FINITE ABELIAN GROUPS AND CHARACTER SUMS

PAUL H. KOESTER

Abstract. These are some notes I have written up for myself. I have compiled what I feel to be some of the most important facts concerning characters on finite abelian groups, especially from a number theoretic point of view. I decided to distribute these because I couldn’t find a single reference that covered everything that I thought was relevant to the material I will discuss on Wednesday. Of course, there is significantly more in these notes than I plan to cover in the talk. The talk will most likely cover the definition and very basic properties of characters on finite abelian groups (most importantly the orthogonality relations), the definition of the Fourier transform along with the inversion formula, the Gauss and Weyl sum estimates and their relation to each other, and if I have time, the Polya-Vinogradov estimate.

1. Finite Abelian Groups

1.1. Examples. The three most important examples of finite abelian groups for us will be

1. The group of residues modulo some integer $q$, denoted $\mathbb{Z}/q\mathbb{Z}$ with additive notation.
2. The group of $q^{th}$ roots of unity, $\{\omega^n\}_{n=0}^{q-1}$ with multiplicative notation. Throughout, $\omega = e^{2\pi i/q}$ is a primitive $q^{th}$ root of 1. This group is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ in the obvious way.
3. The group $U(q) = \mathbb{Z}/q\mathbb{Z}^*$, the multiplicative group of units modulo $q$.

1.2. Fundamental Theorems on Finite Abelian Groups. We will implicitly use the following theorems from elementary group theory.

Lagrange’s Theorem. If $H$ is a subgroup of $G$ then $|H|$ divides $|G|$.

Chinese Remainder Theorem. If $(N, M) = 1$ then $\mathbb{Z}/NM\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z}$.

Fundamental Theorem of Finite Abelian Groups. If $G$ is a finite abelian group then

$$G = \bigoplus_{p \in P} \bigoplus_{j=1}^{r_p} \mathbb{Z}/p^{m_j} \mathbb{Z}$$

for some choice of integers $r_p \geq 1$ and $m_j^p \geq 1$. This decomposition is unique, up to permuting the powers $m_j^p$.

For the most part we don’t need the full power of the fundamental theorem of finite abelian groups, just the fact that finite abelian groups can be decomposed into sums of cyclic groups. Note that the asserted uniqueness is with respect to the decomposition into $p$-groups. A given group may have several decompositions into sums of cyclic groups. In fact, that is the content of the Chinese remainder theorem.

1.3. The Structure of $U(q)$. The group of units modulo $q$ is typically not a cyclic group. For example,

$U(8) = \{1, 3, 5, 7\}$

is generated by any two of 3, 5, 7, but each of these elements has order 2. Thus,

$U(8) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The goal of this section is to describe the structure of $U(q)$ in terms of a decomposition into cyclic groups.

Date: October 11, 2006.
Proposition 1. Let $R$ and $S$ be two commutative rings with units. Then

$$(R \oplus S)^* = R^* \oplus S^*.$$ 

Proof. Suppose $r \in R^*$ and $s \in S^*$. Then there exist $\rho \in R^*$ and $\sigma \in S^*$ so that $r\rho = 1$ and $s\sigma = 1$. Therefore,

$$(r, s)(\rho, \sigma) = (1, 1).$$ 

Likewise, if $(r, s)$ is a unit then there exists $(\rho, \sigma)$ so that

$$(r, s)(\rho, \sigma) = (1, 1),$$ 

and so $r\rho = 1$ and $s\sigma = 1$. \hfill \Box

In view of the Chinese remainder theorem we only need to determine the structure of $U(q)$ when $q$ is a prime power. First we assume $q = p$ a prime. We recall a more general fact.

Proposition 2. Let $F$ be a field and $M$ a finite multiplicative subgroup of $F^*$. Then $M$ is cyclic.

Proof. Let $g \in M$ have maximal order, say $m$. We prove $|M| = m$. Notice that if $h \in M$ then the order of $h$ divides $m$, for if not, then $gh$ has order larger than $m$. Let $\psi(x) = x^m - 1 \in F[x]$. Then every element of $M$ is a root of $\psi$. As $F$ is a field, $\psi$ has at most $m$ roots. Therefore $|M| \leq m$. The reverse inequality is obvious. \hfill \Box

Proposition 3. If $p$ is an odd prime and $k \geq 1$ then $U(p^k)$ is a cyclic group of order $\varphi(p^k) = p^{k-1}(p-1)$.

Proof. Certainly the order of $U(q)$ is always $\varphi(q)$ for any integer $q$ so we only need to prove cyclicity. For $k = 1$ this follows from the above proposition. For general $k$ the idea is to lift a generator from $\mathbb{Z}/p\mathbb{Z}$ to a generator of $\mathbb{Z}/p^k\mathbb{Z}$. This proof will look familiar if you know Hensel’s lemma.

Let $k \geq 2$ and let $g$ be a generator of $\mathbb{Z}/p\mathbb{Z}$. First we prove that

$$(g + tp)^{p-1} \not\equiv 1 \mod p^2$$

for either $t = 0$ or 1. For suppose that $g^{p-1} \equiv 1 \mod p^2$. Then

$$(g + p)^{p-1} \equiv g^{p-1} + (p-1)pg \equiv 1 + p(p-1)g \mod p^2.$$ 

If this is congruent to 1 then $p^2|(pg - 1)p$, but $p$ does not divide either $p - 1$ or $g$. This proves our claim.

Now let $t$ be so that the claim holds and let $d$ be the order of $g + tp$ modulo $p^k$. This implies $d|\varphi(p^k)$. Also, as $g$ is primitive modulo $p$ we have that $p - 1|d$. We find that $d = p^{e(p-1)}$ for some $0 \leq e \leq k - 1$. Let us suppose $c < k - 1$ and seek a contradiction. As $(g + tp)^{p^e} = 1 + pu_2$ we can find an integer $u_2$ relatively prime to $p$ so that

$$(g + tp)^{p^1} = 1 + pu_2.$$ 

Then

$$(g + tp)^{p^{e(p-1)}} = (1 + pu_2)^p \equiv 1 + p^2u_2 \mod p^3.$$ 

Iteratively, we have

$$(g + tp)^{p^{e(p-1)}(p-1)} = 1 + p^eu_t$$

with $u_t$ relatively prime to $p$. Next, we observe

$$(g + tp)^{p^{e(p-1)}} \equiv 1 \mod p^k.$$ 

This is possible only if $c \geq k - 1$, which therefore finishes the proof. \hfill \Box

We saw in the beginning of this section that $U(8)$ is not cyclic. (If you are a true number theorist $2$ will quickly become your least favorite prime. It always messes everything up.) It turns out that $U(2^k)$ just barely fails to be cyclic, in view of the next proposition.

Proposition 4. $5$ has order $2^{k-3}$ in $U(2^k)$ where $k \geq 3$. 
Proof. This is certainly true for \( k = 3 \) so we induct. In fact, we induct on the statement that
\[
5^{2k-3} \equiv 1 + 2^{k-1} \mod 2^k.
\]
Suppose this is true for some \( k \). Then there exists an integer \( u \) so that
\[
5^{2k-3} = 1 + 2^{k-1} + 2^ku
\]
and so
\[
5^{2k-2} = 5^{2k-3}2 = (1 + 2^{k-1} + 2^ku)^2 = 1 + 2^k + 2^{k+1}w
\]
for some \( w \). This shows the order of 5 modulo \( p^{k+1} \) is \( 2^{k-2} \). \( \square \)

Next, we observe that \( 5^n \) is never congruent to \(-1 \mod 2^k \). For if it is then we obtain \( 1 \equiv -1 \mod 4 \) upon reducing modulo 4. This shows that \( U(2^k) \) is the direct sum of the group generated by 5 and the group generated by \(-1 \). Thus,

**Proposition 5.** \( U(2) = \{1\}, U(4) \cong \mathbb{Z}/2\mathbb{Z} \) and for \( k \geq 3 \),

\[ U(2^k) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z} \]

Thus, we have proved that \( U(p^k) \) is cyclic for odd primes \( p \) and the product of two cyclic groups, one with order 2, when \( p = 2 \). By our previous comments regarding the Chinese remainder theorem we have a complete description of the decomposition of \( U(q) \) into cyclic factors.

**Structure Theorem for \( U(q) \).** Let \( q = 2^kp_1^{k_1} \cdots p_m^{k_m} \) where the \( p_j \) are distinct odd primes. Then

\[ U(q) \cong U(2^k) \oplus \mathbb{Z}/(p_1^{k_1-1}(p_1 - 1)) \oplus \cdots \oplus \mathbb{Z}/(p_m^{k_m-1}(p_m - 1)) \]

where \( U(2^k) = \{1\} \) if \( k = 0 \) or 1, \( \mathbb{Z}/2\mathbb{Z} \) if \( k = 2 \) and \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z} \) if \( k \geq 3 \).

