The least quadratic non-residue

Kevin McGown and Enrique Treviño

July 18, 2019

1 Introduction

The sequence 2, 5, 8, 11, ... contains no perfect squares. This is for the simple reason that $x^2 \equiv 0, 1 \bmod 3$. We say that 2 is a quadratic non-residue modulo 3. In general we say a is a *quadratic non-residue* modulo n if there is no x such that $\gcd(x, n) = 1$ and $x^2 \equiv a \bmod n$. If such an x exists and $\gcd(x, n) = 1$, then we say a is a *quadratic residue.* We will concentrate on the case where $n = p$ an odd prime number. (Throughout p will always denote an odd prime.) The Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if there exists } x \not\equiv 0 \bmod p \text{ such that } x^2 \equiv a \bmod p \\ -1 & \text{if there is no } x \text{ such that } x^2 \equiv a \bmod p \\ 0 & \text{if } x \equiv 0 \bmod p. \end{cases}$$

Notice that a is a quadratic non-residue modulo p if and only if $\left(\frac{a}{p}\right) = -1$.

Our main object of study in this paper is the following question: How large is the least quadratic non-residue modulo p? We will denote the least quadratic non-residue n_p. Our goal is to provide (in one place), the proofs of the main "classical" results on this problem and to survey the more recent explicit results. In section 2 we will describe the history and some heuristics on the size of n_p. In section 3 we will prove the Pólya–Vinogradov theorem. In section 4 we will give a clear and relatively short proof of an explicit Burgess inequality. In section 5 we will mention recent explicit results and we will include a couple of new theorems (Theorems 5.4 and 5.6) to showcase the techniques in the paper. In section 6, we will discuss a classical result of Linnik on n_p for most primes p. Finally, in section 7 we will prove an explicit version of a theorem of Ankeny under the Generalized Riemann Hypothesis.

2 History and Heuristics

Let's first try to get some intuition on how big n_p is. First note that n_p is always prime. This is because if $n_p = ab$ for $1 < a, b < n_p$, then since n_p is the least quadratic non-residue, that means a, b are quadratic residues, but then $m_1^2 \equiv a \bmod p$ and $m_2^2 \equiv b \bmod p$, so $(m_1 m_2)^2 \equiv ab = n_p \bmod p$. But that means n_p is a quadratic residue. Therefore, n_p is prime. Now, let's try to see how often $n_p = 2$ (the smallest prime). A famous result of Gauss is that 2 is a quadratic non-residue whenever $p \equiv 3, 5 \bmod 8$ and 2 is a quadratic residue whenever $p \equiv 1, 7 \bmod 8$. Since primes are equidistributed among the coprime residue classes (this is due to Dirichlet's theorem on primes in arithmetic progressions), then $n_p = 2$ half of the time. In other words if we let x be a real number and $\pi(x)$ is the number of primes less than or equal to x, then

$$\lim_{x\to\infty} \frac{|\{p \le x \,|\, n_p = 2\}|}{\pi(x)} = \frac{2}{4} = \frac{1}{2}.$$

Using quadratic reciprocity, we can see that $n_p = 3$, whenever $p \equiv 7, 17 \bmod 24$. There are 8 residue classes coprime with 24 and each of them has the same number of primes asymptotically (by Dirichlet's Theorem), so

$$\lim_{x\to\infty} \frac{|\{p \le x \,|\, n_p = 3\}|}{\pi(x)} = \frac{2}{8} = \frac{1}{4}.$$

Let $p_1 = 2, p_2 = 3, \ldots, p_k =$ the k-th prime, one can prove (using quadratic reciprocity, the Chinese remainder theorem, and Dirichlet's theorem) that

$$\lim_{x\to\infty} \frac{|\{p \le x \,|\, n_p = p_k\}|}{\pi(x)} = \frac{1}{2^k}.$$

The above suggests the following heuristic: Suppose that $k \approx \log_2 x$, then $\frac{1}{2^k} \approx \frac{1}{x}$. Therefore, the "expected number" of primes with $n_p = p_k$ is 1. If k is much larger, then we wouldn't expect any, and if k is smaller we would expect some. Therefore, it seems that n_p can be as large as $p_{\log_2 x}$ which is (by the Prime Number Theorem) asymptotically $\log_2 x \log\log x$. Table 1 contains the list of smallest primes p satisfying $n_p = p_k$, it also compares to $\log p \log\log p$ to see how good an estimate it is.[1]

The heuristic above suggests that $n_p \le C \log p \log\log p$ for some constant C. It also suggests that $n_p \ge C \log p \log\log p$ for infinitely many p (and some constant C). Evidence in the direction of these conjectures is that Graham and Ringrose [14], in 1990, proved that $n_p \ge C \log p \log\log\log p$ for infinitely many p and some constant C.[2] In fact, assuming the Generalized Riemann Hypothesis (GRH), Montgomery [33, Theorem 13.5], in 1971, proved precisely the lower bound heuristic, namely that $n_p \ge C \log p \log\log p$ for infinitely many p and some constant C. For the upper bound, assuming GRH, Ankeny [1], in 1952, proved $n_p \le C \log^2 p$ for some constant C. Bach [2], in 1985, made the constant explicit, showing $n_p \le 2 \log^2 p$. Finally in 2015, Lamzouri, Li and Soundararajan [21] improved this to $n_p \le \log^2 p$. However, we cannot prove anything remotely close to that upper bound unconditionally. The first breakthrough in getting a good upper bound for the least quadratic non-residue was done by Vinogradov in 1918 (see pages 53–57 of [50]). He came up with the following strategy using Dirichlet characters. For a positive integer q, a function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a Dirichlet character modulo q if

1. $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$, i.e., χ is completely multiplicative;

[1] Salié in 1965 [41], using a table just like the first two columns of Table 1 (but with one extra row), disproved two conjectures: that the first column is increasing and that all of its elements greater than 3 are $7 \bmod 8$.

[2] In 1949, Fridlender [12] and Salié [40], independently proved that $n_p \ge C \log p$ for some constant C.

p	n_p	$\log p \log\log p$
3	2	0.10
7	3	1.30
23	5	3.58
71	7	6.18
311	11	10.03
479	13	11.23
1559	17	14.67
5711	19	18.66
10559	23	20.63
18191	29	22.40
31391	31	24.20
422231	37	33.18
701399	41	40.00
366791	43	32.68
3818929	47	41.20

Table 1: The smallest primes p satisfying that $n_p = p_k$ for $k = 1, 2, \ldots, 15$, and a comparison with $\log p \log\log p$. It is worth noting that not all of the p in the table are 7 mod 8.

2. $\chi(n + kq) = \chi(n)$ for all $n, k \in \mathbb{Z}$, i.e., χ is periodic modulo q;
3. $\chi(n) = 0$ if and only if $(n, q) > 1$.

χ is called a Dirichlet character modulo q in honor of Dirichlet's introduction of such functions in 1839 for his glorious proof of his namesake theorem regarding primes in arithmetic progressions.

Vinogradov then proved what is now known as the Pólya–Vinogradov inequality (Pólya discovered this independently), which is

Theorem 2.1 (Pólya–Vinogradov inequality)**.** *Let χ be a non-principal*[3] *Dirichlet chararcter modulo q. Let N be any positive integer, then there exists a constant C such that*

$$\left|\sum_{n=1}^{N} \chi(n)\right| \leq C\sqrt{q}\log(q).$$

Remark 2.2. *Vinogradov's proof works with $C = 1$ but it assumes q is prime. The best current estimates for C can be found in [13] and [16].*

Now, the Legendre symbol is a Dirichlet character modulo p (for any odd p), and it's not the principal character (since there are $\frac{p-1}{2} > 0$ quadratic non-residues modulo p for any odd prime p). Therefore, if $p > N > C\sqrt{p}\log(p)$, then

$$\sum_{n=1}^{N} \left(\frac{n}{p}\right) \leq C\sqrt{p}\log p < N.$$

[3] The principal Dirichlet character modulo q is the one defined as $\chi(n) = 1$ when $\gcd(n, q) = 1$ and $\chi(n) = 0$ otherwise.

But if the sum is less than N, that means it cannot consist of only 1's. Therefore, one of the values is -1 (since $p > N$, none of the values is 0). This means that (for large enough p)

$$n_p \leq C\sqrt{p}\log p.$$

Remark 2.3. *There is an elementary proof that $n_p < \sqrt{p} + 1$. The proof is as follows. Suppose that $n_p = q \geq \sqrt{p} + 1$. Let $k = \lceil \frac{p}{q} \rceil$. Since $q \geq \sqrt{p} + 1$, then $\frac{p}{q} < \sqrt{p}$, so $\lceil \frac{p}{q} \rceil < \frac{p}{q} + 1 < \sqrt{p} + 1$. Therefore $k < q$, which implies k is a quadratic residue. Furthermore, $p < kq < p + q$, therefore kq is also a quadratic residue. But since q is a quadratic non-residue, and k is a quadratic residue, then kq is a quadratic non-residue. Contradiction!*

Vinogradov then came up with a very clever idea which is now known as Vinogradov's trick. To understand the following we will need a little bit of notation. We say that the function $f(n)$ is *little oh* of the function $g(n)$, and write $f(n) = o(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = 0$.

Theorem 2.4 (Vinogradov's trick)**.** *Let $\chi(n) = \left(\frac{n}{p}\right)$ be the Legendre symbol of n modulo p for p prime. Suppose that x is a large real number such that*

$$\sum_{1\leq n\leq x} \chi(n) = o(x). \tag{1}$$

Let $\varepsilon > 0$ and let $y = x^{\frac{1}{\sqrt{e}}+\varepsilon}$. Then, for large enough x, there exists $n \leq y$ such that $\chi(n) = -1$.

