LEAST QUADRATIC NON-RESIDUE AND LEAST PRIMITIVE ROOT

CARMEN A. BRUNI

1. Introduction

Finding perfect squares seems like a very easy task. It is clear that $1, 4, 9, 16, ...$ are all squares and the other numbers not in this list are not squares. So finding both squares and non-squares is very straightforward when we are dealing with integers. However, suppose we ask to find non-squares in residue fields, for example in the integers modulo p. In fact, let's make the problem even easier and simply ask for the least non-square. At first, we might think that the answer should be 2 or 3 almost all the time. But when we examine primes p congruent to 1 modulo 24 (of which there are infinitely many by Dirichlet's theorem on arithmetic progressions), we notice that by the law of quadratic reciprocity, we have that $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$ and thus both 2 and 3 are squares in $\mathbb{Z}_p$. For an even more concrete example (without assuming quadratic reciprocity knowledge), suppose $p = 73$. Then, we see that $32^2 \equiv 2 \pmod{73}$ and $21^2 \equiv 3 \pmod{73}$. Hence both are actually squares in $\mathbb{Z}_{73}$. The purpose of this article will be to discuss the behaviour of the least quadratic non-square as well as results relating to primitive roots.

In this article, I will discuss results relating to the problems of finding a least quadratic non-residue modulo p and finding a least primitive root. I start with a review of some of the key definitions, lemmas and notation we will need. These include Dirichlet characters, Gauss sums, and primitive roots. The next section will involve results regarding finding the least quadratic non-residue modulo a prime p. The results of this section that I will present are unconditional results meaning that we require no assumptions about the Riemann hypothesis or any similar unproven results. In particular, we will discuss incomplete character sums and explain their importance towards finding good bounds on the least quadratic non-residue. These sums will allow us to progress from trivial upper bounds to non-trivial ones in short order. The next section will be on primitive roots. Again, we will see where incomplete character sums become useful and how bounding these sums can give us upper bounds on least primitive roots. In the final section, we go through some of the history of conditional results as well as mention a few results about problems related to least quadratic non-residues and primitive roots.

2. Definitions

Throughout let $\mathbb{Z}_p$ denote the set of integers modulo p.

Definition 2.1. We define a *Dirichlet character* of modulus $k \in \mathbb{N}$ to be a function $\chi : \mathbb{Z} \to \mathbb{C}$ not identically zero such that

(i) $\chi(n + k) = \chi(n)$ for all $n \in \mathbb{Z}$.
(ii) $\chi(n) = 0$ if and only if $\gcd(n, k) > 1$.
(iii) $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{N}$.

From these properties, we note that $\chi(1) = 1$, χ is completely multiplicative, and for each $n \in \mathbb{Z}_k^*$, we have that $\chi(n)$ is a $\phi(k)$ complex root of unity.

Example 2.2. The Dirichlet character χ_0 corresponding to $\chi_0(n) = 1$ whenever $\gcd(n, k) = 1$ and 0 otherwise is known as the principal character of modulus k.

Example 2.3. Let p be an odd prime number. We say that $a \in \mathbb{Z}_p^*$ is a *quadratic residue* if there exists an $x \in \mathbb{Z}_p^*$ such that $x^2 \equiv a \pmod{p}$. If such an x does not exist, we say that a is a *quadratic non-residue*. We define the *Legendre symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise.} \end{cases}$$

This defines a Dirichlet character of modulus p.

The following are two theorems very fundamental to the study of the Legendre symbol. The first is a well known result while the second is a result that was proven by Gauss.

Theorem 2.4. *(Euler's Criterion) Let $a \in \mathbb{Z}$ and p an odd prime. Them*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Theorem 2.5. *(Law of Quadratic Reciprocity)*[Coh07, p.35] *Let p, q be two distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

The Legendre symbol at times can be too restrictive as we are not always certain whether or not a number n is prime and hence using the Legendre symbol for $\left(\frac{a}{n}\right)$ may not be valid. Fortunately, there is a natural generalization that when restricted to the case of a and integer and p a prime, the two definition coincide.

Definition 2.6. Let a be any integer and let $n = p_1^{k_1}...p_l^{k_l}$ be a odd integer greater than 1. Then we define the *Jacobi symbol* to be

$$\left(\frac{a}{1}\right) = 1$$

and further

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{l} \left(\frac{a}{p_i}\right)^{k_i}.$$

This, like the Legendre symbol, defines a Dirichlet character of modulus n for odd integers n which can be checked directly from the definition or noticing that hte product of two characters of modulus n is also a character of modulus n. Notice that we lose the condition that a corresponds to a square modulo n, for example, we have that

$$\left(\frac{2}{9}\right) = 1$$

but the only squares modulo 9 are $-1, 0, 1$. However, this allows us to generalize the law of quadratic reciprocity when a and n are both odd. More concretely,

Theorem 2.7. *(Law of Quadratic Reciprocity for Jacobi Sums)*[Coh07, p.36] *Let m, n be two distinct odd positive coprime integers. Then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

Let's return back to the general setting of Dirichlet characters. Suppose we have a Dirichlet character modulo $q \in \mathbb{N}$. Create a character modulo rq for $r > 1$ by defining $\hat{\chi}(a) = \chi(a) \pmod{q}$. While this defines a Dirichlet character modulo rq, it in some sense lives in a smaller modulus. This is where we would like to think $\hat{\chi}$ lives. Via this heuristic, we have actually motivated the definition of a conductor of a character.

Definition 2.8. Let χ be a Dirichlet character of modulus $q \in \mathbb{N}$. We say that d is a *quasiperiod* of χ if $\chi(m) = \chi(n)$ whenever $m \equiv n \pmod{d}$ and $\gcd(mn, q) = 1$. We say that χ is *primitive* when q is the least quasiperiod of χ and *imprimitive* otherwise. This least value is called the *conductor* of χ. When χ is imprimitive, then we say that χ is *induced* from another character with modulus equal to its conductor.

As a summary, it helps to think of primitive character as one that does not arise from another character of smaller modulus. Primitive characters actually live in the modulus that we expect them to live in. A natural question to ask is how many, if any, primitive characters are there modulo q. Before attacking this question, we first need some preliminary lemmas.

Lemma 2.9. *Let ϕ denote the Euler phi function and let $n \in \mathbb{N}$. Then*

$$\sum_{m|n} \phi(m) = n$$

Proof. We partition the set of the first n natural numbers into $d(n)$ disjoint subsets where $d(n)$ is the number of divisors of n. For $m \mid n$, define

$$A_m := \{x \in \mathbb{Z} : 1 \leq x \leq n, \gcd(x, n) = m\}$$

Notice that these sets are pairwise disjoint with their union being the first n natural numbers. Let $x \in A_m$. Set $x = my$ where $y \in \mathbb{N}$. Then, notice that $\gcd(my, n) = m$ if and only if $\gcd(y, \frac{n}{m}) = 1$. Hence, if we set

$$A'_m := \{x \in \mathbb{Z} : 1 \leq x \leq n, \gcd(x, \tfrac{n}{m}) = 1\}$$

then we see that A_m and A'_m have the same number of elements. Further, each A'_m has size $\phi(\frac{n}{m})$ and so combining this information, we see that

$$n = \sum_{m|n} \phi(\tfrac{n}{m}) = \sum_{m|n} \phi(m)$$

and we are finished. ∎

Lemma 2.10. *For $\Re(s) > 2$, we have*

$$\zeta(s) \sum_{q \geq 1} \frac{\phi(q)}{n^s} = \zeta(s-1)$$

where $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is the Riemann zeta function.

