For p a prime and (a, p) = 1, let the Legendre symbol (a|p) (classical notation $(\frac{a}{p})$), denote 1 when a is a square mod p and -1 when a is not a square mod p. With this notation, the previous theorem says that $a^{(p-1)/2} \equiv (a|p)(p)$ when p is a prime and a is prime to p. The following important result will be proved in the third section of chapter 4.

THE QUADRATIC RECIPROCITY THEOREM. Suppose that p and q are odd primes. Then

$$(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}.$$

Note. In other words, the product (p|q)(q|p) equals 1 unless both p and q are $\equiv 3 \mod 4$, in which case it equals -1.

Note. This result, first proved by Gauss in 1801, is one of the most famous and beautiful results in number theory.

R. Define (a|p) to be zero when p divides a. It is obvious that (a|p) = (b|p) when $a \equiv b$ (p). Prove that (ab|p) = (a|p)(b|p). (Hint: This amounts to the statement that the product of two squares mod p is a square mod p etc. At one point it is useful to know that there are as many squares as non-squares.)

R. Verify that $(-1|p) = (-1)^{(p-1)/2}$ and that (a|2) = 1 for all odd integers a.

Examples

Any odd prime has the form $6k + \epsilon$ where $\epsilon = \pm 1$. Hence $(p|3) = (6k + \epsilon|3) = (\epsilon|3) = \epsilon$, for 1 is a square mod 3 but not -1. Similarly, $p \equiv \pm 1$ or ± 2 mod 5. In the first case, (p|5) = 1, in the second (p|5) = -1.

Exercise

Do the same computations with 7 taking the place of 5.

The quadratic reciprocity theorem has the following complement:

THEOREM. When p > 2 is a prime, $(2|p) = (-1)^c$, where $c = (p^2 - 1)/8$.

Note. The proof below is similar to one of Gauss's proofs of the quadratic reciprocity theorem.

Note. Using this result and the quadratic reciprocity theorem, we can compute any (n|p) with p prime. In fact, reducing n modulo p, we can assume that $1 \le n < p$ and then factor n into powers of primes. Since (ab|p) = (a|p)(b|p), this reduces the problem to the quadratic reciprocity theorem and the computation of (2|p).

PROOF: We are going to consider the numbers $C = \{1, 2, ..., (p-1)/2\}$, whose sum is $c = (p^2 - 1)/8$, and the set $2C = \{2, 4, ..., p-1\}$. Let