Chapter 10

Quadratic Residues

10.1 Introduction

Definition 10.1. *We say that* $a \in \mathbb{Z}$ *is a* quadratic residue mod n *if there exists* $b \in \mathbb{Z}$ *such that*

$$a \equiv b^2 \bmod n.$$

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 n by computing $b^2 \bmod n$ for $0 \le b < n$. In fact, since

$$(-b)^2 \equiv b^2 \bmod n,$$

we need only consider $0 \le b \le [n/2]$.

Thus the quadratic residues mod 10 are $0, 1, 4, 9, 6, 5$; while $3, 7, 8$ are quadratic non-residues mod 10.

The following result is trivial.

Proposition 10.1. *If* a, b *are quadratic residues* mod n *then so is* ab.

10.2 Prime moduli

We are mainly interested in quadratic residues modulo a prime.

Proposition 10.2. *Suppose* p *is an odd prime. Then just* $(p-1)/2$ *of the numbers* $1, 2, \ldots, p-1$ *are quadratic residues* mod p, *and the same number are quadratic non-residues.*

Proof. Consider $b^2 \bmod p$ for $b = 1, 2, \ldots, (p-1)/2$. We know these give all the quadratic residues, since

$$(p-b)^2 \equiv b^2 \bmod p.$$

Moreover these squares are all different mod p. For

$$\begin{aligned} b^2 \equiv c^2 \bmod p &\implies (b+c)(b-c) \equiv 0 \bmod p \\ &\implies b \equiv \pm c \bmod p. \end{aligned}$$

□

We can express this in group-theoretic terms as follows:

The map

$$\theta : x \mapsto x^2 : (\mathbb{Z}/p)^\times \to (\mathbb{Z}/p)^\times$$

is a homomorphism, and

$$\ker \theta = \{\pm 1\}.$$

By the first isomorphism theorem of group theory, if $\theta : G \to H$ is a homomorphism then

$$\operatorname{im} \theta \cong G / \ker \theta.$$

In particular, if G is finite then

$$\#(\ker \theta) \cdot \#(\operatorname{im} \theta) = \#(G).$$

(This holds for abelian or non-abelian groups.)

In our case, $\operatorname{im} \theta$ is just the set of non-zero quadratic residues. It follows that they constitute just half of the non-zero residues mod p; the other half must be the quadratic non-residues.

Proposition 10.3. *Suppose p is an odd prime; and suppose a, b are coprime to p. Then*

1. *If both of a, b, or neither, are quadratic residues, then ab is a quadratic residue;*

2. *If one of a, b is a quadratic residue and the other is a quadratic non-residue then ab is a quadratic non-residue.*

Proof. Suppose a is a quadratic residue. As b runs over the non-zero residues mod p, so does ab. We know that ab is a quadratic residue if b is a quadratic residue, and we know that just half the non-zero residues are quadratic residues. It follows that ab must be a quadratic non-residue if b is a quadratic non-residue.

Now suppose a is a quadratic non-residue. We have just seen that if b is a quadratic residue then ab is a quadratic non-residues. But we know that only half the residues are quadratic non-residues. It follows that ab must be a quadratic residue in the remaining cases, when b is a quadratic non-residue. □

10.3 The Legendre symbol

Definition 10.2. *Suppose p is a prime; and suppose $a \in \mathbb{Z}$. We set*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \textit{ if } p \mid a \\ 1 \textit{ if } p \nmid a \textit{ and } a \textit{ is a quadratic residue} \bmod p \\ -1 \textit{ if if } a \textit{ is a quadratic non-residue} \bmod p. \end{cases}$$

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

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

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 previous Proposition. □

10.4 Euler's criterion

Proposition 10.5. *Suppose p is an odd prime. Then*

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

Proof. The result is obvious if $p \mid a$.

