Quadratic Residues

Defn. Let p be a prime number.

- Say an integer n (or the congruence class $[n]_p$) is a quadratic residue (QR) modulo p if $T^2 \equiv n \bmod p$ (or equivalently, $T^2 - [n]_p = 0$) has a solution.

Rmk: this property does not dependent on the choice of rep. n.

- Otherwise, we say n (or the congruence class $[n]_p$) is a quadratic non-residue (QNR) modulo p

Defn. Let p be a prime number and a an integer.

Then the **Legendre symbol** is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a QR mod } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a QNR mod } p. \end{cases}$$

Important Observation:

If $a \equiv b \bmod p$, then

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

Theorem (Euler)

Let p be an odd prime number, and $a \in \mathbb{Z}(p)$. Then

(i) a is a quadratic residue mod p if and only if

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

(ii) a is a quadratic non-residue mod p if and only if

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

Using Legendre symbol:

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

Coro. (Complete multiplicativity of Legendre symbol)

Let p be an odd prime number, and a, b be integers. Then

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

Namely, ab is a QR

$\Leftrightarrow$ Both a & b are QRs or are QNRs

$T^2 - \overline{ab} \in \mathbb{F}_p[T]$ is reducible

$\Leftrightarrow$ Both $T^2 - \bar{a}$ and $T^2 - \bar{b}$ are reducible or both are irreducible.

$T^2 - 6$
$\Updownarrow$
$\cdot T^2 - 2$
$\cdot T^2 - 3$

Non trivial!

Proof: We have $p \mid ab \iff p \mid a$ or $p \mid b$.

If this is the case, we have

$$\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

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

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p$$

But bothsides are necessarily ± 1. Since p is odd, $1 \not\equiv -1 \mod p$.

Hence bothsides have to be the same in order to congruent to each other.

Thus,

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

□

Reciprocity laws

Reciprocity refers to:

a property of a mod b $\overset{\text{relate}}{\longleftrightarrow}$ another property of $\alpha(b)$ mod $\beta(a)$

(a: congruence, b: modulus; $\alpha(b)$: congruence only depends on b; $\beta(a)$: modulus only depends on a.)

The first such reciprocity law:

Coro (Reciprocity of -1) Let p be an odd prime number

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

(p: modulus; p: congruence)

Proof: By Coro of Euler's Theorem. Let p be an odd prime number.

Then $T^2 + \bar{1} \in \mathbb{F}_p[T]$ is irreducible if and only if $p \equiv 3 \bmod 4$.

Second Quadratic Reciprocity Law

Let p be an odd prime number. Then

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

p: modulus; $\equiv$: congruence

Proof: Consider the following subproduct of $(p-1)!$

$A = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-3}{2} \cdot \frac{p-1}{2}$ first half of $\Phi(p)$

$B = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-3) \cdot (p-1)$ evens in $\Phi(p)$

$C = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (p-4) \cdot (p-2)$ odds in $\Phi(p)$

Relations between them?

(1) each factor of B is $2\times$ a factor of A

$$A = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-3}{2} \cdot \frac{p-1}{2}$$

$$\times 2 \quad \times 2 \quad \times 2 \quad \cdots \quad \times 2 \quad \times 2$$

