3 Appendix: Gauss's Lemma on Quadratic Reciprocity

We rewrite the proof of Gauss's lemma as given in [Hardy-Wright] along the lines of a course in abstract algebra [Herstein].

For each odd prime p we denote the field of residue classes (mod p) by Z_p, and its group of units (i.e., all its nonzero elements) by U_p. The natural homomorphism $Z \to Z_p$ takes values denoted by $n \longmapsto [n]$, where $[n]$ is the residue class of n. The existence of a solution x to the congruence $x^2 \equiv m \pmod{p}$ means that $[m]$ is a quadratic residue of p; if there is no solution, $[m]$ is called a quadratic nonresidue.

Definition 3.1 *If m is not a multiple of a prime p, define the Legendre symbol $(\frac{m}{p})$ to equal $+1$ if there exists x such that $x^2 \equiv m \pmod{p}$, and equal to -1 if there is no solution x.*

Proposition 3.1 *The quadratic residues of U_p form a subgroup Q_p of index 2 and order $\frac{1}{2}(p-1)$. For any integer m not a multiple of p, we have*

$$m^{\frac{1}{2}(p-1)} \equiv (\frac{m}{p}) \pmod{p}$$

Proof. The group of units U_p has $p-1$ elements and is cyclic [Herstein, Theorem 7.1.6]. If y is a generator, then $U_p = \{y, y^2, \ldots, y^{p-1} = [1]\}$, a group of order $p-1$. It is clear that the subgroup generated by y^2 is a set of quadratic residues in U_p; it is all of them, since we see that there are only $\frac{1}{2}(p-1)$ quadratic residues by squaring each element in U_p and noting that $x^2 \equiv (p-x)^2 \pmod{p}$. Hence, the quadratic residues of p form a subgroup of index 2 and order $\frac{1}{2}(p-1)$,

$$Q_p = \{y^2, y^4, \ldots, y^{p-1} = [1]\}$$

Given an integer m not a multiple of p, then $[m]$ is either in Q_p or it is not. If $[m] \in Q_p$, then $[m]$ is a quadratic residue of p, and has order dividing the order of Q_p It follows that $[m]^{\frac{1}{2}(p-1)} = [1]$. If $[m] \notin Q_p$, it is a quadratic nonresidue, and equal to an odd power y^{2n+1} of the generator y. But $y^{\frac{1}{2}(p-1)} = [-1]$ since it is a root of $x^2 - [1]$ other than $[1]$, and over a field a polynomial only has as many roots as its degree! Hence,

$$[m]^{\frac{1}{2}(p-1)} = (y^{2n+1})^{\frac{1}{2}(p-1)} = y^{n(p-1)} y^{\frac{1}{2}(p-1)} = [-1] \quad \square$$