Chapter 9

Quadratic Residues

9.1 Introduction

Definition 9.1. We say that \( a \in \mathbb{Z} \) is a quadratic residue mod \( n \) if there exists \( b \in \mathbb{Z} \) such that
\[
a \equiv b^2 \mod n.
\]
If there is no such \( b \) we say that \( a \) is a quadratic non-residue mod \( n \).

Example: Suppose \( n = 10 \). We can determine the quadratic residues mod \( 10 \) by computing \( b^2 \mod 10 \) for \( 0 \leq b < n \). In fact, since
\[
(-b)^2 \equiv b^2 \mod 10,
\]
we need only consider \( 0 \leq b \leq [n/2] \).
Thus the quadratic residues mod 10 are 0, 1, 4, 9, 6, 5; while 3, 7, 8 are quadratic non-residues mod 10.

Proposition 9.1. If \( a, b \) are quadratic residues mod \( n \) then so is \( ab \).

Proof. Suppose
\[
a \equiv r^2, \; b \equiv s^2 \mod p.
\]
Then
\[
ab \equiv (rs)^2 \mod p.
\]

9.2 Prime moduli

Proposition 9.2. Suppose \( p \) is an odd prime. Then the quadratic residues coprime to \( p \) form a subgroup of \((\mathbb{Z}/p)^\times\) of index 2.

Proof. Let \( Q \) denote the set of quadratic residues in \((\mathbb{Z}/p)^\times\). If \( \theta : (\mathbb{Z}/p)^\times \to (\mathbb{Z}/p)^\times \) denotes the homomorphism under which
\[
r \mapsto r^2 \mod p
\]
then \( \ker \theta = \{ \pm 1 \} \), \( \operatorname{im} \theta = \mathbb{Q} \).

By the first isomorphism theorem of group theory,
\[
|\ker \theta| \cdot |\operatorname{im} \theta| = |(\mathbb{Z}/p)^\times|.
\]

Thus \( \mathbb{Q} \) is a subgroup of index 2:
\[
|\mathbb{Q}| = \frac{p - 1}{2}.
\]

**Corollary 9.1.** Suppose \( p \) is an odd prime; and suppose \( a, b \) are coprime to \( p \). Then

1. \( 1/a \) is a quadratic residue if and only if \( a \) is a quadratic residue.

2. If both of \( a, b \), or neither, are quadratic residues, then \( ab \) is a quadratic residue;

3. If one of \( a, b \) is a quadratic residue and the other is a quadratic non-residue then \( ab \) is a quadratic non-residue.

### 9.3 The Legendre symbol

**Definition 9.2.** Suppose \( p \) is a prime; and suppose \( a \in \mathbb{Z} \). We set
\[
\left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{if } p \mid a \\
1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue mod } p \\
-1 & \text{if } a \text{ is a quadratic non-residue mod } p.
\end{cases}
\]

**Example:** \( \left( \frac{2}{3} \right) = -1 \), \( \left( \frac{1}{4} \right) = 1 \), \( \left( \frac{-1}{4} \right) = -1 \), \( \left( \frac{3}{5} \right) = -1 \).

**Proposition 9.3.** 1. \( \left( \frac{0}{p} \right) = 0 \), \( \left( \frac{1}{p} \right) = 1 \);

2. \( a \equiv b \mod p \implies \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \);

3. \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \).

**Proof.** (1) and (2) follow from the definition, while (3) follows from the Corollary above. \( \square \)
9.4 Euler’s criterion

**Proposition 9.4.** Suppose $p$ is an odd prime. Then
\[
\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.
\]

**Proof.** The result is obvious if $p \mid a$.
Suppose $p \nmid a$. Then
\[
\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \mod p,
\]
by Fermat’s Little Theorem. It follows that
\[
\left(\frac{a}{p}\right) \equiv \pm 1 \mod p.
\]
Suppose $a$ is a quadratic residue, say $a \equiv r^2 \mod p$. Then
\[
a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p
\]
by Fermat’s Little Theorem.
These provide all the roots of the polynomial
\[
f(x) = x^{(p-1)/2} - 1.
\]
Hence
\[
a^{(p-1)/2} \equiv -1 \mod p
\]
if $a$ is a quadratic non-residue. 

9.5 Gauss’s Lemma

Suppose $p$ is an odd prime. We usually take $r \in [0, p-1]$ as representatives of the residue-classes mod $p$ But it is sometimes more convenient to take $r \in [-\frac{p-1}{2}, \frac{p-1}{2}]$, ie $\{-p/2 < r < p/2\}/$

Let $P$ denote the strictly positive residues in this set, and $N$ the strictly negative residues:
\[
P = \{1, 2, \ldots, (p-1)/2\}, \quad N = -P = \{-1, -2, \ldots, -(p-1)/2\}.
\]
Thus the full set of representatives is $N \cup \{0\} \cup P$.
Now suppose $a \in (\mathbb{Z}/p)^\times$. Consider the residues
\[
aP = \{a, 2a, \ldots, \frac{p-1}{2}a\}.
\]
Each of these can be written as $\pm s$ for some $s \in P$, say
\[
ar = \epsilon(r)\pi(r),
\]

9–3
where $\epsilon(r) = \pm 1$. It is easy to see that the map

$$\pi : P \to P$$

is injective; for

$$\pi(r) = \pi(r') \implies ar \equiv \pm ar' \mod p$$

$$\implies r \equiv \pm r' \mod p$$

$$\implies r \equiv r' \mod p,$$

since $s$ and $s'$ are both positive.

Thus $\pi$ is a permutation of $P$ (by the pigeon-hole principle, if you like). It follows that as $r$ runs over the elements of $P$ so does $\pi(r)$.

Thus if we multiply together the congruences

$$ar \equiv \epsilon(r)\pi(r) \mod p$$

we get

$$a^{(p-1)/2}1 \cdot 2 \cdots (p-1)/2$$

on the left, and

$$\epsilon(1)\epsilon(2) \cdots \epsilon((p-1)/2)1 \cdot 2 \cdots (p-1)/2$$

on the right. Hence

$$a^{(p-1)/2} \equiv \epsilon(1)\epsilon(2) \cdots \epsilon((p-1)/2) \mod p.$$  

But

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

by Euler’s criterion. Thus we have established

**Theorem 9.1.** Suppose $p$ is an odd prime; and suppose $a \in \mathbb{Z}$. Consider the residues

$$a, 2a, \ldots, a(p-1)/2 \mod p,$$

choosing residues in $[-(p-1)/2, (p-1)/2]$. If $t$ of these residues are $< 0$ then

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

**Remarks:**

1. Note that we could equally well choose the residues in $[1, p-1]$, and define $t$ to be the number of times the residue appears in the second half $(p + 1)/2, (p - 1)$.

2. The map $a \mapsto (-1)^t$ is an example of the *transfer homomorphism* in group theory. Suppose $H$ is an abelian subgroup of finite index $r$ in the group $G$. We know that $G$ is partitioned into $H$-cosets:

$$G = g_1H \cup \cdots \cup g_rH.$$  

9–4
If now $g \in G$ then
\[ gg_i = g_jh_i \]
for $i \in [1, r]$. Now it is easy to see — the argument is similar to the one we gave above — that the product $h = h_1 \cdots h_r$ is independent of the choice of coset representatives $g_1, \ldots, g_r$, and the map
\[ \tau : G \to S \]
is a homomorphism, known as the transfer homomorphism from $G$ to $S$.

If $G$ is abelian — which it is in all the cases we are interested in — we can simply multiply together all the equations $gg_i = g_jh_i$, to get
\[ \tau(g) = g^r. \]

### 9.6 Computation of $\left( \frac{-1}{p} \right)$

**Proposition 9.5.** If $p$ is an odd prime then
\[
\left( \frac{-1}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv -1 \mod 4. \end{cases}
\]

**Proof.** The result follows at once from Euler’s Criterion
\[ \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \mod p. \]

But it is instructive to deduce it by Gauss’s Lemma.

We have to consider the residues
\[-1, -2, \ldots, -(p - 1)/2 \mod p.\]

All these are in the range $N = [-(p - 1)/2, (p - 1)/2]$. It follows that $t = (p - 1)/2$; all the remainders are negative.

Hence
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}
= \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv -1 \mod 4. \end{cases}
\]

\[ \square \]

**Example:** According to this,
\[
\left( \frac{2}{3} \right) = \left( \frac{-1}{3} \right) = -1
\]
(since \(3 \equiv -1 \mod 4\)), ie 2 is a quadratic non-residue mod 3.

Again

\[
\left( \frac{12}{13} \right) = \left( \frac{-1}{13} \right) = 1,
\]

since \(13 \equiv 1 \mod 4\). Thus 12 is a quadratic residue \(\mod 13\). In fact it is easy to see that

\[
12 \equiv 25 = 5^2 \mod 13.
\]

### 9.7 Computation of \(\left( \frac{2}{p} \right)\)

**Proposition 9.6.** If \(p\) is an odd prime then

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \mod 8, \\
-1 & \text{if } p \equiv \pm 3 \mod 8.
\end{cases}
\]

**Proof.** We have to consider the residues

\[2, 4, 6, \ldots, (p - 1) \mod p.\]

We have to determine the number \(t\) of these residues in the first half of \([1, p - 1]\), and the number in the second. We can describe these two ranges as \(\{0 < r < p/2\}\) and \(\{p/2 < r < p\}\). Since

\[
p/2 < 2x < p \iff p/4 < x < p/2
\]

it follows that

\[t = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor.\]