2. **Characters and Fourier Analysis**

We want to set up the basics of Fourier analysis in the setting of finite abelian groups. The basic object of study for Fourier analysis is the vector space of all (reasonable) complex valued functions defined on a group \( G \). Here \( G \) will always be finite and abelian. An obvious basis to use for the space of functions is the basis of point masses. It will be much better for us to use a basis which encodes the group structure of \( G \). This leads us to consider the characters of \( G \).

2.1. **The Dual Group and Characters.** Given a finite abelian group \( G \) we define the dual group, or group of characters, to be the set of all complex valued group homomorphisms on \( G \), denoted \( \hat{G} \). This is a group under function multiplication. It is easy to see these functions are in fact \( \mathbb{T} \) valued. The identity is denoted by \( \chi_0 \) and is the function constantly equal to 1. The inverse of \( \chi \) is the complex conjugation.

For our first example, let \( G = \mathbb{Z}/q\mathbb{Z} \) for some integer \( q \) and let \( \omega \) be a fixed primitive \( q^{th} \) root of unity. For each \( r \in \mathbb{Z} \) we define
\[
\chi_r : \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C} \\
\chi_r(n) = \omega^{rn}
\]

It is easy to see that this is a group homomorphism. Also, \( \chi_r = \chi_s \) if and only if \( q|(r-s) \). Thus, we may identify \( \mathbb{Z}/q\mathbb{Z} \) with a subset of its dual group. In fact, every character of \( \mathbb{Z}/q\mathbb{Z} \) is \( \chi_r \) for some \( r \in \mathbb{Z}/q\mathbb{Z} \). For \( \chi(1) \) is necessarily a \( q^{th} \) root of unity, say \( \omega^r \). It then follows that \( \chi(n) = \omega^{rn} \). We have therefore proved that finite cyclic groups are isomorphic to their dual groups. This isomorphism is not canonical, however, as it depends on the particular choice of primitive \( q^{th} \) root we use.

**Proposition 6.** \( \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \).

The operation of forming duals is functorial, in that it behaves nicely with respect to just about any natural group theoretic operation we may perform on the group. We will only need to know how it behaves with respect to products.

**Proposition 7.** \( \hat{G} \oplus \hat{H} = \hat{G} \oplus \hat{H} \)

\(^1\)What we call characters here coincide with the notion of characters used in representation theory. For a detailed account see Lang’s “Algebra.”
Proof. Given characters $\psi$ and $\theta$ on $G$ and $H$ we get the corresponding character $\psi \otimes \theta$ on $G \oplus H$. Likewise, given a character on the product group, it equals the tensor product of its restrictions to the first and second factors.

Combining the little we know about character groups with the fundamental theorem of finite abelian groups we get

**Proposition 8.** $\hat{G} \cong G$ for any finite abelian group.

Characters on finite abelian groups satisfy a sort of Hahn-Banach theorem.

**Proposition 9.** If $H$ is a proper subgroup of $G$, $x \in G \setminus H$ and $\phi$ is a character on $H$, then there exists a character $\chi$ on $G$ extending $\phi$ which is not 1 on $x$.

Proof. It is enough to show $\phi$ extends from $H$ to the group generated by $H$ and $x$. Let $m$ be the smallest positive integer so that $x^m \in H$. We demand $\phi(x^m) = \chi(x)^m$, so we chose $\alpha$ so that $\alpha^m = \phi(x^m)$. As $m \neq 1$, we may always choose $\alpha \neq 1$. Given $hx^n$ in the group generated by $H$ and $x$ we must have

$$\chi(hx^n) = \alpha^n \phi(h).$$

We need to be slightly careful since $G$ need not split as a direct sum of $H$ and its quotient, and so we need to check the defining equation is independent of the decomposition into $hx^n$. Thus, suppose

$$hx^n = kx^m$$

with $h, k \in H$. Then $x^{n-m} = kh^{-1} \in H$ and so

$$\phi(x^{n-m}) = \phi(h)\phi(k)^{-1}.$$ 

As we demand $\chi(x) = \alpha$ and $\chi|_H = \phi$ we have

$$\phi(x^{n-m}) = \chi(x^{n-m}) = \alpha^{n-m}$$

and

$$\phi(h)\phi(k)^{-1} = \chi(h)\chi(k)^{-1}$$

and so $\chi$ is well defined.

As a character of $G$ is a group homomorphism, its kernel is some subgroup of $G$, and so the level sets of the character are the cosets of some subgroup. This Hahn-Banach theorem implies the converse; given a subgroup $H$ of $G$ there exists a character of $G$ which is identically 1 on $H$. Moreover, the number of characters is the index of the subgroup. This correspondence between characters and subgroups will be useful.

2.2. **Double Dual.** Given a finite abelian group $G$ we created a new finite abelian group $\hat{G}$. This is an object for which we may take a dual of. Since we already know $\hat{G} \cong G$ it is not surprising that $\hat{\hat{G}} \cong G$. However, it is worth belaboring this point because the relation between a group and its double dual is a canonical one, whereas the relation between a group and its dual is not canonical.

Given an element of $G$ we need to interpret this element as a character acting on the characters of $G$. But this is done in the usual manner for double duals. The mapping

$$g : \chi \mapsto \chi(g)$$

gives the natural embedding of $G$ into its double dual. The equality follows since the two groups are finite with the same order.
2.3. Orthogonality Relations.

**Proposition 10.** Let $G$ be a finite abelian group and $\chi \neq \chi_0$. Then

$$\sum_{x \in G} \chi(x) = 0.$$  

**Proof.** There exists a $y \in G$ so that $\chi(y) \neq 1$ and so

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{z \in G} \chi(z)$$

and therefore

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$  

As $\chi(y) - 1 \neq 0$ we get the desired conclusion. □

This is perhaps more familiar in the cyclic setting. For $G = \mathbb{Z}/q\mathbb{Z}$ we are thus asserting

$$q - 1 \sum_{n=0}^{q-1} \omega^{rn} = 0$$

when $r$ is not a multiple of $q$. This is a simple exercise with summing geometric sums.

The orthogonality relation usually appears in the following form.

**Proposition 11.** \(\sum_{x \in G} \chi(x)\overline{\phi(x)} = \begin{cases} |G| & \text{if } \chi \neq \phi; \\ 0 & \text{if } \chi = \phi. \end{cases} \)

In view of the duality between $G$ and its character group we have the dual form of the orthogonality relations.

**Proposition 12.** \(\sum_{\chi \in \hat{G}} \chi(x)\overline{\chi(y)} = \begin{cases} |G| & \text{if } x = y; \\ 0 & \text{if } x \neq y. \end{cases} \)

3. Fourier Analysis on Finite Abelian Groups

3.1. Fourier Transform. The orthogonality relations along with the fact $|\hat{G}| = |G|$ show that the characters of $G$ form an orthogonal basis for the space of complex valued functions on $G$. In this finite setting the Fourier transform is simply the change of basis matrix starting in the basis of point masses and moving into the basis of characters. More formally,

$$\mathcal{F}_G f(\chi) = \hat{f}(\chi) = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{\chi(x)}$$

where $f$ is a complex valued function on $G$ and $\chi$ is a character of $G$. \(^2\)

We define the (inverse) Fourier transform on $\hat{G}$ in the following way. Let $F$ be a complex valued function on $\hat{G}$ and $x \in G$. Then

$$\mathcal{F}_G^{-1} F(x) = \sum_{\chi \in \hat{G}} F(\chi) \chi(x).$$

The inverse transform inputs a function on $\hat{G}$ and outputs a function on $G$, and so it makes sense to compose $\mathcal{F}_G$ and $\mathcal{F}_G^{-1}$. The name inverse transform suggests the following.

\(^2\)This definition is not entirely universal. Sometimes the character is not conjugated and sometimes other normalizations are used. Our normalization is the "correct one" if we view the convolution algebra as being the fundamental structure on the space of functions. If we view the pointwise algebra to be the fundamental structure on the space of functions it is more convenient to use no normalization factor, and if we view the inner product as the fundamental structure it is more convenient to divide by $|\hat{G}|$ rather than $|G|$. If we want to be pedantic we could write $\mathcal{F}_G,\mu$ where $\mu$ is a particular choice of Haar measure.
Fourier Inversion. Given \( f : G \to \mathbb{C} \) and \( x \in G \),
\[
f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x).
\]

Proof.
\[
\sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x) = \sum_{\chi \in \hat{G}} \frac{1}{|G|} \sum_{y \in G} f(y) \overline{\chi(y)} \chi(x) \\
= \sum_{y \in G} f(y) \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(xy^{-1}) = f(x),
\]
where we used the orthogonality relation in the last line.

