MATH 152 Problem set 7 solutions

1. First recall that

$$L(1, \chi_8) = \sum_{n=1}^{\infty} \chi_8(n) n^{-1} = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \dots.$$

To compute this, we can use the same technique as in the notes on the Dirichlet's theorem used to evalute $L(1, \chi_4)$.

$$L(1, \chi_8) = \int_0^1 1 - x^2 - x^4 + x^6 + x^8 - x^{10} \dots dx.$$

The integrand is a geometric series with the initial term $1 - x^2$ and the common ratio $-x^4$. Hence all we need is compute the integral

$$\int_0^1 \frac{1 - x^2}{1 + x^4} dx.$$

To do this,[1] we rewrite this as

$$\int_0^1 \frac{1 - x^2}{(1 + \sqrt{2}x + x^2)(1 - \sqrt{2}x + x^2)} dx = \int_0^1 \frac{A_1(x)}{1 + \sqrt{2}x + x^2} + \frac{A_2(x)}{1 - \sqrt{2}x + x^2} dx,$$

where we can compute and find out that $A_1(x) = \frac{1}{2\sqrt{2}}(2x + \sqrt{2})$ and $A_2(x) = \frac{1}{2\sqrt{2}}(-2x + \sqrt{2})$. Therefore, our integral equals

$$\begin{aligned}
&\frac{1}{2\sqrt{2}} \int_0^1 \frac{2x + \sqrt{2}}{x^2 + \sqrt{2}x + 1} - \frac{2x - \sqrt{2}}{x^2 - \sqrt{2}x + 1} dx \\
&= \frac{1}{2\sqrt{2}} \Big[\log(x^2 + \sqrt{2}x + 1) - \log(x^2 - \sqrt{2}x + 1) \Big]_0^1 \\
&= \frac{1}{2\sqrt{2}} \Big(\log(2 + \sqrt{2}) - \log(2 - \sqrt{2}) \Big) \\
&= \frac{1}{2\sqrt{2}} \log 3 + 2\sqrt{2}.
\end{aligned}$$

[1] Fortunately for us, every integral of the form $\int \frac{f(x)}{g(x)} dx$, where $f(x), g(x)$ are polynomials with real coefficients, can be done by a routine method. The strategy is to factorize $g(x) = g_1(x) g_2(x) \dots g_k(x)$ where $g_i(x)$ are linear or quadratic polynomials with real coefficients, and write $\frac{f(x)}{g(x)} = \frac{A_1(x)}{g_1(x)} + \dots + \frac{A_k(x)}{g_k(x)}$ for some appropriate polynomials $A_i(x)$'s. Next, divide $A_i(x)$ by $g_i(x)$ so that we will have $\frac{f(x)}{g(x)} = p(x) + \frac{B_1(x)}{g_1(x)} + \dots + \frac{B_k(x)}{g_k(x)}$ for some polynomials $p(x)$ and $B_i(x)$ with $\deg B_i < \deg g_i$.

Now, if $\deg g_i = 1$, then $\int \frac{B_i(x)}{g_i(x)} dx$ is a log of something. If $\deg g_i = 2$ and $\deg B_i = 0$, then $\int \frac{B_i(x)}{g_i(x)} dx$ is a arctan of something. If $\deg g_i = 2$ and $\deg B_i = 1$, then the integral is a sum of log(something) and arctan(something).

Others values are done in a similar way:

$$L(1,\chi_{-8}) = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \ldots = \int_0^1 1 + x^2 - x^4 - x^6 + x^8 + x^{10} - \ldots dx$$

equals

$$\int_0^1 \frac{1+x^2}{1+x^4} dx = \frac{1}{\sqrt{2}}\Big[\arctan(1+\sqrt{2}x) - \arctan(1-\sqrt{2}x)\Big]_0^1 = \frac{1}{\sqrt{2}}\Big(\arctan(1+\sqrt{2}) - \arctan(1-\sqrt{2})\Big).$$

(See footnote 1 on how to compute this integral.) In fact, we can simplify this expression further, because $-\arctan(1-\sqrt{2}) = \arctan(\sqrt{2}-1)$ (as $\arctan(x)$ is an odd function), and furthermore, if $\theta = \arctan(1+\sqrt{2})$ then $\pi/2 - \theta = \arctan(\frac{1}{1+\sqrt{2}}) = \arctan(\sqrt{2}-1)$. So this actually equals $\pi/2\sqrt{2}$.

