THE QUADRATIC RECIPROCITY THEOREM

MARTIN OLSSON

Theorem 1. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

The following proof is due to Sey Yoon Kim (I learned this proof from John Tate).

Let

$$m = \frac{pq-1}{2} = (\frac{p-1}{2})q + \frac{q-1}{2} = (\frac{q-1}{2})p + \frac{p-1}{2}.$$

Let

$$A = \{n | 1 \leq n \leq m \text{ and } (n, pq) = 1\},$$

and

$$B = \{n | 1 \leq n \leq m \text{ and } (n, p) = 1\}.$$

Let a denote the product of the elements in a, and let b denote the product of the elements in B. Note that

$$B = A \cup \{q, 2q, \ldots, (\frac{p-1}{2})q\}.$$

From this we get

$$b = aq^{\frac{p-1}{2}}((\frac{p-1}{2})!). \tag{1.1}$$

On the other hand, we can also write

$$B = \left(\cup_{j=0}^{\frac{q-1}{2}-1} \cup_{i=1}^{p-1} (jp+i)\right) \cup \left(\cup_{i=1}^{\frac{p-1}{2}} ((\frac{q-1}{2})p+i)\right).$$

From this we get that

$$b \equiv ((p-1)!)^{\frac{q-1}{2}}((\frac{p-1}{2})!) \pmod{p}. \tag{1.2}$$

Combining equations 1.1 and 1.2 we get that

$$((p-1)!)^{\frac{q-1}{2}}((\frac{p-1}{2})!) \equiv aq^{\frac{p-1}{2}}((\frac{p-1}{2})!) \pmod{p}.$$

Cancelling the $((p-1)/2)!$ from both sides, applying Wilson's theorem, and using that $q^{\frac{p-1}{2}}$ is congruent mod p to $(\frac{q}{p})$ we conclude that

$$\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \equiv a \pmod{p}.$$

By symmetry we also have

$$\left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \equiv a \pmod{q}.$$

This now reduces the quadratic reciprocity theorem to a congruence statement for $a \pmod{pq}$. In fact from this we get that the quadratic reciprocity theorem is equivalent to the statement that for p and q both congruent to 1 mod 4 we should have

$$a \equiv \pm 1 \pmod{pq},$$

and in all other cases we should have a not congruent to $\pm 1 \pmod{pq}$.

To verify that this is indeed the case, note that there is an involution

$$\sigma : A \to A$$

sending $n \in A$ to the unique element $n' \in A$ for which

$$nn' \equiv \pm 1 \pmod{pq}.$$

From this we get that

$$a = \prod_{n \in A} n \equiv \pm \prod_{n \in A, \sigma(n) = n} n \equiv \pm \prod_{n^2 \equiv \pm 1} n \pmod{pq}.$$

The congruence $n^2 \equiv 1 \pmod{pq}$ has four solutions $\pm 1, \pm u$, with say $1, u \in A$. The congruence

$$n^2 \equiv -1 \pmod{pq}$$

has no solutions unless $p \equiv q \equiv 1 \pmod 4$. In this case the solutions are $\pm i$ and $\pm iu$, with say i and eiu in A, where e is either 1 or -1 and i is a number with $i^2 \equiv -1 \pmod p$. So if $p \equiv q \equiv 1 \pmod 4$ we get

$$a \equiv \pm ui(eiu) \equiv \pm 1 \pmod{pq},$$

and otherwise

$$a \equiv \pm u \pmod{pq}$$

which is not $\pm 1 \pmod{pq}$. This therefore verifies the quadratic reciprocity theorem. $\square$