Another simple application of the orthogonality relation follows.

Plancheral’s Identity. \( \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)} = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \overline{\hat{g}(\chi)} \).

Particularly important is the case \( f = g \), in which case we find that the Fourier transform is an isometry.

3.2. Fourier Transform on Cyclic Groups. Suppose now that \( G = \mathbb{Z}/q\mathbb{Z} \) for some positive integer \( q \). Upon fixing a primitive \( q^{th} \) root of unity, say \( \omega = e^{2\pi i / q} \), we may identify \( \hat{\mathbb{Z}/q\mathbb{Z}} \) with \( \mathbb{Z}/q\mathbb{Z} \).

Observe that, with respect to the basis of point masses, the Fourier transform is represented by the Vandermonde matrix
\[
\begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{q-1} \\
1 & \omega^2 & \omega^4 & \cdots & \omega^{2(q-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{q-1} & \omega^{2(q-1)} & \cdots & \omega^{(q-1)(q-1)}
\end{pmatrix}.
\]

In particular, the fact that the Fourier transform is invertible is a simple consequence of the Vandermonde determinant
\[
\det((x^j_i)) = \prod_{1 \leq n < m \leq q} (x_m - x_n).
\]

3.3. Poisson Summation. It is interesting to note that the formulas
\[
\frac{1}{|G|} \sum_{x \in G} f(x) \overline{\chi(x)} = \hat{f}(\chi) \\
\hat{f}(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x)
\]
can be put on a more equal footing. The first expresses \( \hat{f} \) on a coset of the trivial subgroup of \( \hat{G} \) as a suitable average of shifts of \( f \) along the full group \( G \), whereas the latter expresses \( f \) on a coset of the trivial subgroup of \( G \) as a suitable average of shifts of \( f \) along the full group \( \hat{G} \). This phenomena extends to any coset of any subgroup of \( G \). First, given \( H \) a subgroup of \( G \), we define
\[
\hat{G}^H = \{ \chi \in \hat{G} : \chi(x) = \chi(xy^{-1}) \text{ for all } x \in G, y \in H \}.
\]

As exercises, you may want to check
1. \( \hat{G}^H \) is a subgroup of \( \hat{G} \).
2. \( \hat{G}^H \cong \hat{G}/\hat{H} \).
3. If \( G \) is a finite abelian group and \( H \) a subgroup, then there exists a subgroup of \( G \) isomorphic to \( G/H \). Prove this using facts about character groups, in particular the self duality of finite abelian groups.
4. Prove the result of the last exercise without using character groups.
As a consequence of the second exercise, we see the smaller \( H \) is, the larger \( \hat{G}^H \) must be. This can be viewed as a ramification of the uncertainty principle. As a heuristic, this principle says strong localization in \( G \) (the so called physical space) forces a lack of localization in \( \hat{G} \) (the so called frequency space). There is an enormous body of results collectively known as “the uncertainty principle” which give various rigorous interpretations of the loose principle.

**Poisson Summation.** Given \( H \) a subgroup of \( G \), \( f : G \to \mathbb{C} \), \( \psi \in \hat{G} \) and \( y \in G \), we have

\[
\sum_{x \in H} f(xy)\overline{\psi(x)} = |H| \sum_{\chi \in \hat{G}^H} \hat{f}(\chi\psi)\chi(y)\psi(y)
\]

I won’t prove this here, but a few exercises may be useful.

1. Recover the formulas for \( f(x) \) and \( \hat{f}(\chi) \) by making appropriate choices of \( H, \psi \) and \( y \).
2. Suppose \( G = G_1 \oplus G_2 \) and \( f : G \to \mathbb{C} \). We may define ”partial Fourier transforms” of \( f \) by freezing one of the variables and thus viewing \( f \) as a function on either \( G_1 \) or \( G_2 \). Express these partial transforms as suitable averages of each other. (This in fact proves the Poisson summation formula in the case that \( G \) splits as \( H \oplus (G/H) \).)
3. Let \( H \) be a subgroup of \( G \). Compute \( \hat{1}_H \) using the Poisson summation formula. Your result should be of the flavor ”The Fourier transform maps subgroups to quotient groups.”
4. What happens in the previous exercise if we replace subgroup with coset of a subgroup? Try to find the most general sort of statement here.

3.4. **An Uncertainty Relation.** Recall that the support of a function \( f : G \to \mathbb{C} \) is the set \( \text{supp} f \subset G \) on which \( f \) is not zero. We give a specific instance of the uncertainty principle which we alluded to above.

**Uncertainty Principle.** Let \( f : G \to \mathbb{C} \) where \( G \) is a finite abelian group. Then

\[
|\text{supp} f| |\text{supp} \hat{f}| \geq |G|,
\]

provided \( f \) is not identically 0.

**Proof.** Choose \( \psi \in \hat{G} \) so that \( |\hat{f}(\psi)| \) is maximal.

\[
|\hat{f}(\psi)|^2 = \left| \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\psi(x)} \right|^2 \leq \frac{1}{|G|^2} \left( \sum_{x \in G} |f(x)| \right)^2
\]

\[
\leq \frac{|\text{supp} f|}{|G|^2} \sum_{x \in G} |f(x)|^2 = \frac{|\text{supp} f|}{|G|} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2 \leq \frac{|\text{supp} f|}{|G|} |\text{supp} \hat{f}| |\hat{f}(\psi)|^2.
\]

The assumption that \( f \) is not identically 0 assures us that \( \hat{f}(\psi) \neq 0 \), so we obtain the result upon division.

The last exercise on Poisson summation shows this inequality is sharp. As an exercise, prove that the only way equality may appear here is if

\[
f(x) = cv(x) \mathbf{1}_{H+p}(x)
\]

where \( c \in \mathbb{C}, \psi \in \hat{G}, y \in G \) and \( H \) is a subgroup of \( G \). Thus, the only cases of equality should coincide with the result in the last exercise on Poisson summation.

This suggests that in the case of \( G = \mathbb{Z}/p\mathbb{Z} \) for \( p \) prime, we may be able to strengthen the inequality, as this group has no nontrivial subgroups. Such a strengthening was found recently by Tao. The paper [11] also gives some applications of this uncertainty principle to additive number theory.

**Uncertainty Principle in \( \mathbb{Z}/p\mathbb{Z} \).** Let \( p \) be prime and \( f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C} \). Then

\[
|\text{supp} f| + |\text{supp} \hat{f}| \geq p + 1.
\]

We won’t prove this here, but we will state the main lemma needed for this. It is a strong sort of invertibility of the Fourier transform on these prime cyclic fields.
Proposition 13. Let $p$ be prime and $A \subseteq \mathbb{Z}/p\mathbb{Z}$. Then for any set $B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|B| = |A|$, the operator $T : \ell^2(A) \to \ell^2(B)$ given by $f \mapsto f|_B$ is invertible.

A brief comment on notation is required. $f$ starts as a function defined on $A$. We extend $f$ to a function on $\mathbb{Z}/p\mathbb{Z} \supset A$ by defining it to be 0 where it is not already defined. We then pass to a function on $\mathbb{Z}/p\mathbb{Z}$ via the Fourier transform. Finally, we obtain a function on $B \subseteq \mathbb{Z}/p\mathbb{Z}$ by restricting to $B$.

Primality is required here. Otherwise we may take $A$ to be some proper subset of $G$ and $B$ to be some subset of the same size as $A$, but is not a coset of any subgroup of $\hat{G}$.

In terms of the Vandermond matrix $(\omega^{nm})_{n,m \in \{0,1,\ldots,p-1\}}$ the above proposition says that not only is this matrix invertible, but every square submatrix is also invertible.

Another common formulation of the uncertainty principle concerns the lack of commutativity of two natural classes of operators acting on functions on $G$. Define the translation operator $T_g$ for each $g \in G$ by

$$T_g f(x) = f(x-g).$$

Define the modulation operator $M_\chi$ for each $\chi \in \hat{G}$ by

$$M_\chi f(x) = \chi(x) f(x).$$

We then have the commutator

$$T_g \circ M_\chi - M_\chi \circ T_g = (\chi(g) - 1) M_\chi \circ T_g.$$

This seemingly different relation is connected to the above uncertainty principles. To see this, we need to observe the following facts.