$$B = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-3) \cdot (p-1)$$

$$\Rightarrow \quad B = 2^{\frac{p-1}{2}} \cdot A$$

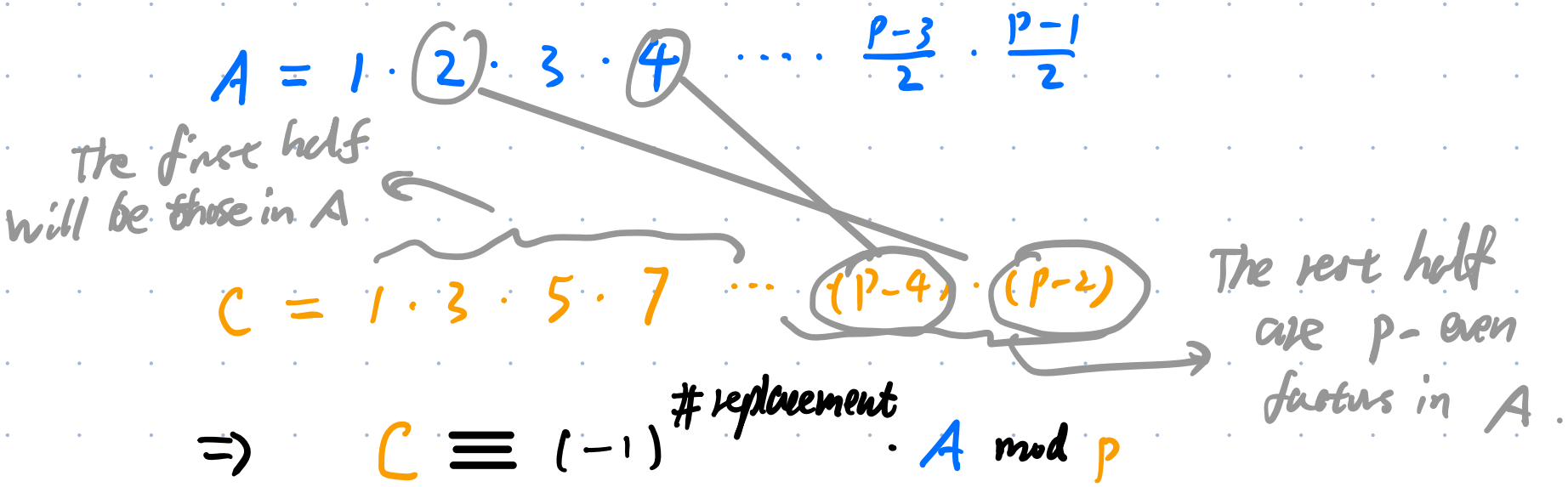
(2) each factor of C is $p-$ of a factor of B

$$B = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-3) \cdot (p-1)$$

$$C = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (p-4) \cdot (p-2)$$

$$\Rightarrow \quad C \equiv (-1)^{\frac{p-1}{2}} \cdot B \mod p$$

(3) In A, replacing each even factor x by $p-x$, we get C



$$\Rightarrow \quad C \equiv (-1)^{\#\text{replacement}} \cdot A \mod p$$

Note that

$$\#\text{replacement} = \#\text{even numbers in } 1, 2, \cdots, \frac{p-1}{2}$$

$$= \left\lfloor \frac{p-1}{4} \right\rfloor$$

floor : the largest integer $\leq \frac{p-1}{4}$,

Combine (1), (2), and (3):

$$C \equiv (-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \cdot A \equiv (-1)^{\lfloor \frac{p-1}{4} \rfloor} \cdot A \bmod p.$$

$C \equiv (-1)^{\frac{p-1}{2}} \cdot B \bmod p$, $B = 2^{\frac{p-1}{2}} \cdot A$ $\qquad$ $C \equiv (-1)^{\#\text{replacement}} \cdot A \bmod p$

Since A is invertible mod p, we can cancel it.

$$(-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \equiv (-1)^{\lfloor \frac{p-1}{4} \rfloor} \bmod p.$$

Therefore, by Euler's Theorem,

$$\left(\frac{2}{p}\right) \equiv \cdot 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot (-1)^{\lfloor \frac{p-1}{4} \rfloor} \bmod p.$$

ALL Possibilities:

$p \bmod 8$	$\frac{p-1}{2} \bmod 2$	$\lfloor \frac{p-1}{4} \rfloor \bmod 2$	$\left(\frac{2}{p}\right)$
1 $p = 8k+1$	$4k$ 0	$\lfloor 2k \rfloor = 2k$ 0	1
3 $p = 8k+3$	$4k+1$ 1	$\lfloor 2k+\frac{1}{2} \rfloor = 2k$ 0	-1
5 $p = 8k+5$	$4k+2$ 0	$2k+1$ 1	-1
7 $p = 8k+7$	$4k+3$ 1	$\lfloor 2k+\frac{3}{2} \rfloor = 2k+1$ 1	1

Third Quadratic Reciprocity Law

Prime factorization + comple mult;
$\left(\frac{n}{p}\right) \rightsquigarrow \left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)^{q \in \text{odd prime}}$.

Theorem (Gauss)

Let p and q be two different odd primes. Then

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

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

$(-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right)$ (Euler)

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

$p^* := (-1)^{\frac{p-1}{2}} \cdot p$

Rmk:

If we introduce $p^* := (-1)^{\frac{p-1}{2}} \cdot p$, then the statement says

congruence ← $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$ → congruence

p: modulus; q: modulus

Application: Effectively compute $\left(\frac{a}{p}\right)$.

$\frac{10337-1}{2} = 5168$

E.g. Is 10 a QR mod 10337?

