Squares and Prime Numbers

Dalai Chadraa

June 7, 2019

We provide a review of *On Legendre's Work on the Law of Quadratic Reciprocity*, by Steven H. Weintraub [1].

Contents

1. Introduction

For sections 2, 3, and 4, see https://www.imomath.com/index.php?options=329&lmm=0. For section 6, see [3]. For sections 7,8, and 9, see [2].

Theorem 1 (Quadratic Reciprocity). *Given distinct odd primes p and q, we have that*

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

Using Quadratic Reciprocity, we can prove necessary conditions on primes being of the form $x^2 + ny^2$. Using the Pigeonhole Principle, we can also prove sufficient conditions on a prime p being of the form $x^2 + ny^2$ for $n = 1, 2$.

Definition 1. Given an integer a and a prime p, we say that a is a **quadratic residue** modulo b iff there exists some integer $p \nmid x$ such that $a \equiv x^2 \pmod{p}$. We define the Legendre symbol as

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

2. Theorem A

Theorem A includes a formulation of Fermat's Little Theorem and a formulation of Euler's Criterion.

Theorem 2 (Fermat's Little Theorem). *If p is an odd prime, and a is an integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Since $\gcd(a, p) = 1$, it follows that

$$\{a \cdot 1, a \cdots 2, \ldots, a \cdot (p-1)\} = \{1, 2, \ldots, p-1\} \pmod{p}$$

Taking the product implies that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$. Since $\gcd(p, (p-1)!) = 1$, multiplying the by the multiplicative inverse of $(p-1)!$ implies that $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem 3 (Euler's Criterion). *Given an odd prime p and integer a such that $p \nmid a$, we have that*

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

Proof. We view $x^{p-1} - 1$ as a polynomial over $\mathbb{F}_p$. By Fermat's Little Theorem, it follows that $x^{p-1} - 1 = (x-1)(x-2)(\cdots)(x-(p-1))$. Difference of squares implies that $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$.

- We claim that there are $\frac{p-1}{2}$ quadratic residues modulus p. This follows by considering the image of the map $x \mapsto x^2$ over $\mathbb{Z}_p$. Note that $x^2 \equiv y^2 \pmod{p}$ iff $x \equiv \pm y \pmod{p}$, by the difference of squares factorization. This implies that $\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$ is the set of quadratic residues modulo p, with each term being distinct.
- We claim that if a is a quadratic residue, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If a is a quadratic residue, then there exists x such that $a \equiv x^2 \pmod{p}$. Fermat's Little Theorem implies that $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$.
- We claim that if a is a quadratic nonresidue, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. From the above fact, the $\frac{p-1}{2}$ quadratic residues are roots of $x^{\frac{p-1}{2}} - 1$ over $\mathbb{F}_p$. Since the degree is $\frac{p-1}{2}$, the set of roots of $x^{\frac{p-1}{2}} - 1$ is the set of quadratic residues. Since

$$(x-1)(\cdots)(x-(p-1)) \equiv (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) \pmod{p},$$

the set of roots of $x^{\frac{p-1}{2}}+1$ is the set of quadratic nonresidues.

If a is a quadratic residue, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If a is a quadratic nonresidue, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. So $a^{\frac{p-1}{2}}$ coincides with the Legendre symbol modulo p. □

Corollary 4. *Legendre's symbol is multiplicative, i.e., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all primes p and all integers a and b.*

Corollary 5. *Given an odd prime p, we have that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, i.e., -1 is a quadratic residue modulo odd prime p iff $p \equiv 1 \pmod{4}$.*

3. Theorem B

Legendre used a formulation of the following fact about a certain diophantine equation to prove results about Quadratic Reciprocity. Weintraub refers to this as Theorem B.

Theorem 6 (Legendre's Diophantine Equation)**.** *Let $a, b,$ and c be squarefree, relatively prime positive integers. Then $ax^2 + by^2 = cz^2$ has a nonzero solution in integers $x, y,$ and z iff*

$$\left(\frac{-ab}{c}\right) = \left(\frac{bc}{a}\right) = \left(\frac{ca}{b}\right) = 1$$

We won't prove this result, but we will show confirm the necessary condition. Since $a, b,$ and c are relatively primes and squarefree, some considerations of prime divisibility imply that

$$\gcd(a, y) = \gcd(a, z) = \gcd(b, z) = \gcd(b, z) = \gcd(c, z) = \gcd(c, y).$$

The constraints of the problem immediately imply that

$$\begin{aligned} -ab &\equiv (byx^{-1})^2 \pmod{c} \\ bc &\equiv (byz^{-1})^2 \pmod{a} \\ ca &\equiv (axz^{-1})^2 \pmod{b}. \end{aligned}$$

This implies that $\left(\frac{-ab}{c}\right) = \left(\frac{bc}{a}\right) = \left(\frac{ca}{b}\right) = 1$ is a necessary condition.

4. Quadratic Reciprocity via Double Counting

In order to prove Quadratic Reciprocity, we will prove some lemmas.

Lemma 7 (Gauss's Lemma)**.** *For integer a and odd prime p such that $p \nmid a$, we have that $\left(\frac{a}{p}\right) = (-1)^S$ where $S = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ka}{p} \right\rfloor$.*

Proof. Let a be an integer and p be an odd prime such that $p \nmid a$. For all $k = 1, 2, \ldots, \frac{p-1}{2}$, there is a unique $r_k \in \{-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}\}$ such that $ka \equiv r_k \pmod{p}$. Note that $|r_1|, \ldots |r_{\frac{p-1}{2}}|$ are all distinct. Define $\epsilon_k \in \{-1, 1\}$ as satisfying $r_k = \epsilon_k |r_k|$. Euler's Criterion implies that

$$\begin{aligned} \left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \pmod{p} && \text{(Euler's Criterion)} \\ &\equiv \frac{a \cdot 2a \cdots \frac{p-1}{2}a}{1 \cdot 2 \cdots \frac{p-1}{2}} && \text{(Expansion)} \\ &\equiv \frac{\epsilon_1 |r_1| \cdot \epsilon_2 |r_2| \cdots \epsilon_{\frac{p-1}{2}} |r_{\frac{p-1}{2}}|}{(\frac{p-1}{2})!} && \text{(Definition of } \epsilon_k\text{)} \\ &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} && \text{(Since } \{|r_1|, \ldots, |r_{\frac{p-1}{2}}|\} \text{ is a permutation of } \{1, 2, \ldots, \tfrac{p-1}{2}\}\text{)} \end{aligned}$$

By definition, we have that $ka \equiv r_k \pmod p$ with $-\frac{p-1}{2} \leq r \leq \frac{p-1}{2}$ and $r_k = \epsilon_k |r_k|$. Note that $\epsilon_k = 1$ iff the remainder of ka when divided by p is greater than $\frac{p-1}{2}$. This is true iff

$$\left\lfloor \frac{2ka}{p} \right\rfloor = 2 \left\lfloor \frac{ka}{p} \right\rfloor + 1.$$

This implies that $\epsilon_k = (-1)^{\left\lfloor \frac{2ka}{p} \right\rfloor}$, which gives Gauss's Lemma. □

Corollary 8. *Given an odd prime p, we have that $\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}$,i.e., 2 is a quadratic residue modulo p iff $p \equiv \pm 1 \pmod 8$.*

Proof. We will use Gauss's Lemma with $a = 2$. By definition, note that

$$S = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{4k}{p} \right\rfloor.$$

Note that $\left\lfloor \frac{4k}{p} \right\rfloor$ is even iff there is some integer a such that $2ap \leq 4k \leq 2ap + p - 1$. Since $1 \leq k \leq \frac{p-1}{2}$, this is true iff $0 \leq k \leq \frac{p-1}{4}$. So $\left\lfloor \frac{4k}{p} \right\rfloor$ is even for exactly $\left\lfloor \frac{p-1}{4} \right\rfloor$ values of k. This implies that $\left\lfloor \frac{4k}{p} \right\rfloor$ is odd for exactly $\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \left\lfloor \frac{p+1}{4} \right\rfloor$ values of k. Gauss's Lemma implies that $\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}$. Also, this is equivalent to $(-1)^{\frac{p^2-1}{8}}$. □

Definition 2. Given distinct odd primes p and q, define $S(p,q) = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$.

Lemma 9. *Given distinct odd primes p and q, we have $S(p,q) + S(q,p) = \frac{p-1}{2} \cdot \frac{q-1}{2}$.*

Proof. Let $ABCD$ be the rectangle with coordinates $A = (0,0)$, $B = (\frac{q-1}{2}, 0), C = (\frac{q-1}{2}, \frac{p-1}{2})$ and $D = (0, \frac{p-1}{2})$ and let E be the point $E = (q,p)$. Geometrically, for any naturals $1 \leq k < q$, note that $\left\lfloor \frac{kp}{q} \right\rfloor$ is the number of lattice points (k,l) such that $1 \leq l < kp/q$. So the construction means that $S(p,q)$ is the number of lattice points (k,l) such that $1 \leq k \leq \frac{q-1}{2}$ and $1 \leq l < kp/q$. This implies that $S(p,q)$ is the number of lattice points lying lying either in the interior or on the boundary of $ABCD$ lying below the line AE. Similarly, $S(q,p)$ is the number of lattice points lying either in the interior or on the boundary of the rectangle $ABCD$ that lie above the line AE. There are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ lattice points in the rectangle, none of which lie on AE. This implies that $S(p,q) + S(q,p) = \frac{p-1}{2} \cdot \frac{q-1}{2}$. □

Proof of Quadratic Recirprocity. Let p and q be distinct odd primes. Then

$$S(p+q,q) - S(p,q) = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{k(p+q)}{q} \right\rfloor - \left\lfloor \frac{kp}{q} \right\rfloor = \sum_{k=1}^{\frac{q-1}{2}} k = \frac{q^2-1}{8}.$$

This equation implies

$$\begin{aligned}
\left(\frac{2}{q}\right)\left(\frac{p}{q}\right) &= \left(\frac{2p}{q}\right) && \text{(Legendre Symbol is Multiplicative)} \\
&= \left(\frac{2(p+q)}{q}\right) = \left(\frac{\frac{p+q}{2}}{q}\right) \\
&= (-1)^{S(p+q,q)} && \text{(Gauss's Lemma)} \\
&= \left(\frac{2}{q}\right)(-1)^{S(p,q)} && \text{(Above Equation, Corollary } \left(\tfrac{2}{p}\right)\text{)}
\end{aligned}$$

In particular, this implies that $\left(\frac{p}{q}\right) = (-1)^{S(p,q)}$. By symmetry, this implies $\left(\frac{q}{p}\right) = (-1)^{S(q,p)}$. Multiplying both together implies Quadratic Reciprocity. □

Weintraub notes that we can also prove Quadratic Reciprocity by considering the Gauss sum $\sum_{d=1}^{c-1} \left(\frac{d}{c}\right) e^{2\pi i d/c}$.