1. The point masses on $G$ form an eigenbasis for $M_\chi$ for all $\chi \in \hat{G}$.
2. The characters on $G$ form an eigenbasis for $T_g$ for all $g \in G$.
3. The families of operators $\{T_g\}$ and $\{M_\chi\}$ do not commute with each other, and so their respective eigenbases are not easily related.
4. The Fourier transform is the change of basis transformation between these two bases.

The challenge in relating these two different seeming principles is to make the vague statement “eigenbases are not easily related” into a rigorous statement.

3.5. Convolution. Let $G$ be a finite abelian group and $f$ and $g$ functions on $G$. We define their convolution as

$$f \ast g(y) = \frac{1}{|G|} \sum_{x \in G} f(x) g(y-x).$$

This should not be confused with Dirichlet convolution, which is defined in terms of the divisor structure of $\mathbb{N}$. Here are some more exercises.

1. $\ast$ is commutative and associative, and distributes over addition.
2. $\delta_0$, the point mass at the identity, is the identity for $\ast$.
3. $(f \ast g) = \hat{\hat{f} \ast \hat{g}}$.
4. $\sum_{a,b,c,d \in G} f(a) \overline{f(b)} f(c) f(d) = \sum_{x \in G} |\hat{f}(x)|^4$

3.6. Connections with the Regular Representation. Given a finite abelian group $G$ we have a natural way of representing $G$ on $L^2(G)$. (In view of finite dimensionality, $L^2(G)$ is just a fancy notation for the the vector space of all complex valued functions on $G$.) Namely

$$\rho : G \to U(L^2(G)),$$

$$\rho : g \mapsto T_g$$

where

$$T_g(f)(x) = f(x-g).$$
It is easy to see this is a unitary representation of \( G \). As \( G \) is abelian, the operators \( \{ T_g \}_{g \in G} \) are a commuting family and are therefore simultaneously diagonalizable. Suppose \( f \) is an eigenfunction for all of the \( T_g \)'s, and let \( \lambda(g) \) denote the corresponding eigenvalue. That is

\[
T_g f = \lambda(g) f.
\]

As an exercise, show that \( \lambda \) is a character of \( G \) and in fact all characters arise in this way.

3.7. The Trace Formula. Recall that if \( A \) is a matrix then the trace of \( A \), \( \text{Tr}(A) \) is the sum of the diagonals. As simple exercises, prove

1. \( \text{Tr}(AB) = \text{Tr}(BA) \)
2. \( \text{Tr}(UAV^{-1}) = \text{Tr}(A) \)
3. If \( A \) is diagonalizable with eigenvalues \( \lambda_1, \lambda_2, \ldots, \lambda_n \), then the trace of \( A \) is the sum of the eigenvalues.

The importance of 2 is that the trace of \( A \) depends only on the linear operator defined by the matrix \( A \) and not the matrix itself. Thus, we may define the trace of a linear operator as the trace of the matrix representing the operator with respect to any basis.

Given any linear operator \( S \) mapping functions on \( G \) to functions on \( G \) we may express \( T \) as

\[
Sf(x) = \sum_{y \in G} K(x,y)f(y)
\]

for some function \( K : G \times G \rightarrow \mathbb{C} \). We will refer to \( K \) as the kernel\(^3\) of \( S \), and we may write \( S_K \) to denote the linear operator with the kernel \( K \).

As \( K \) is simply a basis which represents the operator \( S \) we obtain

**Trace Formula.** \( \text{Tr}(S_K) = \sum_{x \in G} K(x,x) \)

The typical application of the trace formula is to start with some fixed function \( K \) so that \( S_K \) is diagonalizable, and then deduce an identity by equating the sum of the eigenvalues with the sum appearing in the trace formula. We mentioned before that the Fourier inversion formula is a special case of the Poisson summation formula. It turns out that Poisson summation is a special case of the trace formula. (If I am remembering correctly, the trace formula plays a much more fundamental role in harmonic analysis on nonabelian groups. In the nonabelian setting it is no longer sufficient to look at characters, but rather we need to study the actual representations of the group. As a consequence, we no longer have inversion formulae and trace formulae are the required substitute. If you are interested in the nonabelian setting, see [12])

Particularly nice operators are those for which there exists a function \( k : G \rightarrow \mathbb{C} \) so that

\[
K(x,y) = k(x-y).
\]

(that is, the kernel depends only on \( x-y \), and not \( x \) and \( y \) independently.) Such operators are referred to as convolution operators. We will denote these by \( C_k \). Here are some more exercises.

1. Let \( S \) be an operator. \( S \) is a convolution operator if and only if \( S \) commutes with all translation operators \( T_g \) as \( g \in G \).
2. Let \( C_k \) be a convolution operator. Then \( \hat{G} \) is an eigenbasis for \( C_k \) and the eigenvalue associated with \( \chi \in \hat{G} \) is \( \hat{k}(\chi) \). That is, \( C_k(\chi) = \hat{k}(\chi) \chi \).
3. Prove \( \text{Tr}(C_k) = |G|k(0) \). Deduce from the trace formula and the previous exercise that \( k(0) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{k}(\chi) \).

Using basic facts concerning the behavior of the Fourier transform with respect to translations and modulations it is easy to deduce

\[
k(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{k}(\chi) \chi(x)
\]

\(^3\)The kernel of a linear operator is just the matrix which represents the operator with respect to the basis of point masses. The analogue of this representation of operators on infinite dimensional spaces still holds, provided we allow \( K \) to be a distribution. This is the content of the Schwartz kernel theorem, and in my opinion the only reason for studying distributions in the first place.
directly from the last exercise. This illustrates how the inversion formula is a special case of the trace formula. As an exercise, deduce Poisson summation from the trace formula.

4. Dirichlet Characters

The previous section discussed Fourier analysis in the context of finite abelian groups. In this section we specialize to the case $G = U(q)$ for some $q \in \mathbb{N}$. A Dirichlet character modulo $q$, or more simply a character mod $q$, is an element of $\hat{U}(q)$. Notice that characters modulo $q$ are defined in terms of the multiplicative structure of $\mathbb{Z}/q\mathbb{Z}$. It will be convenient to extend functions from $U(q)$ to $\mathbb{Z}/q\mathbb{Z}$ by identifying $U(q)$ with the appropriate subset of $\mathbb{Z}/q\mathbb{Z}$ and defining the function to be zero where it is not already defined. Likewise, it will be convenient to extend functions from $\mathbb{Z}/q\mathbb{Z}$ to either $\mathbb{N}$ or $\mathbb{Z}$ by periodicity, by identifying $\mathbb{Z}/q\mathbb{Z}$ with $\{1, 2, \ldots, q\}$. We will make use of these extensions freely, often without further comment. For instance, in a particular discussion we may interchangeably view a character mod $q$ as a function on $U(q)$, $\mathbb{Z}/q\mathbb{Z}$, and $\mathbb{N}$ at different points of the same argument.

We will always use $\chi_0$ to denote the identity character mod $q$. Viewing this as a function on $\mathbb{N}$, we have

$$\chi_0(a) = \begin{cases} 1 & \text{if } (a, q) = 1; \\ 0 & \text{if } (a, q) \neq 1. \end{cases}$$

4.1. Periodic Functions. Let $f : \mathbb{Z} \to \mathbb{C}$. We say $f$ is periodic if there is a positive integer $k$ so that $f(x + k) = f(x)$ for all $x \in \mathbb{Z}$. We may say $f$ is $k$-periodic, and that $k$ is a period of $f$. Characters on both $\mathbb{Z}/q\mathbb{Z}$ and $U(q)$ are $q$-periodic. This is by definition, as they were originally defined on a much smaller set and were extended by periodicity.

Here are some more exercises.

1. If $k$ is the smallest positive period of $f$, then $k$ divides any other period of $f$.
2. Suppose $f$ is completely multiplicative and is periodic with smallest positive period $q$. Prove $f(x) = 0$ if $(x, q) \neq 1$, and so $f \in \hat{U}(q)$.
3. Suppose $q$ is a squarefree integer and $\chi$ is a character mod $q$. Prove that $q$ is the smallest positive period of $\chi$.

4.2. The Legendre Symbol. Now suppose $q = p$ is a prime. We say $a \in U(p)$ is a quadratic residue mod $p$ if there exists an $x \in U(p)$ so that $x^2 \equiv a \mod p$, and a quadratic nonresidue otherwise. We define the Legendre symbol

$$\left( \frac{a}{p} \right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p; \\ 1 & \text{if } a \text{ is a quadratic residue;}; \\ -1 & \text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

As exercises you should prove the following.

1. $\left( \frac{p}{p} \right)$ is a character mod $p$. That is,$$
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right).
$$

(It may be useful to recall that $U(p)$ is cyclic.)
2. The squares mod $p$ are an index 2 subgroup of $U(p)$.
3. Every element of $\mathbb{Z}/p\mathbb{Z}$ is either a square or a sum of two squares.

