Gauss Lemma: Let p be an odd prime and let $\gcd(a, p) = 1$.

If n denotes the number of integers in the set

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

whose remainders upon division by p exceeds $p/2$ then

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

Proof: As $(a, p) = 1$

None of $\frac{p-1}{2}$ integers in S is congruent to zero and no two are congruent to each other modulo p.

175

Let $r_1, r_2, \ldots r_m$ be those remainder upon divison by p such that $0 < r_i < p/2$.

Let $s_1, s_2, \ldots, s_n$ be those remainders such that $p > s_i > p/2$.

Then $m + n = \frac{p-1}{2}$ and the integers $r_1, r_2, \ldots r_m$, $p - s_1, p - s_2, \ldots p - s_n$ are all positive and less than $p/2$.

To prove that these integers are all distinct, it is sufficient to prove that no $p - s_i = r_j$.

On contrary $p - s_i = r_j$ for some i, j

$\exists$ u, v such that

176

$$s_i \equiv ua \pmod{p}$$

$$r_j \equiv va \pmod{p} \qquad 1 \le u, v \le \frac{p-1}{2}$$

$$\Rightarrow (u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid u+v$$

a contradiction. Hence $p - s_i \neq r_j$ for any i, j.

$r_1, r_2, \ldots r_m, p-s_1, p-s_2, \ldots p-s_n$ are congruent to $1, 2, \ldots \frac{p-1}{2}$ in some order.

$$\therefore \left(\frac{p-1}{2}\right)! \equiv r_1 \ldots r_m (p-s_1) \ldots (p-s_n)$$

$$\equiv r_1 \ldots r_m (-s_1) \ldots (-s_n) \pmod{p}$$

$$\equiv (-1)^n r_1 r_2 \ldots r_m s_1 \ldots s_n \pmod{p}$$

But $r_1, r_2, \ldots r_m, s_1, s_2, \ldots s_n$

177

are congruent modulo p to

$a, 2a, 3a, \ldots \frac{p-1}{2}a$ in some order.

$\therefore$

$$\frac{p-1}{2}! \equiv (-1)^n a \; 2a \ldots \frac{p-1}{2}a \pmod{p}$$

$$\equiv (-1)^n a^{\frac{p-1}{2}} \frac{p-1}{2}! \pmod{p}$$

$$\left(\frac{p-1}{2}!, p\right) = 1$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$$

<u>Exc:</u> $p = 13$, $a = 5$, $\frac{p-1}{2} = 6$

$$S = \{5, 10, 15, 20, 25, 30\}$$

Three are greater than $13/2$,

$\therefore$ $n = 3$

$$\left(5/13\right) = (-1)^3 = -1$$

179

Theorem: Let p be an odd prime, then

$$(2|p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof! According to Gauss Lemma

$$\left(\frac{2}{p}\right) = (-1)^n, \text{ where } n \text{ is}$$

the number of integers in the set

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

which upon division by p have remainders greater than $p/2$. The members of S are less than p, it is sufficient to count the numbes that exceed $p/2$.

For $1 \le k \le \frac{p-1}{2}$, $2k < p/2$ iff $k < p/4$.

There are $[p/4]$ integers in S less than $p/2$.

$$\therefore \quad n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

If $p \equiv 1 \pmod 8$ ie $p = 8k+1$

$$n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$$

If $p \equiv 3 \pmod 8$ ie $p = 8k+3$

$$n = 4k+1 - \left[2k + \frac{3}{4}\right] = 2k+1$$

If $p \equiv 5 \pmod 8$ ie $p = 8k+5$
$\equiv -3 \pmod 8$

$$n = 4k+2 - \left[2k+1 + \frac{1}{4}\right]$$

$$= 2k+1$$

If $p \equiv -1 \equiv 7 \pmod 8$ ie $p = 8k+7$

$$n = 4k+3 - \left[2k+1 + \frac{3}{4}\right] = 2k+2$$

$$\therefore \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

<u>Carollary</u>: $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}$

181

<u>Theorem:</u> There are infinitely many primes of the form $8k-1$