1 (Korea 2000) Let p be a prime number of the form $4k+1$. Show that

PEN I11

$$\sum_{i=1}^{p-1}\left(\left\lfloor\frac{2i^2}{p}\right\rfloor-2\left\lfloor\frac{i^2}{p}\right\rfloor\right)=\frac{p-1}{2}.$$

First Solution. We begin with an example. We list all quadratic residues of 17:

$$\begin{cases}1^2\equiv 16^2\equiv 1,\ \ 2^2\equiv 15^2\equiv 4,\ \ 3^2\equiv 14^2\equiv 9,\ \ 4^2\equiv 13^2\equiv 16,\\ 5^2\equiv 12^2\equiv 8,\ \ 6^2\equiv 11^2\equiv 2,\ \ 7^2\equiv 10^2\equiv 15,\ \ 8^2\equiv 9^2\equiv 13.\end{cases}\tag{1}$$

Hence, a list of all quadratic residues of 17 is given by

$$1,\ \ 2,\ \ 4,\ \ 8,\ \ 9,\ \ 13,\ \ 15,\ \ 16.$$

Can you see the number theoretical *symmetry*? Yeap! Indeed, in the eyes of modulo 17, it becomes

$$1,\ \ 2,\ \ 4,\ \ 8,\ \ -8,\ \ -4,\ \ -2,\ \ -1.$$

In general, the set of quadratic residues of a prime of the form $4k+1$ is symmetric. This observation is the key idea of the solution. We now prepare two simple lemmas without proofs.

Lemma 1. *Let a and b integers such that $a\equiv b\ (mod\ p)$. Then,*

$$\left\lfloor\frac{2a}{p}\right\rfloor-2\left\lfloor\frac{a}{p}\right\rfloor=\left\lfloor\frac{2b}{p}\right\rfloor-2\left\lfloor\frac{b}{p}\right\rfloor.$$

Lemma 2. *Let $\alpha\in\mathbb{R}$. Then, we have*

$$\lfloor 2\alpha\rfloor-2\lfloor\alpha\rfloor=\begin{cases}0, & \alpha-\lfloor\alpha\rfloor\in\left[0,\frac{1}{2}\right),\\ 1, & \alpha-\lfloor\alpha\rfloor\in\left[\frac{1}{2},1\right).\end{cases}$$

Since p is prime and since $p\equiv 1\ (mod\ 4)$, we see that -1 is a quadratic residue modulo p. It thus follows that an integer k is a quadratic residue modulo p if and only if $-k$ is a quadratic residue modulo p. So, we take $\frac{p-1}{4}$ integers $\alpha_1,\cdots,\alpha_{\frac{p-1}{4}}$ in $\{1,\cdots,\frac{p-1}{2}\}$ so that

$$-\alpha_{\frac{p-1}{4}},\cdots,-\alpha_1,\alpha_1,\cdots,\alpha_{\frac{p-1}{4}}$$

is a complete list of all quadratic residues modulo p. In other words, it is a permutation of

$$1^2=(p-1)^2,2^2=(p-2)^2,\cdots,\left(\frac{p-1}{2}\right)^2=\left(\frac{p+1}{2}\right)^2$$

modulo p. It follows from LEMMA 2 that

$$\begin{cases}\lfloor\frac{2\alpha_i}{p}\rfloor-2\lfloor\frac{\alpha_i}{p}\rfloor=0,\\ \lfloor-\frac{2\alpha_i}{p}\rfloor-2\lfloor-\frac{2\alpha_i}{p}\rfloor=1,\end{cases}$$

when $i \in \left\{1, \cdots, \frac{p-1}{4}\right\}$. It therefore follows that

$$\begin{aligned}
& \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{4}} \left(\left\lfloor \frac{2\alpha_i}{p} \right\rfloor - 2 \left\lfloor \frac{\alpha_i}{p} \right\rfloor \right) + 2 \sum_{i=1}^{\frac{p-1}{4}} \left(\left\lfloor -\frac{2\alpha_i}{p} \right\rfloor - 2 \left\lfloor -\frac{\alpha_i}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{4}} 0 + 2 \sum_{i=1}^{\frac{p-1}{4}} 1 \\
= \; & \frac{p-1}{2}.
\end{aligned}$$

□

Second Solution. Since -1 is a quadratic residue modulo p, we can write $\lambda^2 \equiv -1 \; (mod \; p)$ for some $\lambda \in \mathfrak{M}_p := \{1, \cdots, p-1\}$. The number theoretical idea we employ here is the fact that the map $k \mapsto \lambda k$ yields an equivalence relation on the set $\mathfrak{M}_p$. We split the proof in two steps.