5. Theorem C

Legendre uses what Weintraub refers to as Theorem C to prove $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. We will instead use Quadratic Reciprocity and Minkowski's Theorem to prove Theorem C, which is a special case regarding primes of the form $x^2 + ny^2$.

Lemma 10 (Minkowski's Theorem over $\mathbb{Z}^n$)**.** *Suppose A is a bounded centrally symmetric convex body in $\mathbb{R}^n$ having volume strictly larger than 2^n. Then there is a lattice point in A different from the origin.*

Proof. We proceed via the Pigeonhole Principle. Partition $\mathbb{R}^n$ into cubes of side length 2, such that the coordinates of the centers of all the cubes are even. Then the interiors of the cubes are disjoint and the cubes cover $\mathbb{R}^n$. Since A is bounded, A intersects with a finite number of cubes, and the sum of the volumes of the intersection of A with the interiors of these cubes is the volume of A. Via translation, these cubes can be translated so that all of their centers are at the origin. Since translations preserve volume and since the sum of the volumes is greater than 2^n, this implies that two bodies intersect at some point X. This implies that there are two distinct points $x, y \in A$ such that $x - y \in (2\mathbb{Z})^n$. This implies that $\frac{x-y}{2} \in \mathbb{Z}^n$. Since A is convex, this implies that $\frac{x-y}{2} \in A$, implying that there is a nonzero lattice point in A. □

Theorem 11 (Minkowski's Theorem)**.** *Let A be a convex body in $\mathbb{R}^n$ and let $v_1, \ldots, v_n$ be linearly independent vectors in $\mathbb{R}^n$. Consider the fundamental parallelepiped $P = \{\sum_{i=1}^n x_i v_i \mid 0 \le x_i \le 1\}$. Denote by $\mathrm{Vol}(P)$ its volume. If A has volume greater than $2^n \cdot \mathrm{Vol}(P)$, A must contain one point in the lattice $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ different from the origin.*

Proof. Define the $n \times n$ matrix

$$M = \begin{bmatrix} | & | & \cdots & | \\ v_1 & v_2 & \cdots & v_n \\ | & | & \cdots & | \end{bmatrix}.$$

Every lattice point in L is of the form Mv with $v \in \mathbb{Z}^n$. Note that $\mathrm{Vol}(P) = |\det M|$. Define the bijective linear transformation $f : \mathbb{R}^n \to \mathbb{R}^n$ by $f(v) = M^{-1}v$. This implies that $f(v_i) = e_i$ for $i = 1, 2, \ldots, n$, where $e_1, \ldots, e_n$ is the canonical basis of $\mathbb{R}^n$. By definition, $f(L) = \mathbb{Z}^n$. Since f is linear, $f(A)$ is a bounded centrally symmetric centrally symmetric body of volume $\mathrm{Vol}(A) \cdot \mathrm{Vol}(P)^{-1} > 2^n$. The lemma above implies there is some nonzero $p \in \mathbb{Z}^n$ such that $p \in f(A)$. Since $f(v) = M^{-1}v$, this implies that $Mp \in A$, which is the desired result. □

Theorem 12 (Theorem C)**.** *An odd prime p*

(a) is of the form $x^2 + y^2$ iff $p \equiv 1 \pmod 4$

(b) is of the form $x^2 + 2y^2$ iff $p \equiv 1, 3 \pmod 8$

(c) is of the form $x^2 - 2y^2$ iff $p \equiv \pm 1 \pmod 8$

Proof. We are given an odd prime p. For any relatively prime, nonzero integer a and b satisfying $p \nmid a$ and $p \nmid b$, define the lattice $L = \{(x, y) \mid (p \mid bx - ay) \text{ and } (x, y \in \mathbb{Z})\}$. Note that $(p, 0), (0, p), (a, b) \in L$. Bézout's Lemma implies that $(k, 1) \in L$ for some integer k. This implies that the fundamental area of L is at most p. For the following three parts, we will work over the lattice L.

(a) If $p = x^2 + y^2$, then the fact that $\left(\frac{-1}{p}\right)$ implies that $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 4$, then there exists relatively prime integers $p \nmid a, b$ such that $p \mid a^2 + b^2$. Define the centrally symmetric convex region $D = \{(x, y) \mid x^2 + y^2 < 2p\}$. Since $\frac{2p\pi}{p} > 4$, Minkowski's Theorem implies that there is a nonzero point (x, y) such that $p \mid ax - by$ and $x^2 + y^2 < 2p$. Note the identity

$$(ax - by)(bx - ay) = ab(x^2 + y^2) - xy(a^2 + b^2).$$

This implies $p \mid x^2 + y^2$. Since $0 < x^2 + y^2 < 2p$, this implies $p = x^2 + y^2$.

(b) If $p = x^2 + 2y^2$, then the fact that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ and the fact that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ imply that $p \equiv 1, 3 \pmod 8$. If $p \equiv 1, 3 \pmod 8$, then there exists relatively primes integers $p \nmid a, b$ such that $p \mid a^2 + 2b^2$. Define the centrally symmetric convex region $D = \{(x, y) \mid x^2 + 2y^2 < 2p\}$. The area of D is $\sqrt{2}p\pi$. Since $\frac{\sqrt{2}p\pi}{p} > 4$, Minkowski's Theorem implies that there is a nonzero point (x, y) such that $p \mid ax - by$ and $x^2 + 2y^2 < 2p$. Note the identity

$$(ax - 2by)(bx - ay) = ab(x^2 + 2y^2) - xy(a^2 + 2b^2).$$

This implies that $p \mid x^2 + 2y^2$. Since $0 < x^2 + 2y^2 < 2p$, this implies $p = x^2 + 2y^2$.

(c) If $p = x^2 - 2y^2$, then the fact that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$ implies that $p \equiv \pm 1 \pmod 8$. If $p \equiv \pm 1 \pmod 8$, then there exists relatively primes integers $p \nmid a, b$ such that $p \mid a^2 - 2b^2$. Define the centrally symmetric convex region $D = \{(x, y) \mid |x| < \sqrt{2p}$ and $|y| < \sqrt{p}\}$. The area of D is $4\sqrt{2}p$. Since $\frac{4\sqrt{2}p}{p} > 4$, Minkowski's Theorem implies that there is a nonzero point (x, y) such that $p \mid ax - 2by$ and $(x, y) \in D$. Note the identity

$$(ax + 2by)(bx - ay) = ab(x^2 - 2y^2) - xy(a^2 - 2b^2).$$

This implies $p \mid x^2 - 2y^2$. Since $|x| < \sqrt{p}$ and $|y| < \sqrt{2p}$, this implies that $|x^2 - 2y^2| < 2p$. Since $x^2 \neq 2y^2$, this gives $p = |x^2 - 2y^2|$. This implies that

$$p \in \{x^2 - 2y^2, (x - 2y)^2 - 2(x - y)^2\}.$$

This completes the proof. □

6. Merten's Theorem

The remaining results of this paper will rely on ideas from real analysis and complex analysis. In particular, we will think about Abel summation and analytic functions. First, let's discover two results on the summation of prime numbers. This will help in bounding quadratic nonresidues.

Lemma 13. $\sum_{p \leq n} \frac{\ln p}{p} = \ln n + O(1)$

Proof. We will consider the p-adic valuation of $n!$. Note that $\ln(n!) = \sum_{p \leq n} v_p(n!) \ln(p)$. By Legendre's formula, note that $\frac{n}{p} - 1 \leq v_p(n!) \leq \frac{n}{p-1}$. By Stirling's formula, note that $\ln(n!) = n[\ln(n) - 1] + O(\ln n)$. These facts implies

$$n \sum_{p \leq n} \frac{\ln p}{p} - \sum_{p \leq n} \ln(p) \leq n[\ln(n) - 1] + O(\ln n) \leq n \sum_{p \leq n} \frac{\ln p}{p} + n \sum_{p \leq n} \frac{\ln p}{p(p-1)}.$$

Clearly $\sum_{p \leq n} \frac{\ln p}{p}$ converges. From the second lemma, note that $\prod_{p \leq n} p \leq 4^{n-1}$. This implies $\sum_{p \leq n} \ln(p)$ is $O(n)$. This implies that $\sum_{p \leq n} \frac{\ln p}{p} = \ln(n) + O(1)$. □

We can actually get rid of the $\ln(p)$ from $\frac{\ln p}{p}$.

Theorem 14 (Merten's Theorem). *We have*

$$\sum_{p \leq n} \frac{1}{p} = \ln \ln n + O(1).$$

Proof. Define

$$a_n = \begin{cases} \frac{\ln}{n} & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

Define $S_n = a_2 + a_3 + \cdots + a_n$. Notice that

$$S_n = \sum_{p \le n} \frac{\ln p}{p} = \ln(n) + r_n, \qquad \text{(Since } \textstyle\sum_{p \le n} \frac{\ln p}{p} = \ln(n) + O(1)\text{)}$$

for some bounded sequence r_n. This implies that

$$\frac{S_n - S_{n-1}}{\ln n} = \begin{cases} \frac{1}{n} & \text{if } n \text{ is prime} \\ 0 & \text{otherwise.} \end{cases}$$

In particular, this implies

$$\begin{aligned} \sum_{p \le n} \frac{1}{p} &= \sum_{k=2}^{n} \frac{S_k - S_{k-1}}{\ln k} \\ &= \frac{S_n}{\ln n} + \sum_{k=2}^{n} r_n \left(\frac{1}{\ln k} - \frac{1}{\ln(k+1)} \right) + \sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)} \right) \\ &= O(1) + \sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)} \right). \end{aligned}$$

Thus, it suffices to prove that $\sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)}\right)$ is $\ln\ln(n) + O(1)$.

