi(M,N)$ as follows

$$S_\chi(M,N) = \sum_{M<n\le M+N} \chi(n).$$

We have discussed the Pólya–Vinogradov inequality in Chapters 1, 2 and 3. The Pólya–Vinogradov inequality is very useful when N is big compared to $\sqrt{q}$, but not very useful otherwise (since trivially $|S_\chi(M,N)| \le N$). What we want is to have $S_\chi(M,N) = o(N)$, that is, we want an inequality that works well even when N is not large. The best we can do is use the Burgess inequality, which allows us to take N as small as $q^{\frac{1}{4}+o(1)}$.

Theorem 6.1. *Let χ be a primitive character* mod q *with $q > 1$, and let M and N be non-negative reals with $N \ge 1$. Then*

$$|S_\chi(M,N)| \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\varepsilon}$$

for $r = 2, 3$ and for any $r \geq 1$ if q is cubefree, the implied constant depending only on ε and r.

In the thesis, our emphasis has been on making numerically explicit estimates. The literature has few papers concerning explicit estimates for the Burgess inequality, and all of them concern characters of prime modulus. Iwaniec and Kowalski [22] sketched an argument to arrive at the following explicit estimate:

Theorem 6.2. *Let p be a prime. Let χ be a non-principal Dirichlet character* mod p. *Let r be a positive integer, and let M and N be non-negative reals with $N \geq 1$. Then*

$$|S_\chi(M, N)| \leq 30 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Using the techniques from [22], Booker [4] gave the following improvement on the estimate for quadratic characters:

Theorem 6.3. *Let $p > 10^{20}$ be a prime number with $p \equiv 1 \pmod 4$. Let $r \in \{2, 3, 4, \ldots, 15\}$. Let M and N be real numbers such that $0 < M, N \leq 2\sqrt{p}$. Let χ be a non-principal quadratic character* mod p. *Then*

$$|S_\chi(M, N)| \leq \alpha(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} \left(\log p + \beta(r)\right)^{\frac{1}{2r}},$$

where $\alpha(r)$ and $\beta(r)$ are given by Table 6.1.

Also following [22], McGown [25] proved the following theorem which is not as strong as Theorem 6.3 when dealing with quadratic characters, but it works for higher orders too.

r	$\alpha(r)$	$\beta(r)$	r	$\alpha(r)$	$\beta(r)$
2	1.8221	8.9077	9	1.4548	0.0085
3	1.8000	5.3948	10	1.4231	-0.4106
4	1.7263	3.6658	11	1.3958	-0.7848
5	1.6526	2.5405	12	1.3721	-1.1232
6	1.5892	1.7059	13	1.3512	-1.4323
7	1.5363	1.0405	14	1.3328	-1.7169
8	1.4921	0.4856	15	1.3164	-1.9808

Table 6.1: Explicit constants on the Burgess inequality for quadratic characters.

Theorem 6.4. *Let $p \geq 2 \cdot 10^4$ be a prime number. Let M and N be non-negative integers with $1 \leq N \leq 4p^{\frac{1}{2}+\frac{1}{4r}}$. Suppose χ is a non-principal character* $\bmod p$. *Then there exists a computable constant $C(r)$ such that*

$$|S_\chi(M,N)| < C(r)N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}},$$

where $C(r)$ is given by Table 6.2.

r	$C(r)$	r	$C(r)$
2	10.0366	9	2.1467
3	4.9539	10	2.0492
4	3.6493	11	1.9712
5	3.0356	12	1.9073
6	2.6765	13	1.8540
7	2.4400	14	1.8088
8	2.2721	15	1.7700

Table 6.2: Values for the constant $C(r)$ in the Burgess inequality.

The restriction that $N \leq 4p^{\frac{1}{2}+\frac{1}{4r}}$ is necessary to get the exponent $\frac{1}{2r}$ in the $\log p$ term of the inequality. In section 6.2 we improve Theorem 6.2 which works without any restriction on N.

Theorem 6.5. *Let p be a prime. Let χ be a non-principal Dirichlet character* mod p. *Let M and N be non-negative reals with $N \geq 1$ and let $r \leq 10$ be a positive integer. Then for $p \geq p_0$, there exists $c_1(r)$, a constant depending on r and p_0 such that*

$$|S_\chi(M,N)| \leq c_1(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}},$$

where $c_1(r)$ is given by Table 6.3.

r	$p_0 = 10^7$	$p_0 = 10^{10}$	$p_0 = 10^{20}$
2	2.70301	2.59525	2.40850
3	2.00993	1.78600	1.37512
4	1.73508	1.52044	1.31151
5	1.61921	1.45435	1.30224
6	1.56241	1.42431	1.29218
7	1.52077	1.40363	1.28214
8	1.48569	1.38189	1.27196
9	1.45842	1.36260	1.26266
10	1.43281	1.34858	1.25366

Table 6.3: Values for the constant $c_1(r)$ in the Burgess inequality.

In the spirit of Theorem 6.2, where we have no restriction on r, we prove the following corollary:

Corollary 6.1. *Let p be a prime such that $p \geq 10^7$. Let χ be a non-principal Dirichlet character* mod p. *Let r be a positive integer, and let M and N be non-negative reals with $N \geq 1$. Then*

$$|S_\chi(M,N)| \leq 2.71 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Finally, in section 6.3, we improve Theorem 6.4 to be almost as strong as Theorem 6.3.

r	$p_0 = 10^{10}$	$p_0 = 10^{15}$	$p_0 = 10^{20}$
2	3.68544	3.55194	3.53837
3	2.61264	2.51481	2.49562
4	2.20106	2.12453	2.10726
5	1.98627	1.91965	1.90258
6	1.85134	1.79132	1.77669
7	1.75413	1.70003	1.68913
8	1.68092	1.63645	1.61632
9	1.62263	1.58550	1.56369
10	1.57455	1.54497	1.52159

Table 6.4: Values for the constant $c_2(r)$ in the Burgess inequality.

Theorem 6.6. *Let p be a prime. Let χ be a non-principal Dirichlet character* mod p. *Let M and N be non-negative reals with $1 \leq N \leq 2p^{\frac{1}{2}+\frac{1}{4r}}$ and let $r \leq 10$ be a positive integer. Then for $p \geq p_0$, there exists $c_2(r)$, a constant depending on r and p_0 such that*

$$|S_\chi(M,N)| < c_2(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}},$$

where $c_2(r)$ is given by Table 6.4.

Using an idea from [29], we can get rid of the restriction on N for $r \geq 3$.

Corollary 6.2. *Let $p \geq 10^{10}$ be a prime number. Let M and N be non-negative integers with $N \geq 1$. Suppose χ is a non-principal character* mod p *and that $p \geq p_0$ for some positive real p_0. Then for $r \geq 3$, there exists a computable constant $c_2(r)$ depending on r and p_0, such that*

$$|S_\chi(M,N)| < c_2(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}},$$

where $c_2(r)$ is the same as that of Table 6.4 whenever $r \geq 3$.

6.1 Preliminary lemmas

Let A and N be positive integers. Let $v(x)$ be the number of representations of x as $\bar{a}n \pmod p$, where $\bar{a}$ is the inverse of $a \pmod p$, $1 \leq a \leq A$ and $M < n \leq M + N$, that is,

$$v(x) = \#\left\{(a,n) \in \mathbb{N}^2 \mid 1 \leq a \leq A,\ M < n \leq M+N \text{ and } n \equiv ax \bmod p\right\}. \quad (6.1)$$

The main lemma in this section is the following:

Lemma 6.1. *Let p be a prime and let $N < p$ be a positive integer. Let $A \geq 28$ be an integer satisfying $A < \frac{N}{12}$, then*

$$V_2 = \sum_{x \bmod p} v^2(x) \leq 2AN\left(\frac{AN}{p} + \log(1.85A)\right). \quad (6.2)$$

To prove the lemma regarding V_2 we will need a couple of estimates involving the ϕ function; the estimates are the following two lemmas:

Lemma 6.2. *For $x \geq 1$ a real number we have:*

$$\sum_{n \leq x} n\phi(n) \leq \frac{2}{\pi^2}x^3 + \frac{1}{2}x^2 \log x + x^2. \quad (6.3)$$

Proof. For $1 \leq x < 2$, the left hand side of (6.3) is 1, while the right hand side is at least $x^2 \geq 1$. Therefore it is true for $1 \leq x < 2$. Now for $2 \leq x < 3$, the left hand side is 3, while the right hand side is at least $x^2 \geq 4$. Therefore (6.3) is true for $1 \leq x < 3$. In the rest of the proof we will assume that $x \geq 3$. Let's work with the sum:

$$\sum_{n\le x}\phi(n)n=\sum_{n\le x}\sum_{d|n}\frac{\mu(d)n^2}{d}=\sum_{d\le x}\mu(d)d\sum_{dm\le x}m^2$$
$$=\sum_{d\le x}\frac{\mu(d)d}{6}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)\left(2\left\lfloor\frac{x}{d}\right\rfloor+1\right).$$

