

# Chapter 4

## Quadratic residues

### 4.1 Quadratic residues and nonresidues

**Definition (Quadratic residues and nonresidues)** Let  $m \in \mathbf{N}$  and  $a \in \mathbf{Z}$  be such that  $(a, m) = 1$ . Then  $a$  is called a **quadratic residue modulo  $m$**  if the congruence

$$(4.1) \quad x^2 \equiv a \pmod{m}$$

has a solution (i.e., if  $a$  is a “perfect square modulo  $m$ ”), and  $a$  is called a **quadratic nonresidue modulo  $m$**  if (4.1) has no solution.

**Remarks** (i) Note that, by definition, integers  $a$  that do not satisfy the condition  $(a, m) = 1$  are not classified as quadratic residues or nonresidues. In particular, 0 is considered neither a quadratic residue nor a quadratic nonresidue (even though, for  $a = 0$ , (4.1) has a solution, namely  $x = 0$ ).

(ii) While the definition of quadratic residues and nonresidues allows the modulus  $m$  to be an arbitrary positive integer, in the following we will focus exclusively on the case when  $m$  is an *odd prime*  $p$ .

**Proposition 4.1 (Number of solutions to quadratic congruences)** Let  $p$  be an *odd prime*, and let  $a \in \mathbf{Z}$  with  $(a, p) = 1$ .

- (i) If  $a$  is a quadratic nonresidue modulo  $p$ , the congruence (4.1) has no solution.
- (ii) If  $a$  is a quadratic residue modulo  $p$ , the congruence (4.1) has exactly two incongruent solutions  $x$  modulo  $p$ . More precisely, if  $x_0$  is one solution, then a second, incongruent, solution is given by  $p - x_0$ .

**Proposition 4.2 (Number of quadratic residues and nonresidues)** Let  $p$  be an *odd prime*. Then among the integers  $1, 2, \dots, p - 1$ , exactly half (i.e.,  $(p - 1)/2$ ) are quadratic residues modulo  $p$ , and exactly half are quadratic nonresidues modulo  $p$ .

## 4.2 The Legendre symbol

**Definition (Legendre symbol)** Let  $p$  be an odd prime, and let  $a$  be an integer with  $(a, p) = 1$  (or, equivalently,  $p \nmid a$ ). The **Legendre symbol of  $a$  modulo  $p$** , denoted by  $\left(\frac{a}{p}\right)$ , is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a nonquadratic residue modulo } p. \end{cases}$$

**Remark** Note that the modulus in this definition, and in all results below, is restricted to odd primes (i.e., a prime other than 2). One can extend the definition, and most of the results, to composite moduli, but things get a lot more complicated then.

**Proposition 4.3 (Properties of the Legendre Symbol)** Let  $p$  be an odd prime, and let  $a, b \in \mathbf{Z}$  with  $(a, p) = 1$  and  $(b, p) = 1$ .

- (i) (Periodicity in numerator) If  $a \equiv b \pmod{p}$ , then  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .
- (ii) (Complete multiplicativity in numerator)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .
- (iii) (Value at squares)  $\left(\frac{a^2}{p}\right) = 1$ .
- (iv) (Value at  $-1$ )
 
$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$
- (v) (Value at 2)
 
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

**Proposition 4.4 (Euler's Criterion)** Let  $p$  be an odd prime, and let  $a \in \mathbf{Z}$  with  $(a, p) = 1$ . Then  $a$  is a quadratic residue modulo  $p$  if  $a^{(p-1)/2} \equiv 1 \pmod{p}$ , and a quadratic nonresidue if  $a^{(p-1)/2} \equiv -1 \pmod{p}$ ; equivalently,

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

**Proposition 4.5 (Gauss's Lemma)** Let  $p$  be an odd prime, and let  $a \in \mathbf{Z}$  with  $(a, p) = 1$ . Consider the  $(p-1)/2$  integers  $a, 2a, \dots, ((p-1)/2)a$ . Reduce each of these integers modulo  $p$ , obtaining  $(p-1)/2$  integers, all in the interval  $(0, p)$ . Let  $n$  be the number among those latter integers that are greater than  $p/2$  (i.e., which fall in the top half of the interval  $(0, p)$ ). Then  $a$  is a quadratic residue modulo  $p$  if  $n$  is even, and a quadratic nonresidue if  $n$  is odd; equivalently,

$$\left(\frac{a}{p}\right) = (-1)^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

### 4.3 The law of quadratic reciprocity

**Theorem 4.6 (Quadratic reciprocity law (Gauss 1795))** *Let  $p$  and  $q$  be distinct odd primes. Then*

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

*Equivalently,*

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

**Remarks** (i) The first form of the reciprocity law is the cleaner and more elegant form, and the one in which the law is usually stated. However, for applications, the second form is more useful. In this form the law says that numerator and denominator in a Legendre symbol (assuming both are distinct odd primes) can be interchanged in all cases except when both numerator and denominator are congruent to 3 modulo 4, in which case the sign of the Legendre symbol flips after interchanging numerator and denominator. Put differently, this form states that  $p$  is a quadratic residue modulo  $q$  if and only if  $q$  is a quadratic residue modulo  $p$ , except in the case when both  $p$  and  $q$  are congruent to 3 modulo 4; in the latter case  $p$  is a quadratic residue modulo  $q$  if and only if  $q$  is a quadratic nonresidue modulo  $p$ .

(ii) Note that the reciprocity law requires numerator and denominator to be distinct odd primes. In particular, it does not apply directly to cases where the numerator is composite, negative, or an even number. However, these cases can be reduced to the prime case using the multiplicativity of the Legendre symbol along with the special values at  $-1$  and  $2$  (see Proposition 4.3):

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

In fact, these last two relations are called the **First Supplementary Law** and **Second Supplementary Law**, as they “supplement” the quadratic reciprocity law.

(iii) Repeated application of the quadratic reciprocity law, along with the periodicity and multiplicativity properties of the Legendre symbol, allows one to quickly and efficiently compute Legendre symbols, even if the numbers involved are very large. The resulting algorithm is reminiscent of the gcd algorithm.