Lemma. $\sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)}\right) = \ln\ln(n) + O(1)$

Proof. Note that $\int_k^{k+1} \frac{1}{t}\, dt = \ln(k+1) - \ln k$. This implies that

$$\begin{aligned} 0 \le \int_k^{k+1} \frac{1}{t \ln t}\, dt - \left[1 - \frac{\ln k}{\ln(k+1)} \right] &\le \int_k^{k+1} \frac{1}{t \ln t} - \frac{1}{t \log(k+1)}\, dt \\ &\le \int_k^{k+1} \frac{\ln(k+1) - \ln(t)}{t \ln(t)}\, dt \\ &\le \int_k^{k+1} \frac{\ln(k+1) - \ln(k)}{t \ln t}\, dt \\ &\le \frac{1}{k^2 \ln(2)^2}. \end{aligned}$$

This implies that

$$\begin{aligned} \sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)} \right) &= \int_2^n \frac{1}{t \ln t}\, dt + O(1) \\ &= \ln\ln n + O(1). \end{aligned}$$

This completes the lemma. □

Since showing $\sum_{k=2}^{n} \left(1 - \frac{\ln k}{\ln(k+1)}\right) = \ln\ln(n) + O(1)$ is sufficient, we are done. □

There's more extensive exposition in Section 1.10 of Additive Combinatorics.

7. Some Facts About Characters

Since the legendre symbol is multiplicative, the function $\mathbb{F}_p^\times \to \mathbb{C}^\times$ defined by $x \mapsto \left(\frac{x}{p}\right)$ is a group homomorphism from the multiplicative group of $\mathbb{F}_p$ to the multiplicative group of the complex numbers. We will investigate this ideas in this section. I believe the contents of 7.1 and 7.2 can be found in *Abstract Algebra* by Dummit and Foote.

7.1. Dual Group

Recall that if f is an integrable function over $\mathbb{R}$, then the **fourier transform** is defined as

$$\widehat{f} = \int_{-\infty}^{\infty} f(y)e^{2\pi ixy}\, dy.$$

Definition 3. A **character** of G is a group homomorphism $\chi : G \to \mathbb{C}^\times$. We say that $\chi(x+y) = \chi(x)\cdot\chi(y)$ for all $x, y \in G$. The character is trivial iff $\chi(g) = 1$ for all $g \in G$.

Definition 4. Define $\widehat{G}$ as the set of all characters of G. It is a group with respect to multiplication, where we define $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\cdot\chi_2(g)$. This is called the **dual group** of G. If n is the order of G, then $\chi(g)^n = 1$, implying that $|\chi(g)| = 1$.

Example 1. Let $n \geq 2$ and let $G = \mathbb{Z}/n\mathbb{Z}$. Note that $\chi(1)$ is an n-th root of unity, and uniquely defines χ. Note that each map $\chi(1) = \xi$ generates all possible maps. So $\widehat{G} \cong \mathbb{Z}/n\mathbb{Z}$. This isomorphism depends on the choice of a primitive nth root of 1.

Remark 1. Note that $\widehat{G \times H} = \widehat{G} \times \widehat{H}$ for direct products. (Apparently this a easy). Using the Fundamental Theorem of Abelian Groups, it follows that $\widehat{G} \cong G$, since cyclic groups are isomorphic to their dual groups.

- The number of elements in the dual group $\widehat{G}$ is the number of elements in G.
- Suppose $g \in G \setminus \{0\}$. Then there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$. Otherwise, $\chi(g) = 0$ for all $\chi \in \widehat{G}$. Then $1 = \chi(g)^n = \chi(g^n)$ for all integers n. Note that $\chi(g)\chi(h) = \chi(gh)$.

Lemma 15. *For any abelian groups B and C, we have that $\widehat{B \times C} \cong \widehat{B} \times \widehat{C}$.*

Proof. Let $\chi \in \widehat{B \times C}$ be a group homomorphism $B \times C \to \mathbb{C}^\times$. Define $\chi_1 : B \to \mathbb{C}^\times$ by $\chi_1(b) = \chi(b, 1_C)$. Define $\chi_2 : C \to \mathbb{C}^\times$ by $\chi_2(c) = \chi(1_B, c)$. Define the map $\varphi : \widehat{B \times C} \to \widehat{B} \times \widehat{C}$ by $\varphi(\chi) = (\chi_1, \chi_2)$. This is a bijective group homomorphism, implying that the groups are isomorphic. □

Lemma 16. *Let G be an arbitrary abelian group. Then $G \cong \widehat{G}$.*

Proof. Note that G is the direct product of cyclic groups, by the Fundamental Theorem of Abelian Groups. Let $G = \bigoplus H$. Then

$$\begin{aligned}
\widehat{G} &\cong \widehat{\bigoplus H} && \text{(Fundamental Theorem of Abelian Groups)}\\
&\cong \bigoplus \widehat{H} && \text{(Above Lemma)}\\
&\cong \bigoplus H && \text{(Since } H \text{ is Cyclic)}\\
&\cong G. && \text{(Definition of } G\text{)}
\end{aligned}$$

This completes the lemma. □

Lemma 17. *Let G be any abelian group. For any $x \in G \setminus \{1_G\}$, there exists $\chi \in \widehat{G}$ such that $\chi(x) \neq 1$.*

Proof. Suppose that $\chi(g) = 1$ for all $\chi \in \widehat{G}$. Then $|\widehat{G}| = |\widehat{G/\langle g \rangle}|$, since we can ignore g. But recall that $\widehat{G} \cong G$ for all abelian groups G. This implies that $|\langle g \rangle| = 1$. This implies that $g = 1$, a contradiction. □

Theorem 18. *G and $\widehat{\widehat{G}}$ are canonically isomorphic.*

Proof. Define the map $\varphi : G \to \widehat{\widehat{G}}$ by $g \mapsto (\chi \mapsto \chi(g))$.

- This is well-defined group homomorphism. Let $g, h \in G$. Then $\varphi(g)\varphi(h) = \varphi(gh)$.
- This is injective. Suppose $\varphi(g) = \varphi(h)$. Then $\chi(g) = \chi(h)$ for all $\chi \in \widehat{G}$. This implies that $\chi(gh^{-1}) = 1$ for all $\chi \in \widehat{G}$. This contradicts the previous lemma.
- This is surjective. Note that $|\widehat{\widehat{G}}| = |G|$. There is a injective set function. This implies that the map is surjective.

Thus, the maps is a canonical group isomorphism. This map realizes G as a subgroup of $\widehat{\widehat{G}}$. □

Definition 5. Define $F(G, \mathbb{C})$ as the $\mathbb{C}$-vector space of all maps $f : G \to \mathbb{C}$. It is a $\mathbb{C}$-vector space of dimension $|G|$. This fact is true since the map $F(G, \mathbb{C}) \to \mathbb{C}^{|G|}$ sending f to the vector $(f(g))_{g \in G}$ of $|G|$ components is a $\mathbb{C}$-linear isomorphism. If $f, g \in F(G, \mathbb{C})$, then let

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}.$$

Note that this is an inner product on the $\mathbb{C}$ vector space $F(G, \mathbb{C})$. We will now prove the main theorem of Fourier analysis on G.

Lemma. *$F(G, \mathbb{C})$ is a $\mathbb{C}$ vector space of dimension $|G|$ over $\mathbb{C}$.*

Proof. Obviously, $F(G, \mathbb{C})$ is a vector space over $\mathbb{C}$, since $af(g) + bh(g)$ defines another function, and the axioms are satisfied. Define the map $\varphi : F(G, \mathbb{C}) \to \mathbb{C}^{|G|}$ by

$$\varphi(f) = (f(g_1), f(g_2), \ldots, f(g_n)),$$

where n is the order of G. This is a $\mathbb{C}$ linear maps since $\varphi(cf - h) = c\varphi(f) - \varphi(h)$. This is injective since if $\varphi(f) = \varphi(h)$, then $f = h$. This is surjective since we can construct the functions we want. So $F(G, \mathbb{C})$ is isomorphic to $\mathbb{C}^{|G|}$. □

Lemma 19. *The construction of $\langle f, g \rangle$ forms an inner product on the $\mathbb{C}$-vector space $F(G, \mathbb{C})$.*

Proof. Clearly, it satisfies

- $\langle af + h, bg \rangle = ab \langle f, g \rangle + \langle h, g \rangle$.
- $\langle f, g \rangle = \overline{\langle g, f \rangle}$
- $\langle f, f \rangle > 0$ iff $f \neq 0$, and is 0 otherwise.

It satisfies the axioms, so it's an inner product. □

Lemma 20. *We have that $\langle \chi_1, \chi_2 \rangle = 1_{\chi_1 = \chi_2}$.*

Proof. If $\chi_1 = \chi_2$, then the norm is 1 since $|\chi_1| = 1$. Otherwise, $\chi_1 \neq \chi_2$. This implies that

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} \\
&= \frac{1}{|G|} \sum_{x \in G} \frac{\chi_1}{\chi_2}(x) \\
&= \frac{1}{|G|} \sum_{x \in G} \chi(x). && \left(\text{Let } \chi = \tfrac{\chi_1}{\chi_2}\right)
\end{aligned}$$

Define $S = \frac{1}{|G|}\sum_{x\in G}\chi(x)$. This implies that $\chi(g)S = S$ for all $g \in S$ since $x \mapsto gx$ is a permutation of G. Since χ is nontrivial, there exists some $g \in G$ such that $\chi(g) \neq 1$. This implies that $S = 0$. □

Lemma 21. *Consider an $g \in G \setminus \{1\}$. Then we have that $\sum_{\chi\in\widehat{G}}\chi(x) = 0$.*

Proof. Define the sum $S = \sum_{\chi\in\widehat{G}}\chi(g)$. Note that $\chi(g)\widehat{G} = \widehat{G}$. This implies that $\chi(g)S = S$. Since there exists some $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$, this implies that $S = 0$. □

Theorem 22. *The elements of $\widehat{G}$ form an orthonormal basis of $F(G, \mathbb{C})$.*

Proof. We split the proof into three steps.

- $\langle\chi_1, \chi_2\rangle = 1_{\chi_1=\chi_2}$. This follows from the previous lemma.
- $\sum_{\chi\in\widehat{G}}\chi(x) = 0$ for all $x \in G \setminus \{1_G\}$.
- This implies that the set $(\chi)_{\chi\in\widehat{G}}$ is linearly independent. Taking the dual gives $\langle\sum a_i\chi_i, \chi_1\rangle = a_1$. This set also has the same cardinality a the dimension of the vector space $F(G, \mathbb{C})$. In particular, the cardinality is $|G|$. **Facts about vector spaces** (this seems sketchy, but whatever) implies that $(\chi)_{\chi\in\widehat{G}}$ is a basis for $F(G, \mathbb{C})$.

