**Lemma 3.1 (Gauss)** *Given an odd prime $p$ and an integer $m$ not a multiple of $p$, then $x^2 \equiv m \pmod{p}$ has a solution $x$ (no solution $x$) if $\mu$ is even (odd), where $\mu$ is the number of residues (mod $p$) among*

$$[m], [2m], [3m], \ldots, [\frac{1}{2}(p-1)m]$$

*that are equal to residues between $-\frac{1}{2}p$ and 0.*

**Proof.** Let $[-r_1], \ldots, [-r_\mu]$ be the above-mentioned $\mu$ residues where $-\frac{1}{2}p < -r_i < 0$ for each $i = 1, \ldots, \mu$. Let $[r'_1], \ldots, [r'_\lambda]$ be the remaining residues among $\{[am] \mid a = 1, 2, \ldots, \frac{1}{2}(p-1)\}$ with representatives $r'_i$ chosen where $0 < r'_i < \frac{1}{2}p$. Note that $\lambda + \mu = \frac{1}{2}(p-1)$.

It is easy to check that the integers $r'_1, \ldots, r'_\lambda, r_1, \ldots, r_\mu$ just form a reordering of the integers $1, 2, \ldots, \frac{1}{2}(p-1)$. For example, if $r'_i = r_j$, then $am \equiv -bm \pmod{p}$ for some distinct integers a and b. Then $p \mid (a+b)m$, so $p \mid a+b$ since $p$ does not divide $m$. But $0 < a+b \leq p-1$. The other two cases are similarly covered.

Multiplying all listed residue classes in $Z_p$ yields

$$[m][2m]\cdots[\frac{1}{2}(p-1)m] = [r'_1]\cdots[r'_\lambda][-r_1]\cdots[-r_\mu] =$$

$$[1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1)][m]^{\frac{1}{2}(p-1)} = [(-1)^\mu][1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1)]$$

so division gives

$$[m]^{\frac{1}{2}(p-1)} = [(-1)^\mu]$$

But $m^{\frac{1}{2}(p-1)} \equiv (\frac{m}{p}) \pmod{p}$ by the proposition, so we have shown that $(\frac{m}{p}) = (-1)^\mu$. □