Now, let $\theta_d=\frac{x}{d}-\left\lfloor\frac{x}{d}\right\rfloor$. Then we have

$$\sum_{n\le x}\phi(n)n=\frac{x^3}{3}\sum_{d\le x}\frac{\mu(d)}{d^2}+\frac{x^2}{6}\sum_{d\le x}\frac{(3-6\theta_d)\mu(d)}{d}$$
$$+\frac{x}{6}\sum_{d\le x}\left(6\theta_d^2-6\theta_d+1\right)\mu(d)-\frac{1}{6}\sum_{d\le x}\theta_d(1-\theta_d)(1-2\theta_d)\mu(d)d. \quad (6.4)$$

From [17, Theorem 422] it follows that for $x\ge 3$

$$\sum_{d\le x}\frac{1}{d}<\log x+\gamma+\frac{1}{x}<\log x+1-\frac{1}{60}-\frac{1}{60x}. \quad (6.5)$$

Using that $0\le\theta_d\le 1$ we have that $|3-6\theta_d|\le 3$, that $|6\theta_d^2-6\theta_d+1|\le 1$ and $|(1-\theta_d)(1-2\theta_d)(-\theta_d)|\le\frac{1}{10}$. Therefore, using (6.4), (6.5), that $\sum_{d\ge 1}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}$, and that $|\mu(d)|\le 1$, we get

$$\sum_{n\le x}\phi(n)n\le\frac{x^3}{3}\sum_{d\le x}\frac{\mu(d)}{d^2}+\frac{x^2}{2}\sum_{d\le x}\frac{1}{d}+\frac{x}{6}\sum_{d\le x}1+\frac{1}{60}\sum_{d\le x}d$$
$$\le\frac{2}{\pi^2}x^3-\frac{x^3}{3}\sum_{d>x}\frac{\mu(d)}{d^2}+\frac{1}{2}x^2\log x+\frac{x^2}{2}-\frac{x^2}{120}-\frac{x}{120}+\frac{x^2}{6}+\frac{1}{60}\left(\frac{x(x+1)}{2}\right). \quad (6.6)$$

From Claim 4.1 we have

$$\sum_{d>x}\frac{\mu(d)}{d^2}\ge-\frac{1}{x}.$$

Combining this with (6.6) yields the lemma. □

Lemma 6.3. *For $x \geq 1$ a real number we have:*

$$\sum_{n \leq x} \frac{\phi(n)}{n} \leq \frac{6}{\pi^2} x + \log x + 1. \tag{6.7}$$

Proof. For $1 \leq x < 2$, the left hand side of (6.7) is 1, while the right hand side is at least 1. We can manually check that for all integers x satisfying $2 \leq x \leq 42$ we have

$$\sum_{n \leq x} \frac{\phi(n)}{n} \leq \frac{6}{\pi^2}(x-1) + \log(x-1) + 1,$$

implying that (6.7) is true for $x < 42$. Therefore, we may assume that $x \geq 42$.

Let's work with the sum:

$$\sum_{n \leq x} \frac{\phi(n)}{n} = \sum_{n \leq x} \frac{1}{n} \sum_{d \mid n} \mu(d) \frac{n}{d} = \sum_{d \leq x} \sum_{n \leq \frac{x}{d}} \frac{\mu(d)}{d} = \sum_{d \leq x} \left\lfloor \frac{x}{d} \right\rfloor \frac{\mu(d)}{d}.$$

Using that $\displaystyle\sum_{d \leq x} \frac{1}{d} \leq \log x + \gamma + \frac{1}{x}$ yields

$$\sum_{n \leq x} \frac{\phi(n)}{n} \leq x \sum_{d \geq 1} \frac{\mu(d)}{d^2} - x \sum_{d > x} \frac{\mu(d)}{d^2} + \sum_{d \leq x} \frac{1}{d} \leq \frac{6}{\pi^2} x + \log x + \gamma + \frac{1}{x} - x \sum_{d > x} \frac{\mu(d)}{d^2}. \tag{6.8}$$

Moser and Macleod [30] gave a simple proof that for $x \geq 2$ we have

$$\left| \sum_{d > x} \frac{\mu(d)}{d^2} \right| \leq \frac{1}{3x} + \frac{8}{3x^2}. \tag{6.9}$$

Combining (6.9) with (6.8) yields for $x \geq 42$ that

$$\sum_{n \leq x} \frac{\phi(n)}{n} \leq \frac{6}{\pi^2} x + \log x + \gamma + \frac{1}{3} + \frac{8}{3x} \leq \frac{6}{\pi^2} x + \log x + 1.$$

□

Lemma 6.4. *For $x \geq 1$ we have:*

$$\sum_{d \leq x} \log\left(\frac{x}{d}\right) \leq x - 1$$

Proof. For $1 \leq x < 2$ we have $\sum_{d \leq x} \log\left(\frac{x}{d}\right) = \log x \leq x - 1$. Therefore, we may assume $x \geq 2$. Now,

$$\sum_{d \leq x} \log\left(\frac{x}{d}\right) = \lfloor x \rfloor \log x - \sum_{d \leq x} \log d \leq \lfloor x \rfloor \log x - \lfloor x \rfloor \log \lfloor x \rfloor + \lfloor x \rfloor - 1. \tag{6.10}$$

To get the second inequality we used that

$$\sum_{d \leq x} \log d = \sum_{2 \leq d \leq x} \log d \geq \int_1^{\lfloor x \rfloor} \log t \, dt = \lfloor x \rfloor \log \lfloor x \rfloor - \lfloor x \rfloor + 1.$$

Now, notice that $x = \lfloor x \rfloor + \{x\}$ and $\log(1 + y) \leq y$, therefore we have

$$\lfloor x \rfloor \log x = \lfloor x \rfloor \log \lfloor x \rfloor + \lfloor x \rfloor \log(x/\lfloor x \rfloor) \leq \lfloor x \rfloor \log \lfloor x \rfloor + \{x\}. \tag{6.11}$$

Combining equations (6.10) and (6.11) yields

$$\sum_{d \leq x} \log\left(\frac{x}{d}\right) \leq \{x\} + \lfloor x \rfloor - 1 = x - 1.$$

□

Now we are ready to prove Lemma 6.1.

Proof of Lemma 6.1. We'll begin by noting that V_2 is the number of quadruples (a_1, a_2, n_1, n_2) with $1 \leq a_1, a_2 \leq A$ and $M < n_1, n_2 \leq M + N$ such that $a_1 n_2 \equiv a_2 n_1 \pmod{p}$. If $a_1 = a_2$, since $N < p$, we have that $n_1 = n_2$ because $n_1 \equiv n_2 \pmod{p}$ while $|n_1 - n_2| \leq N < p$. Therefore, the number of quadruples in this case is AN. Fix a_1 and a_2 in such a way that $a_1 \neq a_2$. Let k be an integer satisfying

$$a_1 n_2 - a_2 n_1 = kp, \tag{6.12}$$

for some n_1 and n_2. We can put a bound on possible values for k. First of all, k must be a multiple of $\gcd(a_1, a_2)$. Now, if we write $n_1 = n_1^{'} + M$ and $n_2 = n_2^{'} + M$, we have, using $kp - (a_1 - a_2)M = a_1 n_2^{'} - a_2 n_1^{'}$, that

$$-a_2 N \leq -a_2 n_1^{'} < kp - (a_1 - a_2)M < a_1 n_2^{'} \leq a_1 N.$$

Therefore k lies in an interval of length at most $\frac{(a_1+a_2)N}{p}$. Since k is a multiple of $\gcd(a_1, a_2)$ and k lies in such an interval, then there are at most

$$\frac{(a_1 + a_2)N}{\gcd(a_1, a_2)p} + 1,$$

choices for k.

Given a_1, a_2 and k we can count the number of pairs (n_1, n_2) which would satisfy (6.12). The number of pairs is bounded by $N\frac{\gcd(a_1,a_2)}{\max\{a_1,a_2\}} + 1$. Therefore we get

$$V_2 \leq AN + 2\sum_{a_1<a_2}\Big(\frac{(a_1+a_2)N}{\gcd(a_1,a_2)p}+1\Big)\Big(\frac{\gcd(a_1,a_2)N}{\max\{a_1,a_2\}}+1\Big)$$
$$= AN + \frac{2N^2}{p}S_1 + \frac{2N}{p}S_2 + 2NS_3 + A^2 - A, \quad (6.13)$$

where

$$S_1 = \sum_{a_1<a_2}\frac{a_1+a_2}{\max\{a_1,a_2\}},$$

$$S_2 = \sum_{a_1<a_2}\frac{a_1+a_2}{\gcd(a_1,a_2)},$$

and

$$S_3 = \sum_{a_1<a_2}\frac{\gcd(a_1,a_2)}{\max\{a_1,a_2\}}. \quad (6.14)$$

Dealing with S_1 is straightforward, in fact S_1 is

$$\sum_{a_2\leq A}\sum_{a_1<a_2}\frac{a_1+a_2}{a_2} = \sum_{a_2\leq A}\left(a_2 - 1 + \frac{a_2(a_2-1)}{2a_2}\right) = \frac{3}{2}\frac{A(A-1)}{2} = \frac{3}{4}A^2 - \frac{3}{4}A. \quad (6.15)$$