So we have an orthonormal basis for $F(G, \mathbb{C})$ This basis is the set of elements of $\widehat{G}$. □

Now we have the following result.

Theorem 23. *For any finite abelian group G, the following relations hold.*

1. *(Orthogonality) For all $\chi, \chi_1, \chi_2 \in \widehat{G}$ and all $g, h \in G$, we have that*

$$\frac{1}{|G|}\sum_{x\in G}\chi_1(x)\chi_2(x) = 1_{\chi_1=\chi_2}, \qquad \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)} = 1_{g=h}.$$

2. *(Fourier Inversion) For all $f \in F(G, \mathbb{C})$, we have that $f = \sum_{\chi\in\widehat{G}}\langle f, \chi\rangle\chi$.*
3. *(Planceral's Identity) For all $f \in F(G, \mathbb{C})$,*

$$\frac{1}{|G|}\sum_{x\in G}|f(x)|^2 = \sum_{\chi\in\widehat{G}}|\langle f, \chi\rangle|^2.$$

Proof.

1. The first equation is $\langle\chi_1, \chi_2\rangle = 1_{\chi_1=\chi_2}$, which is true from our above theorem. Define

$$S = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)}.$$

Note that $\chi(g)\overline{\chi(h)}S = S$. For the sake of contradiction, suppose $\chi(g)\overline{\chi(h)} = 1$ for all $\chi \in \widehat{G}$. This implies that $\chi(gh^{-1}) = 1$ for all $\chi \in \widehat{G}$. Since $gh^{-1} \neq 1$, this is a contradiction. This completes part (1).

2. Note that we have the expansion

$$\begin{aligned}\left(\sum_{\chi\in\widehat{G}}\langle f, \chi\rangle\chi\right)(x) &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(x)\sum_{y\in G}f(y)\overline{\chi(y)} && \text{(Definition of Inner Product)}\\ &= \frac{1}{|G|}\sum_{y\in G}f(y)\sum_{\chi\in\widehat{G}}\chi(x/y) && \text{(Switching Order of Summation)}\\ &= \sum_{y\in G}f(y)1_{x=y} && \text{(Part (1))}\\ &= f(x).\end{aligned}$$

This gives part (2).

3. Now we can show that

$$\begin{aligned}
\frac{1}{|G|}\sum_{x\in G}|f(x)|^2 &= \langle f,f\rangle && \text{(Definition of Inner Product)}\\
&= \left\langle \sum_{\chi_1\in\widehat{G}}\langle f,\chi_1\rangle\,\chi_1,\ \sum_{\chi_2\in\widehat{G}}\langle f,\chi_2\rangle\,\chi_2\right\rangle && \text{(Part (2))}\\
&= \sum_{\chi_1,\chi_2\in G}\langle\langle f,\chi_1\rangle\,\chi_1,\langle f,\chi_2\rangle\,\chi_2\rangle && \text{(Distributive Property)}\\
&= \sum_{\chi_1,\chi_2\in G}\langle f_1,\chi_1\rangle\,\overline{\langle f,\chi_2\rangle}\,\langle\chi_1,\chi_2\rangle && \text{(Property of Inner Product)}\\
&= \sum_{\chi_1,\chi_2}\langle f_1,\chi_1\rangle\,\overline{\langle f,\chi_2\rangle}1_{\chi_1=\chi_2} && \text{(Since } (\chi)_{\chi\in\widehat{G}} \text{ is an Orthonormal Basis)}\\
&= \sum_{\chi\in\widehat{G}}|\langle f,\chi\rangle|^2.
\end{aligned}$$

This establishes Planceral's Identity. □

Remark 2. Recall the following formula $\widehat{f}(n)=\frac{1}{2\pi}\int_0^{2\pi}f(y)e^{-iny}\,dy$. We have the analogous formula $\widehat{f}(\chi)=\langle f,\chi\rangle$. Basically, note that $e^{inx}:\mathbb{R}\to\mathbb{C}$ forms a basis for 2π-periodic functions $\mathbb{R}\to\mathbb{C}$ just like how χ forms a basis for functions $G\to\mathbb{C}$.

7.2. Finite Fields

Recall the following facts from algebra.

- Every field has an algebraic closure.
- The algebraic closure of a field is unique, up to isomorphism
- Every finite field is $\mathbb{F}_{p^e}$ where the characteristic is p for some prime p and has order p^e for some integer e. Any two finite fields of the same order are isomorphic.
- Also, we denote $\overline{\mathbb{F}_q}$ as the algebraic closure of $\mathbb{F}_q$. By definition, for any $f(x)\in\mathbb{F}_q[x]$, there exists some $a\in\overline{\mathbb{F}_q}$ such that $f(a)=0$.

Proposition 24 (Freshman's Dream)**.** *A ring A with characteristic p satisfies*

$$(a_1+\cdots+a_n)^q=a_1^q+\cdots+a_n^q.$$

Proof. Induction or the generalized binomial theorem. Not too much here. □

Let q be a power of p. Define

$$\mathbb{F}_q=\{x\in\overline{\mathbb{F}_p}\mid x^q=x\}.$$

Theorem 25. *$\mathbb{F}_q$ is the unique field with q elements contained in $\overline{\mathbb{F}_p}$.*

Proof. By our proposition, it is a field. It has q elements since it has q roots and the derivative is -1, implying there are no double roots. For the sake of contradiction, suppose L is a field other that $\overline{\mathbb{F}_p}$ with $q-1$ elements. The multiplicative group $L^\times$ is $q-1$ elements. The product is 1. This implies that $x^q=x$ forall $x\in L$. So $L\subseteq\mathbb{F}_q$, implying that $L=\mathbb{F}_q$, a contradiction. □

Theorem 26 (Subtle Theorem of Gauss)**.** *Let $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$. Let K be a field and let G be a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. Let's just prove the general version. So we have a field K. We let G be a subgroup of $K^{\times}$. Let g be the element of maximal order in G. Let this maximal order by d. Our first claim is that $h^d = 1$ for all $h \in G$. Otherwise, we have that $h^e = 1$ for some $e \nmid d$. This implies that $|gh| = \operatorname{lcm}(e, d) > d$, a contradiction. This implies that $x^d - 1 = 0$ for all $x \in G$. This implies that there are at most d elements G, implying that g generated G. □

Let's also consider a slightly tricky fact.

Remark 3. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ which is true iff $p^m - 1 \mid p^n - 1$ which is true iff $m \mid n$.

Proof. So suppose that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. This actually follows from our weird definition of fields, which is pretty unnatura, but whatever. Our definition says $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$. Since each root is simple, this implies that it's a subsets iff $x^{p^n} - x \mid x^{p^m} - x$, which gives the result. □

Definition 6. The following map is pretty important. Let q be a prime. Then define

$$\mathrm{Fr}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \mathrm{Fr}_q(x) = x^q.$$

Note that Fr_q is an automorphism of $\mathbb{F}_{q^n}$ and fixes $\mathbb{F}_q$.

Some additional facts are that every automorphism is a composition of Frobenius maps are there exactly n automorphisms. In other words, we're saying that

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/q\mathbb{Z}$$

and is generated by the Frobenius map Fr_q. This follows from our subtle theorem of Gauss. Also, if we have a root of an irreducible polynomial over $\mathbb{F}_q$, then we can find the other roots by applying the Frobenius map successively. Let's investigate this.

Theorem 27. *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree n. Let $r \in \overline{\mathbb{F}_p}$ be a root of f. Then the root of f are $r, r^q, \ldots, r^{q^{n-1}}$. So $f(x) = \prod_{i=0}^{n-1}(x - r^{q^i})$.*

Proof. Note that the field generated by r over $\mathbb{F}_q$ has q^n elements. So the field of $\mathbb{F}_{q^n}$. Note that Fr_q generates $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. This implies that $0 = \mathrm{Fr}_q(0) = \mathrm{Fr}_q(f(r)) = f(\mathrm{Fr}_q(r))$. So $\mathrm{Fr}_q(r)$ is another root. We will show that the roots are distinct. Suppose otherwise. Then $r^{q^a} = 1$ for some $a < n$, implying that $r \in \mathbb{F}_{q^a}$. Note that $[\mathbb{F}_{q^a} : \mathbb{F}] = a$, implying that r is the root of some polynomial $g(x) \in \mathbb{F}[x]$ of degree at most a. This implies that $f(x) \mid g(x)$, implying that $g(x) = 0$, a contradiction. So those are the roots. □

sectionIntroduction Recall the following facts from algebra.

- Every field has an algebraic closure.
- The algebraic closure of a field is unique, up to isomorphism
- Every finite field is $\mathbb{F}_{p^e}$ where the characteristic is p for some prime p and has order p^e for some integer e. Any two finite fields of the same order are isomorphic.
- Also, we denote $\overline{\mathbb{F}_q}$ as the algebraic closure of $\mathbb{F}_q$. By definition, for any $f(x) \in \mathbb{F}_q[x]$, there exists some $a \in \overline{\mathbb{F}_q}$ such that $f(a) = 0$.

Proposition 28 (Freshman's Dream)**.** *A ring A with characteristic p satisfies*

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q.$$

Proof. Induction or the generalized binomial theorem. Not too much here. □

Let q be a power of p. Define

$$\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q = x\}.$$

Theorem 29. *$\mathbb{F}_q$ is the unique field with q elements contained in $\overline{\mathbb{F}_p}$.*

Proof. By our proposition, it is a field. It has q elements since it has q roots and the derivative is -1, implying there are no double roots. For the sake of contradiction, suppose L is a field other that $\overline{\mathbb{F}_p}$ with $q-1$ elements. The multiplicative group $L^\times$ is $q-1$ elements. The product is 1. This implies that $x^q = x$ forall $x \in L$. So $L \subseteq \mathbb{F}_q$, implying that $L = \mathbb{F}_q$, a contradiction. □

Theorem 30 (Subtle Theorem of Gauss)**.** *Let $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$. Let K be a field and let G be a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. Let's just prove the general version. So we have a field K. We let G be a subgroup of $K^\times$. Let g be the element of maximal order in G. Let this maximal order by d. Our first claim is that $h^d = 1$ for all $h \in G$. Otherwise, we have that $h^e = 1$ for some $e \nmid d$. This implies that $|gh| = \operatorname{lcm}(ed) > d$, a contradiction. This implies that $x^d - 1 = 0$ for all $x \in G$. This implies that there are at most d elements G, implying that g generated G. □

Let's also consider a slightly tricky fact.