Proof. A direct computation using the above lemma now yields

$$\zeta(s) \sum_{q \geq 1} \frac{\phi(q)}{q^s} = \sum_{n \geq 1} \frac{1}{n^s} \sum_{q \geq 1} \frac{\phi(q)}{q^s} = \sum_{n \geq 1} \sum_{q|n} \frac{\phi(q)}{n^s} = \sum_{n \geq 1} \frac{n}{n^s} = \zeta(s-1).$$

The condition $\Re(s) > 2$ is needed to ensure that $\zeta(s-1)$ and $\zeta(s)$ are actually defined to be their series expansion as in the first and last equality. ∎

Lemma 2.11. *Let $\zeta(s)$ be the Riemann zeta function and assume that $\Re(s) > 2$.*

$$\frac{\zeta(s-1)}{\zeta(s)^2} = \prod_p \left(1 + (p-2)p^{-s} + (p-1)^2p^{-2s} + p(p-1)^2p^{-3s} + p^2(p-1)^2p^{-4s} + \ldots\right)$$

Proof. Using the results from [MV07, p.20-22], we have the following Euler product expansion for the function in question

$$\begin{aligned}\frac{\zeta(s-1)}{\zeta(s)^2} &= \prod_p \left(1 + pp^{-s} + p^2p^{-2s} + ...\right)\left(1 - \tfrac{1}{p}\right)^2 \\ &= \prod_p \left(1 + pp^{-s} + p^2p^{-2s} + ...\right)\left(1 - 2p^{-s} + p^{-2s}\right).\end{aligned}$$

Expanding the last product gives

$$\begin{aligned}\frac{\zeta(s-1)}{\zeta(s)^2} = \prod_p \big(1 \quad &+pp^{-s} \quad +p^2p^{-2s} \quad +p^3p^{-3s} \quad +p^4p^{-4s} \quad +... \\ &-2p^{-s} \quad -2pp^{-2s} \quad -2p^2p^{-3s} \quad -2p^3p^{-4s} \quad -... \\ &\qquad +p^{-2s} \quad +pp^{-3s} \quad +pp^{-4s} \quad +...\big)\end{aligned}$$

collecting like terms (or adding the previous equality column wise), we get

$$\frac{\zeta(s-1)}{\zeta(s)^2} = \prod_p \left(1 + (p-2)p^{-s} + (p-1)^2p^{-2s} + p(p-1)^2p^{-3s} + p^2(p-1)^2p^{-4s} + \ldots\right)$$

which is precisely what we wanted to show. ■

Lemma 2.12. *Let f and g be multiplicative functions. Then $F(m) := \sum_{d|m} f(d)g(\frac{m}{d})$ is also multiplicative.*

Proof. To show F is multiplicative, it suffices to show that for all $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$, we have that $F(mn) = F(m)F(n)$. So let $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$. We have that

$$F(mn) = \sum_{d|mn} f(d)g(\tfrac{mn}{d}) = \sum_{d|m}\sum_{e|n} f(ed)g(\tfrac{mn}{ed}) = \sum_{d|m} f(d)g(\tfrac{m}{d}) \sum_{e|n} f(e)g(\tfrac{n}{e}) = F(m)F(n)$$

where in the third equality, we used the fact that both f and g are multiplicative. This completes the proof. ■

Theorem 2.13. *Let $N(q)$ be the number of primitive characters modulo q. Then*

$$N(q) = q\prod_{p\|q}(1 - \tfrac{2}{p})\prod_{p^2|q}(1 - \tfrac{1}{p})^2$$

Proof. Let $\widetilde{\mathbb{Z}_q^*}$ denote the dual group of $\mathbb{Z}_q^*$. In this setting, this is simply the set of Dirichlet characters with modulus q. As the dual group and the original group have the same size [MV07, p.116], we see that

$$\phi(q) = |\mathbb{Z}_q^*| = |\widetilde{\mathbb{Z}_q^*}| = \sum_{m|q} N(m).$$

Now, using the Möbius inversion formula [IR90, p.20], we see that

$$N(m) = \sum_{d|m} \mu(d)\phi(\tfrac{m}{d})$$

Then as $\mu(n)$ is a multiplicative function by [MV07, p.21] and $\phi(n)$ is a multiplicative function, clear from [IR90, p.20], we have $N(m)$ is a multiplicative function by (2.12). Let $\zeta(s)$ be the Riemann zeta function. Looking at the Dirichlet series of $\phi(q)$ where $\Re(s) > 2$ and using the lemma (2.10), we see that

$$\zeta(s)\sum_{m\geq 1}\frac{N(m)}{m^s} = \sum_{q\geq 1}\frac{1}{q^s}\sum_{m\geq 1}\frac{N(m)}{m^s} = \sum_{q\geq 1}\sum_{m|q}\frac{N(m)}{q^s} = \sum_{q\geq 1}\frac{\phi(q)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

Hence $\sum_{m\geq 1}\frac{N(m)}{m^s} = \frac{\zeta(s-1)}{\zeta(s)^2}$. As $N(m)$ is multiplicative, we can invoke [MV07, p. 20] to see that

$$\sum_{m\geq 1}\frac{N(m)}{m^s} = \prod_p \left(1 + N(p)p^{-s} + N(p^2)p^{-2s} + ...\right).$$

Hence, to compute $N(q)$, we need to look at the q^{-s} coefficient of the Euler product of $\frac{\zeta(s-1)}{\zeta(s)^2}$. By (2.11),

$$\frac{\zeta(s-1)}{\zeta(s)^2} = \prod_p \left(1 + (p-2)p^{-2} + (p-1)^2p^{-2s} + p(p-1)^2p^{-3s} + p^2(p-1)^2p^{-4s} + \ldots\right).$$

From this, it is clear that the q^{-s} coefficient of this function depends on whether or not a prime fully divides q. If $p \parallel q$, then we get a $p-2$ term. Otherwise, whenever $p^k \parallel q$ for $k \geq 2$, we get a $p^{k-2}(p-1)^2$ term. Hence, the q^{-s} coefficient of the function $\frac{\zeta(s-1)}{\zeta(s)^2}$ is

$$\prod_{p\|q}(p-2)\prod_{\substack{p^k\|q\\ k\geq 2}}p^{k-2}(p-1)^2 = q\prod_{p\|q}(1-\tfrac{2}{p})\prod_{p^2|q}(1-\tfrac{1}{p})^2$$

which gives the formula we sought. ■

Corollary 2.14. *There are no primitive characters with $q \equiv 2 \pmod 4$*

Proof. By the above theorem, notice that when $q \equiv 2 \pmod 4$, then $2 \parallel q$ and so in particular, the first product is 0 and hence $N(q) = 0$. ■

We finish our digression with primitive characters to prove one more theorem on sums of primitive characters.