Proof. We may assume $x < p$ since the sum is 0 for $x = p$ and χ is periodic modulo p. Observe that since χ is totally multiplicative, then $\chi(n) = -1$ implies n has a prime divisor q satisfying $\chi(q) = -1$. Now suppose that for all $q \leq y$, $\chi(q) = 1$. Then

$$\sum_{1\leq n\leq x} \chi(n) = \sum_{1\leq n\leq x} 1 - 2 \sum_{\substack{1\leq n\leq x \\ \chi(n)=-1}} 1 = \lfloor x \rfloor - 2 \sum_{\substack{y<q\leq x \\ \chi(q)=-1}} \sum_{n\leq\frac{x}{q}} 1.$$

Therefore

$$\sum_{n\leq x} \chi(n) \geq \lfloor x \rfloor - 2 \sum_{y<q\leq x} \left\lfloor \frac{x}{q} \right\rfloor \geq x - 1 - 2x \sum_{y<q\leq x} \frac{1}{q}.$$

Merten's theorem says that

$$\sum_{y<q\leq x} \frac{1}{q} = \log\log x - \log\log y + O\left(\frac{1}{\log y}\right)$$

and therefore there is a $\delta > 0$ such that for large enough x we have

$$\sum_{y<q\leq x} \frac{1}{q} \leq \log\log x - \log\log y + \delta = -\log\left(\frac{1}{\sqrt{e}} + \varepsilon\right) + \delta < \frac{1}{2}.$$

Therefore, there exists a constant $C > 0$ such that $\sum_{n\leq x} \chi(n) \geq Cx$, which contradicts (1). □

Translating this to our interests, from the Pólya–Vinogradov inequality we have that for $x = \sqrt{p}(\log p)^2$, equation (1) is satisfied. But then that means that for any $\varepsilon > 0$, for a large enough p (depending on ε),

$$n_p \leq p^{\frac{1}{2\sqrt{e}}+\varepsilon}.$$

One interesting thing about the Pólya–Vinogradov inequality is that it does not depend on the number of summands, the upper bound of $\sqrt{p}\log p$ works regardless of how many terms N are summed. One heuristic for how Dirichlet characters behave is to model them as if they were uniformly random on the unit circle. The Central Limit Theorem from probability would then suggest that a constant multiple of $\sqrt{N}$ works as an upper bound. But characters are not random, so Vinogradov conjectures that for any $\varepsilon > 0$,

$$\left|\sum_{n=1}^{N}\chi(n)\right| \leq \sqrt{N}q^{\varepsilon}.$$

From this heuristic, he predicts:

Conjecture 2.5 (Vinogradov)**.** *Given $\varepsilon > 0$, we have $n_p \leq p^{\varepsilon}$ for sufficiently large primes p.*

In the 1940s, Linnik introduced the large sieve in order to prove that $n_p \ll p^{\varepsilon}$ holds for most primes ([25], [26]); this will be discussed in section 6. A big breakthrough in the direction of Vinogradov's conjecture came from Burgess in a series of papers in the early 1960s ([6], [8], [7]), where he proved a slightly weaker version of the following inequality, which can be found in [18]:

Theorem 2.6 (Burgess inequality)**.** *Let χ be a non-principal character* mod *q, where $q > 1$ is prime, and r is a positive integer. Then, there exists a constant C, such that*

$$\left|\sum_{n=1}^{N}\chi(n)\right| \leq CN^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}}(\log q)^{1/r},$$

where the constant C depends only on ε and r.

Remark 2.7. *Burgess proved a slightly weaker inequality, but it also holds when q is cubefree, as well as for any q when $r = 1, 2, 3$.*

Remark 2.8. *When $r = 1$, one recovers the Pólya–Vinogradov inequality. When $r = 2$ one gets the desired $\sqrt{N}$ term, at the cost of a big power of q. As r is larger, the power of q is smaller, so as $r \to \infty$, the bound tends to the trivial inequality.*

What does this imply for the least quadratic non-residue modulo p? If $\chi(n) = 1$ for all $n \leq N$, then by the Burgess inequality one would have

$$N = \left|\sum_{n\leq N}\chi(n)\right| \leq CN^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}}(\log p)^{1/r},$$

and consequently

$$N \leq C^r q^{\frac{1}{4}+\frac{1}{4r}} \log p.$$

For $\delta > 0$ and q large enough , we can see that $N = q^{1/4+\delta}$ satisfies (1). Therefore, given $\varepsilon > 0$, for all large enough p, we have

$$n_p \leq p^{\frac{1}{4\sqrt{e}}+\varepsilon}.$$

No significant unconditional improvements have been done on this result from the 1960s. The modern improvements are in terms of making the constants explicit. These results will be described in section 5.

3 The Pólya–Vinogradov inequality

Let $q \in \mathbb{Z}^+$. Recall that a function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a Dirichlet character modulo q if

1. $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$;

2. $\chi(n + kq) = \chi(n)$ for all $n, k \in \mathbb{Z}$;

3. $\chi(n) = 0$ if and only if $(n, q) > 1$.

There is a one-to-one correspondence between Dirichlet characters $\chi : \mathbb{Z} \to \mathbb{C}$ and group homomorphisms $\chi : (\mathbb{Z}/q\mathbb{Z})^\star \to \mathbb{C}^\star$. The principal character mod q is defined by

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, q) = 1 \\ 0 & \text{if } (n, q) > 1. \end{cases}$$

As mentioned before, the Legendre symbol $\chi(n) = (n/p)$ is a Dirichlet character modulo p. Since this is our main focus, we will simplify our exposition by considering only Dirichlet characters modulo p. Our goal in this section is to prove the Pólya–Vinogradov inequality for prime moduli.

Remark 3.1. *Let p be an odd prime. Choose a primitive root g modulo p; that is, $(\mathbb{Z}/p\mathbb{Z})^\star = \langle g \rangle$. For $a = 0, 1, \ldots, p-2$, we can define a Dirichlet character χ_a by the mapping $g^\nu \mapsto \zeta_{p-1}^{a\nu}$, where $\zeta_{p-1} = e^{\frac{2\pi i}{p-1}}$. This gives all Dirichlet characters mod p. In fact, the map $g^\nu \mapsto \chi_\nu$ gives an isomorphism between $(\mathbb{Z}/p\mathbb{Z})^\star$ and the group all Dirichlet characters modulo p.*

Example. *There are 6 Dirichlet characters modulo 7. Choosing $g = 5$, and using that $\zeta_6 = -\zeta_3^2$, we get the following table*

n	*0*	*1*	*2*	*3*	*4*	*5*	*6*
$\chi_0(n)$	0	1	1	1	1	1	1
$\chi_1(n)$	0	1	ζ_3^2	$-\zeta_3$	ζ_3	$-\zeta_3^2$	-1
$\chi_2(n)$	0	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	1
$\chi_3(n)$	0	1	1	-1	1	-1	-1
$\chi_4(n)$	0	1	ζ_3^2	ζ_3	ζ_3	ζ_3^2	1
$\chi_5(n)$	0	1	ζ_3	$-\zeta_3^2$	ζ_3^2	$-\zeta_3$	-1

To simplify our notation going forward, let $e(x) = e^{2\pi i x}$. For example $\zeta_{p-1} = e^{\frac{2\pi i}{p-1}} = e(\frac{1}{p-1})$.

Definition 3.2. *If χ is a Dirichlet character modulo p, then the Gauss sum associated to χ is defined as*

$$\tau(\chi) = \sum_{n=1}^{p} \chi(n) e(n/p)\,.$$

For $a = 0, 1, \ldots, p-1$, we also define $\tau_a(\chi) = \sum_{n=1}^{p} \chi(n)e(an/p)$. Notice that $\tau(\chi) = \tau_1(\chi)$.

The following lemma is a consequence of the fact that if $a \not\equiv 0 \bmod p$, then $a, 2a, \ldots, pa \bmod p$ is a permutation of $0, 1, 2, \ldots, p-1$.

Lemma 3.3.

$$\tau_a(\chi) = \begin{cases} \chi(a^{-1})\tau(\chi) & \textit{if } \chi \neq \chi_0, \textit{ and } a \neq 0 \\ 0 & \textit{if } \chi \neq \chi_0, \textit{ and } a = 0 \\ 0 & \textit{if } \chi = \chi_0, \textit{ and } a \neq 0 \\ p-1 & \textit{if } \chi = \chi_0, \textit{ and } a = 0. \end{cases}$$

We are now ready to prove a classical result due to Gauss.

Theorem 3.4. *If χ is a non-principal Dirichlet character modulo p, then*

$$|\tau(\chi)| = \sqrt{p}\,.$$

Proof. The idea is to evaluate the sum

$$S = \sum_{a=0}^{p-1} \tau_a(\chi)\overline{\tau_a(\chi)}$$

in two different ways. On the one hand, $|\tau_a(\chi)| = |\tau(\chi)|$ when $a \neq 0$ and therefore $S = (p-1)|\tau(\chi)|^2$. On the other hand, we can write

$$S = \sum_{a} \sum_{n,m} \chi(n)\overline{\chi}(m) e(a(n-m)/p)$$

and push the $\sum_a$ to the inside to find that $S = p(p-1)$. □

First, we will prove a result where the evaluation of a Dirichlet character at n is written in terms of a Gauss sum.