Remark 4. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ which is true iff $p^m - 1 \mid p^n - 1$ which is true iff $m \mid n$.

Proof. So suppose that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. This actually follows from our weird definition of fields, which is pretty unnatura, but whatever. Our definition says $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$. Since each root is simple, this implies that it's a subsets iff $x^{p^n} - x \mid x^{p^m} - x$, which gives the result. □

Definition 7. The following map is pretty important. Let q be a prime. Then define

$$\mathrm{Fr}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \mathrm{Fr}_q(x) = x^q.$$

Note that Fr_q is an automorphism of $\mathbb{F}_{q^n}$ and fixes $\mathbb{F}_q$.

Some additional facts are that every automorphism is a composition of Frobenius maps are there exactly n automorphisms. In other words, we're saying that

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/q\mathbb{Z}$$

and is generated by the Frobenius map Fr_q. This follows from our subtle theorem of Gauss. Also, if we have a root of an irreducible polynomial over $\mathbb{F}_q$, then we can find the other roots by applying the Frobenius map successively. Let's investigate this.

Theorem 31. *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree n. Let $r \in \overline{\mathbb{F}_p}$ be a root of f. Then the root of f are $r, r^q, \ldots, r^{q^{n-1}}$. So $f(x) = \prod_{i=0}^{n-1}(x - r^{q^i})$.*

Proof. Note that the field generated by r over $\mathbb{F}_q$ has q^n elements. So the field of $\mathbb{F}_{q^n}$. Note that Fr_q generates $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. This implies that $0 = \mathrm{Fr}_q(0) = \mathrm{Fr}_q(f(r)) = f(\mathrm{Fr}_q(r))$. So $\mathrm{Fr}_q(r)$ is another root. We will show that the roots are distinct. Suppose otherwise. Then $r^{q^a} = 1$ for some $a < n$, implying that $r \in \mathbb{F}_{q^a}$. Note that $[\mathbb{F}_{q^a} : \mathbb{F}] = a$, implying that r is the root of some polynomial $g(x) \in \mathbb{F}[x]$ of degree at most a. This implies that $f(x) \mid g(x)$, implying that $g(x) = 0$, a contradiction. So those are the roots. □

7.3. Characters over Finite Fields

A choice of a basis implies that $\mathbb{F}_{p^n} \cong \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ as a group isomorphism. (Also $\mathbb{F}_{p^n}^\times$ is cyclic). Recall that the character group of an abelian group G is $\widehat{G} = \mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{C}^\times)$, and that $G \cong \widehat{G}$ as groups.

Proposition 32 (Dual Group Lifting)**.** *Suppose $q = p^n$ is a power of. prime p. Then there is an isomorphism of groups $\varphi : \mathbb{F}_q \to \widehat{\mathbb{F}_q}$ where $a \mapsto \psi_a$ and where we define*

$$\psi_a = e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}}(ax)}.$$

Proof. I feel like we've proven this already, but let's do it anyways.

We have. Just recall the dual group properties from before. □

Definition 8. The next result will help with examining the zeta function of *diagonal hypersurfaces*. This is a fancy way of describing a set of solutions satisfying $a_0 x_0^m + \cdots + a_k x_k^m$ over some finite field.

Proposition 33. *Let d be a divisor of $q - 1$. The map $\chi \to \chi_n$ where $\chi_n(x) = \chi(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ is a bijection between characters of order d of $\mathbb{F}_q^\times$ and characters of order d of $\mathbb{F}_{q^n}^\times$.*

Proof. We prove the map is well-defined, the map is injective, and the map is surjective.

- Suppose χ is a character of $\mathbb{F}_q$ of order d. Then $\chi(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$ is a character since the norm is multiplicative. Also, it has order d, since χ has order d. So the map is well-defined.
- Recall that N is a surjective map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. This means that if $\chi_1(N(x)) = \chi_2(N(x))$ for all $x \in \mathbb{F}_{q^n}$, then $\chi_1(x) = \chi_2(x)$ forall $x \in \mathbb{F}_q$, implying that $\chi_1 = \chi_2$. So it's injective.
- Suppose $f : \mathbb{F}_{q^n} \to \mathbb{C}^\times$ is a character. Let u generate $\mathbb{F}_{q^n}^\times$. We want a character $\chi : \mathbb{F}_q \to \mathbb{C}^\times$ such that $\chi(N(x)) = f(x)$. Since everything is multiplicative, this is true iff $\chi(N(u)) = f(u)$. This is true iff $\chi(u^{1+q+\cdots+q^{n-1}}) = f(u)$. Note that $\zeta = u^{1+q+\cdots+q^{n-1}}$ generates $\mathbb{F}_q^\times$. So we want $\chi(\zeta) = f(u)$. This is sufficient, since it implies that χ has order d and that $\chi(N(x)) = f(x)$.

This completes the proof. □

Definition 9. Let's say a thing about making characters more useful.

- If χ is trivial, then define $\chi(0) = 1$.
- If χ is nontrivial, then define $\chi(0) = 0$.

Proposition 34 (Equation Enumeration)**.** *Suppose $d \mid q - 1$. Suppose $x \in \mathbb{F}_q$. The number of solutions of the equation $y^d = x$ with $y \in \mathbb{F}_q$ is $\sum_{\chi^d = 1} \chi(x)$ where the sum is taken over the multiplicative characters with order that divides d.*

Proof. Let's consider cases.

- $x = 0$. Then $y^d = 0$ has 1 solution. Note that $\sum_{\chi^d} \chi(0) = 1$, by our convenient definition.
- $x \in \mathbb{F}_q^\times$. Let u generate $\mathbb{F}_q^\times$. Then $x = u^r$ for some r. Let $y = u^k$ where k is a parameter. Then $y^d = x$ iff $du \equiv r \pmod{q-1}$.
  - $d \nmid r$. Then there are no solutions. Note that the dual group of $\mathbb{F}_q^\times$ is cyclic of order $q - 1$. Since $d \mid q - 1$, there are exactly d solutions χ to $\chi^d = 1$. They are $\chi, \chi^2, \ldots, \chi^d = 1$. This implies that the sum is

    $$\sum_{i=1}^{d} \chi(u)^{ri} = \chi(u)^r \frac{\chi^{dr}(x) - 1}{\chi^r(x) - 1} = 0. \qquad \text{(Geometric Series Formula)}$$

    This is the desired result.

- $d \mid r$. Then there are d solutions. Since $\mathbb{F}_q^\times$ is cyclic, the dual group is also cyclic of order $q-1$. So there are exactly d characters χ with order d. They evaluate to $\chi(x) = 1$, implying that the sum is one.

By casework, we are done. □

There's something called the Davenport Hasse relation which is apparently important. For example, this theorem can help in counting the number of solutions to an equation of the form $a_0x^m + \cdots + a_kx_k^m = 0$ over a projective space $\mathbb{P}^k$, which is basically $\mathbb{F}_p^{k+1}/\mathbb{F}^\times$. In essence, it is the set of solutions, modded out by the multiplicative group $\mathbb{F}_p^\times$. Also, this next result helps with it I guess. Basically, thinking about vector spaces is good for us.

Proposition 35. *Suppose $x \in \mathbb{F}_{q^n}$. Let the minimal polynomial of x over $\mathbb{F}_q$ be*

$$f = X^d - a_1X^{d-1} + \cdots + (-1)^d a_d \in \mathbb{F}_q[X].$$

Then $d \mid n$ and $\prod_{j=0}^{n-1}(x - x^{q^j}) = f^{\frac{n}{d}}$. In particular, this implies that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = a_d^{\frac{n}{d}}$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} = \frac{n}{d}a_1$.

Proof. Note that $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. This implies that $d \mid n$.

Supose $h \in \mathbb{F}_q[X]$ is irreducible and that $h(X) \mid \prod_{j=0}^{n-1}(X - x^{q^j})$. This implies that there is some j such that $h(x^{q^j}) = 0$. Also since $f(x) = 0$, this implies that $f(x^{q^j}) = 0$. This implies that h and f share a common factor, implying that $h = f$ since f and h are irreducible. This implies that $\prod_{j=0}^{n-1}(X - x^{q^j}) = f(X)^{\frac{n}{d}}$ by considering the degree. □

We can extend these ideas to say things about zeta function of a variety. This is basically just a formal series, but related to the number of solutions of a system of polynomial equation over finite fields $\mathbb{F}_{p^n}$ where we make n bigger.

8. Bounds on Quadratic Nonresidues

Now that we're comfortable with finite fields and characters over finite fields, we can think about how to solve hard problems related to characters and finite fields. In particular, since the legendre function acts as a character of $\mathbb{F}_p^\times$ extended to $\mathbb{F}_p$, it's possible to place a nontrivial bound on the minimal nonquadratic residue. First, let's explore how characters can help over finite fields. Once we see the power of this approach, we will prove that the minimal quadratic residue is $O(p^{\frac{1}{2\sqrt{e}}}(\ln p)^2)$ using ideas from analytic number theory.

Theorem 36. *Let q be a prime power. Let d be a positive integer. Let $A \subset \mathbb{F}_q^d$ be a subset of of d-tuples, where the terms are elements of the field F_q. Suppose $|A| > q^{\frac{d+1}{2}}$. Let x be an element in the multiplicative group $F_q^\times$. Then there exists $a, b \in A$ such that $a \cdot b = x$, where $\cdot$ denotes the standard inner product in $\mathbb{F}_q^d$.*

Proof. Define $n(x)$ to be the number of solutions to $a \cdot b = x$ with $a, b \in A$. Note that $n(x) = \sum_{a,b\in} 1_{ab=x}$.

