Thus

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

so

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

Now

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

since for each r, the set $\{ap+r\colon\ 0\le a\le q-1\}$ is a complete system of residues modulo q.

Also solved by O. P. Lossers (Netherlands), R. E. Prather, Barclays Capital Problems Solving Group (U.K.), and the proposer.

A Prime Multiple of the Identity Matrix

11532 [2010, 834]. *Proposed by Cezar Lupu (student), University of Bucharest, Bucharest, Romania, and Vicentiu Rădulescu, Institute of Mathematics "Simon Stoilow" of the Romanian Academy, Bucharest, Romania.* Find all prime numbers p such that there exists a 2×2 matrix A with integer entries, other than the identity matrix I, for which $A^p+A^{p-1}+\cdots+A=pI$.

Solution by Stephen Pierce, San Diego State University, San Diego, CA. The only primes that qualify are 2 and 3. Let $f(x)=-px^0+\sum_{i=1}^{p}x^i$.

For $p=2$, let $A=\left(\begin{smallmatrix}1&0\\0&-2\end{smallmatrix}\right)$. For $p=3$, note that $f(x)=(x-1)(x^2+2x+3)$. Let A be the "companion matrix" of x^2+2x+3, that is, $A=\left(\begin{smallmatrix}0&-3\\1&-2\end{smallmatrix}\right)$. We obtain $A^2+2A+3I=\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.

For $p\ge 5$, we make some elementary observations about f.

(a) From the triangle inequality, $f(x)=0$ for x in the closed unit disk only when $x=1$.

(b) The root 1 is a simple root (by differentiation).

(c) If $f(A)=0$, then the minimal polynomial of A divides f.

Given a matrix A with $f(A)=0$, let λ and μ be the eigenvalues of A. If A is a multiple of the identity, then λ is an integer dividing p, and $f(\lambda)$ has the same sign as λ. The only such solution is $A=I$.

If A is not a multiple of the identity, then $\lambda\mu$ is an integer dividing p, by (c). Since p is prime, $|\lambda\mu|\in\{1,p\}$. If $|\lambda\mu|=1$, then $\lambda=\mu=1$ from (a), but this contradicts (b). If $|\lambda\mu|=p$, then then the product of the other roots of f is ±1. Now the rest of the roots must all be 1, which contradicts (b) when $p>3$.