Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 6, 2023

What we have seen last week:

- Chinese Remainder Theorem
- Reduction and lifting

They are all methods to assembling information in different modular worlds.

Today, we will dip into quadratic problems in modular worlds. Namely, ***Quadratic residue***.

$$\{\text{roots of } f(T) \text{ in } \mathbb{Z}/M\} \xrightarrow{\sim} \prod_{\substack{p \text{ is a prime} \\ p | m}} \left\{\text{roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(M)}\right\}$$

$$\begin{tikzcd} \left\{\text{roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(M)}\right\} \arrow[d, shift right, "\text{Reduction}"'] \\ \{\text{roots of } f(T) \text{ in } \mathbb{F}_p\} \arrow[u, shift right, "\text{Lifting}"'] \end{tikzcd}$$

Specify to $f(T)$ quadratic

Part VIII

Quadratic Residues

Quadratic Residues

Definition 21.1

Let p be a prime number. We say an integer n (or the congruence class $[n]_p$) is a ***quadratic residue*** (***QR*** for short) modulo p if the quadratic polynomial $T^2 - n$ has a solution in $\mathbb{F}_p$. Otherwise we say n (or the congruence class $[n]_p$) a ***quadratic non-residue*** (***NQR*** for short) modulo p.

N.B. This property does not dependent on the choice of representative n.

QR = take square root in $\mathbb{F}_p$

Example 21.2

For each $x \in \mathbb{F}_7$, we have

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$

Hence, the quadratic residues modulo 7 are $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{4}$, and the quadratic non-residues modulo 7 are $\overline{3}$, $\overline{5}$, and $\overline{6}$.

Question

How to determine whether n is a quadratic residue modulo p effectively.

E.g. $\mathbb{F}_2$: $\overline{0}, \overline{1}$ are QR.

Theorem 21.3 (Euler) $\bar{a} \neq \bar{0}$ N.B. $\bar{0}^2 = \bar{0}$

Let p be an odd prime number and $a \in \Phi(p)$. Then

1. *a is a quadratic residue modulo p if and only if*

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

2. *a is a quadratic non-residue modulo p if and only if*

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

N.B. By Fermat Little Theorem, we always have $a^{p-1} \equiv 1 \pmod{p}$. Since p is odd, $\frac{p-1}{2}$ is an integer and $a^{\frac{p-1}{2}}$ has to be congruent to either 1 or -1 since it is a root of $T^2 - 1$ modulo p.

a prime

Method of Partnership

One idea to prove the theorem is the method of partnership.

Example 21.4

left over

Compute $1+2+\cdots+49 = \underbrace{24}_{\#\text{ pairs}} \cdot \underbrace{50}_{\text{sum of partners in each pair}} + 25 = 1225$

$$1 + 2 + \cdots + 24 + 25 + 26 + \cdots + 48 + 49$$

50

50

50

Method of Partnership

Example 21.5

Compute $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \pmod{11}$

$$1 \cdot 2 \cdot \overbrace{3 \cdot 4}^{1} \cdot 5 \cdot 6 \cdot \underbrace{7 \cdot 8}_{1} \cdot 9 \cdot 10$$

$10! \pmod{11} \equiv 10 \bmod 11.$

Theorem 21.6 (Wilson)

Let p be a prime number. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. We may focus on the case $p > 2$ since $p = 2$ case is obvious. Considering $\Phi(p)$, partner x and y whenever $xy \equiv 1 \pmod{p}$. Let's see what are left over.

A natural representative x is left over after the partnering, if $x^2 \equiv 1 \pmod{p}$. We know (from the knowledge of polynomials over $\mathbb{F}_p$) that such natural representatives can only be 1 or $p-1$. Therefore,

$$\begin{aligned}(p-1)! &= 1 \cdot (p-1) \cdot \text{the product of partners}\\ &\equiv -1 \cdot \text{the product of } 1 = -1 \pmod{p}.\end{aligned}$$ □

Quadratic Residues

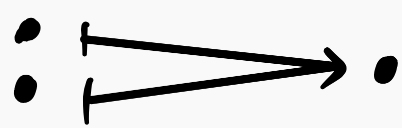
Theorem 21.7

Suppose p is an odd prime. Then exactly half (i.e. $\frac{p-1}{2}$) members of $\Phi(p)$ are quadratic residues.

Proof. Consider the map

$$\Phi(p) \xrightarrow{x \mapsto x^2 \pmod{p}} \Phi(p).$$

We will show that this is a 2-to-1 map. Hence, the number of members in its images is exactly half of $\phi(p)$. $\square$



Quadratic Residues

So why the map $\Phi(p) \xrightarrow{x \mapsto x^2 \pmod{p}} \Phi(p)$ is 2-to-1?

This amounts to say, for any quadratic residue $a \in \Phi(p)$, there are exactly two roots of the polynomial $T^2 - a$ modulo p.