Theorem 2.15. *Let χ be a primitive Dirichlet character of modulus $q \in \mathbb{N}$. Let d be an integer with $d \mid q$ and $d < q$. Then*

$$S := \sum_{\substack{a=1\\ a\equiv h \pmod d}}^{q} \chi(a) = 0$$

Proof. Since χ is primitive, there are integers $\alpha \equiv \beta \pmod d$ with $\chi(\alpha) \neq \chi(\beta)$ and also $\gcd(\alpha\beta, q) \neq 0$ (for otherwise, d is a quasiperiod less than q, contradicting the primitivity of χ). Notice that the greatest common divisor condition implies that $\chi(\alpha\beta) \neq 0$. Pick an

integer γ so that $(\gamma, q) = 1$ and $\gamma\alpha \equiv \beta \pmod{q}$. Notice that by definition of a Dirichlet character, we have

$$\chi(\gamma)\chi(\alpha) = \chi(\gamma\alpha) = \chi(\beta) \quad \Rightarrow \quad \chi(\gamma) \neq 1$$

and $\gamma \equiv 1 \pmod{d}$. Now, consider $a = h\gamma + k\gamma d$. Note this reduces to $a \equiv h \pmod{d}$. Further, as k runs through a complete residue system for $\frac{q}{d}$, we see that $h\gamma + k\gamma d$ will as well since $\gcd(\gamma, q) = 1$. Hence, we have that

$$\begin{aligned} S = \sum_{\substack{a=1 \\ a\equiv h \pmod{d}}}^{q} \chi(a) &= \sum_{k=1}^{\frac{q}{d}} \chi(h\gamma + k\gamma d) = \chi(\gamma) \sum_{k=1}^{\frac{q}{d}} \overline{\chi(h + kd)} = \chi(\gamma) \sum_{\substack{a=1 \\ a\equiv h \pmod{d}}}^{q} \overline{\chi(a)} \\ &= \chi(\gamma) S. \end{aligned}$$

Thus $S(\chi(\gamma) - 1) = 0$ and by choice of γ we must have that $S = 0$ and we are done. ■

We shift gears now and discuss Gauss sums. One of the first applications of these sums was to prove the law of quadratic reciprocity. We will see these sums appear in the proof of the Pólya–Vinogradov bound in section 3.

Definition 2.16. Let χ be a Dirichlet character of modulus q. Define the *Gauss sum* to be

$$G(x, \chi) = \sum_{a=1}^{q} \chi(a) e^{2\pi i a x/q}$$

and further, let $G(\chi) := G(1, \chi)$.

Lemma 2.17. *Let χ be a Dirichlet character of modulus q. Suppose that $\gcd(n, q) = 1$ for some integer n. Then*

$$G(x, \chi) = \chi(n) \sum_{b=1}^{q} \chi(b) e^{2\pi i b n/q}$$

Proof. We apply a change of coordinates $a \mapsto bn$ in the Gauss sum and see that

$$G(x, \chi) = \sum_{a=1}^{q} \chi(a) e^{2\pi i a/q} = \chi(n) \sum_{b=1}^{q} \chi(b) e^{2\pi i b n/q}.$$

This change of coordinates is valid since bn runs over all the same residue classes as a does under the assumption that $\gcd(n, q) = 1$. This completes the proof. ■

Lemma 2.18. *Let χ be a primitive Dirichlet character of modulus q. Let x be a non negative integer and when $q \neq 1$, suppose that $\gcd(x, q) > 1$. Then*

$$G(x, \chi) = \begin{cases} 1 & \text{if } q = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. If $\gcd(x, q) = q$, then notice that

$$G(x, \chi) = \sum_{a=1}^{q} \chi(a) e^{2\pi i a x/q} = \sum_{a=1}^{q} \chi(a) = G(q, \chi).$$

I claim this last sum is 0 if $q \neq 1$ and 1 if $q = 1$. The latter claim is obvious so suppose $q \neq 1$. Then choose b so that $\chi(b) \neq 1$ (possible as χ is not principal). Then using (2.17), which is valid as $\gcd(b, q)$ must be 1 since its value at χ is nonzero, we have

$$G(q, \chi) = \chi(b) G(q, \chi).$$

Hence, $(\chi(b)-1)G(q,\chi)=0$ and as $\chi(b)\neq 1$, we have that $G(q,\chi)=0$. Now, assume $1<d:=\gcd(x,q)<q$. Let $\frac{x}{q}=\frac{m}{n}$ where $\gcd(m,n)=1$ and $n\mid q$. Then by organizing the Gauss sum by the exponential term, we get

$$G(x,\chi)=\sum_{a=1}^{q}\chi(a)e^{2\pi iax/q}=\sum_{h=1}^{d}\sum_{\substack{a=1\\ a\equiv h \pmod d}}^{q}\chi(a)e^{2\pi ihm/n}=\sum_{h=1}^{d}e^{2\pi ihm/n}\sum_{\substack{a=1\\ a\equiv h \pmod d}}^{q}\chi(a)=0$$

where the last equality holds by using d with (2.15). This completes the proof. ■

Theorem 2.19. *If χ is a primitive Dirichlet character modulo $q\in\mathbb{N}$, then $|G(\chi)|=\sqrt{q}$*

Proof. The claim is trivial when $q=1$ since $G(x,\chi)=1$ by (2.18) so without loss of generality, suppose that $q>1$. We evaluate the sum

$$\sum_{x\in\mathbb{Z}_q}G(x,\chi)\overline{G(x,\chi)}$$

in two different ways. First,

$$\begin{aligned}\sum_{x\in\mathbb{Z}_q}G(x,\chi)\overline{G(x,\chi)}&=\sum_{x\in\mathbb{Z}_q}\sum_{a=1}^{q}\chi(a)e^{2\pi iax/q}\overline{\sum_{b=1}^{q}\chi(b)e^{2\pi ibx/q}}\\&=\sum_{x\in\mathbb{Z}_q}\sum_{a=1}^{q}\sum_{b=1}^{q}\chi(a)e^{2\pi iax/q}\overline{\chi(b)}e^{-2\pi ibx/q}\\&=\sum_{a=1}^{q}\sum_{b=1}^{q}\chi(a)\overline{\chi(b)}\sum_{x\in\mathbb{Z}_q}e^{2\pi i(a-b)x/q}\end{aligned}$$

Now, the last sum is simply a sum of ones if $a=b$ and hence gives us the value q. If $a\neq b$, then this is a sum of primitive qth roots of unity and hence is 0 (alternatively, one can use the geometric series formula to get this answer as well). Thus,

$$\sum_{x\in\mathbb{Z}_q}G(x,\chi)\overline{G(x,\chi)}=\sum_{a=1}^{q}\sum_{b=1}^{q}\chi(a)\overline{\chi(b)}\delta_{a,b}q=\sum_{a=1}^{q}|\chi(a)|^2q=q\phi(q)\tag{1}$$

where $\delta_{a,b}$ is the Kronecker delta (1 if $a=b$ and 0 otherwise). Also, for $x\in\mathbb{Z}_q^*$, we apply (2.17) and see that

$$G(\chi)=\chi(x)G(x,\chi)\quad\Rightarrow\quad G(x,\chi)=\chi(x^{-1})G(\chi)$$

and hence

$$\sum_{x\in\mathbb{Z}_q^*}G(x,\chi)\overline{G(x,\chi)}=\sum_{x\in\mathbb{Z}_q^*}\chi(x^{-1})G(\chi)\overline{\chi(x^{-1})G(\chi)}=\sum_{x\in\mathbb{Z}_q^*}|\chi(x^{-1})|^2|G(\chi)|^2=\phi(q)|G(\chi)|^2.$$

