Math 539—Group Work #9

Thursday, April 3, 2025

1. Throughout this problem, p is an odd prime and χ is a nonprincipal Dirichlet character (mod p)*, and $S_\chi(b)$ is defined by*

$$S_\chi(b) = \sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+b)}.$$

(a) *If $p \nmid bb'$, show that $S_\chi(b) = S_\chi(b')$. (Hint: change variables $n \mapsto bn$.)*

Since $p \nmid b$, the product bn runs through a complete residue system (mod p) as n does. Therefore, using total multiplicativity,

$$\begin{aligned} S_\chi(b) = \sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+b)} &= \sum_{n=0}^{p-1} \chi(bn)\overline{\chi(bn+b)} \\ &= \sum_{n=0}^{p-1} \chi(b)\chi(n) \cdot \overline{\chi(b)\chi(n+1)} = \sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+1)} = S_\chi(1) \end{aligned}$$

since $\chi(b)\overline{\chi(b)} = |\chi(b)|^2 = 1$ for $p \nmid b$. In particular, since p divides neither b nor b', we conclude that $S_\chi(b) = S_\chi(1) = S_\chi(b')$.

(b) *By evaluating the double sum*

$$\sum_{b=0}^{p-1}\sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+b)}$$

in two different ways, show that $S_\chi(b) = -1$ for all $b \not\equiv 0$ (mod p).

On one hand, note that

$$S_\chi(0) = \sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+0)} = 0 + \sum_{n=1}^{p-1} |\chi(n)|^2 = p-1.$$

Thus, from part (a),

$$\sum_{b=0}^{p-1}\sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+b)} = \sum_{n=0}^{p-1} S_\chi(b) = p-1+\sum_{n=1}^{p-1} S_\chi(1) = (p-1)\big(1+S_\chi(1)\big).$$

On the other hand, exchanging the order of summation yields

$$\sum_{b=0}^{p-1}\sum_{n=0}^{p-1} \chi(n)\overline{\chi(n+b)} = \sum_{n=0}^{p-1} \chi(n)\overline{\sum_{b=0}^{p-1} \chi(n+b)} = \sum_{n=0}^{p-1} \chi(n)\bar{0} = 0$$

by orthogonality, since for each fixed n, the sum $n+b$ runs through a complete residue system (mod p) as b does. We conclude that $(p-1)\big(1+S_\chi(1)\big) = 0$, which shows that $S_\chi(1) = -1$ and therefore $S_\chi(b) = -1$ whenever $p \nmid b$ by part (a).

2. Throughout this problem, p is an odd prime, and $\left(\frac{n}{p}\right)$ is the Legendre symbol (which is a quadratic Dirichlet character (mod p) *when considered a function of n).*

(a) *For any arithmetic function $f(n)$ that is periodic with period p, convince yourself that*

$$\sum_{x=0}^{p-1} f(x^2) = \sum_{y=0}^{p-1} \left(1 + \left(\frac{y}{p}\right)\right) f(y).$$

(Hint: group the summands according to the value of x^2 (mod p).*)*

More generally, suppose that $q \in \mathbb{N}$ and that f and g are any two functions with period q defined on the integers, and suppose further that the values of g are also integers. Then

$$\sum_{x \pmod q} f\big(g(x)\big) = \sum_{y \pmod q} f(y) \# \big\{x \pmod q \colon g(x) \equiv y \pmod q\big\}$$

is a valid change-of-variables formula, justified by "grouping the terms according to the value of $g(x)$ (mod q)". Analogously, if $r_2(y)$ is the number of ways to write y as the sum of squares of two integers, then $\big(\sum_{m \in \mathbb{Z}} e^{-m^2}\big)^2 = \sum_{m,n \in \mathbb{Z}} e^{-(m^2+n^2)} = \sum_{y \in \mathbb{Z}} r_2(y) e^{-y^2}$ (and that identity quickly generalizes to sums of k squares for $k > 2$).

When $g(x) = x^2$ and the modulus is a prime p, it is merely a convenient coincidence that $\#\big\{x \pmod p \colon x^2 \equiv y \pmod p\big\} = 1 + \left(\frac{y}{p}\right)$.

(b) *If $p \nmid d$, show that*

$$\sum_{x=0}^{p-1} \left(\frac{x^2 - d}{p}\right) = -1.$$

If χ is the (nonprincipal) Dirichlet character $\chi(n) = \left(\frac{n}{p}\right)$, then using part (a),

$$\sum_{x=0}^{p-1} \left(\frac{x^2 - d}{p}\right) = \sum_{y=0}^{p-1} \left(1 + \left(\frac{y}{p}\right)\right)\left(\frac{y-d}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y-d}{p}\right) + S_\chi(-d) = 0 + (-1)$$

by orthogonality (since $y - d$ runs over a complete set of residues (mod p) as y does) and problem #1(b).

