

SOLUTIONS TO HOMEWORK 1
Math 104B - Dr. Evans
UCSD Spring 2004

1. Let n be any positive integer. Show that

$$\sum_{j=0}^{n-1} y^j = \frac{y^n - 1}{y - 1}$$

Proof. Let $S = \sum_{j=0}^{n-1} y^j = 1 + y + y^2 + \cdots + y^{n-1}$. Multiplying by y results in $yS = y + y^2 + \cdots + y^{n-1} + y^n$. Subtracting the two equations,

$$(y - 1)S = yS - S = y^n - y^{n-1} + y^{n-1} + \cdots - y + y - 1 = y^n - 1$$

Dividing through by $y - 1$ gives the result.

2. Let p be an odd prime. Show that

$$\sum_{j=0}^{p-1} \zeta_p^{j^2} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m.$$

Hint: First prove

$$\sum_{j=0}^{p-1} \zeta_p^{j^2} = \sum_{m=0}^{p-1} \left[1 + \left(\frac{m}{p}\right)\right] \zeta_p^m$$

Proof. We first prove that if $a \equiv b \pmod{p}$, then $\zeta_p^a = \zeta_p^b$. Suppose $a = b + kp$ for some integer k . Then

$$\zeta_p^a = \zeta_p^{b+kp} = \zeta_p^b \cdot \zeta_p^{kp} = \zeta_p^b (\zeta_p^p)^k = \zeta_p^b \cdot 1^k = \zeta_p^b$$

j^2 takes on the value 0 exactly once, when $j = 0$. Since $j^2 \equiv (-j)^2 \pmod{p}$, j^2 takes on the value of each nonzero square modulo p exactly twice. j^2 never takes on any of the nonsquares modulo p . From the definition of the Legendre symbol,

$$1 + \left(\frac{m}{p}\right) = \begin{cases} 2 & \text{if } m \text{ is a nonzero square modulo } p \\ 0 & \text{if } m \text{ is a nonsquare modulo } p \\ 1 & \text{if } p \mid m \end{cases}$$

Hence, $1 + \left(\frac{m}{p}\right)$ counts exactly how many times $j^2 \equiv m \pmod{p}$ as j ranges from 0 to $p-1$. Hence,

$$\sum_{j=0}^{p-1} \zeta_p^{j^2} = \sum_{m=0}^{p-1} \left[1 + \left(\frac{m}{p}\right)\right] \zeta_p^m$$

Now distributing the second sum and using the fact that $\sum_{m=0}^{p-1} \zeta_p^m = \frac{\zeta_p^p - 1}{\zeta_p - 1} = 0$,

$$\sum_{m=0}^{p-1} \left[1 + \left(\frac{m}{p}\right)\right] \zeta_p^m = \sum_{m=0}^{p-1} \zeta_p^m + \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m = 0 + \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m.$$

3. Let p be a prime such that $p \equiv 3 \pmod{4}$. Show that the Gauss sum

$$\sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m$$

is purely imaginary.

Proof. Let \mathcal{G} be the Gauss sum above. First note that \mathcal{G} may be written as

$$\mathcal{G} = \sum_{m \bmod p} \left(\frac{m}{p}\right) \zeta_p^m$$

since the Legendre symbol $\left(\frac{m}{p}\right)$ and the power ζ_p^m depend only on what m is modulo p (the first assertion is true by definition, the second follows from the argument at the beginning of problem 2).

We show that $\overline{\mathcal{G}} = \left(\frac{-1}{p}\right)\mathcal{G}$. Note that $\overline{\left(\frac{-1}{p}\right)} = \left(\frac{-1}{p}\right)$ since it is either 1, 0, or -1. Also, $\overline{\zeta_p^a} = \zeta_p^{-a}$. This can be easily shown using the definition of ζ_p and trigonometric identities. Hence,

$$\overline{\mathcal{G}} = \sum_{m \bmod p} \left(\frac{m}{p}\right) \zeta_p^{-m}$$

Let $n = -m$. Then n runs through all integers modulo p since m does. Thus,

$$\overline{\mathcal{G}} = \sum_{n \bmod p} \left(\frac{-n}{p}\right) \zeta_p^n = \left(\frac{-1}{p}\right) \sum_{n \bmod p} \left(\frac{n}{p}\right) \zeta_p^n = \left(\frac{-1}{p}\right)\mathcal{G}$$

To show \mathcal{G} is purely imaginary, it is enough to show the real part is 0. A basic fact from complex numbers states that $\operatorname{Re}(z) = \frac{1}{2}(z + \overline{z})$. Therefore,

$$\operatorname{Re}(\mathcal{G}) = \frac{1}{2}(\mathcal{G} + \overline{\mathcal{G}}) = \frac{1}{2}\left[\mathcal{G} + \left(\frac{-1}{p}\right)\mathcal{G}\right] = \frac{1}{2}\mathcal{G}\left[1 + \left(\frac{-1}{p}\right)\right]$$

Since $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod{4}$, we conclude $\operatorname{Re}(\mathcal{G}) = 0$.