Lemma 3.5. *If χ is a non-principal Dirichlet character modulo p, then*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{p} \overline{\chi}(a)\, e(an/p)\,. \tag{2}$$

Proof.

$$\tau(\overline{\chi})\chi(n) = \sum_{m=1}^{p} \overline{\chi}(m)\chi(n)e(m/p).$$

When $n \not\equiv 0 \bmod p$, then $m \equiv an \bmod p$ has a unique solution $a \bmod p$. But then $\overline{\chi}(m)\chi(n) = \overline{\chi}(an)\chi(n) = \overline{\chi}(a)$, and $e(m/p) = e(an/p)$. Therefore

$$\sum_{m=1}^{p} \overline{\chi}(m)\chi(n)e(m/p) = \sum_{a=1}^{p} \overline{\chi}(a)e(an/p).$$

If $n \equiv 0 \bmod p$, then the left hand side of (2) is 0 and the right hand side can be computed (using Remark 3.1)

$$\frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{p} \overline{\chi}(a) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{p} e\left(\frac{-a\nu}{p-1}\right) = 0.$$

□

We now have all the ingredients to prove the Pólya–Vinogradov inequality.

Theorem 3.6 (Pólya–Vinogradov)**.** *If χ is a non-principal Dirichlet character modulo p, then*

$$\left|\sum_{H \le n < H+N} \chi(n)\right| \le \sqrt{p}\log p\,.$$

Proof. First, observe that

$$\frac{1}{p}\sum_{a=0}^{p-1} e(ax/p)e(-an/p) = \begin{cases} 1 & \text{if } x \equiv n \bmod p \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathbb{F}_p$ be the field with p elements $\{0, 1, 2, \dots, p-1\}$. Then

$$\begin{aligned} \sum_{H \le n < H+N} \chi(n) &= \sum_{x \in \mathbb{F}_p} \sum_{H \le n < H+N} \chi(x) \left(\frac{1}{p}\sum_{a=0}^{p-1} e(ax/p)e(-an/p)\right) \\ &= \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x \in \mathbb{F}_p} \chi(x)e(ax/p) \sum_{H \le n < H+N} e(-an/p) \\ &= \frac{1}{p}\sum_{a=0}^{p-1} \tau_a(\chi) \sum_{H \le n < H+N} e(-a/p)^n \\ &= \frac{1}{p}\sum_{a=1}^{p-1} \tau_a(\chi)\frac{e(-a(H+N)/p) - e(-aH/p)}{1 - e(-a/p)}. \end{aligned}$$

Thus

$$\begin{aligned} \left|\sum_{H \le n < H+N} \chi(n)\right| &\le \frac{1}{p}\sum_{a=1}^{p-1} |\tau_a(\chi)|\frac{2}{|1 - e(-a/p)|} \\ &\le \frac{4}{p}\sum_{a=1}^{(p-1)/2} |\tau_a(\chi)|\frac{1}{|1 - e(-a/p)|}. \end{aligned}$$

We have

$$|1 - e(-a/p)| \geq \frac{4a}{p},$$

for $a = 1, \dots (p-1)/2$ and we have $|\tau_a(\chi)| = \sqrt{p}$, so

$$\left| \sum_{H \leq n < H+N} \chi(n) \right| \leq \sqrt{p} \sum_{a=1}^{(p-1)/2} \frac{1}{a}.$$

To conclude the proof, we need only show that $\sum_{a=1}^{(p-1)/2} \frac{1}{a} \leq \log p$. Note that for $p = 3, 5, 7$, one can verify this manually.[4] For $p \geq 11$, we know $(p-1)/2 \geq 5$. Since $1/t$ is a decreasing function, for an integer $x \geq 5$, we have

$$\sum_{a \leq x} \frac{1}{a} \leq 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \int_5^x \frac{1}{t}\, \mathrm{d}t = \frac{137}{60} + \log(x) - \log(5).$$

Therefore

$$\sum_{a=1}^{(p-1)/2} \frac{1}{a} \leq \frac{137}{60} + \log(p-1) - \log(2) - \log 5 < \log p.$$

□

4 The Burgess inequality

There are many explicit estimates for the Burgess inequality in the literature. For example, in [47], Treviño proves

Theorem 4.1. *Suppose χ is a non-principal Dirichlet character modulo a prime $p \geq 10^7$. Let r be a positive integer, and let N and H be integers with $H \geq 1$. Then*

$$\left| \sum_{n \in (N, N+H]} \chi(n) \right| \leq 2.74\, H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Booker [5] has better constants for quadratic characters under certain restrictions on the range of H with respect to p. For characters of any order, there is work of McGown [28] and Treviño [47] that gets explicit estimates for different ranges of H with respect to p where the estimate gains a power of $\log p$, by getting an exponent of $1/(2r)$ as opposed to the exponent of $1/r$. Recent work of Kerr, Shparlinski, and Hung Yau [19] is able to improve the exponent of $\log p$ to $1/(4r)$ but without finding the constants explicitly. More recent work, by de la Bretèche and Munsch [11], given $H \leq p^{\frac{1}{2}+\frac{1}{4r}}$, improves the exponent of $\log p$ further to $(\delta_0 + o(1))/(2r)$, where $\delta_0 \approx 0.16656$.

For this paper, we want to show the techniques to prove explicit estimates on the Burgess inequality without aiming at the best possible constants. To simplify the proof, we have an exponent of $3/(2r)$ for $\log p$ instead of an exponent of $1/r$ or $1/(2r)$.

Our main goal this section will be proving the following explicit Burgess inequality

[4] The case $p = 2$ is omitted, since the statement of the theorem is vacuously true; there are no non-principal characters modulo 2.

Theorem 4.2. *Suppose χ is a non-principal Dirichlet character modulo a prime $p \geq 10^{11}$. Let $N, H \in \mathbb{Z}$ with $H \geq 1$. Fix a positive integer $r \geq 2$. Then*

$$\left| \sum_{n \in (N, N+H]} \chi(n) \right| < 5\, H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{3}{2r}} .$$

4.1 An important upper bound

To be able to prove Theorem 4.2, we need to get an upper bound on a particular character sum. To do that, we use the following character sum estimate, first given by Weil as a consequence of his deep work on the Riemann hypothesis for function fields (see [51]). It is also proved as Theorem 2C' in [43] using an elementary method due to Stepanov (see [44]), which was later extended by both Bombieri (see [4]) and Schmidt (see [42]).

Lemma 4.3. *Let χ be a non-principal Dirichlet character to the prime modulus p, having order n. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with m distinct roots which is not an n-th power in $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ denotes the finite field with p elements. Then*

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

Let $S(\chi, h, r)$ be defined as

$$S(\chi, h, r) = \sum_{x \bmod p} \left| \sum_{b=1}^{h} \chi(x+b) \right|^{2r} .$$

We will require bounds which follow from an explicit version of Stirling's formula (for example, see [38]):

$$\left(\frac{2r}{e}\right)^r < \frac{(2r)!}{2^r r!} < \sqrt{2} \left(\frac{2r}{e}\right)^r .$$

The following Lemma is due to Treviño, building on work of Burgess, Norton, and Booker [48, 47, 6, 8, 36, 5]. Some of the following exposition appears in applications of the lemma in [32, 27].

Lemma 4.4. *Suppose χ is any non-principal Dirichlet character to the prime modulus p. If $r, h \in \mathbb{Z}^+$, then*

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

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

$$S(\chi, h, r) \leq h^{2r} p \leq \left(\frac{2r}{e}\right)^r h^r p < \frac{(2r)!}{2^r r!} h^r p .$$

This establishes the claim.

Now, to begin the proof proper, we observe that

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

Define

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

We can rewrite the above as

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

where

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

and n denotes the order of χ. If $f_{\mathbf{m}}(x)$ is not an n-th power mod p, then by Lemma 4.4 we have

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

Otherwise, we employ the trivial bound of p.

It remains to count the number of exceptions – that is, the number of $\mathbf{m} \in \mathcal{M}$ such that $f_{\mathbf{m}}(x)$ is an n-th power mod p. If $n = 2$, it is easy to see that the number of exceptions is bounded above by $(2r-1)(2r-3)\ldots(3)(1) = (2r)!/(2^r r!)$ simply by pairing each m_j with a duplicate. When $n > 2$, the counting problem is much more difficult. To avoid this difficulty, Burgess in [6] counts the number of $\mathbf{m} = (m_1, \ldots, m_{2r}) \in \mathcal{M}$ such that each m_j is repeated at least once and arrives at the expression $(4r)^{r+1}h^r$.

Treviño in [48] shows that the number of exceptions is bounded above by the quantity

$$c_r(h, n) = \sum_{d=0}^{\lfloor \frac{r}{n} \rfloor} \left(\frac{w!}{d!(k!)^d}\right)^2 \frac{h^{r-(n-2)d}}{(r-nd)!}\,;$$

moreover, under the condition $r \le 9h$, he shows that $c_r(h, n)$ is a decreasing function of n and hence $c_r(h, n) \le c_w(h, 2) = (2r)!/(2^r r!)h^r$. But since we have $r < (e/2)h$ in the context of our proof, this condition is automatic. □

4.2 Proof of Theorem 4.2

Throughout this section, χ will denote a Dirichlet character modulo an odd prime p and N, H will be integers with $0 \le N < p$ and $1 \le H < p$. The latter assumption is justified as reducing N and H modulo p leaves the sum in Theorem 4.2 unchanged. Defining the quantities

$$S_\chi(H) := \sum_{n \in (N, N+H]} \chi(n)\,, \quad E(H) := H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{3}{2r}}\,,$$

we seek a bound of the form $S_\chi(H) < C\,E(H)$, for some constant C.

Fix $A \in \mathbb{Z}$ with $1 < A < p$. For $x \in \mathbb{F}_p$, we define $\nu_A(x)$ to be the number of ways we can write $x \equiv \overline{a}n \pmod{p}$, where $a \in [1, A]$ is a prime and $n \in (N, N+H]$ is an integer. Here the notation $\overline{a}$ denotes a multiplicative inverse of a modulo p.