The analogues of all three of these are false in whole number arithmetic. The first implies that the product of two nonsquares is always a square. The second says the squares mod $p$ take up a huge amount of space inside of $U(p)$, or $\mathbb{Z}/p\mathbb{Z}$, whereas the squares are very thin inside of $\mathbb{Z}$. For the third statement, a theorem of Lagrange says it is necessary and sufficient to use four squares in $\mathbb{Z}$ to represent $\mathbb{N}$.}
4.3. Some Real Characters. Supposing that $p$ is an odd prime, then we know $U(p)$ is a cyclic group of even order. It therefore has a unique subgroup of index 2, which must be the squares since you showed above that the squares are an index 2 subgroup. Likewise, $\hat{U}(p)$ has a unique subgroup of order 2, and therefore there is a unique character mod $p$ of order 2. Thus, this is the Legendre symbol. Notice that if $\chi$ is any real valued character on $\mathbb{Z}/p\mathbb{Z}$ then either $\chi$ is trivial or it has order 2. Thus, for prime $p$ we have that the only real characters mod $p$ are the trivial character and the Legendre symbol.

For composite $q$ $U(q)$ is not necessarily cyclic, and may therefore have several index 2 subgroups, and so there may exist several different real characters. We take a brief look at some real characters here.

The two functions will be very useful in most questions concerning quadratic equations. They are both defined for even integers.

$$\varepsilon(n) = \begin{cases} 0 & \text{if } n \equiv 1 \mod 4, \\ 1 & \text{if } n \equiv -1 \mod 4, \end{cases}$$

$$\omega(n) = \begin{cases} 0 & \text{if } n \equiv \pm 1 \mod 8, \\ 1 & \text{if } n \equiv \pm 5 \mod 8, \end{cases}$$

The group $U(4)$ has order 2 and so there is only one nontrivial character mod 4. It is the character $x \mapsto (-1)^{\varepsilon(x)}$.

The group $U(8)$ has order 4 and is isomorphic to the direct sum of two cyclic groups each of order 2. Thus, there are three nontrivial characters mod 8 and they are all of order 2. They are

$$x \mapsto (-1)^{\varepsilon(x)}$$

$$x \mapsto (-1)^{\omega(x)}$$

$$x \mapsto (-1)^{\varepsilon(x)+\omega(x)}.$$ 

There is a general representation of real characters in terms of the Legendre symbol. We state the result here without proof. (I think the proof required quadratic reciprocity. See [9].)

**Proposition 14.** Let $a$ be a squarefree odd integer and put $q = 4a$. There exists a unique character mod $q$ so that for each prime $p$ not dividing $q$, we have

$$\chi(p) = \left(\frac{a}{p}\right).$$

4.4. Structure of Characters Modulo $q$. Suppose $q = nm$ is composite and $\psi$ is a character mod $n$. Then $\psi$ can also be considered as a character mod $q$. It is possible then to partition the characters mod $q$ into characters that are “truly” characters mod $q$ and those that are characters corresponding to certain divisors of $q$. Characters of the former type are called primitive characters. A rigorous definition is that $\chi$ is a primitive character mod $q$ if, for every positive proper divisor $n$ of $q$, there is some $x \in U(q)$ so that $x \equiv 1 \mod n$ and $\chi(x) \neq 1$. A divisor $n$ of $q$ is called an induced modulus of $\chi$ if $\chi(x) = 1$ for all $x \in U(q)$ with $x \equiv 1 \mod n$. Thus, a character mod $q$ is primitive if and only if the only induced modulus of $\chi$ is $q$. It is easy to see that if $n$ is an induced modulus of $\chi$ and $nm|q$ then $nm$ is also an induced modulus of $\chi$, and so it is natural to seek the smallest induced modulus of $\chi$. The conductor of $\chi$ is this smallest induced modulus. We now can partition the characters mod $q$ according to their conductors.

We may decompose a general character mod $q$ as the product of the principal (trivial) character mod $q$ and a primitive character modulo the conductor of $\chi$.

**Proposition 15.** Let $\chi$ be a character mod $q$ and let $n$ be the conductor of $\chi$. Then there exists a character $\psi$ mod $n$ which is primitive and

$$\chi \equiv \psi\chi_0.$$ 

As nonprimitive characters correspond to the existence of divisors of $q$, we see that every character modulo a prime is primitive, except for the trivial character.
4.5. **$L$-series.** In a few weeks, Brian will talk about a beautiful theorem of Dirichlet, which asserts that given any two integers $a$ and $q$ which are coprime, there exists infinitely many prime numbers satisfying the congruence

$$p \equiv a \mod q.$$  

Like the prime number theorem, proving the existence of lots of primes of a certain form will be achieved by proving statements about poles and zeros of certain Dirichlet series. The particular Dirichlet series we need to consider is

$$\sum_{p \equiv a \mod q} p^{-s},$$

and in particular the behavior as $s \to 1^+$. This particular series is a bit difficult to work with directly, but it has an expansion in terms of the series

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

as $\chi$ runs through all of the Dirichlet characters mod $q$. Such series are referred to as $L$-series and play a fundamental role in multiplicative number theory. A priori, such a series is defined for $\Re s > 1$.

We will prove a little later that $L(\chi, s)$ converges in the larger range $\Re s > 0$ provided $\chi$ is not the trivial character. In the case of the trivial character $\chi_0 \mod q$, prove

1. $L(\chi_0, s) = \prod_{p \mid q} (1 - \frac{1}{p^s}) \zeta(s)$.
2. $L(\chi_0, s)$ is meromorphic for $\Re s > 0$ with a simple pole at $s = 1$, and holomorphic away from $s = 1$. Also, compute the residue at the pole.

Thus, $L(\chi, s)$ exists, at least as a meromorphic function, for all characters mod $q$ and $\Re s > 0$.

The very definition of an $L$-series describes how two different algebraic operations behave with respect to each other, namely multiplication mod $q$ and real multiplication. As an exercise you can try to prove that the characters of $\mathbb{R}^+$ under multiplication are exactly the functions $t \mapsto n^{-it}$ for real $t$.

### 5. Exponential Sums and Character Sums

#### 5.1. Cancellation Estimates.** A basic procedure in analytic number theory is to convert some problem concerning arithmetic mod $q$ into an estimate on a sum of the form

$$\sum_{n \leq x} f(n)\chi(n),$$

say, where $f$ is some smooth function and $\chi$ is a character mod $q$, or occasionally a character of $\mathbb{Z}/q\mathbb{Z}$. These sums are usually referred to as character sums when $\chi \in \hat{U}(q)$ and exponential sums when $\chi \in \mathbb{Z}/q\mathbb{Z}$. Summation by parts instantly yields

$$\sum_{n \leq x} f(n)\chi(n) = \left( \sum_{n \leq x} \chi(n) \right) f(x) - \int_1^x f'(t) \sum_{n \leq t} \chi(n) dt,$$

and so it will be useful to have estimates on the sum

$$\left| \sum_{n \leq x} \chi(n) \right|.$$  

For now, let us suppose $\chi \neq \chi_0$ is a character mod $q$. We obtain a very simple estimate which is sufficient for most purposes.

---

4We defined characters only for finite abelian groups, and they were simply the group homomorphisms into the circle group. For locally compact abelian groups there are typically too many homomorphisms into the circle, and it is also natural to preserve the topological structure in addition to the algebraic structure, so for general abelian groups we require the characters to be continuous group homomorphisms.
Proposition 16. If \( \chi \neq \chi_0 \) is a character mod \( q \) then
\[
| \sum_{n \leq x} \chi(n) | \leq \varphi(q).
\]

Proof. There exists a nonnegative integer \( m \) and a real number \( 0 \leq y < q \) so that \( x = mq + y \). The orthogonality relation implies
\[
\sum_{j=1}^{q} \chi(lq + j) = 0
\]
for each \( l \) and so
\[
| \sum_{n \leq x} \chi(n) | = | \sum_{n \leq y} \chi(n) | \leq \sum_{n \leq y} |\chi(n)| \leq \varphi(q).
\]
\[\square\]

A considerable strengthening is provided by the next result, which we will prove as a special case after we develop some basic theory of Gauss sums.

Polya-Vinogradov. If \( \chi \neq \chi_0 \) is a character mod \( q \) then
\[
| \sum_{n \leq x} \chi(n) | \lesssim \sqrt{q} \log q.
\]

Recall that \( \varphi(q) \gtrsim q/(1 + \log q) \) and so the Polya-Vinogradov gains a \( \sqrt{q} \).