First, since a is a quadratic residue modulo p, we know that the polynomial $T^2 - a$ has at least one root in $\mathbb{F}_p$. Let b be its natural representative, then $p - b \in \Phi(p)$.

Since p is odd, $p - b \neq b$. We thus obtain two different roots of $T^2 - a$ modulo p. But theorem 18.12 tells us that this polynomial has at most two roots in $\mathbb{F}_p$. Hence, we conclude that there are exactly two roots of the polynomial $T^2 - a$ modulo p.

Method of Partnership

Definition 21.8

Let p be a prime number and $a, x, y \in \Phi(p)$. We say x and y form a pair of ***a-partners*** if

$$xy \equiv a \pmod{p}.$$

E.g. For $p = 7$, we have the following a-partners:

$a = 1$ 1   2   3   4   5   6

$a = 2$ 1   2   3   4   5   6

$a = 3$ 1   2   3   4   5   6

Proof. If a is a quadratic residue modulo p, then there is $x \in \Phi(p)$ such that $x^2 \equiv a \cancel{\equiv}$ mod p. Therefore,

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

where the last congruence follows from the Fermat's little theorem.

If a is a quadratic non-residue modulo p, then any member of $\Phi(p)$ admits an a-partner distinct from it. Then the product of members of $\Phi(p)$ is precisely the product of $\frac{p-1}{2}$ pairs of a-partners. Therefore,

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p},$$

where the last congruence follows from the Wilson's theorem. $\square$

Example 21.9

Determine whether 3 is a quadratic residue modulo 43.

To apply Euler's theorem, we need to find the minimal representative of $3^{\frac{43-1}{2}} \pmod{43}$.

3^x	$\pmod{43}$
3^1	3
3^2	9
3^4	−5
3^8	25
3^{16}	−20

$$
\begin{aligned}
3^{\frac{43-1}{2}} &\equiv 3^{16+4+1} \pmod{43} \\
&\equiv -20 \cdot -5 \cdot 3 \pmod{43} \\
&\equiv 300 \pmod{43} \\
&\equiv -1 \pmod{43}
\end{aligned}
$$

Hence, 3 is a quadratic non-residue modulo 43.

Corollary 21.10

Let p be an odd prime number. Then T^2+1 is irreducible modulo p if and only if $p \equiv 3 \pmod{4}$.

role of congruence & modulus exchanged

Proof. T^2+1 is irreducible modulo p if and only if it has no roots in $\mathbb{F}_p$ if and only if -1 is a quadratic non-residue modulo p.

By Euler's theorem, this is equivalent to say

$$(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \qquad (*)$$

But we know that $(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ is even,} \\ -1 & \text{if } \frac{p-1}{2} \text{ is odd.} \end{cases}$

Hence, $(*)$ is equivalent to $p \equiv 3 \pmod{4}$. $\square$

Question

Suppose p is an odd prime number and $p \equiv 1 \pmod{4}$. How to find a root of $T^2 + 1$ modulo p?

Let A be the product of $1, 3, \cdots, p-2$, namely odd numbers in $\Phi(p)$.
Let B be the product of $2, 4, \cdots, \boxed{p-1}$, namely even numbers in $\Phi(p)$.
The factors of A and B can be paired by $x \leftrightarrow p - x$. Therefore,

$p - x \equiv -x \bmod p$

$$B \equiv (-1)^{\frac{p-1}{2}} A \equiv A \pmod{p}.$$

$\hookrightarrow 1$

On the other hand, we have

$$AB \equiv (p-1)! \equiv -1 \pmod{p}.$$

Hence, $\pm A$ are roots of $T^2 + 1$ modulo p.

$\pm A = \sqrt{-1}$ in $\mathbb{F}_p$

Legendre Symbols

Definition 21.11

Let p be a prime number and a be an integer. Then the ***Legendre symbol*** is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

This is NOT a fraction

If we use Legendre symbols, Euler's theorem can be interpreted as

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

Corollary 21.12

Let p be an odd prime number. Then the function $\left(\frac{-}{p}\right)$ is completely multiplicative:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \textit{for all} \quad a, b \in \mathbb{Z}.$$

If we translate the statement back to the definition of quadratic (non)-residue (and assume $p \nmid ab$), it says that $T^2 - ab$ is irreducible modulo p if and only if exactly one of the two polynomials $T^2 - a$ and $T^2 - b$ is irreducible modulo p.

Proof. First, since p is a prime, $p \mid ab$ if and only if $p \mid a$ or $p \mid b$. In this case, both $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ equals 0.

Now, assume $p \nmid ab$. Then by Euler's theorem,

$$\left(\frac{ab}{p}\right) \equiv \underbrace{(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}}_{\text{c.m.}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since both sides are valued in ± 1 and $-1 \not\equiv 1 \pmod{p}$, we conclude that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □