NOTE ON A THEOREM ON QUADRATIC RESIDUES

KAI-LAI CHUNG

In this note we shall give a short proof of a known result:

THEOREM. *For every prime* $p \equiv 3 \pmod 4$ *there are more quadratic residues* mod p *between* 0 *and* $p/2$ *than there are between* $p/2$ *and* p.

An equivalent statement of this theorem is as follows (see E. Landau, *Vorlesungen über Zahlentheorie*, vol. 1, p. 129):

Für $p \equiv 3 \pmod 4$ *haben mehr unter den Zahlen* $1^2, 2^2, \cdots, (p-1)^2/4$ *ihren Divisionsrest* mod p *unter* $p/2$ *als über* $p/2$.

For proof we shall use Fourier series with one of its applications, namely Gaussian sums.

Write $s^2 = qp + r$, $0 \leqq r < p$, so that

$$\left[\frac{s^2}{p}\right] = q.$$

It is evident that we have

$$\left[\frac{2s^2}{p}\right] - 2\left[\frac{s^2}{p}\right] = \begin{cases} 0 & \text{if} \quad r < p/2; \\ 1 & \text{if} \quad r > p/2. \end{cases}$$

Therefore we have to prove that $\sum_{s=1}^{(p-1)/2}([2s^2/p] - 2[s^2/p]) < (p-1)/4$, or $\leqq (p-1)/4$ since $p \equiv 3 \pmod 4$.

By a well known expansion in Fourier series, we have

$$x - [x] - \tfrac{1}{2} = -\sum_{n=1}^{\infty} \frac{\sin 2n\pi x}{n\pi},$$

so that

$$[x] = x - \tfrac{1}{2} + \sum_{n=1}^{\infty} \frac{\sin 2n\pi x}{n\pi}.$$

Substituting, we get

$$\begin{aligned} \left[\frac{2s^2}{p}\right] - 2\left[\frac{s^2}{p}\right] &= \frac{2s^2}{p} - \tfrac{1}{2} + \sum_{n=1}^{\infty} \frac{\sin(4n\pi s^2/p)}{n\pi} \\ &\quad - 2\left\{\frac{s^2}{p} - \tfrac{1}{2} + \sum_{n=1}^{\infty} \frac{\sin(2n\pi s^2/p)}{n\pi}\right\} \\ &= \tfrac{1}{2} + \sum_{n=1}^{\infty} \frac{1}{n\pi}\left\{\sin\frac{4n\pi s^2}{p} - 2\sin\frac{2n\pi s^2}{p}\right\}; \end{aligned}$$