An analogue of the trivial estimate holds for additive characters as well.

Proposition 17. If \( \chi \in \hat{\mathbb{Z}}/q\mathbb{Z} \) is a nontrivial character then
\[
| \sum_{n \leq x} \chi(n) | \leq q.
\]

A nice consequence of these cancellation estimates is that often we can make sense of infinite series of the form
\[
\sum_{n=1}^{\infty} f(n) \chi(n)
\]
even when the series is not absolutely convergent. Using summation by parts, with \( y < x \), we find
\[
\left| \sum_{y < n \leq x} f(n) \chi(n) \right| = \left| \left( \sum_{y < n \leq x} \chi(n) \right)f(x) + \left( \sum_{n \leq y} \chi(n) \right)(f(x) - f(y)) - \int_{y}^{x} \left( \sum_{n \leq t} \chi(n) \right)f'(t) \, dt \right|
\]
\[
\leq \varphi(q) \left( |f(x)| + |f(x) - f(y)| + \int_{y}^{x} |f'(t)| \, dt \right).
\]

Suppose now that \( f \) is nonincreasing and \( f \) tends to 0. Nonincreasing implies
\[
\int_{y}^{x} |f'(t)| \, dt = | \int_{y}^{x} f'(t) \, dt | = |f(x) - f(y)|.
\]

Letting \( x \) and \( y \) go to infinity, we find that
\[
\sum_{y < n \leq x} f(n) \chi(n) \to 0.
\]

This proves
Proposition 18. If \( f \in C^1([1, \infty)) \) tends to zero and is nonincreasing, and \( \chi \not= \chi_0 \) is a character mod \( q \) then
\[
\sum_{n=1}^{\infty} f(n) \chi(n)
\]
converges. Similarly if \( \chi \) is a nontrivial character of \( \mathbb{Z}/q\mathbb{Z} \).

As exercises, prove
1. \( L(\chi, s) \) converges for any \( \Re s > 0, \chi \not= \chi_0 \). (Absolute convergence is only guaranteed for \( \Re s > 1 \).)
2. \( \sum_{n=1}^{\infty} \frac{\chi(n) \log(n)}{n} \) converges for \( \chi \not= \chi_0 \).

5.2. Gauss Sums. As \( \mathbb{Z}/q\mathbb{Z} \) is a ring we have two different algebraic operations, addition and multiplication. Often we are interested in how these two operations fit together. For instance, Dirichlet’s theorem asserts the existence of primes (multiplicative objects) inside of arithmetic progressions (additive objects). To understand how addition and multiplication are intertwined it is often useful to consider expansions of multiplicative characters in terms of additive characters and vice versa. Such expansions are referred to as Gauss sums, which we will consider now.

Throughout, \( \omega \) will be a fixed \( q \)th root of unity. We identify \( \hat{\mathbb{Z}}/q\mathbb{Z} \) with \( \mathbb{Z}/q\mathbb{Z} \) by defining
\[
\psi_r(x) = \omega^{rx}.
\]
Thus, we identify the character \( \psi_r \) with \( r \). Define
\[
G : \hat{U}(q) \oplus \hat{\mathbb{Z}}/q\mathbb{Z} \to \mathbb{C}
\]
\[
G(\chi, r) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \chi(x) \omega^{rx}.
\]
Notice that
\[
G(\chi, r) = \frac{1}{q} \chi(r) \frac{1}{q} \mathcal{F}_{\mathbb{Z}/q\mathbb{Z}} \chi(r).
\]

Proposition 19. If \( (r, q) = 1 \) then
\[
G(\chi, r) = \overline{\chi(r)} G(\chi, 1).
\]

Proof.
\[
\overline{\chi(r)} G(\chi, 1) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \chi(x r^{-1}) \omega^x
\]
\[
= \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(y) \omega^{ry} = G(\chi, r).
\]

Fix \( \chi \). We say \( G(\chi, \cdot) \) is separable if
\[
G(\chi, r) = \overline{\chi(r)} G(\chi, 1)
\]
for all \( r \in \mathbb{Z}/q\mathbb{Z} \). The above proposition says, in particular, that Gauss sums for characters modulo a prime are always separable. We leave the following proposition as an easy exercise.

Proposition 20. \( G(\chi, \cdot) \) is separable if and only if \( G(\chi, r) = 0 \) whenever \( (r, q) \not= 1 \).

Also, separability of the Gauss sum \( G(\chi, \cdot) \) is related to primitivity of \( \chi \).

Proposition 21. The Gauss sum \( G(\chi, \cdot) \) is separable if and only if \( \chi \) is a primitive character mod \( q \).

The main fact about Gauss sums we want is that separable Gauss sums have significant cancellation.

Gauss Sum Estimate. Suppose \( G(\chi, \cdot) \) is separable. Then
\[
|G(\chi, 1)|^2 = q.
\]
Proof.

\[ |G(\chi, 1)|^2 = G(\chi, 1)G(\chi, 1) = G(\chi, 1) \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \chi(m)\omega^{-m} \]

\[ = \sum_{m \in \mathbb{Z}/q\mathbb{Z}} G(\chi, m)\omega^{-m} = \sum_{n, m \in \mathbb{Z}/q\mathbb{Z}} \chi(n)\omega^{m(n-1)} \]

\[ = \sum_{n \in \mathbb{Z}/q\mathbb{Z}} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \chi(n)\omega^{m(n-1)}. \]

The orthogonality relation implies the inner sum is 0 unless \( n = 1 \), and so we find the sum is \( q \).

Recall our discussion several sections back concerning characters and cosets of subgroups. We discuss the significance of the point of view to Gauss sums. Thus, given a character \( \chi \mod q \) and a character \( r \) of \( \mathbb{Z}/q\mathbb{Z} \), we have a naturally associated multiplicative subgroup corresponding to \( \chi \) and an additive subgroup corresponding to \( r \). The Gauss sum \( G(\chi, r) \) is a measurement of the correlation between \( \chi \) and \( r \). The only way for a Gauss sum to be near maximal or minimal in size is if there is almost no cancellation or almost perfect cancellation between \( \chi \) and \( r \). This would require the level sets of \( \chi \) and \( r \) to essentially line up, and thus requires the existence of a subset \( R \) of \( \mathbb{Z}/q\mathbb{Z} \) so that the level sets of \( \chi \) are essentially multiplicative shifts of \( R \) and the level sets of \( r \) are essentially additive shifts of \( R \). This should be possible only if \( R \) behaves very much like a subring of \( \mathbb{Z}/q\mathbb{Z} \). In view of the fact that \( \mathbb{Z}/p\mathbb{Z} \) has no nontrivial subrings for prime \( p \), this heuristic discussion suggests that we must have a decent estimate on \( G(\chi, r) \) for prime \( p \), which we already saw by direct computation.

The intuition developed in the preceding is central in some recent work of Bourgain on exponential sums (see below). Bourgain deduces new nontrivial estimates on certain exponential sums by making use of sum-product estimates. The basic idea of a sum-product theorem is that if \( A \) is a subset of a ring which is not too close to a subring, then \( A \) must have either a lot of sums or \( A \) must have a lot of products.

Perhaps this intertwining of addition and multiplication is best seen from the following computation.

\[ G(\chi, r)G(\chi, r) = \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \chi(m)\omega^m \sum_{n \in \mathbb{Z}/q\mathbb{Z}} \chi(n)\omega^{-n} = \sum_{m, n \in \mathbb{Z}/q\mathbb{Z}} \chi(mn^{-1})\omega^{r(m-n)}. \]

Thus, \( |G(\chi, r)|^2 \) is expressed as an average over the pairs \((mn^{-1}, m - n)\).

5.3. Weyl Sums. We define the (quadratic) Weyl sum mod \( q \) by

\[ W(r) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \omega^{rx^2} \]

where \( r \in \hat{G} \).

The Gauss sum estimate also holds for the quadratic Weyl sum, and perhaps the proof is a bit more transparent in this case.

Weyl Sum Estimate.

\[ \left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{rx^2} \right|^2 = p \]

for \( p \) prime and \( (r, p) = 1 \).