Now, suppose $x\in\mathbb{Z}_q$ but not a unit so that $1<\gcd(x,q)<q$. By (2.18), we see that $G(x,\chi)=0$. Hence combining this with the above, we see that

$$\sum_{x\in\mathbb{Z}_q}G(x,\chi)\overline{G(x,\chi)}=\sum_{x\in\mathbb{Z}_q^*}G(x,\chi)\overline{G(x,\chi)}=\phi(q)|G(\chi)|^2\tag{2}$$

Equating (1) and (2), we see that

$$q\phi(q)=\sum_{x\in\mathbb{Z}_q}G(x,\chi)\overline{G(x,\chi)}=\phi(q)|G(\chi)|^2\Rightarrow|G(\chi)|=\sqrt{q}$$

as claimed. ■

Theorem 2.20. *If χ is a Dirichlet character modulo $q \in \mathbb{N}$ and $\gcd(n, q) = 1$, then*

$$\chi(n)G(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi(a)} e^{2\pi i a n/q}.$$

Further, the result holds in the case when χ is a primitive Dirichlet character modulo q and $\gcd(n, q) > 1$.

Proof. Let χ be a Dirichlet character modulo $q \in \mathbb{N}$ and $\gcd(n, q) = 1$. Then (2.17) tells us that

$$\chi(n)G(\overline{\chi}) = \chi(n)\overline{\chi(n)} \sum_{b=1}^{q} \overline{\chi(b)} e^{2\pi i b n/q} = \sum_{b=1}^{q} \overline{\chi(b)} e^{2\pi i b n/q}$$

Now, suppose χ is a primitive Dirichlet character modulo q and $\gcd(n, q) > 1$. In this case, the left hand side is 0 as $\chi(n) = 0$. Applying (2.18), we have that $G(n, \overline{\chi}) = 0$ which completes the proof. ∎

Corollary 2.21. *Let χ be a primitive Dirichlet character of modulus q. Then*

$$\chi(n) = \frac{1}{G(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi(a)} e^{2\pi i a n/q}$$

Proof. From (2.19) we know that $G(\overline{\chi}) \neq 0$ and applying (2.20) and isolating for $\chi(n)$ gives the desired result. ∎

The last preliminary tool we will need are primitive roots.

Definition 2.22. Let p be an odd prime. We say that g is a primitive root for $\mathbb{Z}_p$ if $\langle g \rangle = \mathbb{Z}_p^*$.

A standard result from elementary number theory is the following.

Theorem 2.23. *There are $\phi(p-1)$ primitive roots modulo p.* [IR90, p. 40]

Definition 2.24. Fix a primitive root g modulo p. Define for $n \in \mathbb{Z}_p^*$, the index of n, $\operatorname{ind}_g(n)$, to be the least positive integer k with $n = g^k$.

Theorem 2.25. *Let p be a prime and $\langle g \rangle = \mathbb{Z}_p^*$. Then $n \in \mathbb{Z}_p^*$ is a primitive root modulo p if and only if $\gcd(\operatorname{ind}_g(n), p-1) = 1$*

Proof. Let $d = \gcd(\operatorname{ind}_g(n), p-1)$ and $k = \operatorname{ind}_g(n)$. Notice that n is a primitive root modulo p if and only if $\operatorname{ord}_p(n) = \phi(p) = p-1$ where $\operatorname{ord}_p(n)$ denotes the least such integer so that $n^{\operatorname{ord}_p(n)} \equiv 1 \pmod{p}$. As g is a primitive root, we know that the order of g is $p-1$. Hence, $n \equiv g^k \pmod{p}$ implies that

$$n^{\frac{p-1}{d}} \equiv g^{\frac{k(p-1)}{d}} \equiv (g^{p-1})^{\frac{k}{d}} \equiv 1 \pmod{p}$$

This means that n has order $p-1$ if and only if $d = 1$ as required. ∎

3. Least Quadratic Non-Residue

We begin this section with a basic starting bound on the least quadratic non-residue.

Theorem 3.1. *Let p be an odd prime. Let n be the least quadratic non-residue of $\mathbb{Z}_p$. Then $n < 1 + \sqrt{p}$.*

Proof. First, note that $0 < n < p$. Now, choose $m \in \mathbb{Z}$ minimal so that $mn > p$. Then, $(m-1)n \leq p$. As p is prime, combining this with the bounds on n, we have that $(m-1)n \neq p$. Rearranging, we have that $0 < mn - p < n$ and so, by choice of n, we have that $\left(\frac{mn-p}{p}\right) = 1$. By the properties of the Legendre symbol, we have that

$$1 = \left(\frac{mn-p}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = -\left(\frac{m}{p}\right)$$

and hence $\left(\frac{m}{p}\right) = -1$. Thus $m \geq n$. Combining these results gives

$$(n-1)^2 < (n-1)n \leq (m-1)n < p$$

and isolating gives $n < 1 + \sqrt{p}$. ■

Here, we discuss the work of Pólya and Vinogradov in 1918. One of the key components in getting nontrivial results with regard to the least quadratic non-residue will be to bound certain types of *incomplete sums*. The first of which is known as the Pólya–Vinogradov inequality, discovered by George Pólya and Ivan Vinogradov independently in 1918. One of the key important parts to the inequality as we will see is that we can consider the sums of characters to be over any integer interval. Thus not only will we get a bound on where the least quadratic residue is, but also bounds on the number of primitive roots modulo a prime in any interval.

Definition 3.2. Let χ be a Dirichlet character modulo $q \in \mathbb{N}$ and let $M, N \in \mathbb{Z}$ with $N > 0$. We say that the sum $\sum_{n=M+1}^{M+N} \chi(n)$ is *incomplete* if $N < q$.

Using the techniques developed for Gauss sums, we will show that if χ is a non-principal character, then this sum is $o(N)$ provided that N is relatively large when compared to q. First, we require a few lemmas before we get to the main theorem.

