Theorem: There are infinitely many primes of the form $4k+1$.

Proof: Suppose that there are finitely many primes of the form $4k+1$ say $p_1, p_2, \ldots, p_n$.

Consider

$$N = (2p_1p_2 \ldots p_n)^2 + 1$$

Clearly N is odd, $\exists$ odd prime p

s.t $p \mid N$

$\Rightarrow \quad N \equiv 0 \pmod{p}$

$\Rightarrow \quad (2p_1p_2 \ldots p_n)^2 \equiv -1 \pmod{p}$

$\Rightarrow \quad \left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod{4}$

$\Rightarrow$ p is one of the primes p_i,

$i = 1, 2, \ldots n.$

(172)

$$\Rightarrow \quad p_i \mid N - (2p_1p_2 \ldots p_n)^2$$

$$\Rightarrow \quad p_i \mid 1$$

a contradiction.

$\therefore$ there are infinitely many primes of the form $4k+1$.

<u>Theorem:</u> If p is an odd prime, then $\sum_{a=1}^{p-1} (a/p) = 0$.

Hence there are precisely $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.

<u>Proof:</u> Let r be a primitive root of p.

The powers $r, r^2, \ldots r^{p-1}$ are congruent to $1, 2, \ldots p-1$ in some

(173)

order.

$\therefore$ for any a, $1 \le a \le p-1$

$\exists$ unique K, $1 \le K \le p-1$

such that $a = r^K \pmod{p}$

By Euler's criterion

$$\left(\frac{a}{p}\right) = \left(\frac{r^K}{p}\right) \equiv \left(r^K\right)^{\frac{p-1}{2}} \pmod{p}$$

$$= \left(r^{p-1/2}\right)^K \equiv (-1)^K \pmod{p}$$

$\left(\because \ O(r) = p-1 \right.$

$\left. \Rightarrow r^{p-1/2} \equiv -1 \pmod{p} \right)$

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{K=1}^{p-1} (-1)^K \pmod{p}$$

$$= 0$$