Proof.

\[ \left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{rx^2} \right|^2 = \sum_{x, y \in \mathbb{Z}/p\mathbb{Z}} \omega^{(x^2 - y^2)r}. \]
Change variables so that \( x = y + z \). Then
\[
\sum_{y, z \in \mathbb{Z}/p\mathbb{Z}} \omega^{(y^2 + 2yz + z^2 - y^2)r} = \sum_{z \in \mathbb{Z}/p\mathbb{Z}} \omega^{rz^2} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \omega^{ryz}.
\]
The inner sum is 0 unless \( z = 0 \), and so we find the total sum is \( p \). □

The Weyl sum has an interesting property concerning its distribution along the additive characters of \( \mathbb{Z}/p\mathbb{Z} \). Given a function \( f \) on \( \mathbb{Z}/q\mathbb{Z} \) and \( t \in \mathbb{Z}/q\mathbb{Z} \), define the function
\[
\Delta(f; t)(x) = f(x + t) \overline{f(x)}.
\]
Now suppose \( f(r) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{rx^2} \). Show
1. \( |\hat{f}(s)| = \sqrt{p} \) for \( (s, p) = 1 \).
2. For each \( t \), there exists an \( s = s_t \) so that \( |\Delta(f; t)^\wedge(s)| = p \).

The first shows that \( f \) has no significant Fourier coefficients, and so \( f \) is in a sense ”uniformly distributed.” The second says, essentially, that \( f \) has a spike at a single ”quadratic Fourier coefficients,” and so in another sense \( f \) is far from being uniformly distributed. Recent years have seen an explosion of interest in this sort of ”generalized Fourier analysis.” See [5] for a harmonic analytic/ number theoretic point of view and [6] for a dynamical point of view of this generalized Fourier analysis.

It turns out that the Weyl sum is actually a Gauss sum (almost) for an appropriate character mod \( p \), namely, the Legendre symbol. It’s easiest to see this using an indirect argument. Let \( S \) denote the squares modulo \( p \). Suppose \( (a, p) = 1 \). Then
\[
1_S(a) = \frac{1}{2} \left\{ \left( \frac{a}{p} \right) + 1 \right\}.
\]
For if \( a \) is a square, the left hand side is 1, the Legendre symbol is 1, and so this is satisfied. If \( a \) is not a square, the left hand side is 0 and the Legendre symbol is \(-1\), so again the formula holds. We need to modify the formula for \( a = 0 \mod p \), namely
\[
1_S(0) = \frac{1}{2} \left\{ \left( \frac{0}{p} \right) + 1 + 1 \right\}.
\]
Therefore,
\[
1_S = \frac{1}{2} \left\{ \left( \frac{0}{p} \right) + 1 + \delta_0 \right\}.
\]
We now take the \((\mathbb{Z}/p\mathbb{Z})\) Fourier transform of both sides, and we recall \( \hat{1} = \delta_0 \) and \( \delta_0 = 1 \). This gives
\[
\hat{1}_S = \frac{1}{2} \left\{ \left( \frac{0}{p} \right) + 1 + \delta_0 \right\}.
\]
In particular, for \((r, p) = 1\) we have
\[
\hat{1}_S(r) = \frac{1}{2} \left\{ \left( \frac{r}{p} \right) + 1 \right\},
\]
which rearranges to
\[
1 + 2\hat{1}_S(r) = \left( \frac{r}{p} \right).
\]
By definition, the right hand side is \( G\left( \frac{r}{p} \right) \). A quick computation (essentially the observation that each nonzero square has two square roots) shows the left hand side is the Weyl sum \( \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{rx^2} \).
Proposition 22. For \((r, p) = 1, p\) a prime, we have

\[
\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{rx^2} = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \left( \frac{y}{p} \right) \omega^{ry}.
\]

Give another proof of this proposition based on the following observations:
1. Let \(S = \{a \in U(p) : x^2 = a \mod p \text{ for some } x \in U(p)\}\). Prove \(S\) is a subgroup of \(U(p)\) of index 2.
2. Let \(\hat{U}(p) = \{\chi \in \hat{U}(p) : \chi|_S = 1\}\). Prove \(\hat{U}(p)\) is order 2 subgroup of \(\hat{U}(p)\) generated by the Legendre symbol.
3. By making appropriate choices of the involved functions and groups, deduce the above proposition as a consequence of the Poisson summation formula on \(U(p)\).

In particular, we have

Proposition 23. For \((r, p) = 1,\)

\[|G\left(\left(\frac{\cdot}{p}\right), r\right)|^2 = p.\]

This plays an important role in the quadratic reciprocity theorem. (At least in one of the 150 proofs of this theorem.)

5.4. Gauss Sums and the Quadratic Reciprocity Law. Above, we had determined

\[|G\left(\left(\frac{\cdot}{p}\right), 1\right)|^2 = p.\]

We can almost as easily determine the sign of the square of the Gauss sum for the Legendre symbol.

Proposition 24.

\[G\left(\left(\frac{\cdot}{p}\right), 1\right)G\left(\left(\frac{\cdot}{p}\right), 1\right) = \left(\frac{-1}{p}\right) p.\]

Proof.

\[G\left(\left(\frac{\cdot}{p}\right), 1\right)G\left(\left(\frac{\cdot}{p}\right), 1\right) = \sum_{x,y \in \mathbb{Z}/p\mathbb{Z}} \omega^{xy} \omega^{x+y}.\]

For fixed \(x \neq 0\), replace the variable \(y\) with \(zx\). Then the sum is

\[
= \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} \omega^{x(1+z)} = \sum_{z \in \mathbb{Z}/p\mathbb{Z}} \omega^{z} \sum_{x,z \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} \omega^{xz(1+z)}
\]

\[= \sum_{z \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{z}{p} \right) \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{xz(1+z)} - \sum_{z \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{z}{p} \right).\]

But the second sum here is zero, and using the orthogonality relation on the inner sum in the first term we get

\[= \left(\frac{-1}{p}\right) p.\]

Suppose now that \(p\) and \(q\) are two distinct odd primes. We will compute \(G((\frac{1}{p}), 1)^q\) in two different ways and deduce the quadratic reciprocity law.

Proposition 25. \(G((\frac{1}{p}), 1)^q \equiv (\frac{p}{q})G((\frac{1}{p}), 1) \mod q.\)
Proof. We expand $G((\frac{1}{p}), 1)^q$ using the multinomial theorem, observing that only the pure terms remain upon reduction modulo $q$. That is,

$$G((\frac{1}{p}), 1)^q = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x}{p})^q \omega^{xq}.$$ 

As $q$ is odd and $(\frac{x}{p})$ is real we have

$$= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x}{p}) \omega^{xq}.$$ 

As $p$ and $q$ are distinct, we may change variables to get

$$= \sum_{y \in \mathbb{Z}/p\mathbb{Z}} (\frac{yq-1}{p}) \omega^y = \left(\frac{q-1}{p}\right) \sum_{y \in \mathbb{Z}/p\mathbb{Z}} (\frac{y}{p}) \omega^y = \left(\frac{q-1}{p}\right) G((\frac{1}{p}), 1).$$

Finally, we observe

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

and thus conclude the proposition. \hfill \Box

Next, we will compute $G((\frac{1}{p}), 1)$ using the result on the square of the Gauss sum. Before we do this we record a lemma on the Legendre symbol.

**Lemma 1.** Let $p$ be a prime and $a \in \mathbb{Z}/p\mathbb{Z}$. Then

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

**Proof.** If $a = 0$ then so are both sides of the desired identity. Thus, we may assume $a$ is invertible mod $p$. Let $g$ be a generator of $U(p)$, and so $a = g^k$ for some $1 \leq k \leq p-1$. Write $k = 2l + r$ with $r \in \{0, 1\}$. Now,

$$a^{\frac{p-1}{2}} = g^{\frac{p-1}{2}k} = g^{(p-1)l} g^{\frac{p-1}{2}r} = g^{\frac{p-1}{2}r}.$$ 

This is either $1$ or $-1$, and is $1$ if and only if $r = 0$, if and only if $k$ is even, if and only if $a$ is a quadratic residue. \hfill \Box

The quadratic reciprocity law requires us to know when $-1$ is a square mod $p$. The next lemma answers this.

**Lemma 2.** $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{p-1}{2}}$. That is, $-1$ is a square mod $p$ if and only if $p \equiv 1 \mod 4$ for $p$ an odd prime.

This follows immediately from the previous lemma.

We can now prove

**Proposition 26.** $G((\frac{1}{p}), 1)^q = (-1)^{\frac{q-1}{2} \frac{p-1}{2}} G((\frac{1}{p}), 1)$ for distinct odd primes $p$ and $q$.

**Proof.**

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

By the lemma, $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$ and

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

It is now easy to piece together the various propositions to obtain the Quadratic Reciprocity Law, or as Gauss called it
**Theorema Auruem.** If \( p \) and \( q \) are distinct odd primes, then

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

That is, if \( p \) and \( q \) are both congruent to 3 modulo 4 then \( p \) is a quadratic residue mod \( q \) if and only if \( q \) is not a quadratic residue mod \( p \), and if at least one of \( p \) and \( q \) is congruent to 1 modulo 4, then \( p \) is a quadratic residue mod \( q \) if and only if \( q \) is a quadratic residue mod \( p \).