Suppose $p \nmid a$. Then

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

by Fermat's Little Theorem. It follows that

$$\left(\frac{a}{p}\right) \equiv \pm 1 \bmod p.$$

Consider the map

$$\theta : a \mapsto a^{(p-1)/2} : (\mathbb{Z}/p)^\times \to \{\pm 1\}.$$

Evidently θ is a homomorphism.

We know that $(\mathbb{Z}/p)^\times$ is cyclic. It follows that θ is surjective. (In fact it is clear that

$$a^{(p-1)/2} = -1$$

if a is a primitive root mod p; for otherwise a would have order $\leq (p-1)/2$) It follows that

$$\#(\ker \theta) = (p-1)/2.$$

But since the group $(\mathbb{Z}/p)^\times$ is cyclic, it only has one subgroup of each possible order. Thus there is only one non-trivial homomorphism

$$(\mathbb{Z}/p)^\times \to \{\pm 1\}.$$

It follows that θ must be the same as the homomorphism

$$a \mapsto \left(\frac{a}{p}\right) : (\mathbb{Z}/p)^\times \to \{\pm 1\},$$

which proves the Proposition. □

Alternatively, and perhaps more directly, suppose a is a quadratic residue mod p, say $a \equiv b^2 \bmod p$. Then

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \bmod p,$$

by Fermat's Little Theorem.

We have seen that

$$a^{(p-1)/2} \equiv \pm 1 \bmod p.$$

Since $(\mathbb{Z}/p)^\times$ is cyclic, not all a satisfy

$$a^{(p-1)/2} \equiv 1 \bmod p.$$

Say

$$c^{(p-1)/2} \equiv -1 \bmod p.$$

Evidently c must be a quadratic non-residue mod p. If a is a quadratic residue mod p then

$$(ca)^{(p-1)/2} = c^{(p-1)/2} a^{(p-1)/2} \equiv -1 \bmod p.$$

But as a runs over the quadratic residues mod p, ca must run over the quadratic non-residues, whence the result.

10.5 Computing $\left(\frac{a}{p}\right)$

Suppose p is an odd prime. We usually take $0, 1, 2, \ldots, p-1$ as representatives of the residue-classes mod p

Let S denote the first half of the residue-set mod p:

$$S = [1, 2, \ldots, (p-1)/2].$$

Then each residue x mod p can be written as

$$x \equiv \pm s \bmod p$$

for a unique $s \in S$. (In other words, instead of taking $0, 1, \ldots, p-1$ as representatives of the residue-classes we could take $-(p-1)/2, \ldots, -1, 0, 1, \ldots, (p-1)/2\}$.)

Now suppose $a \in (\mathbb{Z}/p)^{\times}$. Consider the residues

$$aS = \{a, 2a, \ldots, \frac{p-1}{2}a\}.$$

Each of these can be written as $\pm s$ for some $s \in S$, say

$$as = \epsilon(s)\pi(s),$$

where $\epsilon(s) = \pm 1$.

The map

$$\pi : S \to S$$

is injective, ie if $s, s' \in S$ then

$$s \neq s' \implies \pi(s) \neq \pi(s').$$

For

$$\begin{aligned} \pi(s) = \pi(s') &\implies as \equiv \pm as' \bmod p \\ &\implies s \equiv \pm s' \bmod p \end{aligned}$$

(since $p \nmid a$)

$$\implies s \equiv -s' \bmod p$$

(since $s \neq s'$)

$$\implies s + s' \equiv 0 \bmod p,$$

which is impossible.

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

Thus if we multiply together the congruences

$$as \equiv \epsilon(s)\pi(s) \bmod p$$

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

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

But

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

by Euler's criterion. Thus we have established

Theorem 10.1. *Suppose p is an odd prime; and suppose $a \in \mathbb{Z}$. Consider*

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

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

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

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 $(p+1)/2, (p-1)$.

10.6 $a = -1$

Proposition 10.6. *If p is an odd prime then*

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

Proof. We have to consider the residues

$$-1, -2, \ldots, -(p-1)/2 \bmod p.$$

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

Hence

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

□

Example: According to this,

$$\left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

(since $3 \equiv -1 \bmod 4$), ie 2 is a quadratic non-residue mod 3.

