

## QUADRATIC RESIDUES

**DEFINITION:** We say that an element  $x \in \mathbb{Z}_n$  is a **square** or a **quadratic residue** if there is some  $y \in \mathbb{Z}_n$  such that  $y^2 = x$ , and in this case, we call  $y$  a **square root** of  $x$ .

- (1) Let  $n$  be an odd positive integer. Suppose that  $[a]$  is a unit in  $\mathbb{Z}_n$ . Show that<sup>1</sup> the solutions  $x$  to the equation  $[a]x^2 + [b]x + [c] = [0]$  in  $\mathbb{Z}_n$  are exactly the elements of the form

$$x = \frac{-[b] + u}{[2a]} \quad \text{such that } u \text{ is a square root of } [b^2 - 4ac].$$

- (2) Let  $p$  be an odd prime and  $x \in \mathbb{Z}_p^\times$ . Show that if  $x$  is a quadratic residue, then  $x$  has exactly two square roots  $y \neq y'$ , and for these roots,  $y' = -y$ .
- (3) Let  $p$  be a prime number and  $g$  be a primitive root of  $\mathbb{Z}_p$ . Show that  $[n] \in \mathbb{Z}_p^\times$  is a quadratic residue if and only if the index of  $[n]$  with respect to  $g$  is even.

**DEFINITION:** Let  $p$  be an odd prime. For  $r \in \mathbb{Z}$  not a multiple of  $p$  we define the **Legendre symbol** of  $r$  with respect to  $p$  as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

**THEOREM (EULER'S CRITERION):** For  $p$  an odd prime and  $r \in \mathbb{Z}$  not a multiple of  $p$ , we have

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} \pmod{p}.$$

**THEOREM (QUADRATIC RECIPROCITY PART -1):** If  $p$  is odd, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}.$$

**PROPOSITION:** Let  $p$  be an odd prime and  $a, b$  integers not divisible by  $p$ . Then

- (1)  $a \equiv b \pmod{p}$  implies that  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .
- (2)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .
- (3)  $\left(\frac{a^2}{p}\right) = 1$ .

---

<sup>1</sup>Hint: Complete the square!

- (4) (a) Without using the Proposition above, explain why  $\left(\frac{4}{p}\right) = 1$  for  $p$  an odd prime. Now explain why part (3) of the Proposition above is true in general.
- (b) Use the Proposition above to explain the following: If  $a, b$  are not squares modulo  $p$ , then  $ab$  is a square modulo  $p$ .
- (c) Use<sup>2</sup> the Proposition and Corollary above to determine how many solutions  $x$  to
- $$[3]x^2 + [12]x - [2] = [0]$$
- there are in  $\mathbb{Z}_{43}$ .
- (5) Use problem #3 to prove Euler's criterion.
- (6) Prove the proposition above.
- (7) Use Euler's criterion to prove QR part  $-1$  above.
- (8) When  $n$  is not a prime...
- (a) Does the conclusion of #4(b) hold if  $n$  is replaced by a general positive integer  $n$  instead of a prime  $p$ ?
- (b) Suppose that  $n = pq$  for primes  $p \neq q$ . Show that  $a$  is a quadratic residue modulo  $n$  if and only if  $a$  is a quadratic residue modulo  $p$  and a quadratic residue modulo  $q$ .

---

<sup>2</sup>You might find it convenient to write  $168 = 4 \cdot 42$ .