**5.5. Ramanujan Sums.** Above, we showed the Gauss sum for the Legendre symbol has special significance (it was a Weyl sum). Here we look at the Gauss sum corresponding to the trivial character mod \( q \), that is, the character which is 1 on numbers coprime to \( q \) and 0 otherwise. These sums are called Ramanujan sums.

\[
c_q(r) = \sum_{m \in \mathbb{U}(q)} \omega^{rm} = qF_{\mathbb{Z}/q\mathbb{Z}}(r) = q\hat{1}_{\mathbb{U}(q)}(r).
\]

The Ramanujan sums can be computed explicitly, using an indirect argument (i.e., Mobius inversion). We leave the argument as an exercise.

**Proposition 27.**

\[
c_q(r) = \sum_{d | (q,r)} \mu(q/d).
\]

In particular, \( c_q(r) = \mu(d) \) if \( (q,r) = 1 \) and \( c_q(r) = \varphi(q) \) if \( (q,r) = q \).

**5.6. Proof of Polya-Vinogradov.** We now use the Gauss sum estimate to prove the Polya-Vinogradov estimate, at least when \( q = p \) is a prime. Thus, we have some nontrivial character mod \( p \) and we seek to prove

\[
\left| \sum_{n \leq x} \chi(n) \right| \leq \sqrt{q} \log q.
\]

Now, for \((n,p) = 1\) we have

\[
G(\chi, n) = \overline{\chi(n)}G(\chi, 1).
\]

Then

\[
G(\chi, 1) \sum_{n \leq x} \overline{\chi(n)} = \sum_{n \leq x} G(\chi, n)
= \sum_{n \leq x} \sum_{0 < |m| \leq q/2} \chi(m)\omega^{nm}
= \sum_{0 < |m| \leq q/2} \chi(m) \sum_{n \leq x} \omega^{nm}.
\]

The inner sum is geometric and sums to

\[
\left| \frac{\omega^m - 1}{\omega^m - 1} \right| \leq \frac{2}{|\omega^m - 1|} = \frac{2}{|\sin \pi m/q|}.
\]

We therefore get

\[
|G(\chi, 1) \sum_{n \leq x} \overline{\chi(n)}| \leq \sum_{0 < |m| \leq q/2} \frac{2}{|\sin \pi m/q|} \leq \sum_{0 < |m| \leq q/2} \frac{1}{m/q} = q \sum_{0 < |m| \leq q/2} \frac{1}{m} \leq Cq \log q.
\]

But \( |G(\chi, 1)| = \sqrt{q} \), and so

\[
\left| \sum_{n \leq x} \chi(n) \right| \leq C\sqrt{q} \log q.
\]
5.7. Exponential Sums and Distribution of Points. The material in the section is concerned with characters of the infinite additive group $\mathbb{R}$. The characters here are of the form $x \mapsto e^{2\pi i x \xi}$ where $\xi \in \mathbb{R}$. Suppose we have a finite set of points $A = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ on the unit circle. For each real number $\beta$ we define

$$N_A(\beta) = |\{j : \beta \leq \alpha_j < \beta + \frac{1}{2}\}|$$

where the inequality is read modulo $\mathbb{Z}$. The points of $A$ are distributed essentially uniformly if $N_A(\beta)$ is near $\frac{k}{2}$ for all $\beta$. The distribution of the points of $A$ is closely related to estimates on certain exponential sums. We give an particular instance, due to Freiman, of this general principle.

**Proposition 28.**

$$|\sum_{j=1}^{k} e^{2\pi i \alpha_j}| \leq 2 \max_{\beta \in \mathbb{R}} \{N_A(\beta)\} - k.$$

Notice that if the points are distributed exactly evenly then $A = \{\frac{j}{k} + \alpha : 0 \leq j < k\}$ for some fixed $\alpha$. The left side of the estimate is 0 by the orthogonality relations on $\mathbb{Z}/k\mathbb{Z}$. The right side is 0 as $N(\beta) = \frac{k}{2}$ for all $\beta$. Thus, this estimate can be viewed as a generalization of the orthogonality relations.

This kind of estimate is particularly useful when used in conjunction with a nontrivial lower bound. Here one starts with a set $A$ where the points of $A$ are not known but certain statistics are known. These stats give may give an estimate of the form

$$|\sum_{j=1}^{k} e^{2\pi i \alpha_j}| \geq \frac{3}{4} k,$$

say. Using the above estimate we then obtain $N_A(\beta) \geq \frac{7}{8} k$, which says the points of $A$ are distributed in a rather lopsided manner.

5.8. Mordell’s, Hua’s, and Bourgain’s Exponential Sum Estimates. It is natural to replace the quadratic $x^2$ in the exponent of the Weyl sum with some arbitrary polynomial $\Phi(x)$ and ask if there is still a nontrivial estimate. We state a few results about such sums here. The first is the Mordell-Hua estimate. This was established first by Mordell in the case $q = p$ a prime, and extended by Hua to general $q$.

**Mordell-Hua Exponential Sum Estimate.** If $\Phi$ is a polynomial of degree $n$ and all of the coefficients of $\Phi$ are relatively prime to $q$, then

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} \omega^{\Phi(x)} \leq q^{1 - 1/n}.$$

This is a rather powerful estimate for reasonably small $n$. For instance, it recovers (essentially) the above estimate for quadratics. However, the estimate approaches the trivial estimate as $n$ increases. Very recently, Bourgain gave a new estimate which gives much better results for large $n$. In fact, his estimate gives an estimate uniform in the degree, under certain sparseness assumptions.

**Bourgain’s Exponential Sum Estimate.** Let $p$ be a prime, $r \in \mathbb{N}$ and $\epsilon > 0$. There exists $\delta = \delta(\epsilon, r) > 0$ so that if

$$\Phi(x) = \sum_{j=1}^{r} a_j x^{k_j}$$
is a polynomial so that \((a_j, p) = 1\), \((k_j, p - 1) < p^{1-\epsilon}\) and \((k_j - k_i, p - 1) < p^{1-\epsilon}\), then

\[
\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \omega^{\Phi(x)} \lessapprox p^{1-\delta}.
\]

The point is that as long as the polynomial has only a few terms (in typical applications \(\Phi\) will be a monomial), and the powers don’t have too many shared factors with \(p - 1\) (this prevents the set \(\{x^k : x \in \mathbb{Z}/p\mathbb{Z}\}\) from behaving like a subgroup of very small order), then we may still obtain a nontrivial estimate on the sum. The really nice and unexpected thing is that the factor \(\delta\) depends only on \(r\) and \(\epsilon\), and not on the particular powers present. One drawback is that \(\delta\) is not an effective constant (thus, we know that Bourgain’s estimate wins out over the Mordell estimate for large enough \(n\), but we don’t know what large enough means). The proof requires repeated applications of the so called Gowers-Balog-Szemerédi lemma which typically loses quantitative control over implied constants.

5.9. **Connections to Cryptography.** The typical protocol in cryptography is based on the supposed hardness of solving some number theoretic problem. Often times the hardness of a problem is measured in terms of the distribution of certain points inside of some finite dimensional vector space over some finite field. The problem is believed to be hard if the corresponding points are distributed randomly. This essentially means that knowing where some of the points are located gives absolutely no information as to where other points may be. (Compare to when the points are located along an algebraic curve of degree \(d\), in which case knowledge of the location of \(d + 1\) points gives very strong information regarding the remaining points.) A method of Weyl allows one to convert questions on random distribution of points to estimates on some corresponding exponential sum.

An exponential sum of particular importance in cryptography is

\[
\sum_{x, y \in U(p)} \omega^{ag^x+bg^y+cg^{xy}},
\]

where \(p\) is prime, \(g\) is an element of \(U(p)\) usually assumed to have large, but not maximal, order, and \(a, b, c\) are characters of \(\mathbb{Z}/p\mathbb{Z}\). This sum is of relevance to the Diffie-Hellman distribution. The security of the Diffie-Hellman protocol is based on the assumption that it is computationally difficult to determine \(g^{xy}\) if we are given \(p, g, g^x, g^y\). (It is easy to solve this mathematically; given \(g\) and \(g^x\) we find \(x\) using the discrete log. Once we have \(x\), then \(g^{xy} = (g^x)^y\). The problem is that discrete logs are hard from a computational point of view.)

Nontrivial estimates on this Diffie-Hellman sum were obtained by Freidlander, Konyagin, Shparlinski, and a few authors I am forgetting now. A stronger estimate was obtained as a consequence of Bourgain’s above estimate.

**References**


