MA 341: Advanced Problems for Fun: # 2

This advanced problem set is about *Gauss sums* with an application at the end to proving quadratic reciprocity, modeled on the exposition given by W. Stein. It requires a bit of experience with complex numbers.

1. Let $\zeta_n = \cos(2\pi i/n) + i\sin(2\pi i/n)$. Show that $\zeta_n^n = 1$. (Hint: Use Euler's identity for complex exponentials!) Show that $\zeta_n^a = 1$ for any a, and that $\zeta_n^a \equiv \zeta_n^b$ if and only if $a \equiv b \bmod n$. (So the exponents "work mod n") The numbers ζ_n^a are called *nth roots of unity.*

2. Let p be an odd prime, set $\zeta = \zeta_p$, and $a \in \mathbb{Z}$. We define the Gauss sum associated to a as

$$g_a = \sum_{n=0}^{p-1} \left(\frac{a}{p}\right) \zeta^{an}.$$

   where the Legendre symbol is used. Try computing a few values of g_a by hand (draw some pictures in the complex plane!). Then compute some values of g_a^2.

3. Show $g_a = \left(\frac{a}{p}\right) g_1$, where we used the Legendre symbol.

4. Show that $g_a \cdot g_{-a} = (-1)^{(p-1)/2} g_1^2$.

5. Compute $\sum_{a=0}^{p-1} g_a \cdot g_{-a}$ in two different ways to deduce $g_1^2 = (-1)^{(p-1)/2} p$. (And hence $g_a^2 = (-1)^{(p-1)/2} p$.)

6. Let $p^* = (-1)^{(p-1)/2} p$, so $g^2 = p^*$ where $g = g_1$. Use Euler's criterion for p^* to deduce

$$g^q \equiv g \left(\frac{p^*}{q}\right) \bmod q$$

   where we interpret this congruence happening in the number system $\mathbb{Z}[\zeta]$ (i.e. q divides the difference in this ring).

7. Use $(x + y)^q \equiv x^q + y^q \bmod q$ to show

$$g^q \equiv g_q \bmod q.$$

8. Use $g_q = \left(\frac{q}{p}\right) g$ to deduce that

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

   (Be careful in checking to "cancel g" in this step!) This is equivalent to Quadratic Reciprocity by a homework problem.