Lemma 3.3. *Let $a, q, M, N \in \mathbb{Z}$ with $N > 0$ and set $m_a = \frac{a}{q}$. Then*

$$\sum_{n=M+1}^{M+N} e^{2\pi i n m_a} = \begin{cases} N & \text{if } m_a \in \mathbb{Z} \\ e^{(2M+N+1)\pi i m_a}\left(\frac{\sin(\pi N m_a)}{\sin(\pi m_a)}\right) & \text{if } m_a \notin \mathbb{Z}. \end{cases}$$

Proof. Let $m_a := \frac{a}{q}$. Notice that the right most inner sum is actually a geometric series and hence

$$\sum_{n=M+1}^{M+N} e^{2\pi i n m_a} = \begin{cases} N & \text{if } m_a \in \mathbb{Z} \\ e^{2\pi i (M+1) m_a}\left(\frac{e^{2\pi i (N) m_a} - 1}{e^{2\pi i m_a} - 1}\right) & \text{if } m_a \notin \mathbb{Z}. \end{cases}$$

So we consider only the case when $m_a \notin \mathbb{Z}$. Here, we further simplify to see

$$\begin{aligned} \sum_{n=M+1}^{M+N} e^{2\pi i n m_a} &= e^{2\pi i (M+1) m_a + \pi i (N) m_a - \pi i m_a}\left(\frac{e^{\pi i (N) m_a} - e^{-\pi i (N) m_a}}{e^{\pi i m_a} - e^{-\pi i m_a}}\right) \\ &= e^{(2M+N+1)\pi i m_a}\left(\frac{\sin(\pi N m_a)}{\sin(\pi m_a)}\right) \end{aligned}$$

where in the last equality, we use the fact that $2i\sin(x) = e^{ix} - e^{-ix}$. ■

Lemma 3.4. *In $[0, \frac{1}{2}]$, we have that $\sin(\pi x) \geq 2x$.*

Proof. Notice that $\sin(\pi x)$ is concave down in $[0, \frac{1}{2}]$. Thus, it lies above the line segment through the origin and $(\frac{1}{2}, 1)$. Hence, $\sin(\pi x) \geq 2x$ on $[0, \frac{1}{2}]$ as claimed. ■

Lemma 3.5. *For $x \in [1, \infty]$, we have that $\frac{1}{x} < \log(\frac{2x+1}{2x-1})$.*

Proof. Notice that $1 < \log(3)$ so without loss of generality, suppose $0 < \frac{1}{x} < 1$. By changing $\frac{1}{x}$ to x, it suffices to show that $x < \log(\frac{2+x}{2-x})$ on $(0, 1)$. Set $f(x) := \log(\frac{2+x}{2-x})$. Notice that $f'(x) = \frac{1}{2+x} - \frac{1}{2-x} = \frac{4}{4-x^2}$ and so $f'(0) = 0$. Thus, the tangent line at $x = 0$ is $y = x$. As the derivative is increasing on the interval, $f(x)$ is convex there. Hence, the function lies above the tangent line and thus the inequality holds. ■

Theorem 3.6. *(Pólya–Vinogradov Inequality) Let χ be a non-principal Dirichlet character modulo q for $q > 1$ an integer and $M, N \in \mathbb{Z}$ with $N > 0$. Then*

$$\sum_{n=M+1}^{M+N} \chi(n) \ll \sqrt{q} \log(q).$$

Proof. First, assume χ is primitive. Then we apply (2.21) and (3.3) to see that

$$\begin{aligned}\sum_{n=M+1}^{M+N} \chi(n) &= \frac{1}{G(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi(a)} \sum_{n=M+1}^{M+N} e^{2\pi i a n/q} \\ &= \frac{1}{G(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi(a)} e^{(2M+N+1)\pi i \frac{a}{q}} \left(\frac{\sin(\pi N \frac{a}{q})}{\sin(\pi \frac{a}{q})} \right).\end{aligned}$$

When $\frac{a}{q} \in \mathbb{Z}$, notice that we would have that $\gcd(a, q) > 1$ and hence that $\overline{\chi(a)} = 0$ so we only get a right hand side contribution when $\frac{a}{q} \notin \mathbb{Z}$. Using (2.19), the triangle inequality, and the fact that $\sin(x)$ is non-negative from $[0, \pi]$, we combine this information with the above to see that

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq \frac{1}{\sqrt{q}} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q-1} \frac{1}{\sin(\pi \frac{a}{q})}.$$

By the symmetry of the sine function, we see that the above sum contributes the same amount over the first half as it does over the second half. So we can consider only half the interval and take twice the value. This reduces us to the case when the interval is $1 \leq a \leq \frac{q-1}{2}$ when q is odd. When q is even we have to worry about the pivot case. Notice that when q is even, then $4 \mid q$ as well for if not, then $q \equiv 2 \pmod 4$ and so we have a primitive Dirichlet character with modulus congruent to 2 modulo 4, which contradicts (2.14). Hence in this case $\gcd(\frac{q}{2}, q) > 1$ and so the $\frac{q}{2}$ term is omitted from our sum. thus, in this case, our interval is symmetric about $1 \leq a \leq \frac{q}{2} - 1 = \lfloor \frac{q-1}{2} \rfloor$. Thus, the above sum reduces to

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq \frac{2}{\sqrt{q}} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{\lfloor \frac{q-1}{2} \rfloor} \frac{1}{\sin(\pi \frac{a}{q})}.$$

Applying (3.4) and (3.5) to our sum, we see that

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq \frac{2}{\sqrt{q}} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{\lfloor \frac{q-1}{2} \rfloor} \frac{1}{\sin(\pi \frac{a}{q})} < \sqrt{q} \sum_{a=1}^{\lfloor \frac{q-1}{2} \rfloor} \frac{1}{a} < \sqrt{q} \sum_{a=1}^{\lfloor \frac{q-1}{2} \rfloor} \log(\frac{2a+1}{2a-1}) \leq \sqrt{q} \log(q)$$

where the last equality holds by noticing that the previous sum is telescoping.

Now, we suppose that χ is an imprimitive non-principal character. Suppose that χ is induced by χ^* modulo t. Define

$$r := \prod_{\substack{p|q, p\nmid t \\ p \text{ prime}}} p$$

Then, letting μ denote the Möbius function

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

$$= \left|\sum_{k|r} \mu(k) \sum_{\substack{M<n\leq M+N \\ k|n}} \chi^*(n)\right| = \left|\sum_{k|r} \mu(k)\chi^*(k) \sum_{\frac{M}{k}<m\leq\frac{M+N}{k}} \chi^*(m)\right|.$$

Now, notice that the last summation is the sum over a primitive non-principal Dirichlet character and hence by the above

$$\sum_{\frac{M}{k}<m\leq\frac{M+N}{k}} \chi^*(m) \ll \sqrt{t}\log(t).$$

Thus, applying this inequality gives

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \ll \left|\sum_{k|r} \mu(k)\chi^*(k)\sqrt{t}\log(t)\right| \leq \sqrt{t}\log(t)\sum_{k|r} 1 \leq \sqrt{t}\log(t)d(r)$$

$$\ll \sqrt{t}\log(t)\sqrt{r} \leq \sqrt{t}\log(t)\sqrt{\frac{q}{t}} \leq \sqrt{q}\log(q).$$

This finish the proof for imprimitive non-principal characters. ■

Since Pólya and Vinogradov announced their proof, there has been other research done on incomplete character sums. Burgess [Bur62] in the early 1960's had managed to improve the 1918 bound with the following result.