Suppose

\[p = 8n + r,
\]

where \(r = 1, 3, 5, 7\). Then

\[\lfloor p/2 \rfloor = 4n + \lfloor r/2 \rfloor, \quad \lfloor p/4 \rfloor = 2n + \lfloor r/4 \rfloor.
\]

Thus

\[t \equiv \lfloor r/2 \rfloor + \lfloor r/4 \rfloor \mod 2.
\]

The result follows easily from the fact that

\[\lfloor r/2 \rfloor = \begin{cases} 
0 & \text{for } r = 1, \\
1 & \text{for } r = 3, \\
2 & \text{for } r = 5, \\
3 & \text{for } r = 7,
\end{cases}
\]

while

\[\lfloor r/4 \rfloor = \begin{cases} 
0 & \text{for } r = 1, 3, \\
1 & \text{for } r = 5, 7.
\end{cases}\]
Example: Since $71 \equiv -1 \mod 8$,

$$\left(\frac{2}{71}\right) = 1,$$

Can you find the solutions of

$$x^2 \equiv 2 \mod 71?$$

Again Since $19 \equiv 3 \mod 8$,

$$\left(\frac{2}{19}\right) = -1.$$  

So by Euler’s criterion,

$$2^9 \equiv -1 \mod 19.$$  

Checking,

$$2^4 \equiv 3 \implies 2^8 \equiv 9 \implies 2^9 \equiv 18 \mod 19.$$  

9.8 Composite moduli

Proposition 9.7. Suppose $m, n$ are coprime; and suppose $a$ is coprime to $m$ and $n$. Then $a$ is a quadratic residue modulo $mn$ if and only if it is a quadratic residue modulo $m$ and modulo $n$.

Proof. This follows at once from the Chinese Remainder Theorem. For

$$a \equiv r^2 \mod mn \implies a \equiv r^2 \mod m \text{ and } a \equiv r^2 \mod n.$$  

Conversely, suppose

$$a \equiv r^2 \mod m \text{ and } a \equiv s^2 \mod n.$$  

By the Chinese Remainder Theorem, we can find $t$ such that $t \equiv r \mod m$ and $t \equiv s \mod n$; and then

$$t^2 \equiv r^2 \equiv a \mod m \text{ and } t^2 \equiv s^2 \equiv b \mod n.$$  

9.9 Prime power moduli

Proposition 9.8. Suppose $p$ is an odd prime; and suppose $a \in \mathbb{Z}$ is coprime to $p$. Then $a$ is a quadratic residue $\mod p^e$ (where $e \geq 1$) if and only if it is quadratic residue $\mod p$.

Proof. The argument we gave above for quadratic residues modulo $p$ still applies here.
Lemma 9.1. If \( \theta : (\mathbb{Z}/p^e)^\times \rightarrow (\mathbb{Z}/p^e)^\times \) is the homomorphism under which
\[
t \mapsto t^2 \mod p^e
\]
then
\[
\ker \theta = \{ \pm \}.
\]

Proof. Suppose
\[
a^2 - 1 = (a - 1)(a + 1) \equiv 0 \mod p^e.
\]
Then
\[
p \mid a - 1 \text{ and } p \mid a + 1 \implies p \mid 2a \implies p \mid a,
\]
which we have excluded. If \( p \mid a + 1 \) then \( p^e \mid a - 1 \); and if \( p \mid a - 1 \) then \( p^e \mid a + 1 \). Thus
\[
a \equiv \pm 1 \mod p^e.
\]

It follows that the quadratic residues modulo \( p^e \) coprime to \( p \) form a subgroup of index 2 in \((\mathbb{Z}/p^e)^\times\), ie just half the elements of \((\mathbb{Z}/p^e)^\times\) are quadratic residues modulo \( p^e \). Since just half are also quadratic residues modulo \( p \), the result follows.

Remark: For an alternative proof, we can argue by induction of \( e \). Suppose \( a \) is a quadratic residue \( \mod p^\ell \), say
\[
a \equiv r^2 \mod p^\ell,
\]
\[ie\]
\[
a = r^2 + tp^\ell.
\]
Set
\[
s = r + xp^\ell.
\]
Then
\[
s^2 = r^2 + 2xp^\ell + x^2p^{2\ell} \\
\equiv r^2 + 2xp^\ell \mod p^{\ell+1} \\
\equiv a + (t + 2x)p^\ell \mod p^{\ell+1} \\
\equiv ap^\ell \mod p^{\ell+1}
\]
if
\[
t + 2x \equiv 0 \mod p,
\]
\[ie\]
\[
x = -t/2 \mod p,
\]
using the fact that 2 is invertible modulo an odd prime \( p \).
Corollary 9.2. The number of quadratic residues in $(\mathbb{Z}/p^e)^\times$ is
\[ \frac{\phi(p^e)}{2} = \frac{(p - 1)p^{e-1}}{2}. \]

The argument above extends to moduli $2^e$ with a slight modification.