Lemma 4.5. *Suppose $|S_\chi(H_0)| \le C\,E(H_0)$ for all $H_0 < H$. Fix $H_0 = AB < H$. Then*

$$|S_\chi(H)| \le \frac{1}{\pi(A)B} \sum_{x\in\mathbb{F}_p} \nu_A(x) \left| \sum_{1\le b\le B} \chi(x+b) \right| + 2C\,E(H_0)\,.$$

Proof. Applying a shift $n \mapsto n+h$ with $1 \le h \le H_0$ gives

$$S_\chi(H) = \sum_{n\in(N,N+H]} \chi(n+h) + 2C\theta E(H_0)\,.$$

(The letter θ will denote a complex number with $|\theta| \le 1$, possibly different each time it appears.) We set $h = ab$ in the above, and average over all primes $a \in [1, A]$ and all integers $b \in [1, B]$. This gives

$$S_\chi(H) = \frac{1}{\pi(A)B} \sideset{}{'}\sum_{a,b} \sum_{n\in(N,N+H]} \chi(n+ab) + 2C\theta E(H_0)\,,$$

where $\sum'$ here indicates that we are summing over all primes $a \in [1, A]$ and all integers $b \in [1, B]$. Rearranging the sum in the above expression yields

$$\sideset{}{'}\sum_{a,b} \sum_{n\in(N,N+H]} \chi(n+ab) = \sideset{}{'}\sum_{1\le a\le A} \sum_{n\in(N,N+H]} \chi(a) \sum_{1\le b\le B} \chi(\overline{a}n+b)\,,$$

and hence

$$\left| \sideset{}{'}\sum_{a,b} \sum_{n\in(N,N+H]} \chi(n+ab) \right| \le \sum_{x\in\mathbb{F}_p} \nu_A(x) \left| \sum_{1\le b\le B} \chi(x+b) \right|\,.$$

The result follows. □

Lemma 4.6. *Suppose $a_1 \ne a_2$ are prime and $b \in \mathbb{Z}$. Then the number of integer solutions $(x, y) \in \mathbb{Z}^2$ to the equation $a_1x - a_2y = b$ with $x, y \in (N, N+H]$ is at most*

$$\frac{H}{\max\{a_1, a_2\}} + 1\,.$$

Proof. Let Q denote the number of solutions to $a_1x - a_2y = b$ with $x, y \in (N, N+H]$. We will show $Q \le H/a_2 + 1$. It will immediately follow from the same argument that $Q \le H/a_1 + 1$ as well; indeed, just multiply both sides of the equation by -1 and interchange the roles of x and y. Suppose we have two solutions (x, y) and (x', y'). It follows that $a_1(x-x') = a_2(y-y')$, and since $a_1 \ne a_2$ are prime, we see that a_2 divides $x - x'$ which implies $|x - x'| \ge a_2$. Then, there are at most $H/a_2 + 1$ choices for x, but given x, y is fixed. The result follows. □

Lemma 4.7. *Fix $A \in \mathbb{Z}$ with $1 < A < p$. If $2AH \leq p$, then*

$$\sum_{x \in \mathbb{F}_p} \nu_A(x)^2 < \pi(A) H \left(\frac{5}{3} + \frac{2\pi(A)}{H} \right) .$$

Proof. Define S to be the set of all quadruples (a_1, a_2, n_1, n_2) with

$$a_1 n_2 \equiv a_2 n_1 \pmod{p},$$

where $a_1, a_2 \in [1, A]$ are prime and $n_1, n_2 \in (N, N+H]$ are integers. We observe that $\#S = \sum_{x \in \mathbb{F}_p} \nu_A(x)^2$. Suppose $(a_1, a_2, n_1, n_2) \in S$ with $a_1 = a_2$. Then we have $n_1 \equiv n_2 \pmod{p}$ and hence $n_1 = n_2$ since $n_1, n_2 \in (N, N+H]$ and $H \leq p$. Thus there are exactly $\pi(A)H$ solutions of this form.

Now we treat the remaining cases. Let $(a_1, a_2, n_1, n_2) \in S$ with $a_1 \neq a_2$. Then $a_1 n_2 - a_2 n_1 = kp$ for some k. It is an exercise to verify that a_1 and a_2 determine k. Now Lemma 4.6 tells us that there are at most $H / \max\{a_1, a_2\} + 1$ choices of (n_1, n_2) for each fixed (a_1, a_2). Thus the number of elements in S with $a_1 \neq a_2$ is bounded above by

$$2 \sum_{\substack{a_2 \leq A \\ a_2 \text{ prime}}} \sum_{\substack{a_1 < a_2 \\ a_1 \text{ prime}}} \left(\frac{H}{a_2} + 1 \right) \; < \; 2H \sum_{\substack{a \leq A \\ a \text{ prime}}} \frac{\pi(a) - 1}{a} + 2 \sum_{\substack{a \leq A \\ a \text{ prime}}} (\pi(a) - 1) .$$

It follows that

$$\sum_{x \in \mathbb{F}_p} \nu_A(x)^2 < \pi(A) H \left(1 + \frac{2}{\pi(A)} \sum_{a \leq A} \frac{\pi(a) - 1}{a} + \frac{2}{\pi(A) H} \sum_{a \leq A} (\pi(a) - 1) \right) .$$

Finally we observe

$$\sum_{\substack{a \leq A \\ a \text{ prime}}} (\pi(a) - 1) \leq \pi(A)^2 , \qquad \sum_{\substack{a \leq A \\ a \text{ prime}}} \frac{\pi(a) - 1}{a} < \frac{\pi(A)}{3}.$$

The second inequality can be confirmed manually for $A \leq 49$ and then one can use $\pi(a) < a/3$ for $a \geq 50$, which follows from (3.6) of [39], namely $\pi(a) \leq 1.3a / \log a$ for $a > 1$. The Lemma follows. □

We are now ready to prove the Burgess inequality.

Proof of Theorem 4.2. We may assume

$$C^r p^{\frac{1}{4} + \frac{1}{4r}} \log p \leq H \leq p^{\frac{1}{2} + \frac{1}{4r}} \log p ; \tag{3}$$

otherwise, the result follows from either $|S_\chi(H)| \leq H$ or $|S_\chi(H)| \leq p^{1/2} \log p$. We will prove the result by induction on H. We assume that $|S_\chi(H_0)| \leq CE(H_0)$ for all $H_0 < H$. We choose an integer H_0 with

$$\frac{H}{d+1} < H_0 \leq \frac{H}{d} ,$$

for which we can write $H_0 = AB$ with $A, B \in \mathbb{Z}^+$, where

$$B = \left\lceil \frac{2}{d} p^{\frac{1}{2r}} (\log p)^2 \right\rceil .$$

Accomplishing this is possible provided $H/d - H/(d+1) > B$. Assuming $d = 10$ and $p \geq 10^{10}$ we find $B > 100$ and therefore the desired inequality follows from the estimate

$$H \geq (1.01) 2(d+1) p^{\frac{1}{2r}} (\log p)^2 ,$$

which is implied by

$$C^r p^{\frac{1}{4} - \frac{1}{4r}} \geq 2.02(d+1) \log p ;$$

the latter condition holds upon setting $C = 5$ and assuming $p \geq 10^{11}$. Observe that our choice of B leads to $2AH < 2H^2/(dB) < p$. At this point, we give upper and lower bounds on A. Observe that

$$A \leq \frac{H}{dB} \leq \frac{1}{2} p^{\frac{1}{2} - \frac{1}{4r}} (\log p)^{-1} ,$$

and hence

$$\log A + 1 \leq \frac{1}{2} \log p. \tag{4}$$

We also have

$$A > \frac{H}{(d+1)B} \geq \frac{C^r d}{(2.02)(d+1)} p^{\frac{1}{4} - \frac{1}{4r}} (\log p)^{-1} > 10 .$$

Applying Lemma 4.5 and our inductive hypothesis, we have

$$|S_\chi(H)| \leq \frac{1}{\pi(A)B} \sum_{x \in \mathbb{F}_p} \nu_A(x) \left| \sum_{1 \leq b \leq B} \chi(x+b) \right| + \frac{2C}{d^{1-\frac{1}{r}}} E(H) . \tag{5}$$

In order to bound the sum above, we apply Hölder's inequality to the functions $\nu_A(x)^{1-\frac{1}{r}}$, $\nu_A(x)^{\frac{1}{r}}$, and $\left|\sum_{1 \leq b \leq B} \chi(x+b)\right|$ using the Hölder exponents $(1-1/r)^{-1}$, $2r$, and $2r$ respectively; this yields:

$$\sum_{x \in \mathbb{F}_p} \nu_A(x) \left| \sum_{1 \leq b \leq B} \chi(x+b) \right| \\ \leq \left(\sum_{x \in \mathbb{F}_p} \nu_A(x) \right)^{1-\frac{1}{r}} \left(\sum_{x \in \mathbb{F}_p} \nu_A(x)^2 \right)^{\frac{1}{2r}} \left(\sum_{x \in \mathbb{F}_p} \left| \sum_{1 \leq b \leq B} \chi(x+b) \right|^{2r} \right)^{\frac{1}{2r}} .$$

We bound each of the three sums above in turn. Clearly, one has

$$\sum_{x \in \mathbb{F}_p} \nu_A(x) = \pi(A) H .$$

We invoke Lemma 4.7 to conclude that

$$\sum_{x \in \mathbb{F}_p} \nu_A(x)^2 \leq 2\pi(A) H .$$

Indeed, using (3.6) of [39], we have $\pi(A) \le 1.3\,A/\log A$ for $A > 1$ and therefore

$$\frac{\pi(A)}{H} \le \frac{1.3A}{H\log A} \le \frac{1.3}{dB\log A} \le \frac{1.3}{2p^{\frac{1}{2r}}(\log p)^2\log A} < 0.1\,.$$