Now, let's estimate S_2:

$$S_2 = \sum_{a_1<a_2\leq A}\frac{a_1+a_2}{\gcd(a_1,a_2)} = \sum_{d\leq A}\sum_{b_2\leq\frac{A}{d}}\sum_{b_1<b_2,(b_1,b_2)=1}(b_1+b_2)$$
$$= \sum_{d\leq A}\sum_{2\leq b_2\leq\frac{A}{d}}\left(\phi(b_2)b_2 + \frac{\phi(b_2)}{2}b_2\right) = \frac{3}{2}\sum_{d\leq A}\sum_{2\leq b_2\leq\frac{A}{d}}\phi(b_2)b_2.$$

Using Lemma 6.2, we get

$$S_2 \leq \frac{3}{\pi^2}\sum_{d\leq A}\big(\frac{A}{d}\big)^3 + \frac{3}{4}\sum_{d\leq A}\big(\frac{A}{d}\big)^2\log\big(\frac{A}{d}\big) + \frac{3}{2}\sum_{d\leq A}\big(\frac{A}{d}\big)^2.$$

Using that $\log\left(\frac{A}{d}\right) = \log A - \log d$, and that $\sum_{d\geq 1} \frac{1}{d^s} = \zeta(s)$, yields

$$S_2 \leq \frac{3\zeta(3)}{\pi^2}A^3 + \frac{3\zeta(2)}{4}A^2 \log A - \frac{3}{4}A^2 \sum_{d\leq A} \frac{\log d}{d^2} + \frac{3}{2}A^2\zeta(2).$$

Using that for $A \geq 11$ we have $\frac{3\zeta(2)}{2} - \frac{3}{4}\sum_{d\leq A} \frac{\log d}{d^2} < 2$ yields

$$S_2 \leq \frac{3\zeta(3)}{\pi^2}A^3 + \frac{3\zeta(2)}{4}A^2 \log(A) + 2A^2. \tag{6.16}$$

Let's estimate S_3. We have

$$S_3 = \sum_{a_1<a_2\leq A} \frac{\gcd(a_1,a_2)}{\max(a_1,a_2)} = \sum_{d\leq A} \sum_{b_2\leq \frac{A}{d}} \sum_{b_1<b_2,(b_1,b_2)=1} \frac{1}{b_2} = \sum_{d\leq A} \sum_{2\leq b_2\leq \frac{A}{d}} \frac{\phi(b_2)}{b_2}.$$

Using Lemma 6.3 yields

$$S_3 \leq \sum_{d\leq A} \left(\frac{A}{d}\frac{1}{\zeta(2)} + \log\left(\frac{A}{d}\right)\right) = \frac{6}{\pi^2}A\sum_{d\leq A}\frac{1}{d} + \sum_{d\leq A}\log\left(\frac{A}{d}\right).$$

From [17, Theorem 422] it follows that for $A \geq 27$

$$\sum_{d\leq A}\frac{1}{d} < \log A + \gamma + \frac{1}{A} < \log(1.85A).$$

Using this and Lemma 6.4 yields

$$S_3 \leq \frac{6}{\pi^2}A\log(1.85A) + A - 1. \tag{6.17}$$

Using (6.15), (6.16) and (6.17) in (6.13) yields the following upper bound for V_2:

$$2AN\Big(\frac{3}{2}+\frac{A-1}{2N}+\frac{3AN}{4p}-\frac{3N}{4p}+\frac{3\zeta(3)A^2}{\pi^2 p}+\frac{3\zeta(2)A\log A}{4p}+\frac{6}{\pi^2}\log(1.85A)-\frac{1}{A}+\frac{2A}{p}\Big) \tag{6.18}$$

For $A \geq 4$, we have

$$\frac{3\zeta(3)A^2}{\pi^2 p}+\frac{3\zeta(2)A\log A}{4p} < \frac{3}{4}\frac{A^2}{p}. \tag{6.19}$$

Since $N \geq 3A$ we have the following two inequalities:

$$\frac{AN}{4p} > \frac{3}{4}\frac{A^2}{p} \text{ and } \frac{3N}{4p} > \frac{2A}{p}. \tag{6.20}$$

Combining (6.19) and (6.20) yields

$$\frac{3AN}{4p}+\left(\frac{3\zeta(3)A^2}{\pi^2 p}+\frac{3\zeta(2)A\log A}{4p}\right)+\left(\frac{2A}{p}-\frac{3N}{4p}\right) < \frac{AN}{p}. \tag{6.21}$$

Finally, using that $A \geq 28$ and that $N > 12A$, yields

$$\Big(1-\frac{6}{\pi^2}\Big)\log(1.85A) \geq \Big(1-\frac{6}{\pi^2}\Big)\log(51.8) \geq 1.54766 > \frac{3}{2}+\frac{1}{24} \geq \frac{3}{2}+\frac{A}{2N}. \tag{6.22}$$

Combining (6.21) and (6.22) in (6.18) yields (6.2). □

Remark 6.1. The main term will come from the $\log(1.85A)$ term and the 1.85 can be changed to a smaller number (the limit being e^{γ}), forcing A to be slightly larger to make the inequalities work. Also, the coefficient on $\log(1.85A)$ can be changed to be as close to $\frac{6}{\pi^2}$ as we want as long as A is big enough. It is important to note that big A's will mean forcing p to be much bigger in the estimates for the Burgess inequality.

Remark 6.2. The constraint $A \geq 28$ is used to get the main term to be $\log(1.85A)$; however, we can relax the condition on A and get a slightly worse main term. We chose our values this way to get the constants in tables 6.3, 6.4 as low as possible for small values of r. Relaxing the $A \geq 28$ condition would make these constants worse, but improve the constants for larger values of r. Since the small values of r seem to be the most useful in applications, we decided to focus on minimizing these cases.

6.2 Explicit Burgess inequality

Proof of Theorem 6.5. Let M and $N \geq 1$ be non-negative integers. Let r be a positive integer. Fix a constant $c_1(r) \geq 1$ (which we will name later). For $r = 1$, the Pólya–Vinogradov inequality implies the Burgess inequality, so assume $r \geq 2$. We will prove the Theorem by induction. Assume that for all positive integers $h < N$, we have

$$|S_\chi(M,h)| \leq c_1(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

The idea is to estimate $S_\chi(M,N)$ by shifting by h ($n \mapsto n+h$) and getting an error that we can deal with by induction.

Note that

$$S_\chi(M,N) = \sum_{M<n\leq M+N} \chi(n+h) + \sum_{M<n\leq M+h} \chi(n) - \sum_{M+N<n\leq M+N+h} \chi(n).$$

Therefore

$$S_\chi(M,N) = \sum_{M<n\leq N+M} \chi(n+h) + 2\theta E(h),$$

where $|\theta| \leq 1$ and $E(h) = \max_K |S_\chi(K,h)|$.

Let A and B be positive reals and let $H = \lfloor A \rfloor \lfloor B \rfloor$. We will use shifts of length $h = ab$ where a and b are positive integers satisfying $a \leq A$ and $b \leq B$. After averaging over all the pairs (a, b) we get

$$S_\chi(N, M) = \frac{1}{H} \sum_{a,b} \sum_{M < n \leq M+N} (\chi(n + ab) + 2\theta E(ab)) . \tag{6.23}$$

Let $v(x)$ be defined as in (6.1), then

$$\left| \sum_{a,b} \sum_{M < n \leq M+N} \chi(n + ab) \right| \leq \sum_{x \pmod p} v(x) \left| \sum_{b \leq B} \chi(x + b) \right| . \tag{6.24}$$

Let

$$V := \sum_{x \pmod p} v(x) \left| \sum_{b \leq B} \chi(x + b) \right| ,$$

then, combining (6.23) with (6.24), we get

$$|S_\chi(N, M)| \leq \frac{V}{H} + \frac{2}{H} \sum_{a,b} E(ab). \tag{6.25}$$

We can now focus on estimating V. Now define $V_1 := \sum_{x \pmod p} v(x)$, $V_2 := \sum_{x \pmod p} v^2(x)$ and $W := \sum_{x \pmod p} \Big| \sum_{1 \leq b \leq B} \chi(x + b) \Big|^{2r}$. Using Hölder's Inequality we get

$$V \leq V_1^{1-\frac{1}{r}} V_2^{\frac{1}{2r}} W^{\frac{1}{2r}}. \tag{6.26}$$

First note that

$$V_1 = \lfloor A \rfloor N \leq AN.$$

From Lemma 6.1, for $\lfloor A \rfloor \geq 28$ and $\lfloor A \rfloor < \frac{N}{12}$, we have

$$V_2 \leq 2AN\left(\frac{AN}{p} + \log(1.85A)\right). \tag{6.27}$$

We can also bound W, since we dealt with it in Chapter 4, in particular, from Theorem 4.2, we have (for $r \leq 9B$):

$$W \leq \frac{(2r)!}{2^r r!}B^r p + (2r-1)B^{2r}\sqrt{p} = (2r-1)!!B^r p + (2r-1)B^{2r}\sqrt{p}, \tag{6.28}$$

where $(2r-1)!! := (2r-1)(2r-3)\dots(3)(1)$.

