

Q4

4. 6 is a quadratic residue modulo 19.

Use prop. 45.3 to find its square roots.

$$(\pm 9^{(p+1)/4}) \bmod p = (\pm 6^{(19+1)/4}) \bmod 19$$

$$= (\pm 6^5) \bmod 19$$

$$= \pm 7776 \bmod 19$$

$$= 2, 11$$