To bound the third sum, we apply Lemma 4.4; this gives

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{1\le b\le B}\chi(x+b)\right|^{2r} \le B^{2r}p^{1/2}\left(\sqrt{2}\left(\frac{2r}{eB}\right)^r p^{1/2} + (2r-1)\right) \le 2rB^{2r}p^{1/2}\,.$$

The final inequality follows from $\sqrt{2}\left(\frac{2r}{eB}\right)^r p^{1/2} \le 1$ whenever $r \le 0.1\log^2 p$. But from (3) we may assume that $r < \frac{1}{4}\log p \le 0.1\log^2 p$. All together, this gives

$$\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\le b\le B}\chi(x+b)\right| \le (\pi(A)H)^{1-\frac{1}{r}}(2\pi(A)H)^{\frac{1}{2r}}\left(2rB^{2r}p^{1/2}\right)^{\frac{1}{2r}}\,.$$

Therefore

$$\frac{1}{\pi(A)B}\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\le b\le B}\chi(x+b)\right| \;\le\; (4r)^{\frac{1}{2r}}H^{1-\frac{1}{r}}p^{\frac{1}{4r}}\left(\frac{H}{\pi(A)}\right)^{\frac{1}{2r}}\,.$$

Using (3.5) of [39] and some simple computation, provided $A \ge 3$ and $A \in \mathbb{Z}$, we have $\pi(A) \ge A/(1+\log A)$; using this, together with (4), we can estimate

$$\frac{H}{\pi(A)} \;\le\; \frac{H(\log A+1)}{A} \;\le\; (d+1)B(\log A+1) \;\le\; 1.01\frac{d+1}{d}\cdot p^{\frac{1}{2r}}(\log p)^3\,.$$

Therefore

$$\left(\frac{H}{\pi(A)}\right)^{\frac{1}{2r}} \le \left(1.01\frac{d+1}{d}\right)^{\frac{1}{2r}} p^{\frac{1}{4r^2}}(\log p)^{\frac{3}{2r}},$$

which leads to

$$\frac{1}{\pi(A)B}\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\le b\le B}\chi(x+b)\right| \;\le\; \left(\frac{4.04\,r(d+1)}{d}\right)^{\frac{1}{2r}} H^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{3}{2r}}\,.$$

Finally, using (5), this gives

$$|S_\chi(H)| \le \left[\left(\frac{4.04\,r(d+1)}{d}\right)^{\frac{1}{2r}} + \frac{2C}{d^{1-\frac{1}{r}}}\right]E(H) \le C\,E(H)\,,$$

when $C = 5$. □

5 Explicit results on the least quadratic non-residue

The inequality $n_p \leq p^{\frac{1}{4\sqrt{e}}+\varepsilon}$ for p large enough (depending on ε), is not explicit, in the sense that we haven't mentioned how big p must be depending on the parameter ε. Also, in some cases we want results that work for all p or for all $p \geq p_0$ for some manageable p_0. In this section we'll discuss several explicit results about n_p.

From Pólya–Vinogradov, we can show the explicit estimate $n_p \leq \sqrt{p}\log p$ for all p. As mentioned in Remark 2.3, one can also show $n_p \leq \sqrt{p}+1$ elementarily. But these results are far from the best asymptotic result. One of the first important explicit estimates was proved by Norton [36] in 1971. Norton proved

Theorem 5.1 (Norton, 1971)**.** *Let p be an odd prime number. Let n_p be the least quadratic non-residue modulo p. Then*

$$n_p \leq \begin{cases} 3.9p^{1/4}\log p & \textit{if } p \equiv 1 \bmod 4 \\ 4.7p^{1/4}\log p & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

Treviño [48], in 2015, improved this to

Theorem 5.2. *Let p be an odd prime number. Let n_p be the least quadratic non-residue modulo p. Then*

$$n_p \leq \begin{cases} 0.9p^{1/4}\log p & \textit{if } p \equiv 1 \bmod 4 \\ 1.1p^{1/4}\log p & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

The proof of the theorem relied on Lemma 4.4 to get a bound when $p \geq 10^{60}$ using $r \approx \log p/4$ and h in terms of r. For the "smaller" p, the idea was to use Lemma 4.4, choosing r and h carefully for different ranges of p.

These estimates are still relatively far from the Burgess estimate of $p^{\frac{1}{4\sqrt{e}}+\varepsilon}$. In that direction, Treviño [47], using an explicit Burgess inequality was able to show

Theorem 5.3. *Let $p \geq 10^{4732}$ be prime. Then*

$$n_p \leq p^{1/6}.$$

The technique of the proof works for any exponent $y > \frac{1}{4\sqrt{e}}$. Indeed, we'll prove the following theorem

Theorem 5.4. *Let $p \geq 10^{19000}$ be prime. Then*

$$n_p \leq p^{4/25}.$$

To prove it we will need the following explicit version of the Vinogradov trick (Lemma 5.3 in [47]):

Lemma 5.5. *Let $x \geq 286$, and let $y = x^{\frac{1}{\sqrt{e}}+\delta}$ for some $\delta > 0$. Let χ be a non-principal character* mod p *for some prime p. If $\chi(n) = 1$ for all $n \leq y$, then*

$$\left|\sum_{n\leq x}\chi(n)\right| \geq x\left(2\log\left(\delta\sqrt{e}+1\right) - \frac{1}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x}\right).$$

Proof of Theorem 5.4. Following the proof of Theorem 1.10 in [47], let χ be the Legendre symbol modulo p. Then, if $n < p$ and $\chi(n) \neq 1$, n is a quadratic non-residue. Let r be an integer. Let $x \geq 286$ be a real number and let $y = x^{\frac{1}{\sqrt{e}}+\delta} = p^{4/25}$ for some $\delta > 0$. Assume that $\chi(n) = 1$ for all $n \leq y$. Now by Theorem 4.2 and Lemma 5.5 we have

$$5x^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{3}{2r}} \geq x\left(2\log(\delta\sqrt{e}+1) - \frac{1}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x}\right).$$

Now, letting $x = p^{\frac{1}{4}+\frac{1}{2r}}$ we get

$$5p^{\frac{3\log\log p}{2r\log p}-\frac{1}{4r^2}} \geq 2\log(\delta\sqrt{e}+1) - \frac{1}{\log^2 x} - \frac{1}{\log^2 y} - \frac{1}{x}. \qquad (6)$$

Picking $r = 40$, one finds that $\delta = 0.002993\ldots$. For $p \geq 10^{19000}$, the right hand side of (6) is bigger than the left hand side, showing that $\chi(n)$ is not always 1 for $n \leq y = p^{4/25}$, and hence the theorem is true. □

We can also consider the case when the modulus is not prime. Suppose q is squarefree and we want to find n_q, the least quadratic non-residue modulo q. Granville, Mollin and Williams [15] proved that $n_q \leq \sqrt{q}/2$ for $q > 3705$. The proof used an explicit Pólya–Vinogradov inequality and extensive computations on a special sieving computer called *Manitoba Scalable Sieve Unit* that calculated bounds up to 10^{18}. Using a "smoothed" version of the Pólya–Vinogradov inequality (appeared in [23]), Treviño [45] improved this result to show that $n_q \leq q^{9/20}$ for $q > 1596$.

One could also consider the n-th least prime quadratic non-residue q_n (the first non-residue is always prime). Explicit bounds for q_2 appear in [31, 24]. Ma, McGown, Rhodes, and Wanner [27], recently proved that for $p \geq p_0$, there is a constant $C = C(n, p_0)$ depending on n, p_0 such that

$$q_n \leq Cp^{\frac{1}{4}}(\log p)^{\frac{n+1}{2}}.$$

In their paper, they calculate C for different values of n and p_0. For example if $n = 4$ and $p_0 = 10^{20}$, then the constant $C = 2.014$ suffices.

Another related problem is to bound $H(p)$, the maximum number of consecutive integers on which the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is constant, i.e.,

$$H(p) = \max_{a \bmod p}\left\{H : \left(\frac{a+1}{p}\right) = \left(\frac{a+2}{p}\right) = \cdots = \left(\frac{a+H}{p}\right)\right\}.$$

Using work of Burgess [7], McGown in [30] proved that $H(p) \leq 7.06p^{1/4}\log p$ when $p \geq 5\cdot 10^{18}$, and $H(p) \leq 7p^{1/4}\log p$ if $p \geq 10^{55}$. Treviño ([46], [49]) improved this to $H(p) \leq 1.55p^{1/4}\log p$ when $p \geq 10^{13}$ and $H(p) \leq 3.38p^{1/4}\log p$ for all odd p.