Theorem 3.7. *(Burgess) For any prime p and any non-principal Dirichlet character χ of modulus p and any $N, r \in \mathbb{N}$ with $M \in \mathbb{Z}$, we have that*

$$\sum_{n=M+1}^{M+N} \chi(n) \ll N^{1-\frac{1}{r+1}} p^{\frac{1}{4r}} \log(p)$$

Let $\epsilon > 0$ and suppose we take p to be a large prime and suppose that $N = \lceil p^{\frac{1}{4}+\epsilon} \rceil$. Choose r with $r > \frac{1}{\epsilon} + 1$ and $\epsilon_1 = \frac{\epsilon}{4(r+1)}$. The Burgess bound then tells us that

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \ll \frac{N}{N^{\frac{1}{r+1}}} p^{\frac{1}{4r}+\epsilon_1}$$

$$< N p^{(\frac{1}{4}+\epsilon)\frac{-1}{r+1}\frac{1}{4r}+\epsilon_1} < N p^{\frac{-\epsilon^2(2+3\epsilon)}{4(1+2\epsilon)(1+\epsilon)}}.$$

Setting $\delta = \frac{\epsilon^2(2+3\epsilon)}{4(1+2\epsilon)(1+\epsilon)} > 0$, we see that

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \ll Np^{-\delta}$$

where $\delta > 0$ depends only on ϵ. Equipped with this power up version of the Pólya–Vinogradov Inequality, we can use this to get results on the least quadratic residue for general characters.

Corollary 3.8. *Let χ be a non-principal Dirichlet character of modulus p a prime. Let n_χ be the least positive integer n with $\chi(n) \neq 1$. Then $n_\chi \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$ for all $\epsilon > 0$.*

Proof. Let $\epsilon > 0$. Let $P(n)$ denote the largest prime dividing n and let $\psi(x, y)$ denote the number of integers between 1 and x all of whose prime factors are less than y. Namely,

$$\psi(x, y) = |\{n \leq x : p \mid n \Rightarrow p \leq y\}|$$

Suppose that $\chi(n) = 1$ for $n \leq y$. Then if we have an integer m that has all of its prime divisors less than y, then $\chi(m) = 1$. Our goal will be to find a bound on y and hence on n_χ. If $y \leq x < y^2$, we see that

$$\sum_{n\leq x} \chi(n) = \psi(x, y) + \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \chi(q)|\{n \leq x : P(n) = q\}| = \psi(x, y) + \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \chi(q) \left\lfloor \frac{x}{q} \right\rfloor$$

Taking the absolute value and simplifying, we see that

$$\begin{aligned} \left| \sum_{n\leq x} \chi(n) \right| &\geq \psi(x, y) - \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \left\lfloor \frac{x}{q} \right\rfloor = \lfloor x \rfloor - \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \sum_{\substack{n\leq x \\ q|n}} 1 - \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \left\lfloor \frac{x}{q} \right\rfloor \\ &= \lfloor x \rfloor - 2 \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \left\lfloor \frac{x}{q} \right\rfloor = x - 2x \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \frac{1}{q} + O(\pi(x)) \end{aligned}$$

Using the estimates of Chebyshev and Mertens [MV07, p.49-50], we have that

$$\begin{aligned} x - 2x \sum_{\substack{y<q\leq x \\ q \text{ prime}}} \frac{1}{q} + O(\pi(x)) &= x - 2x \left(\sum_{q\leq x} \frac{1}{q} - \sum_{y<q} \frac{1}{q} \right) + O(\pi(x)) \\ &= x - 2x \Bigg(\log\log(x) + O\left(\frac{1}{\log(x)}\right) + b - \log\log(y) \\ &\qquad - O\left(\frac{1}{\log(y)}\right) - b \Bigg) + O\left(\frac{x}{\log x}\right) \\ &= x \left(1 - 2\log\left(\frac{\log(x)}{\log(y)}\right)\right) + O\left(\frac{x}{\log x}\right) \end{aligned}$$

where b is a constant arising naturally from the bound. This gives us that

$$\left| \sum_{n\leq x} \chi(n) \right| \geq x \left(1 - 2\log\left(\frac{\log(x)}{\log(y)}\right)\right) + O\left(\frac{x}{\log x}\right)$$

Now[1], set $x = p^{\frac{1}{4}+\epsilon+2\delta}$ where $\epsilon > 0$ and δ is defined as in the Burgess bound (3.7). The Burgess bound tells us that the sum on the left is $o(x)$ while if $y > x^{\frac{1}{\sqrt{e}}+\epsilon}$, the quantity on the right is $\Omega_\epsilon(x)$ since

$$x\left(1-2\log\left(\frac{\log(x)}{\log(y)}\right)\right)+O\left(\frac{x}{\log x}\right) > x\left(1-2\log\left(\frac{\sqrt{e}}{\epsilon\sqrt{e}+1}\right)\right)+O\left(\frac{x}{\log x}\right)$$
$$= 2\log(\epsilon\sqrt{e}+1)x+O\left(\frac{x}{\log x}\right)$$

and this is a contradiction. Thus, for this value of x, we must have that

$$y \leq x^{\frac{1}{\sqrt{e}}+\epsilon} \Rightarrow n_\chi \ll_\epsilon x^{\frac{1}{\sqrt{e}}+\epsilon} \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$$

as claimed. ■

Up to this point, all of these results have been unconditionally true. We can do better than these results if we decide to assume the truth of the generalized Riemann hypothesis. These results we will talk about in the final section. All of the above results have also talked about upper bounds. What about lower bounds on the least quadratic non-residue? In Ankeny ([Ank52]), we have mention of the following result first proven by Chowla. Before I mention the result, I would like to first prove a lemma we will need.

Lemma 3.9. *For $n \geq 2$, the product of all primes less than or equal to n is bounded above by 4^n. That is,*

$$\prod_{p\leq n} p \leq 4^n$$

Proof. We prove this result by strong induction on n. For $n = 2$, the claim is trivial. Further, if the result is true for odd n, then it is true for $n+1$ simply by noting that $n+1$ is even and hence never prime. So, we assume the result is true for all n less than some even number say $2m$. From here, we show that

$$\prod_{m+1<p\leq 2m+1} p \leq 4^m. \tag{3}$$

If this is true, then we have via the induction hypothesis that

$$\prod_{p\leq 2m+1} p = \prod_{1<p\leq m+1} p \prod_{m+1<p\leq 2m+1} p \leq 4^{m+1}4^m = 4^{2m+1}.$$

Now, to prove (3), We notice that every prime p between $m+1$ and $2m+1$ must be present in the numerator (and not in the denominator) of $\binom{2m+1}{m}$. Hence, it is clear that

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m}.$$

Now, notice that $\binom{2m+1}{m}$ must occur exactly twice in the binomial expansion of $(1+1)^{2m+1}$ and hence

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq \frac{1}{2}(1+1)^{2m+1} = 4^m.$$

completing the proof.

■

[1]If we use the Pólya–Vinogradov inequality, then we choose $x = p^{\frac{1}{2}}\log(p)^2$ and we get a weaker bound.

