(182)

Theorem:

Let n be the number defined in Gauss Lemma. Then

$$n = \sum_{t=1}^{p-1/2} \left[\frac{ta}{p}\right] + (a-1)\left(\frac{p^2-1}{8}\right) \pmod 2$$

In particular, if a is odd, then

$$n = \sum_{t=1}^{p-1/2} \left[\frac{ta}{p}\right] \pmod 2$$

Proof: Consider the set

$$S = \left\{ a, 2a, 3a, \ldots \frac{p-1}{2} a \right\}$$

whose remainder exceeds $p/2$ upon division by p.

Consider

$$\frac{ta}{p} = \left[\frac{ta}{p}\right] + \left\{\frac{ta}{p}\right\}, \quad 0 < \left\{\frac{ta}{p}\right\} < 1$$

$$ta = p\left[\frac{ta}{p}\right] + p\left\{\frac{ta}{p}\right\} = p\left[\frac{ta}{p}\right] + r_t'$$

(183)

$$0 < r'_t < p.$$

$$r'_t = ta - p\left[\frac{ta}{p}\right]$$ is the least positive residue of ta modulo p.

By Gauss Lemma

$$\left\{r'_1, r'_2, \ldots r'_{\frac{p-1}{2}}\right\} = \left\{r_1, r_2, \ldots r_m, s_1, s_2, \ldots s_n\right\}$$

Also

$$\left\{1, 2, \ldots \frac{p-1}{2}\right\} = \left\{r_1, r_2, \ldots r_m, p-s_1, p-s_2, \ldots, p-s_n\right\}$$

$$\therefore \sum_{t=1}^{p-1/2} r'_t = \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j \quad -(1)$$

and

$$\sum_{t=1}^{p-1/2} t = \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} (p - s_j)$$

$$= \sum_{i=1}^{m} r_i + np - \sum_{j=1}^{n} s_j \quad -(2)$$

184

Subsitute for r'_t in (1)

$$\sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j = \sum_{t=1}^{\frac{p-1}{2}} ta - p \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{ta}{p}\right]$$

$$= a \sum_{t=1}^{\frac{p-1}{2}} t - p \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{ta}{p}\right] \quad -(3)$$

$$\sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j = -np + \sum_{t=1}^{\frac{p-1}{2}} t \quad -(4)$$

Add (3) & (4)

$$2 \sum_{i=1}^{m} r_i = -np + (a+1) \sum_{t=1}^{\frac{p-1}{2}} t - p \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{ta}{p}\right]$$

$$2 \sum_{i=1}^{m} r_i = -np + (a+1) \frac{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)}{2} - p \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{ta}{p}\right]$$

185

$$2\sum_{i=1}^{m} r_i + np = (a+1)\frac{p^2-1}{8} - p\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right]$$

$$np + 2\sum_{i=1}^{m} r_i = (a+1)\frac{p^2-1}{8} - p\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right]$$

$$n = (a-1)\left(\frac{p^2-1}{8}\right) + \sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right] \pmod 2$$

If a is odd

$$n = \sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right] \pmod 2$$

Quadratic Reciprocity Law:

If p and q are distinct primes $p>2$, $q>2$, then

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

Proof: By Gauss Lemma:

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

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

$$m = \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] \pmod 2$$

$$n = \sum_{\cancel{t}\,s=1}^{\frac{q-1}{2}} \left[\frac{sp}{2}\right] \pmod 2$$

(187)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$$

To prove:

$$\sum_{t=1}^{\frac{p-1}{2}} \left[\frac{tq}{p}\right] + \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Consider the function:

$$f(x, y) = qx - py$$

If x and y are nonzero integers, then $f(x,y)$ is a nonzero integer.

Moreover if,

$x = 1, 2, \ldots \frac{p-1}{2}$ and

$y = 1, 2, \ldots \frac{q-1}{2}$, then

$f(x,y)$ takes $\frac{p-1}{2} \cdot \frac{q-1}{2}$ values, no two of which are equal.

188

Since

$$f(x, y) - f(x', y') = f(x-x', y-y') \neq 0$$

Now $f(x, y) > 0$ iff $y < \frac{qx}{p}$ or

$$y \leq \left[\frac{qx}{p}\right]$$

Hence total number of positive values is

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right].$$

Total number of negative values is

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$$

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

189

Exc: $\left(\frac{29}{53}\right) = ?$

$$\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right)(-1)^{\frac{29-1}{2}\cdot\frac{53-1}{2}}$$

$$= \left(\frac{53}{29}\right)$$

$$\left(\frac{53}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{2^3\cdot 3}{29}\right)$$

$$= \left(\frac{2}{29}\right)\left(\frac{2^2}{29}\right)\left(\frac{3}{29}\right)$$

$$= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$$

$$29 \equiv 5 \pmod 8$$

$$\therefore \left(\frac{2}{29}\right) = -1$$

$$\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{29-1}{2}} = -\left(\frac{29}{3}\right)$$

$$= \left(\frac{2}{3}\right) = -1 \quad \left[\left(\frac{29}{53}\right) = (-1)(-1) = 1\right]$$