Quadratic Residue Summary and Examples

Summary of Theorems and Properties

Quadratic Residues and Non-residues: An element $a \in \mathbb{Z}_p^*$ is a *quadratic residue* modulo p if the congruence $x^2 \equiv_p a$ has a solution. $a \in \mathbb{Z}_p^*$ is a *quadratic non-residue* modulo p if the congruence $x^2 \equiv_p a$ does *not* have a solution.

Euler's Criterion:

- $a \in \mathbb{Z}_p^*$ is a quadratic residue if and only if $a^{\frac{p-1}{2}} \equiv_p +1$.
- $a \in \mathbb{Z}_p^*$ is a quadratic non-residue if and only if $a^{\frac{p-1}{2}} \equiv_p -1$.

Legendre Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic non-residue} \\ 0 & \text{if } \gcd(a,p) \neq 1 \end{cases}$$

Various facts used to compute $\left(\frac{a}{p}\right)$. For all of these, let p, q be odd primes ($p \neq q$) and $a \in \mathbb{Z}_p^*$.

- (Restating Euler's Criterion) $\left(\frac{a}{p}\right) = +1 \iff a^{\frac{p-1}{2}} \equiv_p +1$, and $\left(\frac{a}{p}\right) = -1 \iff a^{\frac{p-1}{2}} \equiv_p -1$.
- $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$
- If $a \equiv_p b$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$
- (Law of Quadratic Reciprocity)

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$$

(The book states it slightly differently - I think this way is more convenient when performing calculations.)

- (Gauss' Lemma) Let n be the number of elements in the set $S = \left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$ that reduce to an element greater than $\frac{p}{2}$ modulo p. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Here are a few specific values of which you should be aware. There are others stated in the book and homework, but these are the most important:

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Examples

1.
$$\begin{aligned}\left(\frac{3}{97}\right) &= (-1)^{\frac{97-1}{2}\frac{3-1}{2}}\left(\frac{97}{3}\right) \\ &= (-1)^{48}\left(\frac{97}{3}\right) \\ &= \left(\frac{1}{3}\right) \\ &= 1\end{aligned}$$

2.
$$\begin{aligned}\left(\frac{3}{389}\right) &= (-1)^{\frac{389-1}{2}\cdot\frac{3-2}{1}}\left(\frac{389}{3}\right) \\ &= (-1)^{194}\left(\frac{389}{3}\right) \\ &= \left(\frac{2}{3}\right) \\ &= -1\end{aligned}$$

3. $\left(\frac{22}{11}\right) = 0$

4.

$$\begin{aligned}
\left(\frac{5!}{7}\right) &= \left(\frac{5}{7}\right)\left(\frac{4}{7}\right)\left(\frac{3}{7}\right)\left(\frac{2}{7}\right)\left(\frac{1}{7}\right) \\
&= \left(\frac{5}{7}\right)\left(\frac{2}{7}\right)^2\left(\frac{3}{7}\right)\left(\frac{2}{7}\right)\left(\frac{1}{7}\right) = \left(\frac{5}{7}\right)\left(\frac{3}{7}\right)\left(\frac{2}{7}\right)^3 \cdot 1 \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{5}\right)(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{3}\right)\cdot 1^3 \\
&= (-1)^6\left(\frac{2}{5}\right)(-1)^3\left(\frac{1}{3}\right) \\
&= (1)(-1)(-1)(1) = 1
\end{aligned}$$

5.

$$\begin{aligned}
\left(\frac{880}{863}\right) &= \left(\frac{2^4\cdot 5\cdot 11}{863}\right) \\
&= \left(\frac{2}{863}\right)^4\left(\frac{5}{863}\right)\left(\frac{11}{863}\right) \\
&= 1\cdot(-1)^{\frac{5-1}{2}\cdot\frac{863-1}{2}}\left(\frac{863}{5}\right)(-1)^{\frac{11-1}{2}\cdot\frac{863-1}{2}}\left(\frac{863}{11}\right) \\
&= \left(\frac{3}{5}\right)(-1)\left(\frac{5}{11}\right) \\
&= (-1)(-1)\left(\frac{5}{11}\right) \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{5}\right) \\
&= \left(\frac{1}{5}\right) \\
&= 1
\end{aligned}$$

6. "Show that there are infinitely many primes of the form $4k+1$."

Proof. Assume that there are finitely many such primes, say $p_1 (= 5), p_2, \ldots, p_n$, and let $N = 4{p_1}^2 \ldots {p_n}^2 + 1$ and $x = 2p_1 \ldots p_n$. Now N is of the form $4k+1$, and $N > p_i$ for all i, so N must be composite. Since N is odd, it's prime divisors are odd (and not of the form $4k+1$). If p is a prime divisor of N, $p|x^2+1$, so $x^2+1 \equiv_p 0$ and $x^2 \equiv_p -1$. Thus -1 is a quadratic modulo p, so $p \equiv 1 \mod 4$ (by exercise 4.1.6) and $p = 4k+1$ for some k. But then $p|N$ and $p|p_1 \ldots p_n$ implies $p|4{p_1}^2 \ldots {p_n}^2$ (since p is one of those primes) and thus $p|N-(N-1) = 1$, a contradiction. Thus there are infinitely many such primes. **Q.E.D.**

7. "Show that there are infinitely many primes of the form $6k+1$." [Proof uses the result of and hint from Exercise 4.3.4.]

Proof. Assume that there are finitely many such primes, say $p_1 (= 7), p_2, \ldots, p_n$, and let $N = 4{p_1}^2 \ldots {p_n}^2 + 3$ and $x = 2p_1 \ldots p_n$. Note that $N > p_i$ for all i, and $N = 4(6(\ldots)+1)+3 \equiv_6 7 \equiv_6 1$ so N is of the form $6k+1$, and so N must be composite. Since N is odd, it's prime

divisors are odd (and not of the form $6k+1$). If p is a prime divisor of N, $p|x^2+3$, so $x^2+3 \equiv_p 0$ and $x^2 \equiv_p -3$. Thus -3 is a quadratic modulo p, so $p \equiv 1 \mod 6$ (by exercise 4.3.4) and $p = 6k+1$ for some k. But then $p|N$ and $p|p_1 \dots p_n$ implies $p|4{p_1}^2 \dots {p_n}^2$ (since p is one of those primes) and thus $p|N-(N-1) = 1$, a contradiction. Thus there are infinitely many such primes. **Q.E.D.**