Lemma 37. *Suppose q is prime power. Suppose $\mathbb{F}_q$ is a field. Let χ be a nontrivial character of the additive group $\mathbb{F}_q^+$. Then the set $\widehat{\mathbb{F}_q^+}$ is set of maps $\{x \mapsto c\chi(x)\}_{c\in\mathbb{F}}$ is*

Proof. Note that $|\{x \mapsto c\chi(x)\}_{c\in\mathbb{F}}| = q$. Note that each map $x \mapsto c\chi(x)$ is a unique group homomorphism. Since $\widehat{\mathbb{F}_q^+} \cong \mathbb{F}_q^+$, their sizes are the same. Since the sizes are the same, and one is contained in the other, they are the same sets. □

Let χ be a nontrivial character of the additive group $\mathbb{F}_q^+$. Using the Orthogonality Relations of the additive group of $\mathbb{F}_q$, this implies that

$$\begin{aligned} n(x) &= \sum_{a,b\in A} \frac{1}{q} \sum_{c\in\mathbb{F}} \chi(c(a\cdot b - x)) && \text{(Orthogonality Relations, Above Lemma)} \\ &= \frac{|A|^2}{q} + \frac{1}{q} \sum_{a,b\in A} \sum_{c\in\mathbb{F}_q^\times} \chi(c(a\cdot b - x)) && \text{(Expansion)} \end{aligned}$$

Define $R = \frac{1}{q}\sum_{a,b\in A}\sum_{c\in\mathbb{F}_q^\times} \chi(c(a\cdot b - x))$. We obtain the upper bound

$$\begin{aligned} R^2 &= \frac{1}{q^2}\left(\sum_{a\in A}\left(\sum_{b\in A}\sum_{c\in\mathbb{F}_q^\times} \chi(c(a\cdot b - x))\right)\right)^2 && \text{(Definition of } R\text{)} \\ &\le \frac{|A|}{q^2}\left(\sum_{a\in A}\left|\sum_{b\in A}\sum_{c\in\mathbb{F}_q^\times} \chi(c(a\cdot b - x))\right|^2\right) && \text{(Cauchy Schwarz Inequality)} \\ &\le \frac{|A|}{q^2}\sum_{a\in\mathbb{F}_q^d}\sum_{b_1,b_2\in A}\sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(c_1(a\cdot b_1 - x))\chi(c_2(a\cdot b_2 - x)) && \text{(Trivial Inequality, Expansion)} \\ &= \frac{|A|}{q^2}\sum_{a\in\mathbb{F}_q^d}\sum_{b_1,b_2\in A}\sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(a(c_1b_1 - c_2b_2))\chi(x(c_2 - c_1)) \\ &&& \text{(Rearrangment with } \chi(x-y) = \chi(x)/\chi(y)\text{)} \\ &= |A|q^{d-2}\sum_{b_1,b_2\in A}\sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(x(c_2 - c_1))\frac{1}{q^d}\sum_{a\in\mathbb{F}_q^d} \chi(a\cdot(c_1b_1 - c_2b_2)) \\ &&& \text{(Switching Order of Summation)} \\ &= |A|q^{d-2}\sum_{b_1,b_2\in A}\sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(x(c_2 - c_1))1_{c_1b_1 = c_2b_2}. \\ &&& \text{(Orthogonality Relation, } \textbf{Hasn't Been Justified, But the Proof is the Same}\text{)} \end{aligned}$$

Now define $s_1 = c_1/c_2$ and $s_2 = c_2$. See that

$$\begin{aligned} &\sum_{b_1,b_2\in A}\sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(x(c_2 - c_1))1_{c_1b_1 = c_2b_2} \\ &\qquad = \sum_{b_1,b_2\in A}\sum_{s_1\in\mathbb{F}_q^\times} 1_{s_1b_1 = b_2} \sum_{c_1,c_2\in\mathbb{F}_q^d} \chi(xs_2(1 - s_1)) && \text{(Substitution)} \\ &\qquad = \sum_{b_1,b_2\in A} (q-1)1_{b_1 = b_2} + \sum_{b_1,b_2\in A}\sum_{s_1\ne 1} 1_{s_1b_1 = b_2} \sum_{s_2\in\mathbb{F}_q^\times} \chi(xs_2(1 - s_1)) \\ &&& \text{(Case when } s_1 = 1 \text{ and when } s_1 \ne 1\text{)} \\ &\qquad = \sum_{b_1,b_2\in A} (q-1)1_{b_1 = b_2} - \sum_{b_1,b_2\in A}\sum_{s_1\ne 1} 1_{s_1b_1 = b_2} && \text{(Orthogonality Relation, since } x \ne 0\text{)} \\ &\qquad \le \sum_{b_1,b_2\in A} (q-1)1_{b_1 = b_2} && \text{(Trivial Inequality)} \\ &< q|A|. \end{aligned}$$

Thus implies that $R^2 < |A|^2 q^{d-1}$, which gives $|R| < |A| q^{\frac{d-1}{2}}$. This implies that

$$\begin{aligned} n(x) &= \frac{|A|^2}{q} + R && \text{(Above Equation)} \\ &\geq \frac{|A|^2}{q} - |A| q^{\frac{d-1}{2}} && \text{(Bound on } R\text{)} \\ &> 0. && \text{(Since } |A| > q^{\frac{d+1}{2}}\text{)} \end{aligned}$$

This gives the desired result. □

Now we prove a basic result in analytic number theory.

Theorem 38 (Polya-Vinogradov). *Let χ be a primitive character modulo N. Then for all positive integer m, n, we have*

$$\left| \sum_{m \leq j < n} \chi(j) \right| \leq \sqrt{N} \ln N.$$

Proof. Let $\xi = e^{\frac{2\pi i}{N}}$ be a primitive root of unity of order N. Recall that Fourier's Inversion formula implies that

$$\chi(j) = \sum_{\gcd(a,N)=1} \widehat{\chi}(a) \xi^{ja}.$$

This implies that

$$\begin{aligned} \left| \sum_{m \leq j < n} \chi(j) \right| &= \left| \sum_{m \leq j < n} \sum_{\gcd(a,N)=1} \widehat{\chi}(a) \xi^{ja} \right| && \text{(Fourier Inversion Formula)} \\ &= \left| \sum_{a,N} \widehat{\chi}(a) \cdot \frac{\xi^{an} - \xi^{am}}{\xi^a - 1} \right| && \text{(Geometric Series Formula)} \\ &\leq \frac{1}{\sqrt{N}} \sum_{\gcd(a,N)} \left| \frac{2}{\xi^a - 1} \right| && \text{(Triangle Inequality)} \\ &= \frac{1}{\sqrt{N}} \sum_{\gcd(a,N)} \frac{1}{\left|\sin\left(\frac{\pi a}{N}\right)\right|}. && \text{(Since } e^{2\theta i} - 1 = 2i \sin(\theta) e^{i\theta}\text{)} \end{aligned}$$

Note the following bound.

Lemma 39. *For $0 \leq x \leq \frac{\pi}{2}$, we have that $\sin x \geq \frac{2}{\pi} x$.*

Proof. Define $f(x) = \sin x - \frac{2}{\pi} x$. Note that $f(\pi/2) = 0$ and $f(0) = 0$. Note that $f''(x) = -\sin(x)$. By convexity, it follows that $f(x) \geq 0$ for $0 \leq x \leq \frac{\pi}{2}$. □

This lemma implies that $\sin \frac{\pi a}{N} \geq \frac{2a}{N}$ if $a \leq \frac{N}{2}$, by letting $x = \frac{\pi a}{N}$ and implies that $\sin \frac{\pi a}{N} \geq \frac{2(N-a)}{N}$ if $a > \frac{N}{2}$ by letting $x = \frac{\pi(N-a)}{N}$. This implies that

$$\begin{aligned} \left| \sum_{m \leq j < n} \chi(j) \right| &\leq \frac{2}{\sqrt{N}} \sum_{a \leq \frac{N}{2}} \frac{1}{\left|\sin\left(\frac{\pi a}{N}\right)\right|} \\ &\leq \sqrt{N} \sum_{a \leq \frac{N}{2}} \frac{1}{a} && \text{(Bound From Our Lemma)} \\ &\leq \sqrt{N} \ln N && \text{(Comparision Test)} \end{aligned}$$

This gives the desired bound. □

Theorem 40 (Vinogradov)**.** *Suppose p is a sufficiently large prime number. Then there exists $1 \leq a < p^{\frac{1}{2\sqrt{e}}}(\ln p)^2$ such that a is a quadratic nonresidue.*

Proof. Define $m = \lfloor \sqrt{p}(\ln p)^2 \rfloor$. Define N as the number of quadratic nonresidues among $\{1, 2, \dots, m\}$. This implies that $m - 2N = \sum_{x=1}^{m} \left(\frac{x}{p}\right)$. For the same of contradiction, suppose that $\left(\frac{a}{p}\right) = 1$ for all $1 \leq a \leq X = \left\lfloor p^{\frac{1}{2\sqrt{e}}}(\ln p)^2 \right\rfloor$. Note that the map $x \mapsto \left(\frac{x}{p}\right)$ is a primitive character mod p, since p is prime, and since it's not the trivial character. The Polya-Vinogradov Inequality implies that

$$|m - 2N| = \left| \sum_{x=1}^{m} \left(\frac{x}{p}\right) \right| \leq \sqrt{p} \ln p.$$

This inequality implies that

$$N > \frac{m}{2} - \frac{1}{2}\sqrt{p} \ln p.$$

Any quadratic nonresidue mod p must have a prime factor q that is a quadratic nonresidue mod q, implying that $q > X$ as well. This gives the upper bound

$$N \leq \sum_{X < \text{prime } q \leq m} \frac{m}{q}.$$

Merten's Theorem implies that

$$N \leq \sum_{X < \text{prime } q \leq m} \frac{m}{q} = m \ln\left(\frac{\ln m}{\ln X}\right) + O\left(\frac{m}{\ln X}\right).$$

Since m is defined $m = \lfloor \sqrt{p}(\ln p)^2 \rfloor$ and since $X = \left\lfloor p^{\frac{1}{2\sqrt{e}}}(\ln p)^2 \right\rfloor$, note that $\frac{m}{\ln X} = O(\sqrt{p} \cdot \ln p)$. We also have that

$$\begin{aligned} \ln\left(\frac{\ln m}{\ln X}\right) &= \ln\left(\frac{\frac{1}{2}\ln p + 2\ln\ln p}{\frac{1}{2\sqrt{e}}\ln p + 2\ln\ln p}\right) + O\left(\frac{1}{X \ln p}\right) && \text{(Definitions of } m \text{ and } X) \\ &= \ln\left(\frac{1 + 4\frac{\ln\ln p}{\ln p}}{1 + 4\sqrt{e}\frac{\ln\ln p}{\ln p}}\right) + O\left(\frac{1}{X \ln p}\right) && \text{(Algebraic Manipulation)} \\ &= \frac{1}{2} - \frac{4(\sqrt{e} - 1)\ln\ln p}{\ln p} + O\left(\frac{1}{\ln p}\right) && \text{(Taylor Expansion } \ln(1+x) = 1 + x + O(x^2)) \end{aligned}$$

Our inequality above implies that

$$\frac{m}{2} - \frac{1}{2}\sqrt{p}\ln p < \frac{m}{2} - \frac{4(\sqrt{e} - 1) m \ln\ln p}{\ln p} + O\left(\frac{m}{\ln p}\right).$$

Since $m = \lfloor \sqrt{p}(\ln p)^2 \rfloor$, this is false for sufficiently large primes p. □

Terry Tao notes in his blog that we can use something called Burgess's Amplification Trick to improve the bound to $O_\epsilon(p^{\frac{1}{4\sqrt{e}} + \epsilon})$. At the time that blog article was posted, this was the best known bound. Apparently, it's possible to get better bounds assuming the Riemann hypothesis is true. Also, there is a quick argument to show that the minimal quadratic nonresidue is at most $1 + \sqrt{p}$ using without any of our machinery.

