Problem 12234
(American Mathematical Monthly, Vol.128, February 2021)

Proposed by N. Osipov (Russia).

Let c, and let $Ax^2 + Bxy + Cy^2$ be a quadratic form with A, B, and C in $\mathbb{Z}$as soon asas soon as such that $B^2 - 4AC$ is neither a multiple of p nor a perfect square modulo p. Prove that

$$\prod_{0<x<y<p} (Ax^2 + Bxy + Cy^2)$$

is 1 modulo p if exactly one or all three of A, C, and $A + B + C$ are perfect squares modulo p and is -1 modulo p otherwise.

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

Solution. We first note that A, C, and $A+B+C$ are not multiple of p otherwise, $D := B^2 - 4AC$ is equal respectively to B^2, B^2, $(A-C)^2$ modulo p which are perfect squares. Moreover $Ax^2+Bxy+Cy^2$ is a multiple of p if and only if both x and y are multiple of p, otherwise again D is a perfect square modulo p.
Since $x^2 \equiv a \pmod p$ has $1 + \left(\frac{a}{p}\right)$ solutions in $\{0, 1, \dots, p-1\}$, it follows that for any integer $0 < n < p$ the number of solutions in $\{0, 1, \dots, p-1\}^2$ of the congruence $Ax^2 + Bxy + Cy^2 \equiv n \pmod p$, i.e. $(2Ax + By)^2 \equiv Dy^2 + 4An \pmod p$ is

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{Dy^2 + 4An}{p}\right)\right) = p + \left(\frac{D}{p}\right) \sum_{y=0}^{p-1} \left(\frac{y^2 + 4AnD^{-1}}{p}\right) = p - \left(\frac{D}{p}\right) = p + 1$$

where we applied the known fact that $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = -1$ when p is an odd prime and a is not a multiple of p.
Therefore, the number of solutions of the same congruence with the restriction $0 < x < y < p$ is

$$\frac{1}{2}\Big(p + 1 - \Big(\underbrace{1 + \left(\frac{A}{p}\right)\left(\frac{n}{p}\right)}_{y=0}\Big) - \Big(\underbrace{1 + \left(\frac{C}{p}\right)\left(\frac{n}{p}\right)}_{x=0}\Big) - \Big(\underbrace{1 + \left(\frac{A+B+C}{p}\right)\left(\frac{n}{p}\right)}_{x=y}\Big)\Big)$$
$$= \begin{cases} \frac{p-2-M}{2} & \text{if } n \text{ is a perfect square modulo } p, \\ \frac{p-2+M}{2} & \text{otherwise,} \end{cases}$$

with $M := \left(\frac{A}{p}\right) + \left(\frac{C}{p}\right) + \left(\frac{A+B+C}{p}\right)$ (which is an odd integer).

By Wilson's Theorem $(p-1)! \equiv -1 \pmod p$, and we have that

$$\prod_{0<n<p, \left(\frac{n}{p}\right)=1} n \equiv \prod_{k=1}^{\frac{p-1}{2}} k^2 \equiv (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \prod_{k=1}^{\frac{p-1}{2}} (p-k) = (-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Finally

$$\begin{aligned} \prod_{0<x<y<p} (Ax^2 + Bxy + Cy^2) &\equiv \left(\prod_{0<n<p, \left(\frac{n}{p}\right)=1} n\right)^{\frac{p-2-M}{2}} \cdot \left(\prod_{0<n<p, \left(\frac{n}{p}\right)=-1} n\right)^{\frac{p-2+M}{2}} \\ &= \left(\prod_{0<n<p, \left(\frac{n}{p}\right)=1} n\right)^{-M} \cdot ((p-1)!)^{\frac{p-2+M}{2}} \\ &\equiv (-1)^{-\frac{p+1}{2}M + \frac{p-2+M}{2}} = (-1)^{\frac{M-3}{2}} \pmod p \end{aligned}$$

which is 1 if exactly one or all three of A, C, and $A + B + C$ are perfect squares modulo p and is -1 otherwise. □