Lecture 8.1

Quadratic Residues

At this point, we can solve linear congruences

$$ax \equiv b \pmod{n}$$

proficiently.

The next step in complexity is quadratic congruences — we will just focus on

$$x^2 \equiv a \pmod{n}.$$

Ex 1 $x^2 \equiv 3 \pmod{7}$

Testing all $0 \leq x \leq 6$, we see that

no x satisfies the congruence.

② $x^2 \equiv 3 \pmod{13}$

This time, $x = 4$ is a solution.

③ $x^2 \equiv -1 \pmod{13}$

A solution is $x = 5$.

④ For which primes p does

$$x^2 \equiv 2 \pmod{p}$$

have a solution? Let's come back to this one later.

Here's some more data:

b	b^2
0	0
1	1
2	4
3	4
4	1

Modulo 5

b	b^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Modulo 7

b	b^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Modulo 11

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Modulo 13

What patterns do you observe?

One interesting pattern is that the squares appear in pairs in each list — there's even a symmetry between the top and

bottom of each list. Let's quantify this as follows.

Lemma If p is prime and $0 < b < p$, then b and $p-b$ have the same square mod p.

Pf: $(p-b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod{p}$. □

Def: A number $a \in \mathbb{N}$ is called a quadratic residue mod p if a is congruent to some b^2 mod p for $b \in \mathbb{Z}$. That is, "a has a square root mod p".

If $a \not\equiv b^2 \pmod{p}$ for any b, we say

a is a quadratic nonresidue.

Let's look at the tables again:

b	b^2
0	0
1	1
2	4
3	4
4	1

Modulo 5

b	b^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Modulo 7

b	b^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Modulo 11

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Modulo 13

QRs: 1, 4 | 1, 2, 4 | 1, 3, 4, 5, 9 | 1, 3, 4, 9, 10, 12

NRs: 2, 3 | 3, 5, 6 | 2, 6, 7, 8 | 2, 5, 6, 7, 8, 11

More patterns:

- if a is a square integer, it's a QR
- the lists of QRs and NRs have the same length

Let's verify the second one.

Theorem For any prime p, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues mod p.

Pf: Define the sets

$$A = \{ 0 < a < p \mid a \text{ is a QR mod } p \}$$

$B = \{ 0 < a < p \mid a \text{ is a NR mod } p \}$.

Then $\#A + \#B = p-1$.

On the other hand, the Lemma says that

$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ is a complete list

of squares mod p, so

$$A = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

and $\#A \leq \frac{p-1}{2}$.

Suppose $i^2 \equiv j^2 \pmod{p}$ for some $1 \leq j \leq i \leq \frac{p-1}{2}$.

Then $i^2 - j^2 \equiv 0 \pmod{p}$

$\Rightarrow (i-j)(i+j) \equiv 0 \pmod{p}$

$\Rightarrow p \mid (i-j)(i+j)$

$\Rightarrow p \mid (i-j)$ or $p \mid (i+j)$ (p is prime!)

But $2 \leq i+j \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$ so p cannot divide $i+j$.

This means $p \mid i-j$, but $0 \leq i-j < \frac{p-1}{2}$, forcing $i-j = 0$.

Hence $\#A = \frac{p-1}{2}$ (all of the squares on the list are distinct mod p) and as a result, $\#B = \frac{p-1}{2}$ as well. □

Here's another pattern you might observe:

/QR if a, b are QRs

ab is a $\begin{cases} \text{NR} & \text{if only one is a QR} \\ \text{QR} & \text{if } a, b \text{ are NRs} \end{cases}$

This multiplication structure is similar to the binary addition table

addition mod 2		
a \ b	0	1
0	0	1
1	1	0

or

addition mod 2		
a \ b	even	odd
even	even	odd
odd	odd	even

For our purposes, it will be easier to track things with the multiplication table for $\{\pm 1\}$ (this is isomorphic to the above table by identifying $a \in \{0,1\}$ with $(-1)^a$).

multiplication in $\{\pm 1\}$		
a \ b	1	-1
1	1	-1
-1	-1	1

How can we identify the sets QR and NR with $\{\pm 1\}$?

Theorem Let $p > 2$ be prime and $0 < a < p$.

(a) If a is a quadratic residue mod p, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(b) If a is a quadratic non-residue mod p, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Pf: By FLT, we know $a^{p-1} \equiv 1 \pmod{p}$

so $x = a^{\frac{p-1}{2}}$ is a solution to

$$x^2 \equiv 1 \pmod{p}.$$

This factors mod p as

$$(x-1)(x+1) \equiv 0 \pmod{p}$$

so by prime divisibility, $x \equiv 1$ or $-1 \pmod{p}$.

If $a \equiv b^2 \pmod{p}$ for some b, then

$$x = a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$$

which proves (a).

For (b), suppose a is a NR mod p.

We know every $0 < i < p$ has a unique inverse mod p, that is, some $0 < j < p$ satisfying $ij \equiv 1 \pmod{p}$.

For every such i, $a \equiv ija \pmod{p}$ but if a is a quad. non-residue mod p, we cannot have $i = ja$ for any i, j pair.

By Wilson's Theorem on HW 4,

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdots (p-1)$$

combining the pairs i and ja

$$\equiv \underbrace{a \cdots a}_{\frac{p-1}{2} \text{ times}}$$

$$\equiv a^{\frac{p-1}{2}} \pmod{p}.$$

This proves (6). □

Def For an odd prime p and any $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$, the expression

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \pmod{p}$$

is called the **Legendre symbol** or **quadratic residue symbol** of a mod p.

By the **Theorem**,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is a QR mod } p \\ -1, & a \text{ is a NR mod } p \end{cases}$$

Theorem For any $a, b \in \mathbb{Z}$ not divisible by p, $\left(\frac{\cdot}{p}\right)$ has the following properties:

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

(b) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

Exercise 1: Prove this Theorem.

Exercise 2: Compute each of the following quadratic residue symbols. If $\left(\frac{a}{p}\right) = 1$, find all solutions to $x^2 \equiv a \pmod{p}$.

(a) $\left(\frac{3}{13}\right)$ (b) $\left(\frac{13}{3}\right)$

(a) $\left(\frac{2}{13}\right)$ (b) $\left(\frac{13}{3}\right)$

(c) $\left(\frac{11}{13}\right)$ (d) $\left(\frac{13}{11}\right)$

(e) $\left(\frac{2}{7}\right)$ (f) $\left(\frac{6}{7}\right)$

(g) $\left(\frac{75}{97}\right)$ (h) $\left(\frac{12}{109}\right)$

Next time: more on quadratic residues.