There are some nice results on a lower bound for $H(p)$. In [37], Peralta shows that for any $C < \frac{1}{\log 4}$, there exists a p_0 such that for $p > p_0$, $H(p) > C\log p$. In the interest of getting a clean, explicit lower bound, we prove the following:

Theorem 5.6. *Let $p > 80000$ be prime. Let $H(p)$ be the maximum number of consecutive integers on which the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is constant. Then*

$$H(p) \geq \frac{1}{2}\log p.$$

Proof. Let $\chi(a) = \left(\frac{a}{p}\right)$. Note that

$$\frac{\chi(a)+1}{2} = \begin{cases} 1 & \text{if } \chi(a) = 1 \\ 0 & \text{if } \chi(a) = -1 \\ \frac{1}{2} & \text{if } \chi(a) = 0. \end{cases}$$

Suppose $H \geq 3$, then we have

$$\prod_{i=1}^{H} \left(\frac{\chi(a+i)+1}{2} \right) = \begin{cases} 1 & \text{if } \chi(a+1) = \chi(a+2) = \cdots = \chi(a+H) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, if

$$S := \sum_{a=0}^{p-1} \prod_{i=1}^{H} \left(\frac{\chi(a+i)+1}{2} \right) > 0,$$

then there exists H consecutive integers that are all quadratic residues. We have

$$S = \frac{1}{2^H} \sum_{a \bmod p} \left(1 + \sum_{j=1}^{2^H} \chi(p_j(a)) \right) = \frac{1}{2^H} \left(p + \sum_{j=1}^{2^H} \sum_{a \bmod p} \chi(p_j(a)) \right),$$

where, for $j \in \{1, 2, \ldots, 2^H\}$, $p_j(a)$ is either a polynomial of degree $\leq H$ or 0. By the Weil estimates (Lemma 4.4),

$$\left| \sum_{a \bmod p} \chi(p_j(a)) \right| \leq (H-1)\sqrt{p}.$$

Therefore

$$|2^H S| \geq p - 2^H (H-1)\sqrt{p} > p - 2^H H \sqrt{p}. \tag{7}$$

When $H = \log p/2$ we have

$$2^H H \sqrt{p} = \frac{1}{2} p^{\frac{1+\log(2)}{2}} \log p.$$

But the last expression is smaller than p whenever $p > 80000$. Therefore, $S > 0$, which implies that there are at least H consecutive quadratic residues. This means $H(p) \geq \frac{1}{2}\log p$. □

Remark 5.7. *Note that from* (7)*, we can recover Peralta's result, namely that given* $C < \frac{1}{\log 4}$*, there is a constant* p_0 *such that for* $p > p_0$*,* $H(p) > C \log p$*.*

6 The large sieve and Linnik's theorem

In this section we will sketch a proof of the following beautiful result (see [26]):

Theorem 6.1 (Linnik)**.** *Fix* $\varepsilon > 0$*. Then we have*

$$\#\{p \leq N \mid n_p > p^{\varepsilon}\} = O(N^{\varepsilon}).$$

This result means that the number of exceptions to Vinogradov's conjecture (that the least quadratic non-residue n_p satisfies $n_p \ll p^{\varepsilon}$) is very small; in particular, the theorem implies:

Corollary 6.2. *The set of primes where Vinogradov's conjecture fails has density zero.*

Linnik introduced the large sieve (see [25]) and it was later studied in detail by Rényi, Roth, Bombieri, Davenport, Halberstam, Gallagher, and other authors. Our discussion here is very brief; more detail, including additional references, can be found in [9, 18, 10, 34].

Let $\{a_n\}$ be a sequence of complex numbers and consider the trigonometric polynomial

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha)\,.$$

Let $\alpha_1, \ldots, \alpha_R \in \mathbb{R}$ and suppose that $\|\alpha_r - \alpha_s\| \geq \delta$ for $r \neq s$ where $\|\theta\|$ denotes the distance to the nearest integer. The large sieve refers to an inequality of the form

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq \Delta(N, \delta) \sum_{n=M+1}^{M+N} |a_n|^2.$$

See [34] for a short proof that this holds with $\Delta = \delta^{-1} + \pi N$. By taking the α_r to be Farey fractions with denominators up to z, one obtains:

Theorem 6.3 (The Large Sieve inequality)**.** *For $x, z \in \mathbb{Z}^+$ we have*

$$\sum_{d \leq z} \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \left| \sum_{n \leq x} a_n e\left(\frac{na}{d}\right) \right|^2 \leq (z^2 + \pi x) \sum_{n \leq x} |a_n|^2\,.$$

One can obtain a sieve out of the previous theorem by the use of so-called Ramanujan sums $\sum_{\substack{a \leq a \leq d \\ (a,d)=1}} e(na/d)$. See [9] for the details.

Theorem 6.4. *Let $\mathcal{A}$ be a positive integers $n \leq x$ and let $\mathcal{P}$ be a set of primes. For each $p \in \mathcal{P}$, suppose we are given a set $\Omega_p = \{w_{1,p}, \ldots, w_{\omega(p),p}\}$ of $\omega(p)$ residue classes modulo p. Let $z > 0$, $P(z)$ the product of the primes $p \in \mathcal{P}$, $p < z$, and set*

$$S(\mathcal{A}, \mathcal{P}, z) := \#\{n \in \mathcal{A} \mid n \not\equiv w_{i,p} \bmod p,\ \forall p | P(z)\}\,.$$

We have

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{z^2 + \pi x}{L(z)},$$

where

$$L(z) := \sum_{d \leq z} \mu^2(d) \prod_{p | d} \frac{\omega(p)}{p - \omega(p)}.$$

Remark 6.5. *In applications, one needs a lower bound on $L(z)$. Often the following estimate suffices:*

$$L(z) \geq \sum_{p<z} \frac{\omega(p)}{p-\omega(p)}.$$

The final ingredient we need before proving Linnik's theorem is a lower bound on the numbers of integers up to x with only small prime factors. A number n is y-smooth if all of its prime factors are $\leq y$. The counting function for all y-smooth numbers up to x is defined as

$$\psi(x,y) := \#\{n \leq x \mid \text{all the prime factors of } n \text{ are} \leq y\}\,.$$

The following is a well-known lower bound on $\psi(x,y)$. The proof we give is suggested in Exercise #12 from Chapter 4 of [9].

Lemma 6.6. *For every $\varepsilon > 0$, there is a constant $c_\varepsilon > 0$ such that for x sufficiently large we have*

$$\psi(x, x^\varepsilon) \geq c_\varepsilon\, x\,.$$

Proof. Fix $\varepsilon > 0$. We consider numbers of the form $n = m\,p_1\,p_2 \dots p_k$ for $k = [\varepsilon^{-1}]$ where $x^{\varepsilon-\varepsilon^2} < p_j < x^\varepsilon$. We set $\alpha = \varepsilon - \varepsilon^2$ and $\beta = \varepsilon$ and estimate:

$$\begin{aligned}
\sum_{x^\alpha \leq p_1,\dots,p_k \leq x^\beta} \left[\frac{x}{p_1 \dots p_k}\right] &\gg \sum_{x^\alpha \leq p_1,\dots,p_k \leq x^\beta} \frac{x}{p_1 \dots p_k} \\
&= x \left(\sum_{x^\alpha \leq p \leq x^\beta} \frac{1}{p}\right)^k \\
&\gg x \left(\log\left(\frac{\beta}{\alpha}\right)\right)^k .
\end{aligned}$$

□

Proof of Theorem 6.1. Fix $\varepsilon > 0$. Let $\mathcal{A} = \mathbb{Z}^+$, $z = N$, $x = N^2$,

$$\mathcal{P} = \{p \mid n_p > p^\varepsilon\ ,\ p \in [N^\varepsilon, N]\}\,,$$

$$\Omega_p = \{\nu \mid (\nu/p) = -1\}\,.$$

Using the Large Sieve, we have:

$$\mathcal{S} = \mathcal{S}(\mathcal{A}, \mathcal{P}, z) \leq \frac{5N^2}{L(z)}.$$

We also have

$$L(z) \geq \sum_{p<z} \frac{\omega(p)}{p-\omega(p)} \geq \frac{1}{3}\#\{p \in \mathcal{P} \mid p \leq N\}.$$

Consider $\mathcal{S}' = \{n \leq N^2 \mid n \text{ has no prime divisors larger than } N^{\varepsilon^2}\}$. We claim that $\mathcal{S}' \subseteq \mathcal{S}$. Let $n \in \mathcal{S}'$. Let $p \in \mathcal{P}$. For any prime q dividing n, we have that $q < N^{\varepsilon^2} < p^\varepsilon$ and therefore

$(q/p) = 1$. It follows that $n \in \mathcal{S}$. By Lemma 6.6 we have $\#\mathcal{S}' \geq d_\varepsilon N^2$ for some $d_\varepsilon > 0$. This implies

$$d_\varepsilon N^2 \leq \frac{5N^2}{L(z)} \leq \frac{15N^2}{\#\{p \in \mathcal{P} \mid p \leq N\}},$$

and hence

$$\#\{p \in \mathcal{P} \mid p \leq N\} \leq \frac{15}{d_\varepsilon}.$$

Now we achieve our desired estimate; namely,

$$\{p \leq N \mid n_p > p^\varepsilon\} \leq \pi(N^\varepsilon) + \frac{15}{d_\varepsilon} = O(N^\varepsilon).$$

□

7 Ankeny's Theorem

Recall that Ankeny [1] proved $n_p \leq C(\log p)^2$ for some constant $C > 0$ under the assumption of the Generalized Riemann Hypothesis (GRH). In particular, this says that the GRH implies Vinogradov's conjecture. Bach [3] proved $n_p \leq 2(\log p)^2$. The main idea behind Bach's proof appears in [33], but to obtain explicit results there are many details to work out; Bach uses a slightly different kernel and introduces a parameter in order to achieve good numerical results. Later, Lamzouri, Li, and Soundararajan [21] prove that $n_p \leq (\log p)^2$.

Our goal here is prove an explicit version of Ankeny's Theorem without too much effort. We follow Bach's approach in [3] as well as some of the exposition given in [29]. For ease of exposition, we make the simplifying assumption that $\chi(-1) = 1$. (The same approach still works when $\chi(-1) = -1$ but the functional equation for $L(s, \chi)$ takes a slightly different form.)

