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 $\sum_{s=1}^{(p-1)/2}\left([2s^2/p] - 2[s^2/p]\right) < (p-1)/4$, 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

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

$$\sum_{s=1}^{(p-1)/2}\left(\left[\frac{2s^2}{p}\right]-2\left[\frac{s^2}{p}\right]\right)$$
$$=\frac{p-1}{4}+\sum_{n=1}^{\infty}\frac{1}{n\pi}\left\{\sum_{s=1}^{(p-1)/2}\left(\sin\frac{4n\pi s^2}{p}-2\sin\frac{2n\pi s^2}{p}\right)\right\}.$$

Therefore we have to prove that

$$\sum_{n=1}^{\infty}\frac{1}{n\pi}\sum_{s=1}^{(p-1)/2}\sin\frac{4n\pi s^2}{p}\leqq\sum_{n=1}^{\infty}\frac{2}{n\pi}\sum_{s=1}^{(p-1)/2}\sin\frac{2n\pi s^2}{p}.$$

Now we have by the results on Gaussian sums,

$$\text{if }\left(\frac{2n}{p}\right)=1,\quad \sum_{s=1}^{(p-1)/2}e^{2n(2\pi i s^2/p)}=\sum_{(r/p)=1}e^{2\pi i r/p}=+\frac{ip^{1/2}}{2};$$
$$\text{if }\left(\frac{2n}{p}\right)=-1,\quad \sum_{s=1}^{(p-1)/2}e^{2n(2\pi i s^2/p)}=\sum_{(r/p)=1}e^{-2\pi i r/p}=-\frac{ip^{1/2}}{2};$$
$$\text{if }\left(\frac{2n}{p}\right)=0,\quad \sum_{s=1}^{(p-1)/2}e^{2n(2\pi i s^2/p)}=\frac{p-1}{2}.$$

Taking imaginary parts, we obtain

$$\sum_{s=1}^{(p-1)/2}\sin\frac{4n\pi s^2}{p}=\left(\frac{2n}{p}\right)\frac{p^{1/2}}{2}.$$

Similarly,

$$\sum_{s=1}^{(p-1)/2}\sin\frac{2n\pi s^2}{p}=\left(\frac{n}{p}\right)\frac{p^{1/2}}{2}.$$

Therefore we have to prove that

$$\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{2n}{p}\right)\frac{p^{1/2}}{2}\leqq\frac{2}{\pi}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{n}{p}\right)\frac{p^{1/2}}{2};$$

that is,

$$\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{2n}{p}\right)\leqq 2\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{n}{p}\right).$$

This is equivalent to the relation

$$\sum_{n=1}^{\infty}\frac{-1}{n}\left(\frac{n}{p}\right)\leqq 2\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{n}{p}\right),\qquad \text{if } p\equiv 3 \pmod 8;$$

$$\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{n}{p}\right) \leqq 2\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{n}{p}\right), \quad \text{if } p \equiv 7 \pmod 8.$$

Thus in each case we have to prove that

$$\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{n}{p}\right) \geqq 0.$$

Now Landau would call this last result trivial. But for the sake of completeness we give its proof here; we have in fact, for $s > 1$,

$$\left\{\sum_{n=1}^{\infty} \frac{1}{n^s}\left(\frac{n}{p}\right)\right\} \prod_{p_1} \left(1 - \frac{1}{p_1^s}\left(\frac{p_1}{p}\right)\right) = 1,$$

where p_1 runs through the sequence of primes. The series being uniformly convergent for $s \geqq 1$ its sum is continuous at $s = 1$. Hence the result follows.

TSING-HUA UNIVERSITY,
KUNMING, CHINA