Another solution proceeds as follows: let $T(d) = \sum_{x=0}^{p-1} \left(\frac{x^2-d}{p}\right)$. If d is a quadratic residue (mod p), say $d \equiv c^2 \pmod p$ with $c \not\equiv 0 \pmod p$, then the change of variables $x \mapsto cx$ yields

$$T(d) = \sum_{x=0}^{p-1} \left(\frac{x^2 - d}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{(cx)^2 - d}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{c^2}{p}\right)\left(\frac{x^2 - 1}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x^2 - 1}{p}\right) = T(1);$$

in particular, $T(d)$ has the same value for all quadratic residues d (mod p). A similar change of variables shows that $T(d)$ has the same value for all quadratic nonresidues d (mod p); and the evaluation $T(0) = p - 1$ is easy. Moreover, note that we can obtain the value of $T(d)$ on quadratic residues:

$$T(1) = \sum_{x=0}^{p-1} \left(\frac{x^2 - 1}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x-1}{p}\right)\left(\frac{x+1}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y+2}{p}\right) = S_\chi(2) = -1$$

by problem #1(b), using the change of variables $y = x - 1$. Now by summing over all $d \pmod p$ as in part (b), we can solve for the remaining values $T(d) = -1$ for quadratic nonresidues $d \pmod p$.

(c) *For any integers a, b, and c such that $p \nmid (b^2 - 4ac)$, prove that*

$$\sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) = -\left(\frac{a}{p}\right).$$

(Hint: complete the square. Note that we are not assuming $p \nmid a$.)

First, if $p \mid a$, then the assumption $p \nmid (b^2 - 4ac)$ implies $p \nmid b$, and therefore (by periodicity and orthogonality)

$$\sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) = \sum_{w=0}^{p-1} \left(\frac{bw + c}{p}\right) = 0 = -\left(\frac{a}{p}\right),$$

since $bw + c$ runs through a complete residue system $\pmod p$ as w does.

On the other hand, if $p \nmid a$, then $\left(\frac{a}{p}\right)\left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$ (since p is odd), and therefore

$$\begin{aligned}
\sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) &= \left(\frac{a}{p}\right)\left(\frac{4a}{p}\right) \sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{w=0}^{p-1} \left(\frac{4a(aw^2 + bw + c)}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{w=0}^{p-1} \left(\frac{(2aw + b)^2 - (b^2 - 4ac)}{p}\right) = \left(\frac{a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{x^2 - (b^2 - 4ac)}{p}\right),
\end{aligned}$$

since $p \nmid 2a$ and therefore $x = 2aw + b$ runs through a complete residue system $\pmod p$ as w does. But by part (b) and the assumption $p \nmid (b^2 - 4ac)$, the right-hand side is simply $\left(\frac{a}{p}\right)(-1)$ as desired.

One can also use the general change of variables formula from the proof of part (a) in the form

$$\sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \#\big\{w \pmod p \colon aw^2 + bw + c \equiv y \pmod p\big\},$$

and then evaluate

$$\begin{aligned}
&\#\big\{w \pmod p \colon aw^2 + bw + c \equiv y \pmod p\big\} \\
&\qquad = \#\big\{v \pmod p \colon v^2 \equiv 4ay + (b^2 - 4ac) \pmod p\big\}
\end{aligned}$$

(again by completing the square) and proceed from there.

(d) *Still assuming $p \nmid (b^2 - 4ac)$, conclude that*

$$\#\big\{(v, w) \colon 0 \le v \le p - 1,\ 0 \le w \le p - 1,\ v^2 \equiv aw^2 + bw + c \pmod p\big\} \tag{1}$$

equals either $p - 1$, p, or $p + 1$.

As before, the number of v (mod p) such that $v^2 \equiv aw^2 + bw + c$ (mod p) is equal to $1 + \left(\frac{aw^2+bw+c}{p}\right)$. Therefore the quantity in equation (1) is exactly

$$\sum_{w=0}^{p-1} \left(1 + \left(\frac{aw^2 + bw + c}{p}\right)\right) = p + \sum_{w=0}^{p-1} \left(\frac{aw^2 + bw + c}{p}\right) = p - \left(\frac{a}{p}\right)$$

by part (c), and $\left(\frac{a}{p}\right)$ equals either 1, 0, or -1.

Remark: over the real numbers, the equation $v^2 = aw^2 + bw + c$ is a hyperbola if $a > 0$ (that is, if a is a quadratic residue in $\mathbb{R}$), an ellipse if $a < 0$ (that is, if a is a nonquadratic residue in $\mathbb{R}$), and a parabola if $a = 0$. Problem 2(d) is actually counting points on these conics (quadratic curves) when considered over the finite field $\mathbb{F}_p$ rather than the field of real numbers. This is a gateway result to algebraic geometry (similar to how the orthogonality relations for Dirichlet characters are a gateway result to representation theory).