Quadratic residues

DEF $x \pmod n$ is a **quadratic residue** if $x \equiv y^2 \pmod n$ for some y

EG mod 11: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$
$(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 \equiv 3$

quadratic residues mod 11 : 0, 1, 3, 4, 5, 9

note Of the $\phi(11) = 10$ invertible residues, exactly 5 ($= \frac{1}{2}\phi(11)$) are quadratic.

$y^2 \equiv 4 \pmod{11}$ only 2 solutions

EG mod 15: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$
$(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv 10$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$

quadratic residues mod 15 : 0, 1, 4, 6, 9, 10 (invertible)

$\phi(3)\,\phi(5)$

note Of the $\phi(15) = 8$ invertible residues, exactly 2 ($= \frac{1}{4}\phi(15)$) are quadratic.

$y^2 \equiv 4 \pmod{15}$ 4 solutions $\pm 2, \pm 7$
$\left[\iff y \equiv \pm 2 \pmod 3 \text{ and } y \equiv \pm 2 \pmod 5\right]$

$y^2 \equiv 9 \pmod{15}$ (not invertible) only 2 solutions
$\left[\iff y \equiv \pm 3 \pmod 3 \text{ and } y \equiv \pm 3 \pmod 5\right]$
$\equiv 0$

THM Let p, q, r be distinct odd primes.

invertible quadratic residues mod p $= \frac{1}{2}\phi(p)$ ($p-1$)
— " — mod pq $= \frac{1}{4}\phi(pq)$ ($(p-1)(q-1)$)
— " — mod pqr $= \frac{1}{8}\phi(pqr)$ ($(p-1)(q-1)(r-1)$)