12

Quadratic residues and quadratic reciprocity

12.1 Quadratic residues

For positive integer n, an integer a is called a **quadratic residue modulo** n if $\gcd(a, n) = 1$ and $x^2 \equiv a \pmod{n}$ for some integer x; in this case, we say that x is a **square root of** a **modulo** n.

The quadratic residues modulo n correspond exactly to the subgroup of squares $(\mathbb{Z}_n^*)^2$ of $\mathbb{Z}_n^*$; that is, a is a quadratic residue modulo n if and only if $[a]_n \in (\mathbb{Z}_n^*)^2$.

Let us first consider the case where $n = p$, where p is an odd prime. In this case, we know that $\mathbb{Z}_p^*$ is cyclic of order $p-1$ (see Theorem 9.16). Recall that the subgroups any finite cyclic group are in one-to-one correspondence with the positive divisors of the order of the group (see Theorem 8.31). For any $d \mid (p-1)$, consider the d-power map on $\mathbb{Z}_p^*$ that sends $\alpha \in \mathbb{Z}_p^*$ to α^d. The image of this map is the unique subgroup of $\mathbb{Z}_p^*$ of order $(p-1)/d$, and the kernel of this map is the unique subgroup of order d. This means that the image of the 2-power map is of order $(p-1)/2$ and must be the same as the kernel of the $(p-1)/2$-power map. Since the image of the $(p-1)/2$-power map is of order 2, it must be equal to the subgroup $\{\pm 1\}$. The kernel of the 2-power map is of order 2, and so must also be equal to the subgroup $\{\pm 1\}$.

Translating from group-theoretic language to the language of congruences, we have shown:

Theorem 12.1. *For an odd prime p, the number of quadratic residues a modulo p, with $0 \leq a < p$, is $(p-1)/2$. Moreover, if x is a square root of a modulo p, then so is $-x$, and any square root y of a modulo p satisfies $y \equiv \pm x \pmod{p}$. Also, for any integer $a \not\equiv 0 \pmod{p}$, we have $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, and moreover, a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Now consider the case where $n = p^e$, where p is an odd prime and $e > 1$. We also know that $\mathbb{Z}_{p^e}^*$ is a cyclic group of order $p^{e-1}(p-1)$ (see Theorem 10.1), and so everything that we said in discussing the case $\mathbb{Z}_p^*$ applies here as well. In particular, for $a \not\equiv 0 \pmod{p}$, a is a quadratic residue modulo p^e if and only if $a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$. However, we can simplify this a bit. Note that $a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$ implies $a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p}$, and by Fermat's little theorem, this implies $a^{(p-1)/2} \equiv 1 \pmod{p}$. Conversely, by Theorem 10.2, $a^{(p-1)/2} \equiv 1 \pmod{p}$ implies $a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$. Thus, we have shown:

Theorem 12.2. *For an odd prime p and integer $e > 1$, the number of quadratic residues a modulo p^e, with $0 \le a < p^e$, is $p^{e-1}(p-1)/2$. Moreover, if x is a square root of a modulo p^e, then so is $-x$, and any square root y of a modulo p^e satisfies $y \equiv \pm x \pmod{p^e}$. Also, for any integer $a \not\equiv 0 \pmod{p}$, we have $a^{p^{e-1}(p-1)/2} \equiv \pm 1 \pmod{p}$, and moreover, a is a quadratic residue modulo p^e iff $a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$ iff $a^{(p-1)/2} \equiv 1 \pmod{p}$ iff a is a quadratic residue modulo p.*

Now consider an arbitrary odd integer $n > 1$, and let $n = \prod_{i=1}^r p_i^{e_i}$ be its prime factorization. Recall the group isomorphism implied by the Chinese remainder theorem:

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Now,

$$(\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*$$

is a square if and only if there exist $\beta_1, \ldots, \beta_r$ with $\beta_i \in \mathbb{Z}_{p_i^{e_i}}^*$ and $\alpha_i = \beta_i^2$ for $i = 1, \ldots, r$, in which case, we see that the square roots of $(\alpha_1, \ldots, \alpha_r)$ comprise the 2^r elements $(\pm\beta_1, \ldots, \pm\beta_r)$. Thus we have:

Theorem 12.3. *Consider an odd, positive integer n with prime factorization $n = \prod_{i=1}^r p_i^{e_i}$. The number of quadratic residues a modulo n, with $0 \le a < n$, is $\phi(n)/2^r$. Moreover, if a is a quadratic residue modulo n, then there are precisely 2^r distinct integers x, with $0 \le x < n$, such that $x^2 \equiv a \pmod{n}$. Also, an integer a is a quadratic residue modulo n if and only if it is a quadratic residue modulo p_i for $i = 1, \ldots, r$.*

That completes our investigation of the case where n is odd. We shall not investigate the case where n is even, as it is a bit messy, and is not of particular importance.

12.2 The Legendre symbol

For an odd prime p and an integer a with $\gcd(a, p) = 1$, the **Legendre symbol** $(a \mid p)$ is defined to be 1 if a is a quadratic residue modulo p, and -1 otherwise. For completeness, one defines $(a \mid p) = 0$ if $p \mid a$. The following theorem summarizes the essential properties of the Legendre symbol.

Theorem 12.4. *Let p be an odd prime, and let $a, b \in \mathbb{Z}$. Then we have*

(i) $(a \mid p) \equiv a^{(p-1)/2} \pmod{p}$*; in particular,* $(-1 \mid p) = (-1)^{(p-1)/2}$*;*

(ii) $(a \mid p)(b \mid p) = (ab \mid p)$*;*

(iii) $a \equiv b \pmod{p}$ *implies* $(a \mid p) = (b \mid p)$*;*

(iv) $(2 \mid p) = (-1)^{(p^2-1)/8}$*;*

(v) if q is an odd prime, then

$$(p \mid q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q \mid p).$$

Part (v) of this theorem is called the **law of quadratic reciprocity**. Note that when $p = q$, both $(p \mid q)$ and $(q \mid p)$ are zero, and so the statement of part (v) is trivially true—the interesting case is when $p \neq q$, and in this case, part (v) is equivalent to saying that

$$(p \mid q)(q \mid p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Part (i) of this theorem follows from Theorem 12.1. Part (ii) is an immediate consequence of part (i), and part (iii) is clear from the definition.

The rest of this section is devoted to a proof of parts (iv) and (v) of this theorem. The proof is completely elementary, although a bit technical.

Theorem 12.5 (Gauss' lemma). *Let p be an odd prime and let a be an integer not divisible by p. Define $\alpha_j := ja \bmod p$ for $j = 1, \ldots, (p-1)/2$, and let n be the number of indices j for which $\alpha_j > p/2$. Then $(a \mid p) = (-1)^n$.*

Proof. Let $r_1, \ldots, r_n$ denote the values α_j that exceed $p/2$, and let $s_1, \ldots, s_k$ denote the remaining values α_j. The r_i and s_i are all distinct and non-zero. We have $0 < p - r_i < p/2$ for $i = 1, \ldots, n$, and no $p - r_i$ is an s_j; indeed, if $p - r_i = s_j$, then $s_j \equiv -r_i \pmod{p}$, and writing $s_j = ua \bmod p$ and $r_i = va \bmod p$, for some $u, v = 1, \ldots, (p-1)/2$, we have $ua \equiv -va \pmod{p}$, which implies $u \equiv -v \pmod{p}$, which is impossible.

It follows that the sequence of numbers $s_1, \ldots, s_k, p - r_1, \ldots, p - r_n$ is just a re-ordering of $1, \ldots, (p-1)/2$. Then we have

$$\begin{aligned} ((p-1)/2)! &\equiv s_1 \cdots s_k (-r_1) \cdots (-r_n) \\ &\equiv (-1)^n s_1 \cdots s_k r_1 \cdots r_n \\ &\equiv (-1)^n ((p-1)/2)!\, a^{(p-1)/2} \pmod{p}, \end{aligned}$$

and canceling the factor $((p-1)/2)!$, we obtain $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$, and the result follows from the fact that $(a \mid p) \equiv a^{(p-1)/2} \pmod{p}$. □

Theorem 12.6. *If p is an odd prime and $\gcd(a, 2p) = 1$, then $(a \mid p) = (-1)^t$ where $t = \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor$. Also, $(2 \mid p) = (-1)^{(p^2-1)}/8$.*