And

$$L(1,\chi_5) = 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \ldots = \int_0^1 1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8 + \ldots dx$$

equals

$$\begin{aligned} &\int_0^1 \frac{1 - x - x^2 + x^3}{1 - x^5} dx \\ = \; & \frac{1}{\sqrt{5}}\Big[\log(2x^2 + (\sqrt{5}+1)x + 2) - \log(2x^2 - (\sqrt{5}-1)x + 2)\Big]_0^1 \\ = \; & \frac{1}{\sqrt{5}}\Big(\log(5+\sqrt{5}) - \log(5-\sqrt{5})\Big) \\ = \; & \frac{1}{\sqrt{5}} \log \frac{3+\sqrt{5}}{2}. \end{aligned}$$

2. Suppose ψ is an additive character (mod q). Then $\psi(0) = \psi(0+0) = \psi(0)\psi(0)$, so $\psi(0) = 0$ or 1. In fact, $\psi(0) = 1$, because otherwise $\psi(n) = \psi(n+0) = \psi(n)\psi(0) = 0$ for all n, contradicting that $\psi(n)$ is not all zero. By periodicity, $\psi(q) = \psi(0) = 1$.

Furthermore, $\psi(1)$ completely determines the function ψ, since $\psi(n) = \psi(1 + \ldots + 1) = (\psi(1))^n$ for all n. And by the earlier remark, $\psi(q) = (\psi(1))^q = 1$, i.e. $\psi(1)$ is a q-th root of unity. This allows us to write

$$\psi(1) = e^{\frac{2\pi i}{q} a}$$

for some integer a, and

$$\psi(n) = e^{\frac{2\pi i}{q} an}.$$

It is easy to see that $e^{\frac{2\pi i}{q}an}$ is indeed an additive character (mod q), and that we have just proved that any additive character (mod q) must be of this form. Also note that two characters $e^{\frac{2\pi i}{q}an}$ and $e^{\frac{2\pi i}{q}bn}$ are the same if and only if $a \equiv b \pmod q$. Therefore, the set of all additive characters (mod q) is precisely $\{e^{\frac{2\pi i}{q}an} : 0 \le a \le q-1\}$.

The first orthogonality relation is:

$$\sum_{n=0}^{q-1} e^{\frac{2\pi i}{q}an}\overline{e^{\frac{2\pi i}{q}bn}} = \sum_{n=0}^{q-1} e^{\frac{2\pi i}{q}(a-b)n} = \begin{cases} q & \text{if } a \equiv b \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

The second orthogonality relation is:

$$\sum_{a=0}^{q-1} e^{\frac{2\pi i}{q}an}\overline{e^{\frac{2\pi i}{q}am}} = \sum_{a=0}^{q-1} e^{\frac{2\pi i}{q}a(n-m)} = \begin{cases} q & \text{if } n \equiv m \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

To prove these orthogonality relations, recall that

$$f(x) := x^{q-1} + x^{q-2} + \ldots + x + 1 = \begin{cases} q & \text{if } x = 1 \\ 0 & \text{if } x \text{ is any other } q\text{-th root of unity} \end{cases}$$

because the roots of $(x-1)f(x) = x^q - 1$ are precisely the q-th roots of unity, and $(x-1)$ accounts for the root $x = 1$, so $f(x)$ accounts for every other root of $x^q - 1$. Now, the expression in the first orthogonality is $f(e^{\frac{2\pi i}{q}(a-b)})$, and in the second orthogonality is $f(e^{\frac{2\pi i}{q}(n-m)})$, which are equal to q if $a - b \equiv 0$ and $n - m \equiv 0 \pmod q$ respectively, and zero otherwise. This completes the proof.

3. Let integers a and q be given. Our work in the previous exercise tells us that

$$\frac{1}{q}\sum_{k=0}^{q-1} e^{\frac{2\pi i}{q}(-a)k} e^{\frac{2\pi i}{q}nk} = \begin{cases} 1 & \text{if } n \equiv a \pmod q \\ 0 & \text{if } n \not\equiv a \pmod q. \end{cases}$$

Therefore

$$\begin{aligned} &\sum_{n=1,\ n\equiv a \pmod q}^{\infty} a(n) \\ &= \sum_{n=1}^{\infty} a(n)\Big(\frac{1}{q}\sum_{k=0}^{q-1} e^{\frac{2\pi i}{q}(-a)k} e^{\frac{2\pi i}{q}nk}\Big) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{q}\sum_{k=0}^{q-1} e^{\frac{2\pi i}{q}(-a)k}\sum_{n=1}^{\infty} a(n)e^{\frac{2\pi i}{q}nk} \\
&= \frac{1}{q}\sum_{n=1}^{\infty} a(n) + \frac{1}{q}\sum_{k=1}^{q-1} e^{\frac{2\pi i}{q}(-a)k}\sum_{n=1}^{\infty} a(n)e^{\frac{2\pi i}{q}nk}.
\end{aligned}
$$

The first sum diverges by assumption, and the second sum looks like it would converge because formally it is a linear combination of $\lim_{r\to 1^-} f(re^{\frac{2\pi i}{q}k})$, where $k = 1, 2, \ldots, q-1$, which is finite by assumption. But strange as it may sound, there is no guarantee that $\lim_{r\to 1^-} f(re^{\frac{2\pi i}{q}k}) = f(e^{\frac{2\pi i}{q}k}) = \sum_{n=1}^{\infty} a(n)e^{\frac{2\pi i}{q}nk}$.[2] So we have to be a little bit more careful.