Again

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

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

$$12 \equiv 25 = 5^2 \bmod 13.$$

10.7 $a = 2$

Proposition 10.7. *If p is an odd prime then*

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

Proof. We have to consider the residues

$$2, 4, 6, \ldots, (p-1) \bmod p.$$

Let

$$p = 8n + r,$$

where $r \in \{1, 3, 5, 7\}$. We have to determine in each case how many of the residues lie in the first half of $[1, p-1]$, and how many in the second.

We can describe these two ranges as $(0, p/2)$ and $(p/2, p)$, or $[1, [p/2]]$ and $[[p/2]+1, p-1]$, where we write $[x]$ for the largest integer $\leq x$.

If $r = 1$ then

$$[p/2] = 4n,$$

and the $2n$ residues

$$2, 4, 6, \ldots, 4n \bmod p$$

are in the first half, while the remaining

$$(p-1)/2 - 2n = 2n$$

are in the second half.

Thus the number $t = 2n$ in the second half of the range is even, and so

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

If $r = 3$ then

$$[p/2] = 4n + 1,$$

so the $2n$ residues

$$2, 4, 6, \ldots 4n \bmod p$$

are in the first half, as before, and the number in the second half is

$$(p-1)/2 - 2n = (4n+1) - 2n = 2n + 1,$$

which is odd. Hence

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

in this case.

If $r = 5$ then

$$[p/2] = 4n + 2,$$

so the $2n + 1$ residues

$$2, 4, 6, \ldots 4n, 4n+2 \bmod p$$

are in the first half, and the number in the second half is

$$(p-1)/2 - (2n+1) = (4n+2) - (2n+1) = 2n + 1,$$

which is odd. Hence

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

in this case.

Finally, if $r = 7$ then

$$[p/2] = 4n + 3,$$

so the $2n + 1$ residues

$$2, 4, 6, \ldots 4n, 4n + 2 \bmod p$$

are in the first half, and the number in the second half is

$$(p - 1)/2 - (2n + 1) = (4n + 3) - (2n + 1) = 2n + 2,$$

which is even. Hence

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

□

10.8 Hensel's Lemma

Suppose $f(x) \in \mathbb{Z}[x]$; and suppose

$$n = p_1^{e_1} \ldots p_r^{e_r}.$$

We know from the Chinese Remainder Theorem that the congruence

$$f(x) \equiv 0 \bmod n$$

reduces to the simultaneous congruences

$$f(n) \equiv 0 \bmod p_i^{e_i}$$

for $1 \le i \le r$.

So we are reduced to solving congruences of the form

$$f(n) \equiv 0 \bmod p^e.$$

We can divide this into two parts: First we must solve

$$f(n) \equiv 0 \bmod p,$$

which is tantamount to solving the equation

$$f(x) = 0$$

in the field $\mathbb{F}_p = \mathbb{Z}/(p)$. Secondly, we must see if a solution mod p can be extended to a solution mod p^e.

Hensel's Lemma is a useful tool for tackling this second part.

Proposition 10.8. *Suppose p is a prime; and suppose $f(x) \in \mathbb{Z}[x]$. If*

$$f(a) \equiv 0 \bmod p^e \text{ but } f'(a) \not\equiv 0 \bmod p$$

(where $e \geq 1$ and $f'(x) = df/dx$ is the derivative of $f(x)$) then there is a unique extension of a to a solution $b \bmod p^{e+1}$ ie

$$f(b) \equiv 0 \bmod p^{e+1} \text{ and } b \equiv a \bmod p^e;$$

and b is unique $\bmod p^{e+1}$.

