Basic facts about quadratic residues

For $p, q$ odd primes we write $\hat{p} = \frac{p-1}{2}, \hat{q} = \frac{q-1}{2}$. Note that $p$ is an upper prime if $\hat{p}$ is even, and $p$ is a lower prime if $\hat{p}$ is odd.

1. For any $n, Q_n$ is a subgroup of $U_n$ of order $\frac{|U_n|}{|K_n|}$, where $K_n = \{x|x^2 = 1\}$ is the kernel of the map $x \mapsto x^2$ from $U_n$ to itself.

2. For arbitrary integers $m, n$ one has $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$.

3. If $U_m$ has a primitive root $g$, then $Q_m$ consists of the even powers of $g$.

4. Euler’s Criterion: $\left(\frac{n}{p}\right) \equiv n^{\hat{p}} \mod(p)$

5. Gauss’s Lemma: $\left(\frac{n}{p}\right) = (-1)^\mu$, where $\mu$ is the number of negative least residues congruent to the numbers $n, 2n, \cdots, \hat{pn}$.

6. $\left(\frac{-1}{p}\right) = (-1)^{\hat{p}}$. In words: $-1$ is a quadratic residue mod($p$) if and only if $\hat{p}$ is even, and it is not one if and only if $\hat{p}$ is odd.

7. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. In words: 2 is a quadratic residue mod($p$) if and only if $p \equiv 1$ or 7 mod(8). It is not one if and only if $p \equiv 3$ or 5 mod(8).

8. Gauss’s Quadratic Reciprocity Theorem: $\left(\frac{p}{q}\right) = (-1)^{\hat{p} \hat{q}} \left(\frac{q}{p}\right)$. In words: $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless both $p$ and $q$ are lower primes, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

9. If the modulus is an odd prime power $p^e$ then $n \in Q_{p^e} \iff n \in Q_p$.

10. If the modulus is a power $2^e$ of 2 then

   - $e = 1$: $n \in Q_2 \iff n \equiv 1 \mod(2)$.
   - $e = 2$: $n \in Q_4 \iff n \equiv 1 \mod(4)$.
   - $e \geq 3$: $n \in Q_{2^e} \iff n \equiv 1 \mod(8)$, $e \geq 3$.

   In particular if $n \equiv 1 \mod(8)$ then $n$ is a quadratic residue mod any power of 2.

11. Composite modulus $m = \prod_{j=1}^{k} p_j^{e_j}$: $n \in Q_m \iff n \in Q_{p_j} \forall j$. 