Proof. Let a be an integer not divisible by p, but which may be even, and let us adopt the same notation as in the statement and proof of Theorem 12.5; in particular, $\alpha_1, \ldots, \alpha_{(p-1)/2}$, $r_1, \ldots, r_n$, and $s_1, \ldots, s_k$ are as defined there. Note that $ja = p\lfloor ja/p \rfloor + \alpha_j$, for $j = 1, \ldots, (p-1)/2$, so we have

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{12.1}$$

Also, we saw in the proof of Theorem 12.5 that the integers $s_1, \ldots, s_k, p - r_1, \ldots, p - r_n$ are a re-ordering of $1, \ldots, (p-1)/2$, and hence

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{12.2}$$

Subtracting (12.2) from (12.1), we get

$$(a-1) \sum_{j=1}^{(p-1)/2} j = p\Big(\sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor - n \Big) + 2 \sum_{j=1}^{n} r_j. \tag{12.3}$$

Note that

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8}, \tag{12.4}$$

which together with (12.3) implies

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor - n \pmod{2}. \tag{12.5}$$

If a is odd, (12.5) implies

$$n \equiv \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor \pmod{2}. \tag{12.6}$$

If $a = 2$, then $\lfloor 2j/p \rfloor = 0$ for $j = 1, \ldots, (p-1)/2$, and (12.5) implies

$$n \equiv \frac{p^2-1}{8} \pmod{2}. \tag{12.7}$$

The theorem now follows from (12.6) and (12.7), together with Theorem 12.5. □

Note that this last theorem proves part (iv) of Theorem 12.4. The next theorem proves part (v).

Theorem 12.7. *If p and q are distinct odd primes, then*

$$(p \mid q)(q \mid p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. Let S be the set of pairs of integers (x, y) with $1 \le x \le (p-1)/2$ and $1 \le y \le (q-1)/2$. Note that S contains no pair (x, y) with $qx = py$, so let us partition S into two subsets: S_1 contains all pairs (x, y) with $qx > py$, and S_2 contains all pairs (x, y) with $qx < py$. Note that $(x, y) \in S_1$ if and only if $1 \le x \le (p-1)/2$ and $1 \le y \le \lfloor qx/p \rfloor$. So $|S_1| = \sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor$. Similarly, $|S_2| = \sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor$. So we have

$$\frac{p-1}{2}\frac{q-1}{2} = |S| = |S_1| + |S_2| = \sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor + \sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor,$$

and Theorem 12.6 implies

$$(p \mid q)(q \mid p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \quad \square$$

12.3 The Jacobi symbol

Let a, n be integers, where n is positive and odd, so that $n = q_1 \cdots q_k$, where the q_i are odd primes, not necessarily distinct. Then the **Jacobi symbol** $(a \mid n)$ is defined as

$$(a \mid n) := (a \mid q_1) \cdots (a \mid q_k),$$

where $(a \mid q_j)$ is the Legendre symbol. Note that $(a \mid 1) = 1$ for all $a \in \mathbb{Z}$. Thus, the Jacobi symbol essentially extends the domain of definition of the Legendre symbol. Note that $(a \mid n) \in \{0, \pm 1\}$, and that $(a \mid n) = 0$

if and only if $\gcd(a,n) > 1$. Also, note that if a is a quadratic residue modulo n, then $(a \mid n) = 1$; however, $(a \mid n) = 1$ does not imply that a is a quadratic residue modulo n. The following theorem summarizes the essential properties of the Jacobi symbol.

Theorem 12.8. *Let m, n be odd, positive integers, an let a, b be integers. Then*

(i) $(ab \mid n) = (a \mid n)(b \mid n)$;

(ii) $(a \mid mn) = (a \mid m)(a \mid n)$;

(iii) $a \equiv b \pmod{n}$ *implies* $(a \mid n) = (b \mid n)$;

(iv) $(-1 \mid n) = (-1)^{(n-1)/2}$;

(v) $(2 \mid n) = (-1)^{(n^2-1)/8}$;

(vi) $(m \mid n) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}(n \mid m)$.

Proof. Parts (i)–(iii) follow directly from the definition (exercise).