Let n_χ denote the least positive integer n for which $\chi(n) \neq 1$. Notice that when $\chi(n) = (n/p)$, the Legendre symbol, one has $n_\chi = n_p$. We prove the following:

Theorem 7.1. *Let χ be a non-principal Dirichlet character modulo $m \geq 10^9$ with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s, \chi)$. Then $n_\chi < 2(\log m)^2$.*

Lemma 7.2. *Let χ be a Dirichlet character modulo m. (Here we allow the possibility that χ is the principal character or even that $m = 1$.) For $x > 1$ and $a \in (0, 1)$, we have*

$$-\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\frac{L'(s,\chi)}{L(s,\chi)}\, ds = \sum_{n<x} \chi(n)\Lambda(n)(n/x)^a \log(x/n)\,.$$

Proof. First, substitute the Dirichlet series

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^{\infty} \chi(n)\Lambda(n)n^{-s}$$

into the left-hand side above and interchange the order of summation and integration. Next, use the fact that for $y > 0$ one has

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{y^s}{(s+a)^2}\, ds = \begin{cases} y^{-a}\log y & \text{if } y > 1 \\ 0 & \text{otherwise}\,. \end{cases}$$

□

Lemma 7.3. *Let χ be a non-principal Dirichlet character modulo m with $\chi(-1) = 1$. For $a \in (0,1)$ and $x > 0$ we have*

$$\begin{aligned}
\frac{x}{(a+1)^2} + \frac{1}{a^2} &= \sum_{\rho \text{ } of \text{ } \zeta} \frac{x^\rho}{(\rho+a)^2} - \sum_{\rho \text{ } of \text{ } L_\chi} \frac{x^\rho}{(\rho+a)^2} \\
&+ \sum_{\substack{n<x \\ \chi(n)\neq 1}} (1-\chi(n))\Lambda(n)(n/x)^a \log(x/n) \\
&+ \frac{\log x}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a)\right] \\
&+ \frac{1}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L'_\chi}{L_\chi}\right)'(-a)\right].
\end{aligned}$$

Proof. Evaluate the integral in Lemma 7.2 using the Residue Theorem to obtain:

$$\begin{aligned}
\sum_{n<x} \chi(n)\Lambda(n)(n/x)^a \log(x/n) &= -\sum_{\rho \text{ of } L_\chi} \frac{x^\rho}{(\rho+a)^2} - \sum_{n=1}^{\infty} \frac{x^{-2n}}{(a-2n)^2} - \frac{1}{a^2} \\
&\quad - \frac{\log x}{x^a}\left(\frac{L'_\chi}{L_\chi}\right)(-a) - \frac{1}{x^a}\left(\frac{L'_\chi}{L_\chi}\right)'(-a),
\end{aligned}$$

$$\begin{aligned}
\sum_{n<x} \Lambda(n)(n/x)^a \log(x/n) &= \frac{x}{(a+1)^2} - \sum_{\rho \text{ of } \zeta} \frac{x^\rho}{(\rho+a)^2} - \sum_{n=1}^{\infty} \frac{x^{-2n}}{(a-2n)^2} \\
&\quad - \frac{\log x}{x^a}\left(\frac{\zeta'}{\zeta}\right)(-a) - \frac{1}{x^a}\left(\frac{\zeta'}{\zeta}\right)'(-a).
\end{aligned}$$

Subtracting these two equations gives the result. □

Define

$$\psi_{\mathbb{Q}}(s) = \frac{1}{2}\left(\psi\left(\frac{s}{2}\right) - \log \pi\right).$$

In order to expedite the proofs in the rest of this section, we quote some formulae, all of which can be derived from (5.9) of [20]. For all $s \in \mathbb{C}$, we have:

$$\frac{\zeta'(s)}{\zeta(s)} = B + \sum_{\rho \text{ of } \zeta}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{s} - \frac{1}{s-1} - \psi_{\mathbb{Q}}(s). \tag{8}$$

If χ is a non-principal primitive Dirichlet character modulo f, with $\chi(-1) = 1$, then for all $s \in \mathbb{C}$ we have:

$$\frac{L'(s,\chi)}{L(s,\chi)} = B_\chi + \sum_{\rho \text{ of } L_\chi}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log f - \psi_{\mathbb{Q}}(s). \tag{9}$$

Each sum above is over the non-trivial zeros ρ of the corresponding functions, and is absolutely and uniformly convergent on compact subsets of $\mathbb{C}$. Henceforth we adopt the notation that ρ will always denote a non-trivial zero with $0 < \Re(\rho) < 1$.

Each of (8), (9) involves a constant B which can be difficult to estimate. Fortunately, in both cases this constant can be eliminated from the equation as follows. Provided the sum is taken in symmetric order[5], one has $B + \sum_{\rho \text{ of } \zeta} \rho^{-1} = 0$, and similarly for B_χ. See [10] for a simple argument which gives this result for the constant B. The analogous result for B_χ is not obvious; in fact, it was not known until the introduction of the Weil formulas (see [52, 53]). Plugging $s = 1$ into (9) and comparing against (2.3.1) of [17] gives a proof of this result.

Lemma 7.4. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s,\chi)$. For $a \in (0,1)$ we have*

$$\sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{|\rho + a|^2} \leq \frac{1}{2a+1}\left(\log f + 2\left(\frac{1}{a+1} + \frac{1}{a}\right) + 4\psi_{\mathbb{Q}}(a+1)\right).$$

Proof. Substitute $s = \sigma$ into (9), add the result to its conjugate, and use the fact that the real part of $B_\chi + \sum_\rho \rho^{-1}$ equals 0 to obtain

$$\sum_{\rho \text{ of } L_\chi} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}}\right) = \log f + 2\Re\frac{L'(\sigma,\chi)}{L(\sigma,\chi)} + 2\psi_{\mathbb{Q}}(\sigma).$$

This equation goes back to Landau (see [22]). In exactly the same manner, one can show

$$\sum_{\rho \text{ of } \zeta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}}\right) = 2\frac{\zeta'(\sigma)}{\zeta(\sigma)} + 2\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1}\right) + 2\psi_{\mathbb{Q}}(\sigma).$$

Setting $\sigma = a + 1$ and supposing that $\Re(\rho) = 1/2$, we find:

$$\frac{1}{|\rho + a|^2} = \frac{1}{2a+1}\left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}}\right).$$

To complete the proof, we combine everything above and note that

$$\frac{\zeta'(\sigma)}{\zeta(\sigma)} + \Re\frac{L'(\sigma,\chi)}{L(\sigma,\chi)} < 0,$$

by considering the Dirichlet series for $(\zeta'/\zeta + L'_\chi/L_\chi)(s)$. □

Lemma 7.5. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. For $a \in (0,1)$ we have*

$$\left|\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a)\right|$$
$$\leq (a+2) \sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{|(\rho + a)(2 - \rho)|} + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{1}{a} + \frac{1}{a+1} + \frac{3}{2}.$$

[5] Taking the sum in symmetric order means: $\sum_\rho = \lim_{T\to\infty} \sum_{\substack{\rho = \sigma + it \\ |t| < T}}$

Proof. We begin with the following formulas which hold for all $s \in \mathbb{C}$, provided the sums are taken in symmetric order:

$$\left(\frac{\zeta'}{\zeta}\right)(s) \;=\; \sum_{\rho \text{ of } \zeta} \frac{1}{s-\rho} - \frac{1}{s} - \frac{1}{s-1} - \psi_{\mathbb{Q}}(s), \tag{10}$$

$$\left(\frac{L'_\chi}{L_\chi}\right)(s) \;=\; \sum_{\rho \text{ of } L_\chi} \frac{1}{s-\rho} - \frac{1}{2}\log f - \psi_{\mathbb{Q}}(s). \tag{11}$$

Formulas (10) and (11) are obtained from (8) and (9) respectively by applying the facts $\sum_{\rho \text{ of } \zeta} \rho^{-1} + B = 0$ and $\sum_{\rho \text{ of } L_\chi} \rho^{-1} + B_\chi = 0$. Plugging $s = 2$ into (10) and subtracting it from itself, and similarly for (11), yields:

$$\begin{aligned}\left(\frac{\zeta'}{\zeta}\right)(s) = \left(\frac{\zeta'}{\zeta}\right)(2) + \sum_{\rho}\left(\frac{1}{s-\rho} - \frac{1}{2-\rho}\right)&\\ +\frac{3}{2} - \frac{1}{s} - \frac{1}{s-1} + \psi_{\mathbb{Q}}(2) - \psi_{\mathbb{Q}}(s),&\\ \left(\frac{L'_\chi}{L_\chi}\right)(s) = \left(\frac{L'_\chi}{L_\chi}\right)(2) + \sum_{\rho}\left(\frac{1}{s-\rho} - \frac{1}{2-\rho}\right) + \psi_{\mathbb{Q}}(2) - \psi_{\mathbb{Q}}(s).&\end{aligned}$$

Using the above, together with the fact

$$\frac{1}{-a-\rho} - \frac{1}{2-\rho} = -\frac{a+2}{(\rho+a)(2-\rho)}\,,$$

we can write

$$\begin{aligned}\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a) = (a+2)\left(\sum_{\rho \text{ of } L_\chi} \frac{1}{(\rho+a)(2-\rho)} - \sum_{\rho \text{ of } \zeta} \frac{1}{(\rho+a)(2-\rho)}\right)&\\ + \left(\frac{\zeta'}{\zeta}\right)(2) - \left(\frac{L'_\chi}{L_\chi}\right)(2) + \frac{3}{2} + \frac{1}{a} + \frac{1}{a+1}\,.&\end{aligned}$$

The result follows upon taking absolute values and using the fact that $\left|\left(L'_\chi/L_\chi\right)(2)\right| \leq |(\zeta'/\zeta)(2)|$. □

In applying the previous lemma, it will be helpful to note that when $\Re(\rho) = 1/2$, one has $|\rho + a|^2 \leq |(\rho+a)(2-\rho)|$.