Theorem 3.10. *(Chowla) There exist infinitely many primes p for which the least quadratic non-residue is $\gg \log(p)$.*

Proof. The idea of this proof will be to choose a prime p that satisfies a lot of congruences. Suppose first that $p \equiv 1 \pmod 8$ so that $\left(\frac{2}{p}\right) = 1$. Further, this choice of p makes the law of quadratic reciprocity work nicely, that is $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Let y be a parameter and for each prime $2 < q < y$, we want $p \equiv 1 \pmod q$. If this is true, then

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

Set $Q := 8\prod_{2<q<y} q$. Applying the Chinese remainder theorem, if $p \equiv 1 \pmod Q$, then the least quadratic non-residue is greater than y. Now, by Linnik's theorem [Lin44] (which gives us a bound on the least prime in an arithmetic progression), there exists a prime p such that $p \ll Q^L$ for some constant L (we can choose $L = 6$ for example). The prime number theorem gives us that

$$Q \ll 4^y$$

and hence, as the least quadratic non-residue is at least the size of y, by the above,

$$y \gg \log_4(Q) \asymp \log(Q) \gg \log(p).$$

This completes the proof. ∎

4. Least Primitive Roots

Our last topic of this article will be least primitive roots. We can use many of the results from the previous section on least quadratic roots to help us to get bounds on primitive roots.

Lemma 4.1. *Let p be a prime and set $Q = \prod_{q_i|(p-1)} q_i$ for distinct primes q_i. Further, for all $n \in \mathbb{Z}_p^*$, set $\chi_0(n) = 1$ and $\chi_i(n) = e^{2\pi i \mathrm{ind}_g(n)/q_i}$. Then*

$$\prod_{i=1}^{r}\left(\chi_0(n) - \frac{1}{q_i}\sum_{a=1}^{q_i}\chi_i(n)^a\right) = \sum_{d|Q}\phi(\tfrac{Q}{d})\tfrac{\mu(d)}{Q}\sum_{\substack{\chi \pmod Q \\ \mathrm{ord}\,(\chi)=d}}\chi(n)$$

for all $n \in \mathbb{Z}_p^*$.

Proof. Rearranging the sum, we see that

$$\prod_{i=1}^{r}\left(\chi_0(n) - \frac{1}{q_i}\sum_{a=1}^{q_i}\chi_i(n)^a\right) = \prod_{i=1}^{r}\left((1-\tfrac{1}{q_i})\chi_0(n) - \frac{1}{q_i}\sum_{a=1}^{q_i-1}\chi_i(n)^a\right)$$

and hence it suffices to show that

$$\prod_{i=1}^{r}\left((1-\tfrac{1}{q_i})\chi_0(n) - \frac{1}{q_i}\sum_{a=1}^{q_i-1}\chi_i(n)^a\right) = \sum_{d|Q}\phi(\tfrac{Q}{d})\tfrac{\mu(d)}{Q}\sum_{\substack{\chi \pmod Q \\ \mathrm{ord}\,(\chi)=d}}\chi(n).$$

We expand term by term. Let $d \mid Q$. Then

$$\prod_{q_i\nmid d}\Big((1-\tfrac{1}{q_i})\chi_0(n)\Big) = \prod_{q_i\nmid d}\Big((\tfrac{\phi(q_i)}{q_i})\chi_0(n)\Big) = \phi(\tfrac{Q}{d})\tfrac{d}{Q}\chi_0(n).$$

Next, we note that

$$\prod_{q_i|d} \frac{-1}{q_i} = \frac{\mu(d)}{d}.$$

Finally, notice that our χ_i form a complete set of characters modulo q_i. Thus, when we multiply all the possible combinations of characters modulo q_i that are not principal, we get a set of all possible Dirichlet characters of modulus d. This can be seen combinatorially. When we multiply this out, we have $\prod_i \phi(q_i) = \phi(d)$ distinct Dirichlet characters and each is of modulus d. As there are only $\phi(d)$ Dirichlet characters of modulus d (see the argument in (2.13)), we see that we have a complete set. Thinking about this in a different light, these also will form the Dirichlet characters of modulus Q whose order (that is, the value f such that $\chi^f = \chi_0$ denoted $\text{ord}\,(\chi)$) is simply d. Hence

$$\prod_{q_i|d} \sum_{a=1}^{q_i-1} \chi_i(n)^a = \sum_{\substack{\chi \pmod Q \\ \text{ord}\,(\chi)=d}} \chi(n).$$

Multiplying the above for each $d \mid Q$ then summing over all such d and in the cases when $d = 1$ or $d = Q$, setting where appropriate the above empty sums to be 1 gives

$$\begin{aligned}\prod_{i=1}^{r} \left((1 - \tfrac{1}{q_i})\chi_0(n) - \frac{1}{q_i} \sum_{a=1}^{q_i-1} \chi_i(n)^a \right) &= \sum_{d|Q} \phi(\tfrac{Q}{d}) \tfrac{d}{Q} \tfrac{\mu(d)}{d} \sum_{\substack{\chi \pmod Q \\ \text{ord}\,(\chi)=d}} \chi(n) \\ &= \sum_{d|Q} \phi(\tfrac{Q}{d}) \tfrac{\mu(d)}{Q} \sum_{\substack{\chi \pmod Q \\ \text{ord}\,(\chi)=d}} \chi(n)\end{aligned}$$

as required. ■

Theorem 4.2. *The number of primitive roots modulo p, an odd prime, inside the interval $[M+1, M+N]$ for $M \in \mathbb{Z}$ and N a positive integer is $\frac{\phi(p-1)}{p} N + O(p^{\frac{1}{4}+\epsilon})$ for all $\epsilon > 0$.*

Proof. By the fundamental theorem of arithmetic, let $p - 1 = \prod_{i=1}^{r} q_i^{c_i}$ for positive c_i where each q_i is prime and further set $Q := \prod_{i=1}^{r} q_i$. Then $n \in \mathbb{Z}_p^*$ is a primitive root modulo p if and only if $\gcd(\text{ind}_g(n), Q) = 1$ by (2.25). For $1 \le i \le r$, set $\chi_i(n) = e^{2\pi i \text{ind}_g(n)/q_i}$. Notice that each χ_i is a Dirichlet character and further that

$$\frac{1}{q_i} \sum_{a=1}^{q_i} \chi_i(n)^a = \begin{cases} 1 & \text{if } q_i \mid \text{ind}_g(n) \\ 0 & \text{otherwise} \end{cases}$$

which holds since if $q_i \mid \text{ind}_g(n)$, then we are summing 1 a total of q_i times and if not, then we note this result by either using a geometric sum expansion or alternatively, by noting that we are summing all of the q_ith roots of unity which will give us 0. Further, we see that by the greatest common divisor characterization of primitive roots given above, we have that

$$\prod_{i=1}^{r} \left(\chi_0(n) - \frac{1}{q_i} \sum_{a=1}^{q_i} \chi_i(n)^a \right) = \begin{cases} 1 & \text{if } n \text{ is a primitive root modulo } p \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where we note that $\chi_0(n) = 1$ for each n. We need this term to get a 0 value whenever $q_i \mid \text{ind}_g(n)$. Thus, we have a formula that computes whether or not n is a primitive root.