9. Dirichlet's Theorem

Now using facts about characters, facts about complex analysis, and facts about the sums of primes numbers, it will be possible to prove the following claim.

Theorem 41 (Dirichlet's Theorem)**.** *Let a and B be relatively prime integers. Then as $s \to 1^+$, we have*

$$\sum_{p \equiv a \pmod{N}} \frac{1}{p^s} = \frac{1}{\varphi N} \ln\left(\frac{1}{s-1}\right) + O(1).$$

We will prove this with machinery.

Definition 10. We define the **L function** of a Dirichlet character χ mod N as

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

Lemma 42. *Let D be a compact subset of $\mathrm{Re}(s)$. Then $L(s,\chi)$ is uniformly convergent on D.*

Proof. We proceed via the Weierstrass M-Test. Note that $m = \min_{s \in D} \operatorname{Re} S$ exists and there is some $s \in D$ such that $m = \operatorname{Re} s$, since D is compact. This implies that $m > 1$. This implies that $\left|\frac{\chi(n)}{n^s}\right| \leq \frac{1}{n^m}$, since $|\chi(n)| = 1$. Note that $\sum_{n=1}^{\infty} \frac{1}{n^s} < \infty$, by the integral test. The Weierstrass M-Test implies that $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly. □

Lemma 43. *$L(s,\chi)$ is holomorphic on any compact subset of $\mathrm{Re}(s) > 1$.*

Proof. Each of the function $\frac{\chi(n)}{n^s}$ is holomorphic. Since the sum of these functions converges uniformly, they converges uniformly to an analytic function. □

Basically, the idea comes from generating functions. Note that χ is a multiplicative function over $\mathbb{Z}$, i.e., $\chi(a)\chi(b) = \chi(ab)$ for all $a, b \in \mathbb{Z}$. By intuition (fundamental theorem of arithmetic) it follows that

$$\sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \cdots\right)$$

Note that $\frac{1}{1-x} = 1 + x + x^2 + \cdots$. This equation suggests that

$$\sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}.$$

Let's prove this claim.

Lemma 44. *The infinite product $\prod_{i=1}^{\infty}(1 + a_i)$ converges absolutely iff $\sum_{i=1}^{\infty} |a_n|$ converges.*

Proof. https://cornellmath.wordpress.com/2008/01/26/convergence-of-infinite-products/

Taking the logarithm of the product gives the series $\sum \ln(1 + |a_i|)$. The converges is this series is equivalent to the convergence of $\prod(1 + |a_i|)$. Assume, $|a_i| \to 0$. Otherwise, both the product and the sum diverge. Note that $\lim_{x \to 0} \ln(1+x)/x = 1$. This implies that $\lim_{n \to \infty} \ln(1 + |a_n|)/|a_n| = 1$. By the limit comparision test, we are done. □

Lemma 45. *For $\operatorname{Re} s > 1$, we have that*

$$\frac{1}{L(s,\chi)} = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right).$$

Proof. (Proof from Gamelin)

Note that the series the series $\sum 1/p^{x+yi}$ converges absolutely for any $x > 1$. It converges uniformly in any half-plane $\{x \geq 1 + \epsilon\}$. This implies that the product converges absolutely, implying that it converges. Now consider the geometric series

$$\frac{1}{1-\chi(p)p^{-s}} = 1 + \chi(p)p^{-s} + \chi(p^2)p^{-2s} + \cdots, \qquad \operatorname{Re} s > 1 \qquad \text{(Since } \chi \text{ is multiplicative)}$$

Multiplying the m series corresponding to primes $p_1, \ldots, p_m$ gives

$$\frac{1}{(1-\chi(p_1)p_1^{-s})(\cdots)(1-\chi(p_m)p_m^{-s})} = \sum_{k_1,\ldots,k_m=0}^{\infty} \chi(p_1^{k_1}\cdots p_m^{k_m})(p_1^{k_1}\cdots p_m^{k_m})^{-s}.$$

By the Fundamental Theorem of Arithmetic, every integer $n \geq 1$ has a unique representation as a product of powers of distinct primes. A summand $\chi(n)n^{-s}$ appears at most once in the series. The sum is a subsum of $\sum \chi(n)n^{-s}$. As we incorporate more terms into the product, for every N, we eventually capture all terms n^{-s} with $n \leq N$. By absolute convergence, in the limit we have

$$\prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}} = \sum_{n=1}^{\infty} \chi(n)n^{-s} = L(s,\chi).$$

This completes the proof. □

Now choose a branch of the complex logarithm $\ln(z)$. From the product expansion of $L(s,\chi)$, this implies that

$$\begin{aligned} \ln(s,\chi) &= -\sum_{p \text{ prime}} \ln(1-\chi(p)p^{-s}) && \text{(Product Expansion of } L(s,\chi)\text{)} \\ &= \sum_{p \text{ prime}} \sum_{n \geq 1} \frac{\chi(p^n)p^{-ns}}{n}. && \text{(Taylor Expansion, Converges since } |\chi(p)p^{-s}| < 1\text{)} \end{aligned}$$

Now we will use our results to expression the condition $n \equiv a \pmod N$ in an analytic way. Again, we are working over the group $G = (\mathbb{Z}/N\mathbb{Z})^\times$. Let a be some integer satisfying $\gcd(a, N) = 1$. Using the extension of primitive character mod N over the integers, this implies that

$$\begin{aligned} \frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L(s,\chi) &= \frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \sum_{p \text{ prime}} \sum_{n \geq 1} \frac{\overline{\chi(a)}\chi(p^n)p^{-ns}}{n} && \text{(Above Expansion)} \\ &= \sum_{p \text{ prime}} \sum_{n \geq 1} \frac{p^{-ns}}{n} \cdot \frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \chi(p^n)\overline{\chi(a)} && \text{(Switching Order of Summation)} \\ &= \sum_{p \text{ prime}} \sum_{n \geq 1} \frac{p^{-ns}}{n} \cdot \frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \chi(p^n)\overline{\chi(a)} \\ &= \sum_{p \text{ prime}} \sum_{n \geq 1} \frac{p^{-ns}}{n} \cdot 1_{a \equiv p^n \pmod N} \\ & && \text{(Fourier Inversion Formula, Extension of } \chi \text{ over } \mathbb{Z}\text{)} \\ &= \sum_{p \text{ prime}} \sum_{\substack{n \geq 1 \\ p^n \equiv a \text{Mod} N}} \frac{1}{np^{ns}} \\ &= \sum_{p \equiv a \text{Mod} N} \frac{1}{p^s} + \sum_{p \text{ prime}} \sum_{\substack{n \geq 2 \\ p^n \equiv a \text{Mod} N}} \frac{1}{np^{ns}}. \end{aligned}$$

Note the bound

$$\begin{aligned}
\left| \sum_{p \text{ prime}} \sum_{\substack{n \geq 2 \\ p^n \equiv a \text{Mod} N}} \frac{1}{np^{ns}} \right| &\leq \sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{p^{n \operatorname{Re} s}} && \text{(Triangle Inequality)} \\
&\leq \sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{p^n} && \text{(Since } \operatorname{Re} s > 1\text{)} \\
&= \sum_{p \text{ prime}} \frac{1}{p(p-1)} && \text{(Geometric Series)} \\
&< 1. && \text{(Telescoping)}
\end{aligned}$$

This implies that

$$\frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L(s, \chi) = \sum_{p \equiv a \text{Mod} N} \frac{1}{p^s} + O(1).$$

If χ is the trivial character, than $L(s, \chi)$ is not the **zeta function**, since $\chi(n) = 0$ when $\gcd(n, N) \neq 1$. If χ is a nontrivial character, then (apparently) $\ln L(s, \chi)$ is bounded, even as $s \to 1^+$.

Theorem 46. *Let χ be a character mod N. Then $L(s, \chi)$ extends to a function on $\operatorname{Re} s > 0$ which is holomorphics expect possibly for $s = 1$.*

- *If χ is nontrivial, then this function is holomorphic at $s = 1$.*
- *If χ is trivial ($\chi(n) = 1$ when $\gcd(n, N) = 1$ and $\chi(n) = 0$ when $\gcd(n, N) \neq 1$), then*

$$\lim_{s \to 1^+} (s-1) L(s, 1) = \prod_{p \mid N} \left(1 - \frac{1}{p}\right)$$

Proof. We will use Abel summation.

Lemma 47. *Suppose χ is a nontrivial character. Then for all n, we have that $|\chi(1) + \cdots + \chi(n)| \leq N$.*

Proof. Recall that the orthogonality relations imply that

$$\sum_{\gcd(n,N)} \chi(n) = 0.$$

This implies that $|\sum_{k=1}^{n} \chi(k)| = \left|\sum_{k=1}^{n \pmod N} \chi(k)\right|$. Since $|\chi| \leq 1$, the triangle inequality implies that this is at most N. □

Just believe that (apparently it's an easy computation)

$$n^{-s} - (n+1)^{-s} = sn^{-s-1} + O(n^{s-2})$$

over s in compact sets. In particular, this is uniform as $n \to \infty$ over s in compact sets of $\operatorname{Re} s > 0$.