$10^{5168} \bmod 10337$

1.) $10 = 2 \times 5$ Hence, $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = 1 \cdot (-1) = -1$

2.) $\left(\frac{2}{p}\right) = ?$ $\rightsquigarrow$ $p \equiv ? \bmod 8$

$8 \mid 1000$ $8 \mid 32$ $8 \mid 16$

$10337 \equiv 337 \equiv 17 \equiv 1 \bmod 8$

Hence, $\left(\frac{2}{p}\right) = 1$ by Second Quadratic Reciprocity Law.

3.) $\left(\frac{5}{p}\right) = \left(\frac{p^*}{5}\right)$ $(-1)^{\frac{10337-1}{2}} = (-1)^{5168} = 1$ (5168 even)

Hence, $p^* = 10337 \equiv 7 \equiv 2 \bmod 5$

But we know $\left(\frac{2}{5}\right) = -1$ by SQRL Conclusion: 10 is QNR.!

Application: Reducibility of quadratic polynomials.

E.g. $f(T) = T^2 - 2T + 4$.

Q: For which prime number p, $f(T)$ is irreducible mod p?

($\Leftrightarrow$ $f(T)$ has no roots in $\mathbb{F}_p$.)

1. Complete square

$$f(T) = (T-1)^2 + 3$$

2. Then $f(T)$ is reducible mod p

$\Leftrightarrow$ $f(T)$ has a roots in $\mathbb{F}_p$

$\Leftrightarrow$ $\exists\, a \in \mathbb{F}_p$ s.t. $(a-\bar{1})^2 + \bar{3} = \bar{0}$

$\Leftrightarrow$ -3 is a QR mod p

$\Leftrightarrow$ $\left(\frac{-3}{p}\right) = 1$ or 0

3. Looking at the contrapositive,

$f(T)$ is irreducible mod p $\Leftrightarrow$ $\left(\frac{-3}{p}\right) = -1$.

Note that $\frac{3-1}{2} = 1$, hence, $3^* = -3$.

By Gauss' Quadratic Reciprocity Law,

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

Note that: $\Phi(3) = \{1, 2\} \xrightarrow{(\cdot)^2} \{1\}$ $\bar{1}$ is a QR mod 3

Hence, $\bar{2}$ is the only QNR mod 3.

Therefore, $\left(\frac{p}{3}\right) = -1 \Leftrightarrow p \equiv 2 \bmod 3$

Conclusion: $T^2 - 2T + 4$ is irreducible mod p $\Leftrightarrow p \equiv 2 \bmod 3$

How about this one:

e.g. $f(T) = T^2 - T + 1$.

Q: For which prime number p, $f(T)$ is irreducible mod p?

After all, we need to complete the square over $\mathbb{F}_p$

If we can do this over $\mathbb{Z}$, we are done by mod p.

However, we CANNOT complete the square over $\mathbb{Z}$!

$$T^2 - T + 1 = \left(T - \tfrac{1}{2}\right)^2 + \tfrac{3}{4}$$

NOT INTEGERS!!!

What to do ?

$f(T) = T^2 - T + 1$.

1. Complete the square over $\mathbb{F}_p$.

- First note that $f(T)$ has NO roots in $\mathbb{F}_2$.

  Hence, $f(T)$ is irreducible mod 2

- In what follows, we may assume p is odd.

  Note that $p - 1 \equiv -1 \bmod p$

  But $p - 1$ is even

  $\rightsquigarrow T^2 + (p-1)T + 1$ is

  able to complete the square over $\mathbb{Z}$.

$$f(T) \equiv T^2 + (p-1)T + 1 \mod p$$ Note that $p-1$ is even!

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

This is an integer! ↑ ↑ an integer!

$$\left(\frac{p-1}{2}\right)^2 - 1 = \frac{p+1}{2} \cdot \frac{p-3}{2}$$ ← $A^2 - B^2 = (A+B)(A-B)$

2. Then $f(T)$ is reducible mod p

$\Leftrightarrow$ $f(T)$ has a roots in $\mathbb{F}_p$

$\Leftrightarrow$ $\exists\, a \in \mathbb{F}_p$ s.t. $\left(a + \left[\frac{p-1}{2}\right]_p\right)^2 = \left[\frac{p+1}{2}\right]_p \left[\frac{p-3}{2}\right]_p$

$\Leftrightarrow$ $\frac{p+1}{2} \cdot \frac{p-3}{2}$ is a QR mod p

$\Leftrightarrow$ Both $\frac{p+1}{2}$ & $\frac{p-3}{2}$ are QR mod p or both are QNR mod p or one of them is $\bar{0}$

$\Leftrightarrow \left(\frac{\frac{p+1}{2}}{p}\right) = \left(\frac{\frac{p-3}{2}}{p}\right)$ or one of them is 0