Rewrite

$$
\sum_{n=1,\ n\equiv a \pmod q}^{\infty} a(n) = \sum_{n=1}^{\infty} a(n) \lim_{r\to 1^-}\Big(\frac{1}{q}\sum_{k=0}^{q-1}(re)^{\frac{2\pi i}{q}(-a)k}(re)^{\frac{2\pi i}{q}nk}\Big). \tag{1}
$$

Since

$$
a(n)\Big(\frac{1}{q}\sum_{k=0}^{q-1}(re)^{\frac{2\pi i}{q}(-a)k}(re)^{\frac{2\pi i}{q}nk}\Big) \longrightarrow a(n)\Big(\frac{1}{q}\sum_{k=0}^{q-1} e^{\frac{2\pi i}{q}(-a)k}e^{\frac{2\pi i}{q}nk}\Big)
$$

uniformly as $r \to 1^-$, we can rewrite (1) as

$$
\lim_{r\to 1^-}\sum_{n=1}^{\infty} a(n)\Big(\frac{1}{q}\sum_{k=0}^{q-1}(re)^{\frac{2\pi i}{q}(-a)k}(re)^{\frac{2\pi i}{q}nk}\Big),
$$

which is equal to

$$
\lim_{r\to 1^-}\Big(\frac{1}{q}\sum_{n=1}^{\infty} a(n) + \frac{1}{q}\sum_{k=1}^{q-1}(re)^{\frac{2\pi i}{q}(-a)k}\sum_{n=1}^{\infty} a(n)(re)^{\frac{2\pi i}{q}nk}\Big).
$$

Here the first sum diverges, and the second sum converges by the assumptions.

4. Suppose χ has order l. Then $(\chi(n))^l = (\chi_0(n))^l = 1$ for all n with $(n,p) = 1$, i.e. $\chi(n)$ is an l-th root of unity.

Next, suppose g is a primitive root (mod p). We need to show that the order of $\chi(g)$ is l. Certainly $(\chi(g))^l = 1$. If there exists $k < l$ such that $(\chi(g))^k = 1$, then $(\chi(g^i))^k = 1$ for all integers i; g being a primitive root, this means that $(\chi(n))^k = 1$ for all n such that

[2] A theorem of Abel says that if the right-hand side converges then this equality is true; but in our situation we do not know yet if it converges.

$(n, p) = 1$, which in turn means that χ has order at most k, contradicting the assumption that χ has order $l > k$.

As for the last question of the problem, the answer is no. Here is a counterexample; let $\chi(n) = (n|7)$ be a character mod 7. χ has order 2. And $\chi(6) = -1$ is a primitive 2nd root of unity. But 6 is not a primitive root (mod 7).

5. Let g be a primitive root (mod p). By the multiplicativity of a character χ (mod p), χ is entirely determined by $\chi(g)$. Furthermore, χ is real if and only if $\chi(g)$ is real. Therefore $\chi(g) = 1$ or -1, and consequently there are precisely two real characters (mod p).

In the mod p^α case, we know that there exists a primitive root g (mod p^α). Again a character χ (mod p^α) is entirely determined by $\chi(g)$, and χ is real if and only if $\chi(g)$ is. Therefore there are two real characters, one with $\chi(g) = 1$ and the other with $\chi(g) = -1$.

Mod 2^α case: if $\alpha = 1$, there is only a single character (mod 2), namely the principal character, which happens to be real. If $\alpha \geq 2$, recall from Problem Set 3, Exercise 5 that the reduced residue class mod 2^α (i.e. $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$) is generated by -1 and 5. So any χ (mod 2^α) is determined by $\chi(-1)$ and $\chi(5)$, and if in addition χ is real, these can only map to ± 1. Hence there are 4 real characters (mod 2^α).

In general, if $q = p_0^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k}$, (here $p_0 = 2$, p_i for $i \geq 1$ are distinct odd primes and $\alpha_i \geq 1$), then a character (mod q) is a multiple of characters (mod $p_i^{\alpha_i}$), $i = 0, 1, \dots, k$. And two characters (mod q) are the same if and only if they are multiples of the same characters (mod $p_i^{\alpha_i}$) for all i. Therefore, if $\alpha_0 \geq 2$ then there are 2^{k+2} real characters (mod q), and if $\alpha_0 = 0, 1$ then there are 2^k real characters (mod q).