Lemma 48. *We have that $n^{-s} - (n+1)^{-s} = sn^{-s-1} + O(n^{s-2})$. This is uniform as $n \to \infty$ over s in compact sets.*

Proof. It is equivalent to show that $1 - (n/(n+1))^s = sn^{-1} + O(n^{-2})$. Let $A = \min \operatorname{Re}(s)$ on our domain and let $B = \max \operatorname{Im}(s)$ on our compact domain. Then jsut bound using the binomial theorem, and bound using the binomial theorem like we did in homework 2. This will prove uniform convergence on our compact domain. □

Since $|\chi(1)+\cdots+\chi(n)|$ is bounded and since $n^{-s}-(n+1)^{-s}$ converges uniformly to sn^{-s-1} on compact subsets of $\operatorname{Re} s>0$, this implies that the series

$$\sum_{n\geq 1}(\chi(1)+\cdots+\chi(n))(n^{-s}-(n+1)^{-s})$$

also converges uniformly on compact subsets of $\operatorname{Re} s$. By Abel Summation, this series telescopes to $L(s,\chi)$ if $\operatorname{Re} s>1$. This means that the above sum is a holomorphic extension of $L(s,\chi)$ to $\operatorname{Re} s>0$.

Suppose χ is trivial. By definition,

$$\chi(n)=\begin{cases}1 & \text{if } \gcd(n,N)=1\\ 0 & \text{if } \gcd(n,N)\neq 1.\end{cases}$$

Recall that we define $\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p \text{ prime}}\frac{1}{1-p^{-s}}$. (Gamelin) Since $L(s,\chi)=\prod_{p\nmid N}\frac{1}{1-p^{-s}}$, this implies that $L(s,\chi)\prod_{p|N}\frac{1}{1-p^{-s}}=\zeta(s)$. In essence, we have

$$L(s,\chi)=\prod_{p|N}\left(1-\frac{1}{p^s}\right)\cdot\zeta(s).$$

Note the identity

$$\int_n^{n+1}(n^{-s}-t^{-s})\,dt=\frac{1}{n^s}+\frac{(n+1)^{1-s}-n^{1-s}}{s-1}.$$

Summing over $n\in\mathbb{N}$ implies that

$$\begin{aligned}\sum_{n\geq 1}\int_n^{n+1}(n^{-s}-t^{-s})\,dt&=\sum_{n\geq 1}\frac{1}{n^s}+\sum_{n\geq 1}\frac{(n+1)^{1-s}-n^{1-s}}{s-1} && \text{(Our equation above)}\\ &=\zeta(s)-\frac{1}{s-1}.\end{aligned}$$

In particular, this implies that

$$\zeta(s)=\frac{1}{s-1}+\sum_{n\geq 1}\int_n^{n+1}(n^{-s}-t^{-s})\,dt.$$

For $t\in[n,n+1]$, note that we have the bound

$$\begin{aligned}\left|t^{-s}-n^{-s}\right|&=\left|\int_n^t -sx^{-s-1}\right|\\ &\leq\int_n^t\frac{|s|}{x^{\operatorname{Re} s+1}}\,dx && \text{(Triangle Inequality for Integrals)}\\ &\leq\frac{|s|}{n^{1+\operatorname{Re} s}} && \text{(Since } n\leq t\leq n+1\text{)}\end{aligned}$$

In particular, this implies that

$$\left|\int_n^{n+1}(n^{-s}-t^{-s})\,dt\right|\leq\frac{|s|}{n^{1+\operatorname{Re} s}}.$$

This implies that on any compact subsets if $\operatorname{Re} s$, we have the uniform convergence of the series

$$g(s)=\sum_{n\geq 1}\int_n^{n+1}(n^{-s}-t^{-s})\,dt.$$

This implies that g is holomorphic on $\operatorname{Re} s > 0$. Recall that $\zeta(s) = \frac{1}{s-1} + g(s)$. Substitution implies that

$$(s-1)L(s,\chi) = (1+(s-1)g(s)) \prod_{p \mid N} \left(1 - \frac{1}{p^s}\right).$$

Letting $s \to 1^+$ gives the limit. □

Let's prove the following theorem. Apparently it's harder.

Theorem 49. *Suppose χ is a nontrivial character mod N. Then $L(1,\chi) \neq 0$. In particular, $L(s,\chi)$ is bounded as $s \to 1^+$.*

Proof. Recall that we found for all $s > 1$, the equation

$$\frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L(s,\chi) = \sum_{p \text{ prime}} \sum_{\substack{n \geq 1 \\ p^n \equiv a \pmod{N}}} \frac{1}{np^{ns}}.$$

In particular, this value is at least 0. Letting $a = 1$ implies that $\prod_{\chi \in \widehat{G}} L(s,\chi) \geq 1$. Our previous theorem states that if χ is nontrivial, then $L(s,\chi)$ is holomorphic at $s = 1$. Also, $L(s,\chi)$ has a simple pole at $s = 1$, from the second part. This implies that either at most one of the nontrivial characters χ satisfies $\chi(1,\chi) = 0$. For the sake of contradiction, supose χ is that character. This implies that $\overline{\chi}$ is another such character. This implies that $\chi = \overline{\chi}$, since there's at most one.

Now we know that χ takes on values in $\{1,-1,0\}$ over $\mathbb{Z}$. Let's make some magic. Define the function

$$f(x) = \sum_{n \geq 1} \chi(n) \frac{x^n}{1-x^n}.$$

Note that $x \in [0,1)$ means absolute convergence (not uniform convergence though). Due to absolute convergence, we can rearrange terms to obtain

$$\begin{aligned} f(x) &= \sum_{n \geq 1} \sum_{j \geq 1} \chi(n) x^{nj} \\ &= \sum_{a \geq 1} x^a \sum_{d \mid a} \chi(d). \end{aligned}$$

Let's define $c_n = \sum_{d \mid n} \chi(d)$. Since χ is multiplicative, it also follows that if n has factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, then $c_n = c_{p_1^{e_1}} \cdots c_{p_k^{e_k}}$. There are two cases to consider.

- $p \mid N$. Then $c_{p^k} = \sum_{d \mid p^k} \chi(p) = 1$, since $\chi(n) = 0$ when $\gcd(n,N) = 0$, and $\chi(1) = 1$.
- $p \nmid N$. Then $c_{p^k} = \sum_{d \mid p^k} \chi(p)$.
  - Suppose $\chi(p) = 1$. Then $c_{p^k} = k+1$.
  - Suppose $\chi(p) = -1$. Then $c_{p^k} = 1$ if k is even and $c_{p^k} = 0$ if k is odd.

This implies that $c_{p^k} \geq 0$ for all primes p and integers k, implying that $c_n \geq 0$ for all naturals n. Note that there are infinitely many c_n such that $c_n = 1$. This implies that $f(x)$ goes to ∞ as $x \to 1$. Recall that we assume for the sake of contradiction that $L(1,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n} = 0$. This implies that $L(1,\chi) \cdot \frac{1}{1-x} = \sum_{n \geq 1} \frac{\chi(n)}{(1-x)n} = 0$ for all $x < 1$. Now now that

$$L(1,\chi) - f(x) = \sum_{n \geq 1} \frac{\chi(n)}{1-x} \left[\frac{1}{n} - \frac{x^n}{1+x+\cdots+x^{n-1}}\right].$$

Now let's think about the coefficients of $\chi(n)$. Define

$$b_n(x) = \frac{1}{n(1-x)} - \frac{x^n}{1-x^n}.$$

Note that

$$b_n(x) - b_{n+1}(x) = \frac{1}{1-x}\left(\frac{1}{n(n+1)} - \frac{x^n}{(1+x+\cdots+x^{n-1})(1+x+\cdots+x^n)}\right) \geq 0$$

(AM-GM Inequality)

So we know that $b_n(x)$ is monotonically decreasing with respect to n and $b_1(x) = 1$ for all x. Recall that $|\sum_{k=1}^{n} \chi(k)|$ is bounded. By Abel Summation, this implies that $L(1,\chi) - f(x)$ is bounded, a contradiction. This implies that $L(1,\chi) \neq 0$ for all χ nontrivial. So this implies that as $s \to 1^+$ we have that $\ln L(s,\chi)$ is bounded. □

Based on this theorem, it follows that as $s \to 1^+$, we have that $\frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L(s,\chi)$ only depends on the trivial character $\chi = 1$, since $\ln L(s,\chi)$ is bounded otherwise. But recall that $\lim_{s\to 1^+}(s-1)L(s,1) = \prod_{p|N}\left(1 - \frac{1}{p}\right)$. In particular, we have that as $s \to 1^+$,

$$\frac{1}{\varphi(N)} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L(s,\chi) = \frac{1}{\varphi(N)} \ln L(s,1) + O(1) \quad \text{(Since } \ln L(s,\chi) \text{ is bounded if } \chi \text{ is nontrivial)}$$

$$= \frac{1}{\varphi(N)} \ln\left(\frac{1}{s-1}\right) + O(1). \quad \text{(From the Theorem Before the Hard One)}$$

But this is also equal to

$$\sum_{p \equiv a \text{ Mod} N} \frac{1}{p^s} + O(1).$$

So we can conclude that as $s \to 1^+$, we have that

$$\sum_{p \equiv a \text{ Mod} N} \frac{1}{p^s} = \frac{1}{\varphi(N)} \ln\left(\frac{1}{s-1}\right) + O(1)$$

In particular, there are infinitely many primes p such that $p \equiv a \pmod{N}$.

10. Hypotheses A and B

Weintraub notes that with Dirichlet's Theorem and the Chinese Remainder Theorem, it easier to prove Hypotheses A and B.

11. References

[1] Steven H. Weintraub (2011) *On Legendre's Work on the Law of Quadratic Reciprocity*, The American Mathematical Monthly, 118:3, 210-216, DOI: 10.4169/amer.math.monthly.118.03.210

[2] Titu Andreescu and Gabriel Dospinescu. *Straight from the Book*. XYZ Press, 2012. ISBN 978-0-9799269-3-8.

[3] Terence Tao and Van Vu. *Additive Combinatorics*. Cambridge University Press, 2016. ISBN 978-0-511-24530-5.

[4] Terence Tao. *The Least Quadratic Nonresidue and the Square Root Barrier.* August 2009. https://terrytao.wordpress.com/2009/08/18/the-least-quadratic-nonresidue-and-the-square-root-barrier/