Lemma 7.6. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. For $a \in (0,1)$ we have*

$$\left|\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L'_\chi}{L_\chi}\right)'(-a)\right| < \sum_{\rho \textit{ of } \zeta, L_\chi} \frac{1}{|\rho+a|^2} + \frac{1}{a^2} + \frac{1}{(a+1)^2}\,.$$

Proof. We start by differentiating (10) and (11); this gives

$$\left(\frac{\zeta'}{\zeta}\right)'(s) \;=\; -\sum_{\rho \text{ of } \zeta} \frac{1}{(s-\rho)^2} + \frac{1}{s^2} + \frac{1}{(s-1)^2} - \psi'_{\mathbb{Q}}(s), \tag{12}$$

$$\left(\frac{L'_\chi}{L_\chi}\right)'(s) \;=\; -\sum_{\rho \text{ of } L_\chi} \frac{1}{(s-\rho)^2} - \psi'_{\mathbb{Q}}(s)\,, \tag{13}$$

which allows us to write

$$\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L'_\chi}{L_\chi}\right)'(-a)$$
$$= \sum_{\rho \text{ of } L_\chi} \frac{1}{(\rho+a)^2} - \sum_{\rho \text{ of } \zeta} \frac{1}{(\rho+a)^2} + \frac{1}{a^2} + \frac{1}{(a+1)^2}\,.$$

The result follows. □

Proposition 7.7. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s,\chi)$. We define*

$$\sum_\rho := \sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{|\rho+a|^2}\,.$$

For $x > 0$ we have

$$\frac{x}{(a+1)^2} + \frac{1}{a^2} \;\le\; \sqrt{x}\sum_\rho + 2 \sum_{\substack{n<x \\ \chi(n)\neq 1}} \Lambda(n)(n/x)^a \log(x/n)$$
$$+\frac{\log x}{x^a}\left((a+2)\sum_\rho + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{1}{a} + \frac{1}{a+1} + \frac{3}{2}\right)$$
$$+\frac{1}{x^a}\left(\sum_\rho + \frac{1}{a^2} + \frac{1}{(a+1)^2}\right)\,.$$

Proof. Combine Lemmas 7.3, 7.5, and 7.6. □

Proof of Theorem 7.1. The result for a general character follows from the corresponding result for primitive characters and hence we may assume χ is a primitive character modulo f. Define $x := 2(\log f)^2$. Since $f \ge 10^9$, we have $x > 858$. By way of contradiction, suppose that $\chi(n) = 1$ for all $n < x$.

Apply Proposition 7.7 and set $a = 1/2$. We find

$$\frac{x}{9/4} + 4 \;\le\; \sqrt{x}\sum_\rho + 2 \sum_{\substack{n<x \\ \chi(n)\neq 1}} \Lambda(n)(n/x)^{1/2} \log(x/n)$$
$$+\frac{\log x}{\sqrt{x}}\left(\frac{5}{2}\sum_\rho + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{25}{6}\right) + \frac{1}{\sqrt{x}}\left(\sum_\rho + \frac{40}{9}\right),$$

where $\zeta'(2)/\zeta(2) \approx -0.56996$. Apply Lemma 7.4, together with the fact $\psi_{\mathbb{Q}}(3/2) \approx -1.1153$, to obtain

$$\sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} \leq \frac{1}{2}\log f + 0.437\,.$$

This ultimately leads to $\sqrt{x} < 1.2\log f$ which implies $x < 1.5(\log f)^2$, a contradiction. □

8 Conclusion

We have surveyed some classical results concerning the least quadratic non-residue n_p. Although asking about the size of n_p seems like an innocent question, it has been studied via many different techniques. The proof of the Polya–Vinogradov inequality in section 3 has a Fourier-analytic flavor, a deep theorem from algebraic geometry is employed to prove the Burgess inequality in section 4, we have the large sieve in section 6 which can be couched in terms of functional analysis, and we have complex analysis and use of the Generalized Riemann Hypothesis in section 7. We have also showcased the techniques that one can use to get some explicit results by showing how to recover constants in most of the sections. Despite how well-studied this problem is, we are still far from proving (unconditional) upper bounds that are anywhere close to the truth. We hope that this survey has given the reader an idea of what is known and not known about the least quadratic non-residue.

Acknowledgements

We would like to thank the referee for the careful reading of our manuscript and the suggestions made that improved the paper.

References

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

[2] Eric Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, ACM Distinguished Dissertations, MIT Press, Cambridge, MA, 1985.

[3] ______, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[4] Enrico Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, (1974), 234–241. Lecture Notes in Math., Vol. 383.

[5] Andrew R. Booker, *Quadratic class numbers and character sums*, Math. Comp. **75** (2006), no. 255, 1481–1492.

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

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

[8] ———, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536.

[9] Alina Carmen Cojocaru and M. Ram Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, vol. 66, Cambridge University Press, Cambridge, 2006.

[10] Harold Davenport, *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.

[11] Régis de la Bretèche and Marc Munsch, *Minimizing GCD sums and applications to non-vanishing of theta functions and to Burgess' inequality*, arXiv e-prints (2018), arXiv:1812.03788v4.

[12] V. R. Fridlender, *On the least nth-power non-residue*, Doklady Akad. Nauk SSSR (N.S.) **66** (1949), 351–352.

[13] D. A. Frolenkov and K. Soundararajan, *A generalization of the Pólya-Vinogradov inequality*, Ramanujan J. **31** (2013), no. 3, 271–279.

[14] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 269–309.

[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.

[16] Adolf Hildebrand, *On the constant in the Pólya-Vinogradov inequality*, Canad. Math. Bull. **31** (1988), no. 3, 347–352.

[17] Yasutaka Ihara, V. Kumar Murty, and Mahoro Shimura, *On the logarithmic derivatives of Dirichlet L-functions at $s = 1$*, Acta Arith. **137** (2009), no. 3, 253–276.

[18] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[19] Bryce Kerr, Igor E. Shparlinski, and Kam Hung Yau, *A refinement of the Burgess bound for character sums*, arXiv:1711.10582v1 [math.NT], Nov. 28, 2017.

[20] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[21] Youness Lamzouri, Xiannan Li, and Kannan Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), no. 295, 2391–2412.

[22] Edmund Landau, *Zur Theorie der Heckeschen Zetafunktionen, welche komplexen Charakteren entsprechen*, Math. Z. **4** (1919), no. 1-2, 152–162.

[23] Mariana Levin, Carl Pomerance, and K. Soundararajan, *Fixed points for discrete logarithms*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 6–15.

[24] Pierre Lezowski and Kevin J. McGown, *The Euclidean algorithm in quintic and septic cyclic fields*, Math. Comp. **86** (2017), no. 307, 2535–2549.

[25] Yu. V. Linnik, *The large sieve.*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **30** (1941), 292–294.

[26] ———, *A remark on the least quadratic non-residue*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **36** (1942), 119–120.

[27] Shilin Ma, Kevin J. McGown, Devon Rhodes, and Mathias Wanner, *Explicit bounds for small prime nonresidues*, arXiv:1902.04194v1, Feb. 12, 2019.

[28] Kevin J. McGown, *Norm-Euclidean cyclic fields of prime degree*, Int. J. Number Theory **8** (2012), no. 1, 227–254.

[29] ———, *Norm-Euclidean Galois fields and the generalized Riemann hypothesis*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 425–445.

[30] ———, *On the constant in Burgess' bound for the number of consecutive residues or non-residues*, Funct. Approx. Comment. Math. **46** (2012), no. 2, 273–284.

[31] ———, *On the second smallest prime non-residue*, J. Number Theory **133** (2013), no. 4, 1289–1299.

[32] Kevin J. McGown and Tim Trudgian, *Explicit upper bounds on the least primitive root*, arXiv e-prints (2019), arXiv:1904.12373.

[33] Hugh L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin-New York, 1971.

[34] ———, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), no. 4, 547–567.

[35] 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.

[36] 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.

[37] René Peralta, *On the distribution of quadratic residues and nonresidues modulo a prime number*, Math. Comp. **58** (1992), no. 197, 433–440.

[38] Herbert Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

[39] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[40] Hans Salié, *Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl*, Math. Nachr. **3** (1949), 7–8.

[41] ______, *Über die kleinste Primzahl, die eine gegebene Primzahl als kleinsten positiven quadratischen Nichtrest hat*, Math. Nachr. **29** (1965), 113–114.

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

[43] ______, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976.

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

[45] Enrique Treviño, *The least inert prime in a real quadratic field*, Math. Comp. **81** (2012), no. 279, 1777–1797.

[46] ______, *On the maximum number of consecutive integers on which a character is constant*, Mosc. J. Comb. Number Theory **2** (2012), no. 1, 56–72.

[47] ______, *The Burgess inequality and the least kth power non-residue*, Int. J. Number Theory **11** (2015), no. 5, 1653–1678.

[48] ______, *The least k-th power non-residue*, J. Number Theory **149** (2015), 201–224.

[49] ______, *Corrigendum to "On the maximum number of consecutive integers on which a character is constant" [MR2988388]*, Mosc. J. Comb. Number Theory **7** (2017), no. 3, 1–2.

[50] 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.

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

[52] ______, *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Sém. Math. Univ. Lund [Medd. Lunds Univ. Mat. Sem.] **1952** (1952), no. Tome Supplementaire, 252–265.

[53] ______, *Sur les formules explicites de la théorie des nombres*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 3–18.