Let's head back to proving the Burgess bound. We will let $AB = kN$ for k a real number to be chosen later. Using the inequalities of V_1, V_2 and W together with (6.26) yields the following bound upper bound for $\frac{V}{H}$:

$$\begin{aligned}\frac{V}{H} &\leq \frac{1}{\lfloor A \rfloor \lfloor B \rfloor} V_1^{1-\frac{1}{r}} V_2^{\frac{1}{2r}} W^{\frac{1}{2r}} \leq \frac{\frac{AB}{\lfloor A \rfloor \lfloor B \rfloor}}{(AB)^{\frac{1}{2r}}} \cdot \frac{(2WB)^{\frac{1}{2r}}}{B}\left(\frac{AN}{p} + \log(1.85A)\right)^{\frac{1}{2r}} N^{1-\frac{1}{2r}} \\ &\leq \frac{A}{A-1} \cdot \frac{B}{B-1} \cdot \frac{1}{k^{\frac{1}{2r}}} \cdot \frac{(2WB)^{\frac{1}{2r}}}{B}\left(\frac{AN}{p} + \log(1.85A)\right)^{\frac{1}{2r}} N^{1-\frac{1}{r}}. \end{aligned} \tag{6.29}$$

Because of (6.29) we can see that a good choice for B is the one that minimizes $\frac{WB}{B^{2r}}$. Using (6.28), we seek to minimize the expression $(2r-1)!!\frac{p}{B^{r-1}} + (2r-1)Bp^{\frac{1}{2}}$. We take the derivative with respect to B and equal it to zero. After this process we get that a good B is

$$B = \left((2r-3)!!(r-1)\right)^{\frac{1}{r}} p^{\frac{1}{2r}}. \tag{6.30}$$

Using this value of B we get

$$\frac{(2WB)^{\frac{1}{2r}}}{B} \leq \left(\frac{2r(2r-1)}{r-1}\right)^{\frac{1}{2r}} (r-1)^{\frac{1}{2r^2}} \big((2r-3)!!\big)^{\frac{1}{2r^2}} p^{\frac{r+1}{4r^2}}. \tag{6.31}$$

Now we must try to bound $\frac{AN}{p} + \log(1.85A)$. To do this, we can use the Pólya–Vinogradov inequality to give an upper bound for N, since for N large, the Pólya–Vinogradov inequality would be a better bound than the Burgess inequality. Indeed, if

$$N \geq p^{\frac{1}{2}+\frac{1}{4r}} \log p, \tag{6.32}$$

then, since $c_1(r) \geq 1$, we have

$$c_1(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}} \geq \sqrt{p} \log p.$$

Therefore, from the Pólya–Vinogradov inequality (see section 9.4 in [29]) we can conclude that $|S_\chi(M,N)| \leq c_1(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} \log p^{\frac{1}{r}}$, whenever we have (6.32).

If we have $r \geq 3$, then we can use the Burgess inequality with $r-1$ instead of the Pólya–Vinogradov inequality, to get a better upper bound on N. Indeed, if we assume that $c_1(r-1) \leq s^{\frac{1}{r(r-1)}} c_1(r)$, where s is a real number, then if

$$N \geq s\, p^{\frac{1}{4}+\frac{1}{2r}+\frac{1}{4r(r-1)}} \log p,$$

then

$$c_1(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}} \geq c_1(r-1) N^{1-\frac{1}{r-1}} p^{\frac{r}{4(r-1)^2}} (\log p)^{\frac{1}{r-1}}.$$

Similarly, we can put a lower bound on N, by noting that $|S_\chi(M,N)| \leq N$.

Indeed,

$$c_1(r)N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{r}} \geq N,$$

whenever

$$N \leq c_1(r)^r p^{\frac{1}{4}+\frac{1}{4r}} \log p.$$

Therefore, we may assume that

$$c_1(2)^2 p^{\frac{3}{8}} \log p < N < p^{\frac{5}{8}} \log p, \tag{6.33}$$

for $r = 2$, and that

$$c_1(r)^r p^{\frac{1}{4}+\frac{1}{4r}} \log p < N < s\, p^{\frac{1}{4}+\frac{1}{2r}+\frac{1}{4r(r-1)}} \log p, \tag{6.34}$$

for $r \geq 3$.

Using that $A = \frac{kN}{B}$, the upper bound for N in (6.33), and (6.30), we get

$$\frac{AN}{p} = \frac{kN^2}{pB} \leq \frac{kp^{\frac{5}{4}} \log^2 p}{pB} \leq k \log^2 p, \tag{6.35}$$

for $r = 2$, and for $r \geq 3$, we get

$$\frac{AN}{p} = \frac{kN^2}{pB} \leq \frac{s^2 k p^{\frac{1}{2}+\frac{1}{r}+\frac{1}{2r(r-1)}} \log^2 p}{pB} \leq \frac{s^2 k}{((2r-3)!!(r-1))^{\frac{1}{r}}\, p^{\frac{1}{2}-\frac{1}{2r}-\frac{1}{2r(r-1)}}} \log^2 p, \tag{6.36}$$

Now we consider what happens to $\log(1.85A)$.

$$\log(1.85A) = \log\left(\frac{1.85kN}{B}\right) \leq \log(1.85k \log p) + \frac{3\log p}{8}, \tag{6.37}$$

for $r = 2$, and for $r \geq 3$, we get

$$\log(1.85A) = \log\left(\frac{1.85kN}{B}\right) \leq \log\left(\frac{1.85s\,k\log p}{((2r-3)!!(r-1))^{\frac{1}{r}}}\right) + \frac{\log p}{4} + \frac{\log p}{4r(r-1)}. \tag{6.38}$$

Now, let's bound the error term, the part we have labeled as $E(h)$.

For any a, b such that $ab = h < N$, we have by induction hypothesis $E(h) \leq c_1(r)(ab)^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}$. Therefore,

$$\begin{aligned}
\frac{1}{c_1(r)p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{r}}} \cdot \frac{2}{H}\sum_{a,b} E(ab) &\leq \frac{2}{\lfloor A\rfloor\lfloor B\rfloor}\sum_{1\leq a\leq A}\sum_{1\leq b\leq B}(ab)^{1-\frac{1}{r}} \\
&\leq 2\frac{1}{AB}\left(1+\int_1^A t^{1-\frac{1}{r}}\,dt\right)\left(1+\int_1^B t^{1-\frac{1}{r}}\,dt\right)\frac{AB}{(A-1)(B-1)} \\
&\leq (AB)^{1-\frac{1}{r}}\frac{2}{(2-\frac{1}{r})^2}\left(1+\frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}}+\frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}}+\frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}}\right)\frac{AB}{(A-1)(B-1)} \\
&= \frac{2r^2}{(2r-1)^2}k^{1-\frac{1}{r}}N^{1-\frac{1}{r}}\left(1+\frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}}+\frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}}+\frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}}\right)\frac{AB}{(A-1)(B-1)}.
\end{aligned} \tag{6.39}$$

Combining equations (6.29), (6.31), (6.35), (6.37) and (6.39) with (6.25) yields (for $r = 2$)

$$\begin{aligned}
\frac{|S_\chi(N,M)|}{N^{\frac{1}{2}}p^{\frac{3}{16}}(\log p)^{\frac{1}{2}}} \leq \frac{AB}{(A-1)(B-1)}(12)^{\frac{1}{4}}&\left(1+\frac{3}{8k\log p}+\frac{\log(1.85k\log p)}{k\log^2 p}\right)^{\frac{1}{4}} \\
&+\frac{8}{9}k^{\frac{1}{2}}c_1(2)\left(1+\frac{1}{2A^{\frac{3}{2}}}+\frac{1}{2B^{\frac{3}{2}}}+\frac{1}{4(AB)^{\frac{3}{2}}}\right)\frac{AB}{(A-1)(B-1)}.
\end{aligned} \tag{6.40}$$

Similarly, for $r \geq 3$, combining equations (6.29), (6.31), (6.36), (6.38) and (6.39) with (6.25) yields

$$\frac{|S_\chi(N,M)|}{N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{r}}} \leq \left(\frac{2r(2r-1)}{r-1}\right)^{\frac{1}{2r}} \left((2r-3)!!(r-1)\right)^{\frac{1}{2r^2}} \frac{AB}{(A-1)(B-1)}$$
$$\left(\frac{s^2}{((2r-3)!!(r-1))^{\frac{1}{r}}p^{\frac{r-2}{2(r-1)}}} + \frac{1}{4k\log p} + \frac{1}{4r(r-1)k\log p} + \frac{\log\left(\frac{1.85s\,k\log p}{((2r-3)!!(r-1))^{\frac{1}{r}}}\right)}{k\log^2 p}\right)^{\frac{1}{2r}}$$
$$+ \frac{2r^2}{(2r-1)^2}k^{1-\frac{1}{r}}c_1(r)\left(1+\frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}}+\frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}}+\frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}}\right)\frac{AB}{(A-1)(B-1)}. \quad (6.41)$$