Lemma 3. *Let $\alpha, \beta \notin \mathbb{Z}$ with $\alpha + \beta \in \mathbb{Z}$. Then, we obtain*

$$\lfloor \alpha \rfloor + \lfloor \beta \rfloor = \alpha + \beta - 1.$$

When $a + b \equiv 0 \; (mod \; p)$ and when p does not divide a and b, we have

$$\left\lfloor \frac{2a}{p} \right\rfloor - 2 \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2b}{p} \right\rfloor - 2 \left\lfloor \frac{b}{p} \right\rfloor = \left\lfloor \frac{2a}{p} \right\rfloor + \left\lfloor \frac{2b}{p} \right\rfloor - 2 \left(\left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{b}{p} \right\rfloor \right) = 1.$$

Lemma 4. *Let $\zeta : \mathfrak{M}_p \to \mathfrak{M}_p$ be the function with $\zeta(k) \equiv \lambda k \; (mod \; p)$.*

(A) Since the function ζ satisfies the equation $\zeta^{(2)}(k) = \zeta(\zeta(k)) = -k$ for all $k \in \mathfrak{M}_p$, we see that $\zeta^{(4)} = \zeta \circ \zeta \circ \zeta \circ \zeta$ is the identity function on $\mathfrak{M}_p$. The bijection ζ naturally offers a partition of the set $\mathfrak{M}_p$ into sets of the type $\left\{k, \zeta(k), \zeta^{(2)}(k), \zeta^{(3)}(k)\right\} = \{k, \zeta(k), -k, -\zeta(k)\}$.[1]

(B) When $k \in \mathfrak{M}_p$, we obtain

$$\begin{cases} \left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = 1, \\ \left\lfloor \frac{2(-k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{(-k)^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(-k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{\zeta(-k)^2}{p} \right\rfloor = 1. \end{cases} \tag{2}$$

Hence, each equivalence class $\{k, \zeta(k), -k, -\zeta(k)\}$ which has four distinct elements contributes 2 in the sum.

Since there are $\frac{p-1}{4}$ quadruples, we conclude that the total sum is $\frac{p-1}{2}$.

PROOF OF LEMMA 4 The first claim comes easily from the definition of the map ζ. For the second part, since $k^2 + \zeta(k)^2 \equiv 0 \; (mod \; p)$, LEMMA 3 implies the result. □

[1] In other words, $\mathfrak{M}_p$ is a union of distinct orbits of ζ.

Third Solution. Since -1 is a quadratic residue modulo p, we can write $\lambda^2 \equiv -1 \ (mod\ p)$ for some $\lambda \in \mathfrak{M}_p := \{1, \cdots, p-1\}$.

Lemma 5. *Let $\zeta : \mathfrak{M}_p \to \mathfrak{M}_p$ be the function with $\zeta(k) \equiv \lambda k \ (mod\ p)$. Then, the map ζ is a bijection. When $k \in \mathfrak{M}_p$, we obtain*

$$\begin{cases} \left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = \frac{k^2}{p} + \frac{\zeta(k)^2}{p} - 1, \\ \left\lfloor \frac{2k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor = \frac{2k^2}{p} + \frac{2\zeta(k)^2}{p} - 1. \\ \left\lfloor \frac{2k^2}{p} \right\rfloor - 2\left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2\left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = 1. \end{cases}$$

PROOF OF LEMMA 5 The first claim comes easily from the definition of the map ζ. Consider the second part. Since p is prime, it is clear that $\frac{k^2}{p} \notin \mathbb{Z}$. Since $k^2 + \zeta(k)^2 \equiv 0 \ (mod\ p)$ or $\frac{k^2}{p} + \frac{\zeta(k)^2}{p} \in \mathbb{Z}$, this and LEMMA 3 give the first identity. Similarly, LEMMA 3 yields the second one. The third one follows from these two identities.

Now, we compute the sum. Set

$$S(p) = \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2k^2}{p} \right\rfloor - 2\left\lfloor \frac{k^2}{p} \right\rfloor \right),$$

$$T(p) = \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2\left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor \right).$$

On the one hand, since $\zeta(1), \cdots, \zeta(p-1)$ is a permutation of $1, \cdots, p-1$, we obtain

$$S(p) = T(p).$$

On the other hand, the last summation identity in LEMMA 5 implies that

$$S(p) + T(p) = p - 1.$$

It therefore follows that $S(p) = T(p) = \frac{S(p)+T(p)}{2} = \frac{p-1}{2}$. □