Name:
Due date: 02/14

Problem 1

Let χ_0 be the principal character mod 3, that is

$$\chi_0(n) = \begin{cases} 1, & \gcd(n,3) = 1 \\ 0, & \text{otherwise} \end{cases}$$

Define

$$\chi(n) = \begin{cases} 1, & n \equiv 1 \pmod 3 \\ -1, & n \equiv 2 \pmod 3 \\ 0, & \text{otherwise} \end{cases}$$

Prove that χ_0 and χ are completely multiplicative functions. Verify the identity

$$\mathbb{1} = \frac{1}{2}(\chi_0 + \chi)$$

Proof.

Let $m, n \in \mathbb{Z}$ be arbitrary integers. We consider the following cases:

1. At least one of m, n is divisible by 3. WLOG, we can assume $3 \mid m$. Then it is clear that $3 \mid mn$. By definition, we must have $\chi_0(m) = \chi(m) = 0$ and $\chi_0(mn) = \chi(mn) = 0$. Thus we have

$$\chi(m)\chi(n) = 0 \cdot \chi(n) = 0 = \chi(mn) \quad \text{and } \chi_0(m)\chi_0(n) = 0 \cdot \chi(n) = 0 = \chi(mn).$$

2. Both m, n are coprime to 3. There will be then two subcases
   - $m \equiv n \pmod 3$. Then clearly we have $\chi_0(m) = \chi_0(n) = 1$ and $\chi(m) = \chi(n)$. Moreover $mn \equiv 1 \pmod 3$, thus $\chi(mn) = \chi_0(mn) = 1$. In particular, we have

$$\chi(m)\chi(n) = 1 \cdot 1 = 1 = \chi(mn) \quad \text{and } \chi_0(m)\chi_0(n) = 1 \cdot 1 = 1 = \chi(mn).$$

   - $m \not\equiv n \pmod 3$. We can further assume that $m \equiv 1 \pmod 3$ and $n \equiv 2 \pmod 3$. clearly

$$\chi_0(m)\chi_0(n) = 1 \cdot 1 = 1 = \chi_0(mn),$$

   as $\gcd(mn, 3) = 1$.
   On the other hand, $mn \equiv 1 \cdot (-1) \equiv 2 \pmod 3$, thus

$$\chi(m)\chi(n) = 1 \cdot (-1) = -1 = \chi(mn)$$

In conclusion, χ and χ_0 are completely multiplicative. To verify the given identity, we consider the following cases

(a) $m \not\equiv 1 \pmod 3$: Then $\mathbb{1}(m) = 0$. On the other hand, we have

$$\frac{1}{2}\left(\chi(m) + \chi_0(m)\right) = \begin{cases} 0 + 0, & m \equiv 0 \pmod 3 \\ -1 + 1, & m \equiv 2 \pmod 3 \end{cases} = 0$$

(b) $m \equiv 1 \pmod 3$: Then $\mathbb{1}(m) = 1 = 1/2(\chi(m) + \chi_0(m))$

Thus we are done. $\square$

Problem 2

Let G be a finite abelian group. Show that $\#\hat{G} \leq \#G$.

Proof. First we will prove that the set S of maps $f\colon G \to \mathbb{C}$ has a vector space structure. The sum and the scalar multiplication of maps are defined as follows

- $(\chi_1 + \chi_2)(a) := \chi_1(a) + \chi_2(a)$ for all $a \in G$.
- $(c\chi)(a) := c \cdot \chi(a)$ for any $\chi \in S$ and $c \in \mathbb{C}$.

But we can check all the axioms for a set being a vector space pointwisely, with the zero beging the zero map. So S have a a structure of vector space. Let's compute the dimension of S as as $\mathbb{C}-$ vector space. Since G is finite, we can assume that, as a set

$$G = \{a_1, \ldots, a_n\}$$

Then we can define the map f_i to be the "dual" of a_i in the following sense: $f_i(a_j) = \delta_{ij}$, i.e. $f_i(a_i) = 1$ and vanishes at $a_j \neq a_i$. We claim that $\mathfrak{B} = \{f_i\}$ forms a basis of S. Indeed, let $f\colon G \to \mathbb{C}$ be arbitrary. Since G is finite, f is determined by its value at each $a_i \in G$. Assume that $c_i = f(a_i)$. Then for any $1 \leq i \leq n$, we have

$$f(a_i) = c_i = \sum_{i=1}^{n} c_i f_i(a_i)$$

In particular, we can rewrite the following identity as

$$f = c_1 f_1 + c_2 f_2 + \ldots + c_n f_n,$$

which implies $\mathfrak{B}$ spans S. On the other hand, if

$$0 = c_1 f_1 + \ldots + c_n f(n)$$

Applying both sides to a_i yields

$$0 = c_i f_i(a_i) = c_i$$

which means $\mathfrak{B}$ is a set of linearly independent vectors. Thus $\dim S = \#\mathfrak{B} = n$. In the note, we proved that the character $\chi_1, \chi_2, \ldots, \chi_m$ are mutually orthogonal. In particular, they are a subset of S comprising of linearly independent vectors. Thus

$$m = \#\hat{G} \leq n = \#G.$$

Remark: In fact, if we assume the theorem about the structure of finite abelian group, we can prove that the equality always happens, namely $\#\hat{G} = \#G$ $\square$

Problem 3

Consider the finite abelian group G_9 consisting of the invertible elements of $\mathbb{Z}/9\mathbb{Z}$. Find all the characteres of G_9. Make sure you prove that the characters of G_9 you find are all distinct and there are no others.

Proof. Using the Remark in the previous exercise, we predict that there are 6 characters in total. It can be checked easily that 2 generates G_9, so it is a cyclic group of order 6. Indeed, we have

$$\begin{aligned} 2^1 &\equiv 2 \pmod 9 \\ 2^2 &\equiv 4 \pmod 9 \\ 2^3 &\equiv 8 \pmod 9 \\ 2^4 &\equiv 7 \pmod 9 \\ 2^5 &\equiv 5 \pmod 9 \\ 2^6 &\equiv 1 \pmod 9 \end{aligned}$$

So the character is defined solely by determining where it sends $[2]$ in $\mathbb{C}$. Let $\chi \in \hat{G}_9$ be any character, we then have

$$\chi(2)^6 = \chi(2^6) = \chi(1) = 1 \in \mathbb{C}$$

thus implies $\chi(2)$ must be a $6-th$ root of unity. There are 6 choices in total, namely

$$\chi(2) = e^{\frac{2i\pi k}{6}}, 0 \leq k \leq 6$$

Clearly these are 6 distinct characters, and they are all possible characters of G_9. □

Problem 4

Show that there is exactly one real, non-principal Dirichlet character $\chi \pmod 9$. Find $\chi(916)$.

Proof. Continueing from the previous exercise, with a note that a character is called real character if its image lies entirely in $\mathbb{R}$, namely we have a group homomorphism $\chi\colon G_9 \to \mathbb{R}$. Since we know that all character $\chi \in \hat{G}$ satisfy

$$|\chi(a)| = 1, \text{ for all } a \in G_9,$$

we can deduce that a real character χ must satisfy $\chi(G_9) \subset \{\pm 1\}$. Since we want to find a non-principal character, the only choices is that $\chi(G_9) = \{\pm 1\}$. As shown above, χ is defined solely by its value at 2, so we must choose $\chi(2) = -1$. This implies that there is only one non-principal, real Dirichlet character over G_9.

Note that $916 \equiv 16 = 2^4 \pmod 9$. Thus

$$\chi(916) = \chi(2^4) = (\chi(2)^4) = (-1)^4 = 1.$$

And we are done. □