Now, if we let $c_1(r)$ be defined as follows

$$c_1(2) = \frac{AB}{(A-1)(B-1)}(12)^{\frac{1}{4}} \frac{\left(1+\frac{3}{8k\log p}+\frac{\log(3.7k\log p)}{k\log^2 p}\right)^{\frac{1}{4}}}{1-\frac{8}{9}k^{\frac{1}{2}}\left(1+\frac{1}{2A^{\frac{3}{2}}}+\frac{1}{2B^{\frac{3}{2}}}+\frac{1}{4(AB)^{\frac{3}{2}}}\right)}, \quad (6.42)$$

for $r = 2$, and

$$c_1(r) = \frac{AB}{(A-1)(B-1)}\left(\frac{2r(2r-1)\left((2r-3)!!(r-1)\right)^{\frac{1}{r}}}{r-1}\right)^{\frac{1}{2r}}$$
$$\cdot \frac{\left(\frac{s^2}{((2r-3)!!(r-1))^{\frac{1}{r}}p^{\frac{1}{2}-\frac{1}{2r}-\frac{1}{2r(r-1)}}} + \frac{1}{4k\log p} + \frac{1}{4r(r-1)k\log p} + \frac{\log\left(\frac{1.85s\,k\log p}{((2r-3)!!(r-1))^{\frac{1}{r}}}\right)}{k\log^2 p}\right)^{\frac{1}{2r}}}{1-\frac{2r^2}{(2r-1)^2}k^{1-\frac{1}{r}}\left(1+\frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}}+\frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}}+\frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}}\right)}, \quad (6.43)$$

for $r \geq 3$. Therefore from (6.40) and (6.41), we get that

$$|S_\chi(M,N)| \leq c_1(r)N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{r}}.$$

All we have to do is pick k to minimize $c_1(r)$ in such a way that $\lfloor A \rfloor \geq 28$, and

that $N \geq 12A$. First, we'll start by showing that

$$B \geq 15.$$

Since $B = ((2r-3)!!(r-1))^{\frac{1}{r}} p^{\frac{1}{2r}}$, we can just manually check for $2 \leq r \leq 20$ that the inequality is satisfied. To show that it works for $r \geq 21$, we can show that

$$((2r-3)!!(r-1))^{\frac{1}{r}} \geq 15, \tag{6.44}$$

by noticing that it works for $r = 21$ and that the left hand side of (6.44) is increasing. Indeed, the left hand side is increasing; by noticing that $(2r-3)(r-1) < (2r-1)(r+1)$, we get

$$(2r-3)!!(r-1) < \frac{(2r-1)^{r-1}(r+1)^{r-1}}{(r-1)^{r-2}} < \frac{(2r-1)^r(r+1)^r}{(r-1)^r},$$

implying that

$$\frac{1}{r}\log\left((2r-3)!!(r-1)\right) < \log\left((2r-1)(r+1)\right) - \log\left(r-1\right),$$

which implies

$$\frac{r+1}{r}\log\left((2r-3)!!(r-1)\right) < \log\left((2r-1)!!\right) + \log\left(r+1\right),$$

and hence

$$\log\left(((2r-3)!!(r-1))^{\frac{1}{r}}\right) < \log\left(((2r-1)!!)(r+1)\right)^{\frac{1}{r+1}}\Big).$$

r	$p \geq 10^7$	$p \geq 10^{10}$	$p \geq 10^{20}$
2	2.26242	1.22920	0.20612
3	1.68121	1.01700	0.22461
4	1.48333	0.98150	0.28047
5	1.38599	0.97900	0.33930
6	1.32751	0.98413	0.39415
7	1.28789	0.99064	0.44339
8	1.25889	0.99677	0.48700
9	1.23649	1.00209	0.52547
10	1.21852	1.00656	0.55942

Table 6.5: Lower bounds for the constant $c_1(r)$ in the Burgess inequality to satisfy $\lfloor A \rfloor \geq 28$.

Using that $B \geq 15$, since $A = \frac{kN}{B}$, then

$$A = \frac{kN}{B} < \frac{kN}{12} < \frac{N}{12},$$

whenever $k < 1$.

Let $k \geq \frac{3}{64}$. To check that $\lfloor A \rfloor \geq 28$, we use (6.34) and we note that

$$\lfloor A \rfloor \geq A - 1 \geq \frac{3N}{64B} - 1 \geq \frac{3c_1(r)^r p^{\frac{1}{4}-\frac{1}{4r}} \log p}{64((2r-3)!!(r-1))^{\frac{1}{r}}} - 1.$$

Table 6.5 shows the lower bound $c_1(r)$ must satisfy to have $\lfloor A \rfloor \geq 28$ in different situations.

We can now find a good value of $k \in [\frac{3}{64}, 1)$ and a good value of s for each r and p_0, and plug in the values of B, k and a lower bound for A on (6.42) to find $c_1(2)$ and on (6.43) to find $c_1(r)$ for $r \geq 3$ in Table 6.3 and conclude the theorem. The values of k and s we chose can be found on Table 6.6.

□

	$p_0 = 10^7$		$p_0 = 10^{10}$		$p_0 = 10^{20}$	
r	k	s	k	s	k	s
2	3/64	NA	3/64	NA	3/64	NA
3	1/16	6	3/64	10	7/64	29
4	1/16	6	3/32	7	1/8	2
5	3/32	4	7/64	3	7/64	2
6	7/64	4	1/8	2	3/32	2
7	7/64	4	3/32	3	3/32	2
8	3/32	4	5/64	3	5/64	2
9	3/32	5	5/64	3	5/64	2
10	7/64	5	3/32	3	1/16	2

Table 6.6: Values chosen for k and s to build Table 6.3.

Proof of Corollary 6.1. We begin by pointing out that Theorem 6.5 proves this for $2 \leq r \leq 10$ and $p \geq 10^7$. We also know that it is true for the $r = 1$ case by the Pólya–Vinogradov inequality.

Following the proof of Theorem 6.5, we also have that $B \geq 15$ for all r and hence, for any $k < 1$, we have $A < \frac{N}{12}$. It is also worth pointing out that we can use $s = 1$, since now the constant 2.71 is fixed as the constant in our upper bound, instead of a constant depending on r.

We need to show that you can pick a k such that $\lfloor A \rfloor \geq 28$. First, let's prove that $2.71^r \geq ((2r-3)!!(r-1))^{\frac{1}{r}}$. Indeed, for all $r \geq 1$ we have

$$2.71^r > 2r \geq ((2r-3)!!(r-1))^{\frac{1}{r}}.$$

Now we have

$$A = \frac{kN}{B} \geq \frac{k(2.71)^r p^{\frac{1}{4}-\frac{1}{4r}} \log p}{((2r-3)!!(r-1))^{\frac{1}{r}}} \geq k p^{\frac{1}{4}-\frac{1}{4r}} \log p > 29,$$

whenever $k > \frac{29}{p^{\frac{1}{4}-\frac{1}{4r}}\log p}$.

Looking at (6.43), we can see that the only factors that don't decrease with r are the $k^{1-\frac{1}{r}}$ term which appears in the denominator, and the $\left(1-\frac{1}{r}\right)$ factors in the denominator. With this in mind, let $c(r)$ be defined as follows for $r \geq 3$:

$$c(r) = \frac{15A}{14(A-1)}\left(\frac{2r(2r-1)\left((2r-3)!!(r-1)\right)^{\frac{1}{r}}}{r-1}\right)^{\frac{1}{2r}} \cdot \frac{\left(\frac{1}{((2r-3)!!(r-1))^{\frac{1}{r}}p^{\frac{1}{2}-\frac{1}{2r}-\frac{1}{2r(r-1)}}} + \frac{1}{4k\log p} + \frac{1}{4r(r-1)k\log p} + \frac{\log\left(\frac{1.85\,k\log p}{((2r-3)!!(r-1))^{\frac{1}{r}}}\right)}{k\log^2 p}\right)^{\frac{1}{2r}}}{1-\frac{2r^2}{(2r-1)^2}k\left(1+\frac{1}{A^{2-\frac{1}{r}}}+\frac{1}{(15)^{2-\frac{1}{r}}}+\frac{1}{(15A)^{2-\frac{1}{r}}}\right)}. \quad (6.45)$$

Letting $k = \frac{9}{64}$, $A \geq kp^{\frac{1}{4}-\frac{1}{4r}}$ and $p \geq 10^7$ we confirm that $c(r) \leq 2.71$ whenever $r \geq 3$. Since it is also true for $r \leq 2$, we conclude our corollary.

□

6.3 Extending Booker's theorem

The main obstacle in improving the $(\log p)^{\frac{1}{r}}$ factor in the Burgess inequality is the bound on V_2. However, if we put a bound on N, we can make the proof cleaner while also improving the exponent in $\log p$ to $\frac{1}{2r}$. First we prove a lemma regarding V_2 and then we will be able to prove Theorem 6.6.

