Problem 11529
(American Mathematical Monthly, Vol.117, October 2010)

Proposed by W. Blumberg (USA).

For $n \geq 1$, let

$$A_n = 3\sum_{k=1}^{n}\left\lfloor \frac{k^2}{n}\right\rfloor - n^2.$$

Let p and q be distinct primes with $p \equiv q \pmod 4$. Show that $A_{pq} = A_p + A_q - 2$.

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

Let $r_n(m)$ be the remainder of the division of m by n then, since $m = n\lfloor m/n\rfloor + \mathrm{r}_n(m)$, we have that

$$\begin{aligned} A_n &= 3\sum_{k=1}^{n}\left\lfloor \frac{k^2}{n}\right\rfloor - n^2 = \frac{3}{n}\sum_{k=1}^{n} k^2 - \frac{3}{n}\sum_{k=1}^{n} r_n(k^2) - n^2 \\ &= \frac{(n+1)(2n+1)}{6} - n^2 - \frac{1}{n}\sum_{k=1}^{n} r_n(k^2) = \frac{3n+1}{2} - \frac{3}{n}\sum_{k=0}^{n-1} r_n(k^2). \end{aligned}$$

Let p and q be two distinct odd primes (by hypothesis p and q are different from 2). Note that $r_p(k^2) = j$ for some $j \in \{1,\ldots,p-1\}$ iff $k^2 = j \bmod p$, that is iff j is a square mod p which means that $\left(\frac{j}{p}\right) = 1$ where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Therefore the number of $k \in \{1,\ldots,p-1\}$ such that $r_p(k^2) = j$ is $\left(\frac{j}{p}\right) + 1$ (it gives 0 or 2) and

$$\sum_{k=0}^{p-1} r_p(k^2) = \sum_{j=0}^{p-1}\left(\left(\frac{j}{p}\right)+1\right) j.$$

In a similar way, by the Chinese Remainder Theorem,

$$\sum_{k=0}^{pq-1} r_{pq}(k^2) = \sum_{j=0}^{pq-1}\left(\left(\frac{j}{p}\right)+1\right)\left(\left(\frac{j}{q}\right)+1\right) j.$$

Hence

$$A_p = 2 - \frac{3}{p}\sum_{j=0}^{p-1}\left(\frac{j}{p}\right) j, \quad A_q = 2 - \frac{3}{q}\sum_{j=0}^{q-1}\left(\frac{j}{q}\right) j$$

and

$$A_{pq} = 2 - \frac{3}{pq}\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right) j - \frac{3}{pq}\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right) j - \frac{3}{pq}\sum_{j=0}^{pq-1}\left(\frac{j}{q}\right) j.$$

Since $\sum_{j=0}^{p-1}\left(\frac{j}{p}\right) = 0$, it follows that

$$\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right) j = \sum_{a=0}^{q-1}\sum_{r=0}^{p-1}\left(\frac{ap+r}{p}\right)(ap+r) = p\sum_{a=0}^{q-1} a\sum_{r=0}^{p-1}\left(\frac{r}{p}\right) + q\sum_{r=0}^{p-1}\left(\frac{r}{p}\right) r = q\sum_{r=0}^{p-1}\left(\frac{r}{p}\right) r.$$

So, it suffices to prove that for $p = q \pmod 4$

$$\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right) j = 0.$$

We first notice that $p = q = 1 \pmod 4$ or $p = q = 3 \pmod 4$ and in both cases

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

which implies

$$\sum_{j=1}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right)j = \sum_{j=1}^{pq-1}\left(\frac{pq-j}{p}\right)\left(\frac{pq-j}{q}\right)(pq-j) = \sum_{j=1}^{pq-1}\left(\frac{-j}{p}\right)\left(\frac{-j}{q}\right)(pq-j) = \sum_{j=1}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right)(pq-j)$$

that is

$$2\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right)j = pq\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right).$$

Moreover

$$\sum_{j=0}^{pq-1}\left(\frac{j}{p}\right)\left(\frac{j}{q}\right) = \sum_{a=0}^{q-1}\sum_{r=0}^{p-1}\left(\frac{ap+r}{p}\right)\left(\frac{ap+r}{q}\right) = \sum_{r=0}^{p-1}\left(\frac{r}{p}\right)\sum_{a=0}^{q-1}\left(\frac{ap+r}{q}\right) = \sum_{r=0}^{p-1}\left(\frac{r}{p}\right)\sum_{k=0}^{q-1}\left(\frac{k}{q}\right) = 0$$

because p and q are distinct primes and

$$\{ap + r \pmod q) : a = 0, \ldots, q-1\} = \{k \pmod q : k = 0, \ldots, q-1\}.$$

$\square$