Proof. Let

$$b = a + tp^e.$$

Suppose $f(x) = x^n$. By the binomial theorem,

$$\begin{aligned} f(a + tp^e) &= a^n + ntp^e + \binom{2}{n} t^2 p^{2e} + \cdots \\ &\equiv a^n + na^{n-1}tp^e \bmod p^{e+1} \\ &\equiv f(a) + f'(a)tp^e \bmod p^{e+1}. \end{aligned}$$

By addition,

$$f(a + tp^e) \equiv f(a) + f'(a)tp^e \bmod p^{e+1}$$

for any $f(x) \in \mathbb{Z}[x]$.

By hypothesis, $f(a) \equiv 0 \bmod p^e$, say

$$f(a) = cp^e.$$

Thus we have to solve

$$cp^e + f'(a)tp^e \equiv 0 \bmod p^{e+1},$$

ie

$$c + f'(a)t \equiv 0 \bmod p.$$

Since $p \nmid f'(a)$ this has a unique solution $t \bmod p$. □

Corollary 10.1. *Suppose $f[x] \in \mathbb{Z}[x]$; and suppose*

$$f(a) \equiv 0 \bmod p \text{ and } f'(a) \not\equiv 0 \bmod p.$$

Then the solution $a \bmod p$ has a unique extension to a solution $\bmod p^e$ for any $e \geq 1$, ie there is a unique $b \bmod p^e$ such that

$$f(b) \equiv 0 \bmod p^e \text{ and } b \equiv a \bmod p.$$

Example: Consider the congruence

$$x^3 \equiv 3 \bmod 25.$$

The homomorphism

$$\theta : x \mapsto x^3 : (\mathbb{Z}/5)^\times \to (\mathbb{Z}/5)^\times$$

is injective since the group $(\mathbb{Z}/5)^\times$ has order 4, and so contains no element of order 3. Hence θ is bijective; and so there is a unique x mod 5 such that

$$x^3 \equiv 3 \bmod 5.$$

It is easy to see that this unique solution is $x \equiv 2 \bmod 5$:

$$2^3 \equiv 3 \bmod 5.$$

Now let $f(x) = x^3 - 3$. Then

$$f'(x) = 3x^2;$$

and so

$$f'(2) \not\equiv 0 \bmod 5.$$

It follows that the solution 2 mod 5 extends to a unique solution mod 5^2. To find this solution, note that

$$(2 + 5t)^3 - 3 \equiv 5 + 60t \bmod 5^2.$$

Thus

$$1 + 12t \equiv 0 \bmod 5,$$

ie

$$t \equiv 2 \bmod 5.$$

Hence the solution to the congruence mod 5^2 is

$$2 + 5 \cdot 2 = 12 \bmod 25.$$

Unfortunately, Hensel's Lemma as we have stated it does not apply to a congruence like

$$x^2 \equiv 3 \bmod 8;$$

for if

$$f(x) = x^2 - 3$$

then

$$f'(x) = 2x \equiv 0 \bmod 2$$

for all x. We need a slight variant of the Lemma, which can be proved in exactly the same way.

Proposition 10.9. *Suppose p is a prime, and $f(x) \in \mathbb{Z}[x]$; and suppose*

$$f(a) \equiv 0 \bmod p^e \text{ and } p^f \parallel f(a),$$

where $e > 2f$. Then there is a unique extension of a to a solution b mod p^{e+1} ie

$$f(b) \equiv 0 \bmod p^{e+1} \text{ and } b \equiv a \bmod p^e;$$

and b is unique mod p^{e+1}.

Example: If $p = 2$ and $f(x) = x^2 - c$ then we have to start with a solution mod 8.

Consider the congruence

$$x^2 \equiv 9 \bmod 24.$$

This reduces to the congruences

$$x^2 \equiv 9 \equiv 1 \bmod 8, \quad x^2 \equiv 9 \equiv 0 \bmod 3.$$

The first congruence has the solutions

$$x \equiv 1, 3, 5, 7 \bmod 8.$$

The second has the solution

$$x \equiv 0 \bmod 3.$$

Putting these together, the congruence mod 24 has 4 solutions:

$$x \equiv 9, 3, 21, 15 \bmod 24.$$