Lemma 6.5. *Let p be a prime, and N be a positive integer. Let $A \geq 30$ be an integer*

such that $N > 7A$ and $2AN < p$. Let $v(x)$ be defined as in (6.1)*, then*

$$V_2 = \sum_{x \mod p} v^2(x) \leq 2AN \log(1.85A).$$

Proof. The proof is essentially the same as that of Lemma 6.1. Recall that V_2 is the number of quadruples (a_1, a_2, n_1, n_2) with $1 \leq a_1, a_2 \leq A$ and $M < n_1, n_2 \leq M + N$ such that $a_1 n_2 \equiv a_2 n_1 \pmod{p}$. If $a_1 = a_2$, since $N < p$, we have that $n_1 = n_2$ because $n_1 \equiv n_2 \pmod{p}$ while $|n_1 - n_2| \leq N < p$. Therefore, the number of quadruples in this case is AN. Fixing $a_1 \neq a_2$ and writing

$$a_1 n_2 - a_2 n_1 = kp,$$

we can put a bound on possible values for k. As shown in the proof of Lemma 6.1, there are at most $\frac{(a_1+a_2)N}{\gcd(a_1,a_2)p} + 1$ values of k. Since $2AN < p$, then we have that k is uniquely determined.

In the proof of Lemma 6.1, we showed that given a_1, a_2 and k, the number of pairs (n_1, n_2) is bounded by $N\frac{\gcd(a_1,a_2)}{\max\{a_1,a_2\}} + 1$.

Now, for $A \geq 30$ and $N > 7A$ we have

$$\left(1 - \frac{6}{\pi^2}\right) \log(1.85A) \geq \left(1 - \frac{6}{\pi^2}\right) \log(55.5) = 1.57471 > \frac{3}{2} + \frac{1}{14} > \frac{3}{2} + \frac{A}{2N}. \quad (6.46)$$

Using the definition of S_3 as in (6.14), using the inequalities (6.17) and (6.46), for $A \geq 30$ and $N > 7A$, we have

$$V_2 \leq AN + 2 \sum_{a_1 < a_2} \left(\frac{\gcd(a_1, a_2)N}{\max\{a_1, a_2\}} + 1\right)$$

$$= AN + 2NS_3 + A^2 - A \leq 2AN \log(1.85A).$$

□

Now we are ready to prove Theorem 6.6.

Proof of Theorem 6.6. The proof is very similar to the proof of Theorem 6.5. We proceed by induction, assuming that for all $h < N$ we have $|S_\chi(M,h)| \leq c_2(r)p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}}$.

Most of the work in the proof of Theorem 6.6 can be replicated. So I'll just point out the things that change.

The first change is that by employing Lemma 6.5, (6.27) becomes

$$V_2 \leq 2AN \log(1.85A).$$

This change affects (6.29), by deleting $\frac{AN}{p}$ inside the parenthesis. Now it looks as follows:

$$\frac{V}{H} \leq \frac{AB}{(A-1)(B-1)} \frac{1}{k^{\frac{1}{2r}}} \frac{(2WB)^{\frac{1}{2r}}}{B} (\log(1.85A))^{\frac{1}{2r}} N^{1-\frac{1}{r}}. \tag{6.47}$$

The next change is the range for N, which we deduced by using the Pólya–Vinogradov inequality, the trivial bound, and the case for $r-1$. Instead of (6.33), using our hypothesis and the trivial bound, we now have

$$c_2(2)^r p^{\frac{3}{8}} \sqrt{\log p} < N < 2p^{\frac{5}{8}}, \tag{6.48}$$

for $r = 2$. Assuming $c_2(r-1) \leq s^{\frac{1}{r(r-1)}} c_2(r)$ for a real number s, and using the

Burgess inequality for $r-1$ we have, for $r \geq 3$, the following range for N

$$c_2(r)^r p^{\frac{1}{4}+\frac{1}{4r}} \sqrt{\log p} < N < \min\{2p^{\frac{1}{2}+\frac{1}{4r}}, s\, p^{\frac{1}{4}+\frac{1}{2r}+\frac{1}{4r(r-1)}} \sqrt{\log p}\}. \tag{6.49}$$

Using that $A = \frac{kN}{B}$ and (6.48), we get

$$\log(1.85A) = \log\left(\frac{1.85kN}{B}\right) \leq \log(3.7k) + \frac{3\log p}{8}, \tag{6.50}$$

for $r = 2$. Using (6.49), yields

$$\log(1.85A) = \log\left(\frac{1.85kN}{B}\right) \leq \log\left(\frac{1.85s\, k\sqrt{\log p}}{((2r-3)!!(r-1))^{\frac{1}{r}}}\right) + \frac{\log p}{4} + \frac{\log p}{4r(r-1)}, \tag{6.51}$$

for $r \geq 3$.

The bound for $E(h)$ is almost the same as in (6.39), the only difference being the exponent of $\log p$, which is now $\frac{1}{2r}$ instead of $\frac{1}{r}$. Making this change and using both (6.31) and (6.50) with (6.47) yields (for $r = 2$)

$$\begin{aligned}\frac{|S_\chi(M,N)|}{N^{\frac{1}{2}} p^{\frac{3}{16}} (\log p)^{\frac{1}{4}}} \leq{}& \frac{AB}{(A-1)(B-1)} (12)^{\frac{1}{4}} \left(\frac{\log(3.7k)}{k\log p} + \frac{3}{8k}\right)^{\frac{1}{4}} \\ &+ \frac{AB}{(A-1)(B-1)} \frac{8}{9} k^{\frac{1}{2}} c_2(2) \left(1 + \frac{1}{2A^{\frac{3}{2}}} + \frac{1}{2B^{\frac{3}{2}}} + \frac{1}{4(AB)^{\frac{3}{2}}}\right).\end{aligned} \tag{6.52}$$

For $r \geq 3$, using (6.31) and (6.51) with (6.47) yields

$$\frac{|S_\chi(M,N)|}{N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}} \leq \frac{AB}{(A-1)(B-1)} \left(\frac{2r(2r-1)\left((2r-3)!!(r-1)\right)^{\frac{1}{r}}}{r-1}\right)^{\frac{1}{2r}}$$

$$\cdot \left(\frac{\log\left(\frac{1.85s\, k\sqrt{\log p}}{((2r-3)!!(r-1))^{\frac{1}{r}}} \right)}{k \log p} + \frac{1}{4k} + \frac{1}{4r(r-1)k} \right)^{\frac{1}{2r}}$$

$$+ \frac{AB}{(A-1)(B-1)} \frac{2r^2}{(2r-1)^2} k^{1-\frac{1}{r}} c_2(r) \left(1 + \frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}} + \frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}} + \frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}} \right). \quad (6.53)$$

Now, if we let $c_2(r)$ be defined as follows

$$c_2(2) = \frac{A}{A-1} \frac{B}{B-1} \frac{(12)^{\frac{1}{4}} \left(\frac{\log(3.7k)}{k \log p} + \frac{3}{8k} \right)^{\frac{1}{4}}}{1 - \frac{8}{9} k^{\frac{1}{2}} \left(1 + \frac{1}{2A^{\frac{3}{2}}} + \frac{1}{2B^{\frac{3}{2}}} + \frac{1}{4(AB)^{\frac{3}{2}}} \right)}, \quad (6.54)$$

and, for $r \geq 3$,

$$c_2(r) = \frac{A}{A-1} \frac{B}{B-1} \frac{\left(\frac{2r(2r-1)((2r-3)!!(r-1))^{\frac{1}{r}}}{r-1} \left(\frac{\log\left(\frac{1.85s\, k\sqrt{\log p}}{((2r-3)!!(r-1))^{\frac{1}{r}}} \right)}{k \log p} + \frac{1}{4k} + \frac{1}{4r(r-1)k} \right) \right)^{\frac{1}{2r}}}{1 - \frac{2r^2}{(2r-1)^2} k^{1-\frac{1}{r}} \left(1 + \frac{1-\frac{1}{r}}{A^{2-\frac{1}{r}}} + \frac{1-\frac{1}{r}}{B^{2-\frac{1}{r}}} + \frac{\left(1-\frac{1}{r}\right)^2}{(AB)^{2-\frac{1}{r}}} \right)}, \quad (6.55)$$

for $r \geq 3$. Then, from (6.52) and (6.53), we get that

$$|S_\chi(M,N)| \leq c_2(r) N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}.$$

All we have to do is pick k to minimize $c_2(r)$ in such a way that $\lfloor A \rfloor \geq 30$, that $N > 7A$ and $2AN < p$.

Using that $B \geq 15$, it is not hard to check that $N \geq 7A$. Indeed, since $A = \frac{kN}{B}$, we have $A \leq \frac{kN}{15} < \frac{N}{7}$.

