Take Home Final On Quadratic Reciprocity

In all of the problems below, q is an odd prime and ξ_q is a primtive q-th root of unity. We let $\epsilon(q) = (-1)^{\frac{q-1}{2}} q$.

For any integer a and any prime p, we define $\left(\frac{a}{p}\right)$ to be 0 if p divides a, 1 is a is prime to p and a is is square modulo p, and -1 if a is not a square modulo p. It is easily seen that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

1. Let p be any prime and let q be as above with $q \neq p$. Show that

$$\left(\frac{p}{q}\right) = 1$$

if and only if p factors as into an even number of primes in $\mathbb{Q}(\xi_q)$. [Hint: Find the degrees of $\mathbb{Z}[\xi_q]/\mathcal{P}$ for the primes $\mathcal{P}$ such that $\mathcal{P} \cap \mathbb{Z}[\xi_q] = p$.]

2. Show that the unique quadratic extension contained in $\mathbb{Q}(\xi_q)$ is $\mathbb{Q}(\epsilon(q))$. [Hint: Unicity follows immediately from the fact that the extension is cyclic. To see what the unique quadratic is, consider ramification.]

3. Let G be a cyclic group of even order acting transitively on a finite set S, let $s \in S$, and let H_s be the set of $g \in G$ such that $gs = s$. Let G' be the unique subgroup of index 2 in G.

   (a) Show that for any subgroup H of G, we have $[G : H] = [G' : H]$ if and only if H is not contained in G'.

   (b) Show that S is even if and only if $H_s \subseteq G'$.

   (c) Show S is odd if and only if G' acts transitively on S. [Hint: Use (a) and (b) along with the fact that $|S| = [G : H_s]$.]

4. Let G be the Galois group of $\mathbb{Q}(\xi_q)$ over $\mathbb{Q}$ and let G' be the unique subgroup of index 2 in G.

   (a) Show that $\mathbb{Q}(\xi_q)^{G'} = \mathbb{Q}(\epsilon(q))$ (i.e. the fixed field of G' is $\mathbb{Q}(\epsilon(q))$).

   (b) Show that p factors into an even number of primes in $\mathbb{Z}[\xi_q]$ if and only if p factors into two primes in $\mathbb{Z}[\frac{1+\sqrt{\epsilon(q)}}{2}]$. [Hint: Use 3 along with the fact that G acts transitively on the primes of $\mathbb{Z}[\xi_q]$ lying over p]

5. Let a be an integer that is prime to q. Show that $a^{(p-1)/2}$ is equal to 1 if a is square modulo q and equal to -1 is a is not a square modulo q.

6. Let p be odd. Use the previous problems to show that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$