Section 12. Quadratic Reciprocity

Note. In this section we prove two results stated in the previous section. We prove the Quadratic Reciprocity Theorem (Theorem 11.4/12.4) and Theorem 11.6/12.2 which lets us evaluate the Legendre symbol $(2/p)$ for odd prime p. The proofs in this section are among the longest in the book.

Note. As discussed in the last section, Carl F. Gauss (April 20, 1777-February 23, 1855) was the first to prove our modern version of the Quadratic Reciprocity Theorem. He included a proof in his first 1801 edition of *Disquisitiones Arithmeticae* ["Investigations in Arithmetic"]. So we start with a result by Gauss that will be used in the proofs of both the Quadratic Reciprocity Theorem and Theorem 11.6/12.2.

Theorem 12.1. Gauss's Lemma.
Suppose that p is an odd prime, $p \nmid a$, and there are among the least residues (mod p) of

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$$

exactly g that are greater than $(p-1)/2$. Then $x^2 \equiv a \pmod{p}$ has a solution or no solution according as g is even or odd. That is, $(a/p) = (-1)^g$.

Note. To illustrate Gauss's Lemma (Theorem 12.1), consider $a = 5$ and $p = 17$. We have $(p-1)/2 = ((16)-1)/2 = 8$, and the multiples of $a = 5$ are

$5, 10, 15, 20, 25, 30, 35, 40$, which have least residues (mod 17) of $5, 10, 15, 3, 8, 13, 1, 6$, respectively. Since $g = 3$ of these are greater than $(p-1)/2 = 8$, then Gauss's Lemma implies that for $a = 5$ and $p = 17$ we have $(a/p) = (5/17) = (-1)^3 = -1$, so that $a = 5$ is a quadratic nonresidue (mod 17).

Theorem 12.2. If p is an odd prime, then

$$(2/p) = 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod 8, \text{ or } (2/p) = -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod 8.$$

Note. Dudley observes (see page 98): "Not theorem has been proved that will tell which primes 2 is a primitive root of, and it has not even been proved that 2 is a primitive root of infinitely many primes." But we do have the following concerning 2 as a primitive root of some primes.

Theorem 12.3. If p and $4p+1$ are both primes, then 2 is a primitive root $4p+1$.

Note. We need one more lemma before giving a proof of the Quadratic Reciprocity Theorem.

Lemma 12.1. If p and q are different odd primes, then

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Here, $[\,\cdot\,]$ denotes the greatest integer function.

Note. In the previous section, we stated the Quadratic Reciprocity Theorem (Theorem 11.4) as: "If p and q are odd primes and $p \equiv q \equiv 3 \pmod 4$, then $(p/q) = -(q/p)$. Otherwise, $(p/q) = (q/p)$." The statement we now give and prove is equivalent to this original version.

Theorem 12.4. The Quadratic Reciprocity Theorem.
If p and q are odd primes, then $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Revised: 3/13/2022