Quadratic Reciprocity : Part 1

Recall, we have covered Theorem 11.6, but never proven it:

Theorem : (11.6)

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 7 \mod 8$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 8 \quad \text{or} \quad p \equiv 5 \mod 8$$

Proof. By Theorem 12.1, it is sufficient to find out how many of the least residues modulo p of

$$2, \quad 4, \quad 6, \quad \ldots, 2 \cdot \frac{p-1}{2}$$

Are greater than $\frac{p-1}{2}$. Since all the numbers are least residues, we only have to see how many of them are greater than $\frac{p-1}{2}$. Let the first even integer greater than $\frac{p-1}{2}$ be $2a$. Between 2 and $\frac{p-1}{2}$, there are a - 1 even integers, namely

$$2, \quad 4, \quad 6, \quad \ldots, \quad 2(a-1)$$

The number of even integers from 2 to $p-1$ greater than $\frac{p-1}{2}$ is

$$g = \frac{p-1}{2} - (a-1)$$

Since $2a$ is the smallest integer greater than $\frac{p-1}{2}$, it follows that g is the largest integer less than $\frac{p+3}{4}$. Suppose that $p \equiv 1 \mod 8$. Then, $p = 1 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{4+8k}{4} = 1 + 2k$$

It follows that $g = 2k$ and that $(-1)^g = 1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1 \mod 8$. Suppose that $p \equiv 3 \mod 8$. Then, $p = 3 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{6+8k}{4} = \frac{3}{2} + 2k$$

It follows that $g = 2k + 1$ and that $(-1)^g = -1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3 \mod 8$. Suppose that $p \equiv 5 \mod 8$. Then, $p = 5 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{8+8k}{4} = 2 + 2k$$

It follows that $g = 2k + 1$ and that $(-1)^g = -1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = -1$ if $p \equiv 5 \mod 8$. Suppose that $p \equiv 7 \mod 8$. Then, $p = 7 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{10+8k}{4} = \frac{5}{2} + 2k$$

It follows that $g = 2k + 2$ and that $(-1)^g = 1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = 1$ if $p \equiv 7 \mod 8$. $\square$

Lemma : (12.1)

If p and q are different odd primes, then

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

Proof. Let $S(p,q)$ and $S(q,p)$ be defined as

$$S(p,q) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right], \qquad S(q,p) = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]$$

We are trying to prove that $S(p,q) + S(q,p) = \frac{(p-1)(q-1)}{4}$. $S(p,q)$ is the number of lattice points below the line $y = \frac{qx}{p}$ and above the x-axis for $x = 1, 2, \ldots \frac{p-1}{2}$. $S(q,p)$ is the number of lattice points to the left of the line $y = \frac{qx}{p}$ and to the right of the y-axis. Notice that there are no lattice points on the line. If the lattice point (a,b) were on the line $y = \frac{qx}{p}$, then

$$b = \frac{qa}{p} \quad \text{or} \quad bp = qa$$

Since $p \mid qa$ and $(p,q) = 1$, it follows that $p \mid a$. However, $1 \leq a \leq \frac{p-1}{2}$, a contradiction. Each lattice point in or on the boundary of the rectangle is

$$S(p,q) + S(q,p)$$

This number is also $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Therefore we have that,

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

$\square$