To check that $\lfloor A \rfloor \geq 30$ for $k \geq 3$, we do the following:

$$\lfloor A \rfloor \geq A - 1 \geq \frac{3N}{64B} - 1 \geq \frac{3c_2(r)^r p^{\frac{1}{4}-\frac{1}{4r}}\sqrt{\log p}}{64((2r-3)!!(r-1))^{\frac{1}{r}}} - 1.$$

Table 6.7 shows the lower bound c must satisfy to have $\lfloor A \rfloor \geq 30$ in different situations.

r	$p \geq 10^{10}$	$p \geq 10^{15}$	$p \geq 10^{20}$
2	2.78392	1.22500	0.55514
3	1.75393	0.86474	0.43480
4	1.47708	0.81850	0.46029
5	1.35767	0.82260	0.50431
6	1.29240	0.83775	0.54839
7	1.25127	0.85450	0.58848
8	1.22279	0.87022	0.62388
9	1.20171	0.88422	0.65489
10	1.18536	0.89649	0.68202

Table 6.7: Lower bounds for the constant $c_2(r)$ in the Burgess inequality to satisfy $\lfloor A \rfloor \geq 30$.

Let's now verify that $2AN < p$. Indeed, from the fact that $A = \frac{kN}{B}$ and from (6.48), we have

$$2AN = \frac{2kN^2}{B} \leq \frac{8kp}{((2r-3)!!(r-1))^{\frac{1}{r}}} < p,$$

whenever $k < \min\left\{\frac{((2r-3)!!(r-1))^{\frac{1}{r}}}{8}, 1\right\}$.

We can now find a good value of $k \in [\frac{3}{64}, \frac{((2r-3)!!(r-1))^{\frac{1}{r}}}{8})$ and a good value of s for each r and p_0, and plug in the values of B, k, and a lower bound bound for A on (6.54) to find $c_2(2)$ and on (6.55) to find $c_2(r)$ for $r \geq 3$ in Table 6.4 and conclude the theorem. The values of k and s we chose can be found on Table 6.8.

□

	$p_0 = 10^{10}$		$p_0 = 10^{15}$		$p_0 = 10^{20}$	
r	k	s	k	s	k	s
2	1/8	NA	1/8	NA	1/8	NA
3	9/64	8	9/64	8	9/64	9
4	1/8	8	1/8	8	1/8	8
5	7/64	8	7/64	8	7/64	8
6	3/32	9	3/32	9	1/8	8
7	3/32	10	3/32	9	1/8	9
8	3/32	11	7/64	9	3/32	12
9	1/16	13	7/64	10	3/32	12
10	1/16	16	7/64	12	3/32	12

Table 6.8: Values chosen for k and s to build Table 6.4.

Proof of Corollary 6.2. By Theorem 6.6, we have our desired result whenever $N < 2p^{\frac{1}{2}+\frac{1}{4r}}$. Therefore, the only thing we need to prove is that for $p \geq 10^{10}$ and $r \geq 3$, $N < 2p^{\frac{1}{2}+\frac{1}{4r}}$. Since the induction in the proof of Theorem 6.6 relied on the upper bound for N, we can't use the Burgess inequalities in Theorem 6.6 to give an upper bound for N in this corollary. However, we can use the Burgess inequalities from Theorem 6.5 to improve the upper bound for N. Indeed, for $p \geq 10^{10}$, we have

$$|S_\chi(M,N)| \leq 2.6N^{1-\frac{1}{2}}p^{\frac{3}{16}}(\log p)^{\frac{1}{2}}.$$

If

$$N \geq (2.6)^{\frac{2r}{r-1}}p^{\frac{3}{8}-\frac{1}{8r}-\frac{3}{8r(r-1)}}\sqrt{\log p},$$

then

$$N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}} \geq 2.6N^{1-\frac{1}{2}}p^{\frac{3}{16}}\sqrt{\log p} \geq |S_\chi(M,N)|.$$

Therefore, we may assume that

$$N \leq (2.6)^{\frac{2r}{r-1}} p^{\frac{3}{8}-\frac{1}{8r}-\frac{3}{8r(r-1)}} \sqrt{\log p}. \tag{6.56}$$

Now, all we need to conclude is to show that the right hand side of (6.56) is less than $2p^{\frac{1}{2}+\frac{1}{4r}}$. Using that $p \geq 10^{10}$, we can verify this manually for $r \in \{3, 4, \ldots, 21\}$. Now, for $r \geq 22$ we have

$$N \leq (2.6)^{\frac{2r}{r-1}} p^{\frac{3}{8}-\frac{1}{8r}-\frac{3}{8r(r-1)}} \sqrt{\log p} \leq (2.6)^{\frac{44}{21}} p^{\frac{3}{8}} \sqrt{\log p} < 2p^{\frac{1}{2}}.$$

The last inequality is true whenever $p \geq 10^{10}$. □

Appendix A

In this Appendix we will discuss the computer code written to answer some of the questions in the thesis. All of the code was written in Mathematica. Mathematica is not a very useful language when it comes to loops, but it has many arithmetic functions already written and it works great as a calculator. One function that was very useful in Mathematica to help check for optimal constants was the function

`Manipulate[]` .

Tables 4.2, 4.4, 4.3 and 5.2 were all created quickly thanks to the versatility of the function. In section A.1 we will go into more detail regarding the code created for Chapter 3. The other chapters did not need any special computer programming.

A.1 Computer code for the least inert prime in a real quadratic field

To determine the examples where the inequality of Theorem 3.2 fails, we use the following code to check whether an integer is a fundamental discriminant or not:

```
FundamentalDiscriminantQ[n_] :=
 n != 1 && Mod[n, 4] == 1 && SquareFreeQ[n] ||
  ! (Mod[n, 16] != 8 != 12) && SquareFreeQ[Quotient[n, 4]] .
```

Once, we have this defined, we use the following code to create a list with all the examples. It is very easy to change this code to be able to find the examples where the inequality of Theorem 3.1 fails, as we would only need to change (j^(0.45)) to (j^(0.5))/2.

```
listkiks = {};
Do[
 If[
  FundamentalDiscriminantQ[j],
  i = 1;
  While[KroneckerSymbol[j, Prime[i]] != -1, i++];
  If[Prime[i] > (j^(0.45)), Print[j]; listkiks = Append[listkiks, j],
   0],
  0
  ]
 , {j, 1, 380000}
 ]
listkiks .
```

The main code worth writing about is the one that was used to prove Theorem 3.5. In the proof of the theorem, we mention that there are 2^{13} cases, which are all the 41-smooth numbers. We therefore, create all the 41-smooth numbers as follows:

```
smoothG[x_] :=
 Do[If[i == 0, sm[1] = 1; sm[2] = 2,
   Do[sm[2^i + j] = sm[j]*Prime[i + 1], {j, 1, 2^i}]], {i, 0,
   PrimePi[x] - 1}];
smoothG[41] .
```

Note that sm$[i]$ is a 41-smooth number for $i \leq 2^{13}$. Now, we also need to keep track of the number fdo$[i]$ of prime factors for sm$[i]$. We use the following code:

```
fundDiscomega[x_] :=
 Do[If[i == 0, fdo[1] = 0; fdo[2] = 1,
   Do[fdo[2^i + j] = fdo[j] + 1, {j, 1, 2^i}]], {i, 0,
   PrimePi[x] - 1}];
fundDiscomega[41] .
```

We will also need to code the product of consecutive primes, which we do as follows

```
pprod2[v_, k_] := Product[Prime[i],{i,k,v}] .
```

In the main code, we need to define $A_2(D_v(m), m, \omega, u, D_1, D_2)$, which we will call A3[ ]. A3[ ] will have more parameters than A_2; in particular c, c_1, c_2, a and k will be left as variables, where c is the constant we pick for $N = c\sqrt{D}$ (in the proof of the Theorem we used $c = 7.8$), c_1 and c_2 are the constants from Table 3.1, a is defined as $\log B / \log D$ and $k - 1$ is the number of primes which we sieve. In the proof we used 13 primes (since 41 is the 13-th prime). We leave the c, c_1, c_2, a and k variable to be able to experiment with different settings, to find the optimal solution.

```
A3[c_, a_, D1_, D2_, j_, k_, t_, n_, c1_, c2_] :=
 c (1 - 2^(n - 1) Sqrt[D1]/EulerPhi[D1]) - 1 -
  2^(n - 2) Sqrt[D1]/EulerPhi[D1] -
  2 (D1/EulerPhi[D1]) (Sum[
     If[GCD[i, sm[j]] == 1, G[i, c, a, D1, D2, c1, c2], 0], {i,
      1, 2 c (t)^(1/2 - a)}]) .
```