Now, using (4.1) we see that

$$\prod_{i=1}^{r}\left(\chi_0(n)-\frac{1}{q_i}\sum_{a=1}^{q_i}\chi_i(n)^a\right)=\sum_{d|Q}\phi(\tfrac{Q}{d})\frac{\mu(d)}{Q}\sum_{\substack{\chi \pmod Q\\ \mathrm{ord}\,(\chi)=d}}\chi(n)$$

Recalling from (4) we see that the object on the left determines whether or not n is a primitive root, we can see that the number of primitive roots modulo p in the interval $[M+1, M+N]$, denoted $N_{p,M,N}$, is

$$N_{p,M,N}=\frac{1}{Q}\sum_{d|Q}\phi\left(\tfrac{Q}{d}\right)\mu(d)\sum_{\substack{\chi \pmod Q\\ \mathrm{ord}\,(\chi)=d}}\sum_{n=M+1}^{M+N}\chi(n).$$

Now, the only character of order $d=1$ is the principal character and this gives us the main term of

$$\frac{\phi(Q)}{Q}\left(\left(1-\frac{1}{p}\right)N+O(1)\right)=\frac{\phi(p-1)}{p}N+O(1).$$

A character of order $d>1$ is non-principal and for such characters, the inner sum in $N_{p,M,N}$ is $\ll p^{\frac{1}{4}+\epsilon}$ by the Burgess inequality (3.7). Since there are $\phi(d)$ such characters, the contribution in $N_{p,M,N}$ of $d>1$ is bounded by

$$\ll\frac{\phi(Q)}{Q}\sqrt{p}\log p\sum_{d|(p-1)}|\mu(d)|\ll d(p-1)\sqrt{p}\log(p)\ll p^{\frac{1}{4}+\epsilon}$$

and this with the main term above gives the desired result. ■

This theorem immediately gives us a bound on the least primitive root which we get by plugging in $M=0$. It says that the least primitive root can be no bigger than about $p^{\frac{1}{4}}$. A more general implication of this theorem is that the primitive roots are basically uniformly distributed in nice subintervals of length N provided N is sufficiently large (in our case, $N>p^{\frac{1}{4}+\epsilon}$). Notice further that for these values, we actually get a result that is non-trival, that is, the error term does not dominate the expression.

One final note is in regard to the exponent of p. For least quadratic non-residues 3.8 , we were able to obtain a bound that was $p^{\frac{1}{4\sqrt{e}}+\epsilon}$. Here however, we could not quite get this bound. We cannot simply apply the exact same techniques to this problem. In the previous proof, we had took a character and we wanted to know when the least value of it was -1 (or in particular, not 0 or 1). We used the explicit properties of characters such as multiplicativity, trivial on coprime entries, using the fact that characters maps to roots of unity and so on. In this proof, our equation 4 is not a character and does not have many of the properties that we would need this function to have in order to apply the exact same techniques as in 3.8

5. Conditional Results and Extensions

In the previous two sections, we have discussed some of the results known for least quadratic non-residues and least primitive roots. These mentioned above are all known to be unconditionally true. However, under the assumption of the generalized Riemann hypothesis, we can actually get better results in some cases.

Conjecture 5.1. *(Generalized Riemann Hypothesis - GRH) Let χ be a Dirichlet character of modulus q. Define a Dirichlet L-function to be*

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

for each complex number s with $\Re(s) > 1$. Extend this function by analytic continuation to a meromorphic function on the entire complex plane. Then, for every s with $L(\chi, s) = 0$ and $0 < \Re(s) < 1$ we have $\Re(s) = \frac{1}{2}$.

An extension of the results above known as Vinogradov's conjecture [Ank52] regarding the correct answer to the least quadratic non-residue.

Conjecture 5.2. *(Vinogradov's Conjecture) The least quadratic non-residue modulo p is $O(p^{\epsilon})$.*

In 1942, Yuri Linnik [Lin42] proved this result under the assumption of the generalized Riemann hypothesis. Further, in 1951 under the same assumptions, Paul Erdös and Sarvadaman Chowla [CE51] proved that Vinogradov's conjecture is true with $O(e^{(\log(p))^{\frac{1}{2}+\epsilon}})$ showing that Vinogradov's conjecture should actually hold in greater generality. Nesmith Ankeny in 1952 under GRH managed to show that $O(\log(p)^2)$. The current record is held by Sebastian Wedeniwski in 2001 who showed in his doctoral dissertation that at least one quadratic residue is less than $\frac{3}{2}\log(p)^2$ provided the generalized Riemann hypothesis is true.

As for primitive roots, Yuan Wang in 1959 managed to show under GRH that the least primitive root is

$$O(\omega(p-1)^6(\log(p))^2) = O(\log(p)^8)$$

where $\omega(n)$ is the number of distinct primes dividing n. A later bound discovered by Victor Shoup in 1992 showed via an algorithm and under the assumption of GRH that the least primitive root is

$$O(\omega(p-1)^4)(\log(\omega(p-1)) + 1)^4(\log(p)^2) = O(\log(p)^6).$$

Another possible extension of the question of finding a least primitive root is the question of finding the least prime number that is a primitive root. Greg Martin in 1997 shows the following theorem

Theorem 5.3. *Let $Y, \epsilon, \eta > 0$ be real numbers with $\epsilon \leq \frac{20}{21}$ and let $B = \frac{3}{\epsilon} + \frac{5}{4} + \eta$. Then the number of odd prime powers $p^n \leq Y$ for which*

$$g^*(p^r) \ll_{\epsilon,\eta} (\omega(p-1)^2 \log(p))^B$$

fails is $O_{\epsilon,\eta}(Y^{\epsilon})$.

As $\omega(p) \ll \log(p)$, we have that this theorem tells us that the least prime primitive root is almost always less than $\log(p)$ to a power that depends on both ϵ and η. Under GRH, Shoup [Sho92] has managed to show that

$$g^*(p) \ll (w(\phi(p)) \log(2\omega(\phi(p))))^4 \log(q)^2.$$

However, the best result known unconditionally and uniformly is by Heath-Brown [HB92] giving us that $g^*(p) \ll p^{5.5}$.

All of the above results can found in papers below in the bibliography.

References

[Ank52] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[Bur62] D. A. Burgess. On character sums and primitive roots. *Proc. London Math. Soc. (3)*, 12:179–192, 1962.

[CE51] S. Chowla and P. Erdös. A theorem on the distribution of the values of L-functions. *J. Indian Math. Soc. (N.S.)*, 15:11–18, 1951.

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc. (3)*, 64(2):265–338, 1992.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Lin42] U. V. Linnik. A remark on the least quadratic non-residue. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 36:119–120, 1942.

[Lin44] U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):139–178, 1944.

[LW08] Yuk-Kam Lau and Jie Wu. On the least quadratic non-residue. *Int. J. Number Theory*, 4(3):423–435, 2008.

[Mar97] Greg Martin. The least prime primitive root and the shifted sieve. *Acta Arith.*, 80(3):277–288, 1997.

[MV07] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[Sho92] Victor Shoup. Searching for primitive roots in finite fields. *Math. Comp.*, 58(197):369–380, 1992.

[Wan59] Yuan Wang. On the least primitive root of a prime. *Acta Math. Sinica*, 9:432–441, 1959.

[Wed01] Sebastian Wedeniwski. *Primality Tests on Commutator Curves*. PhD thesis, Eberhard-Karls-Universität Tübingen, 2001.

E-mail address: cbruni@math.ubc.ca