A Congruence for a Product of Quadratic Forms

12234 [2021, 179]. Proposed by Nicolai Osipov, Siberian Federal University, Krasnoyarsk, Russia. Let $p$ be an odd prime, and let $Ax^2 + Bxy + Cy^2$ be a quadratic form with $A, B,$ and $C$ in $\mathbb{Z}$ 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 by O. P. Lossers, Eindhoven University of Technology, Eindhoven, The Netherlands. Most expressions indicate modular arithmetic in the finite field $\mathbb{F}_p$ with $p$ elements. We first study the desired product in general, leaving until later a consideration of how many elements of $\{A, C, A + B + C\}$ are squares. For convenience, define

$$Q(x, y) = Ax^2 + Bxy + Cy^2.$$  

Since we are given that $B^2 - 4AC$ is a nonsquare, $A$ and $C$ must be nonzero, and it follows that $Q(x, y) \neq 0$ when $(x, y) \neq (0, 0)$. In order to evaluate the product $\prod_{0 < x < y < p} Q(x, y)$, we want to group the factors by the value of $Q(x, y)$. That is, for each $D$ we seek the number of solutions of $Q(x, y) = D$ such that $0 < x < y < p$.

For $D \neq 0$, since $Q(x, y) - Dz^2 = 0$ is nondegenerate, there are altogether $p^2 - 1$ solution triples $(x, y, z)$ to $Q(x, y) - Dz^2 = 0$. The set of solution triples is invariant under multiplication by any nonzero element of $\mathbb{F}_p$. Hence the solutions come in $p + 1$ multiplicative classes of size $p - 1$, each containing one triple of the form $(x, y, 1)$, yielding $p + 1$ solutions to $Q(x, y) = D$.

This partitions the set of nonzero pairs $(x, y)$ by the value of $Q(x, y)$, with each value $D$ occurring exactly $p + 1$ times. Note that $Q(x, y) = Q(p - x, p - y)$, so for fixed $D$ the number of pairs satisfying $Q(x, y) = D$ with $x < y$ equals the number of pairs with $x > y$. Hence we will need to divide the number of occurrences of $D$ by 2.

Since we require $0 < x < y < p$ in the stated product, we must also exclude occurrences of $D$ that arise when $x = 0$, $y = 0$, or $x = y$. Two nonzero elements of $\mathbb{F}_p$ have the same quadratic character if they are both squares or both nonsquares, equivalent to their ratio being a square. Occurrences of $D$ on the line $x = 0$ have $Cy^2 - D = 0$, or $y^2 = D/C$, so there will be two such pairs yielding $D$ when $D$ and $C$ have the same quadratic character; otherwise none. Similarly, there are two occurrences of $D$ on $y = 0$ if and only if $A$ and $D$ have the same quadratic character (satisfying $x^2 = D/A$), and two occurrences of $D$ on $x = y$ if and only if $A + B + C$ and $D$ have the same quadratic character (satisfying $x^2 = D/(A + B + C)$). Also, such occurrences on the three lines are distinct.

Let the number of squares among $\{A, C, A + B + C\}$ be $s$. Starting with the $p + 1$ pairs $(x, y) \in \mathbb{F}_p^2 - (0, 0)$ that generate $D$, we subtract the occurrences with
\(x = 0, \ y = 0, \) or \(x = y\) and then divide the remaining occurrences by 2, as discussed above. We thus compute that each square \(D\) occurs in the product \((p+1−2s)/2\) times, while each non-square \(D\) occurs in the product \((p+1−2[3−s])/2\) times.

This tells us how many times we have the product of all the squares and how many times we have the product of all the nonsquares. It is well known that the product of all the squares is \((-1)^{(p+1)/2}\), and the product of all the non-squares is \((-1)^{(p−1)/2}\). This uses the fact that an element and its reciprocal have the same quadratic character. After canceling reciprocal pairs and ignoring 1, we are left with \(-1\), which is a square if and only if \(p \equiv 1 \mod 4\).

We thus compute
\[
\prod_{0 < x < y < p} Q(x, y) = (-1)^{\frac{1}{2}(p+1)}\frac{1}{2}(p+1−2s)(-1)^{\frac{1}{2}(p−1)}\frac{1}{2}(p+1+2s−6)
\]
\[
= (-1)^{\frac{1}{2}[(p+1)^2+(p^2−1)−4s−6(p−1)]}
\]
\[
= (-1)^{\frac{1}{2}(p^2−2p+3−2s)} = (-1)^{\frac{1}{2}(p−1)^2+2−2s} = (-1)^{1−s}.
\]

By definition, \((-1)^{1−s}\) equals 1 or \(-1\) when the number \(s\) of squares in \(\{A, C, A+B+C\}\) is odd or even, respectively, as desired.

Also solved by C. Curtis & J. Boswell, Y. J. Ionin, R. Tauraso (Italy), and the proposer.