The function A3[ ] uses the function G[ ] which is defined in Claim 3.3. The code for G[ ] in Mathematica is:

```
G[n_, c_, a_, D1_, D2_, c1_, c2_] :=
 If[
  n > c *D2^(1/2 - a),
  c/(2*n* Log[c *Sqrt[D1]/n]) + (c*
      f[c *Sqrt[D1], n, c1, c2])/(n*(Log[c* Sqrt[D1]/n])^2),
  If[
   n <= c*D1^(1/2 - a),
   c/(n *Log[c*Sqrt[D1]/n]) + (f[c*Sqrt[D1], n, c1, c2] + c2)*
     c/(n*(Log[c *Sqrt[D1]/n])^2) -
    c1* n/(c *(D2^(1 - 2 a))* (Log[D2^(a)])^2) -
    n/(2*c*( D2^(1 - 2 a))* Log[D2^(a)]),
   Max[c/(2*n* Log[c *Sqrt[D1]/n]) + (c*
        f[c *Sqrt[D1], n, c1, c2])/(n*(Log[c* Sqrt[D1]/n])^2),
    c/(n *Log[c*Sqrt[D1]/n]) + (f[c*Sqrt[D1], n, c1, c2] + c2)*
      c/(n*(Log[c *Sqrt[D1]/n])^2) -
     c1* n/(c *(D2^(1 - 2 a))* (Log[D2^(a)])^2) -
```

```
     n/(2*c*( D2^(1 - 2 a))* Log[D2^(a)])
    ]
   ]
  ] .
```

The function G[ ] uses the function f[ ], which is defined as in (3.30) and can be coded in Mathematica as follows:

```
f[N_, n_, c1_, c2_] :=
 c2 + Log[4] (Log[N/n]/Log[2 N/n]) - 4 c1 (Log[N/n]/Log[2 N/n])^2 .
```

We now have all the ingredients to be able to list the main code for the even cases:

```
AbsoluteTiming[
 max = 1;
 k = 14;
 a = .45;
 c1 = 0.239818;
 c2 = 0.29251;
 Do[
  If[j == 1, v = k, v = k - 1];
  While[
   A3[7.8, a, pprod2[v, k]*sm[j], pprod2[v + 1, k]*sm[j], j, k,
     pprod2[v + 1, k]*sm[j], v - 13 + fdo[j], c1, c2] < 0 ,
   v++
  ];
  temp = sm[j]*pprod2[v, k];
```

```
  While[
   pprod2[v + 1, k]*sm[j] < 10^(24),
   If[A3[7.8, a, pprod2[v, k]*sm[j], pprod2[v + 1, k]*sm[j], j, k,
       pprod2[v + 1, k]*sm[j], v - 13 + fdo[j], c1, c2] < 0 ,
    Print["No puede ser"], 0
   ];
   v++
  ];
  If[temp > max, max = temp; Print[j, " ", v, " ", N[max]], 0]
 , {j, 2, 2^(k - 1), 2}
 ]
] .
```

We conclude with the code for the odd cases:

```
AbsoluteTiming[
 max = 1;
 k = 14;
 a = .45;
 c1 = 0.239818;
 c2 = 0.29251;
 Do[
  If[j == 1, v = k, v = k - 1];
  While[
   A3[7.8, a, pprod2[v, k]*sm[j], pprod2[v + 1, k]*sm[j], j, k,
     pprod2[v + 1, k]*sm[j], fdo[j] + v - 13, c1, c2] < 0 ,
```

```
   v++
  ];
  temp = sm[j]*pprod2[v, k];
  While[
   pprod2[v + 1, k]*sm[j] < 10^(24),
   If[A3[7.8, a, pprod2[v, k]*sm[j], pprod2[v + 1, k]*sm[j], j, k,
       pprod2[v + 1, k]*sm[j], v - 13 + fdo[j], c1, c2] < 0 ,
    Print["No puede ser"], 0
   ];
   v++
  ];
  If[temp > max, max = temp; Print[j, " ", v, " ", N[max]], 0]
 , {j, 1, 2^(k - 1), 2}
 ]
] .
```

Bibliography

[1] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72. MR 0045159 (13,538c)

[2] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR 1023756 (91m:11096)

[3] Gennady Bachman and Leelanand Rachakonda, *On a problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality*, Ramanujan J. **5** (2001), no. 1, 65–71. MR 1829809 (2002c:11098)

[4] Andrew R. Booker, *Quadratic class numbers and character sums*, Math. Comp. **75** (2006), no. 255, 1481–1492 (electronic). MR 2219039 (2008a:11140)

[5] Alfred Brauer, *Über die Verteilung der Potenzreste*, Math. Z. **35** (1932), no. 1, 39–50. MR 1545287

[6] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192. MR 0132732 (24 #A2569)

[7] ———, *A note on the distribution of residues and non-residues*, J. London Math. Soc. **38** (1963), 253–256. MR 0148628 (26 #6135)

[8] ———, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR 0148626 (26 #6133)

[9] J. W. S. Cassels and R. C. Vaughan, *Obituary: Ivan Matveevich Vinogradov*, Bull. London Math. Soc. **17** (1985), no. 6, 584–600. MR 813744 (87d:01028)

[10] Richard Crandall and Carl Pomerance, *Prime numbers*, second ed., Springer, New York, 2005, A computational perspective. MR 2156291 (2006a:11005)

[11] Pierre Dusart, *Sharper bounds for ψ, θ, π, p_k, Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation*, 1998.

[12] Paul 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. MR 1950084 (2003j:11001)

[13] John Friedlander, *Primes in arithmetic progressions and related topics*, Analytic number theory and Diophantine problems (Stillwater, OK, 1984), Progr. Math., vol. 70, Birkhäuser Boston, Boston, MA, 1987, pp. 125–134. MR 1018373 (90h:11086)

[14] Leo I. Goldmakher, *Multiplicative mimicry and improvements of the Pólya–Vinogradov inequality*, ProQuest LLC, Ann Arbor, MI, 2009, Thesis (Ph.D.)–University of Michigan. MR 2713875

[15] Andrew Granville, R. A. Mollin, and H. C. Williams, *An upper bound on the least inert prime in a real quadratic field*, Canad. J. Math. **52** (2000), no. 2, 369–380. MR 1755783 (2001d:11123)

[16] Andrew Granville and K. Soundararajan, *Large character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. **20** (2007), no. 2, 357–384 (electronic). MR 2276774 (2007k:11128)

[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, at the Clarendon Press, 1954, 3rd ed. MR 0067125 (16,673c)

[18] Adolf Hildebrand, *On the constant in the Pólya-Vinogradov inequality*, Canad. Math. Bull. **31** (1988), no. 3, 347–352. MR 956367 (89k:11072)

[19] ———, *Introduction to analytic number theory lecture notes*, 2005.

[20] Loo-Keng Hua, *On the least primitive root of a prime*, Bull. Amer. Math. Soc. **48** (1942), 726–730. MR 0007399 (4,130e)

[21] Richard H. Hudson, *On the distribution of k-th power nonresidues*, Duke Math. J. **39** (1972), 85–88. MR 0291064 (45 #158)

[22] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR 2061214 (2005h:11005)

[23] M. Levin, C. Pomerance, and K. Soundararajan, *Fixed points for discrete logarithms*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, 2010, pp. 6–15.

[24] R. F. Lukes, C. D. Patterson, and H. C. Williams, *Some results on pseudosquares*, Math. Comp. **65** (1996), no. 213, 361–372, S25–S27. MR 1322892 (96e:11010)

[25] Kevin J. McGown, *Norm-Euclidean Galois fields*, arXiv:1011.4501v2, April. 14, 2011.

[26] ———, *On the constant in Burgess' bound for the number of consecutive reidues or non-residues*, arXiv:1011.4490v1, Nov. 19, 2010.

[27] Richard A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996. MR 1383823 (97e:11135)

[28] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), no. 1, 69–82. MR 0457371 (56 #15579)

[29] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR 2378655 (2009b:11001)

[30] L. Moser and R. A. MacLeod, *The error term for the squarefree integers*, Canad. Math. Bull. **9** (1966), 303–306. MR 0200251 (34 #150)

[31] Karl 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. MR 0286739 (44 #3948)

[32] ———, *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. MR 0332697 (48 #11023)

[33] ———, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78. MR 1623353 (99j:11096)

[34] R. E. A. C. Paley, *A theorem on characters*, J. Lond. Math. Soc. **7** (1932), 28–32.

[35] Paul Pollack, *Not always buried deep*, American Mathematical Society, Providence, RI, 2009, A second course in elementary number theory. MR 2555430 (2010i:11003)

[36] Carl Pomerance, *Remarks on the Pólya–Vinogradov inequality*, Integers (Proceedings of the Integers Conference, October 2009) **11A** (2011), Article 19, 11pp.

[37] Herbert Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29. MR 0069328 (16,1020e)

[38] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 0137689 (25 #1139)

[39] Wolfgang M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin, 1976. MR 0429733 (55 #2744)

[40] Lowell Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II*, Math. Comp. **30** (1976), no. 134, 337–360. MR 0457374 (56 #15581b)

[41] Mariusz Skałba, *On Euler-von Mangoldt's equation*, Colloq. Math. **69** (1995), no. 1, 143–145. MR 1341690 (96f:11149)

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

[43] Terence Tao, *A remark on partial sums involving the Möbius function*, Bull. Aust. Math. Soc. **81** (2010), no. 2, 343–349. MR 2609115

[44] Ivan Matveevič 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. MR 807530 (87a:01042)

[45] 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. MR 0246488 (39 #7792)

[46] Kjell Wooding, *The sieve problem in one- and two-dimensions*, 2010, Thesis (Ph.D.)–University of Calgary.