For parts (iv) and (vi), one can easily verify (exercise) that for odd integers $n_1, \ldots, n_k$,

$$\sum_{i=1}^{k}(n_i - 1)/2 \equiv (n_1 \cdots n_k - 1)/2 \pmod{2}.$$

Part (iv) easily follows from this fact, along with part (ii) of this theorem and part (i) of Theorem 12.4 (exercise). Part (vi) easily follows from this fact, along with parts (i) and (ii) of this theorem, and part (v) of Theorem 12.4 (exercise).

For part (v), one can easily verify (exercise) that for odd integers $n_1, \ldots, n_k$,

$$\sum_{1 \le i \le k} (n_i^2 - 1)/8 \equiv (n_1^2 \cdots n_k^2 - 1)/8 \pmod{2}.$$

Part (v) easily follows from this fact, along with part (ii) of this theorem, and part (iv) of Theorem 12.4 (exercise). □

As we shall see later, this theorem is extremely useful from a computational point of view—with it, one can efficiently compute $(a \mid n)$, without having to know the prime factorization of either a or n. Also, in applying this theorem it is useful to observe that for odd integers m, n,

- $(-1)^{(n-1)/2} = 1$ iff $n \equiv 1 \pmod{4}$;
- $(-1)^{(n^2-1)/8} = 1$ iff $n \equiv \pm 1 \pmod{8}$;
- $(-1)^{((m-1)/2)((n-1)/2)} = 1$ iff $m \equiv 1 \pmod{4}$ or $n \equiv 1 \pmod{4}$.

It is sometimes useful to view the Jacobi symbol as a group homomorphism. Let n be an odd, positive integer. Define the **Jacobi map**

$$\begin{aligned} J_n : \quad \mathbb{Z}_n^* &\to \{\pm 1\} \\ [a]_n &\mapsto (a \mid n). \end{aligned}$$

First, we note that by part (iii) of Theorem 12.8, this definition is unambiguous. Second, we note that since $\gcd(a, n) = 1$ implies $(a \mid n) = \pm 1$, the image of J_n is indeed contained in $\{\pm 1\}$. Third, we note that by part (i) of Theorem 12.8, J_n is a group homomorphism.

Since J_n is a group homomorphism, it follows that its kernel, $\ker(J_n)$, is a subgroup of $\mathbb{Z}_n^*$.

Exercise 12.1. Let n be an odd, positive integer. Show that $[\mathbb{Z}_n^* : (\mathbb{Z}_n^*)^2] = 2^r$, where r is the number of distinct prime divisors of n.

Exercise 12.2. Let n be an odd, positive integer, and consider the Jacobi map J_n.

(a) Show that $(\mathbb{Z}_n^*)^2 \subseteq \ker(J_n)$.

(b) Show that if n is the square of an integer, then $\ker(J_n) = \mathbb{Z}_n^*$.

(c) Show that if n is not the square of an integer, then $[\mathbb{Z}_n^* : \ker(J_n)] = 2$ and $[\ker(J_n) : (\mathbb{Z}_n^*)^2] = 2^{r-1}$, where r is the number of distinct prime divisors of n.

Exercise 12.3. Let p and q be distinct primes, with $p \equiv q \equiv 3 \pmod 4$, and let $n := pq$.

(a) Show that $[-1]_n \in \ker(J_n) \setminus (\mathbb{Z}_n^*)^2$, and from this, conclude that the cosets of $(\mathbb{Z}_n^*)^2$ in $\ker(J_n)$ are the two distinct cosets $(\mathbb{Z}_n^*)^2$ and $[-1]_n(\mathbb{Z}_n^*)^2$.

(b) Show that the squaring map on $(\mathbb{Z}_n^*)^2$ is a group automorphism.

(c) Let $\delta \in \mathbb{Z}_n^* \setminus \ker(J_n)$. Show that the map from $\{0,1\} \times \{0,1\} \times (\mathbb{Z}_n^*)^2 \to \mathbb{Z}_n^*$ that sends (a, b, γ) to $\delta^a (-1)^b \gamma$ is a bijection.

12.4 Notes

The proof we present here of Theorem 12.4 is essentially the one from Niven and Zuckerman [68]. Our proof of Theorem 12.8 is essentially the one found in Bach and Shallit [12].