Proposition 9.9. Suppose $p$ is an odd prime; and suppose $a \in \mathbb{Z}$ is coprime to $p$. Then $a$ is a quadratic residue modulo $p^e$ (where $e \geq 1$) if and only if it is quadratic residue modulo $p$.

Proof. The argument we gave above for quadratic residues modulo $p$ still applies here.

Lemma 9.2. If $\theta : (\mathbb{Z}/p^e)^\times \to (\mathbb{Z}/p^e)^\times$ is the homomorphism under which
\[ t \mapsto t^2 \mod p^e \]
then $\ker \theta = \{ \pm \}$.

Proof. Suppose
\[ a^2 - 1 = (a - 1)(a + 1) \equiv 0 \mod p^e. \]
Then
\[ p \mid a - 1 \text{ and } p \mid a + 1 \implies p \mid 2a \implies p \mid a, \]
which we have excluded. If $p \mid a + 1$ then $p^e \mid a - 1$; and if $p \mid a - 1$ then $p^e \mid a + 1$. Thus
\[ a \equiv \pm 1 \mod p^e. \]

It follows that the quadratic residues modulo $p^e$ coprime to $p$ form a subgroup of index 2 in $(\mathbb{Z}/p^e)^\times$, ie just half the elements of $(\mathbb{Z}/p^e)^\times$ are quadratic residues modulo $p^e$. Since just half are also quadratic residues modulo $p$, the result follows.

Remark: For an alternative proof, we can argue by induction of $e$. Suppose $a$ is a quadratic residue mod$p^e$, say
\[ a \equiv r^2 \mod p^e, \]
ie
\[ a = r^2 + tp^e. \]
Set
\[ s = r + xp^e. \]
Then
\[ s^2 = r^2 + 2xp^e + x^2p^{2e} \]
\[ \equiv r^2 + 2xp^e \mod p^{e+1} \]
\[ \equiv a + (t + 2x)p^e \mod p^{e+1} \]
\[ \equiv a \mod p^{e+1} \]
\[ 9–9 \]
if

\[ t + 2x \equiv 0 \mod p, \]

ie

\[ x = -t/2 \mod p, \]

using the fact that 2 is invertible modulo an odd prime \( p \).

**Corollary 9.3.** The number of quadratic residues in \( (\mathbb{Z}/p^e)^\times \) is

\[
\frac{\phi(p^e)}{2} = \frac{(p - 1)p^{e-1}}{2}.
\]

The argument above extends to moduli \( 2^e \) with a slight modification.

**Proposition 9.10.** Suppose \( a \) is an odd integer. Then \( a \) is a quadratic residue modulo \( 2^e \) (where \( e \geq 3 \)) if and only if \( a \equiv 1 \mod 8 \)

**Proof.** It is readily verified that 1 is the only odd quadratic residue modulo 8; 3, 5, and 7 are quadratic non-residues.

We show by induction on \( e \) that if \( a \) is an odd quadratic residue modulo \( 2^e \) then it is a quadratic residue modulo \( 2^{e+1} \). For suppose

\[ a \equiv r^2 \mod 2^e, \]

say

\[ a = r^2 + t2^e. \]

Let

\[ s = r + t2^{e-1}. \]

Then

\[ s^2 \equiv r^2 + t2^e \mod 2^{e+1} \]

\[ = a. \]

\( \square \)

**Corollary 9.4.** The number of quadratic residues in \( (\mathbb{Z}/2^e)^\times \) (where \( e \geq 3 \)) is

\[
\frac{\phi(2^e)}{4} = 2^{e-3}.
\]

**Remarks:**

1. It is easy to see that \( p^f \) (where \( f < e \)) is a quadratic residue modulo \( p^e \) if and only if \( f \) is even. This allows us to determine whether residues that are not coprime to the modulus are quadratic residues or not.

Thus the quadratic residues modulo 24 are 0, 1, 4, 7, 17, 23, while the quadratic residues modulo 36 are 0, 1, 4, 9, 17, 31 (noting that the quadratic residue modulo 4 are 0, 1).

2. The inductive argument above is an example of *Hensel’s Lemma*. In the simplest case this says that if \( f(x) \in \mathbb{Z}[x] \) then any solution of \( f(a) \equiv 0 \mod p \) such that \( f'(a) \) is coprime to \( p \) can be extended (in a unique way) to a solution of \( f(a) \equiv 0 \mod p^e \) for all \( e \geq 1 \).