Quadratic residues in $U(p) = \mathbb{Z}_p^\times$

in the group of units modulo p, i.e. the non-zero elements mod p, where p is an odd prime, i.e. $p > 2$.

Def Let $n \not\equiv 0 \mod p$

n is a quadratic residue modulo p iff $\exists\, u \in U(n)$ such that

$$u^2 \equiv n \mod p.$$

n is a quadratic non-residue otherwise

We've seen

- ~~P21~~ there $\frac{p-1}{2}$ residues mod p
- $$(n|p) = \begin{cases} +1, & n \text{ is a quad. res.} \\ -1, & n \text{ is a quad non-res} \end{cases}$$

"Legendre symbol"

- it's completely multiplicative.

$$(nm|p) = (n|p)(m|p).$$

- Euler's criterion.

$$(n|p) \equiv n^{\frac{p-1}{2}} \pmod p$$

An application of this showed

$$(-1|p) = \begin{cases} +1, & p \equiv 1 \bmod 4. \\ -1, & p \equiv 3 \bmod 4. \end{cases}$$

Q? Good ways to evaluate $(n|p) = ?$

$(2|p)$ will follow a regular pattern based on p.

A second application of Euler's criterion.

Eg $\quad (2|p) \equiv 2^{\frac{p-1}{2}} \pmod p$

$\equiv ?$

Approach $2^{\frac{p-1}{2}}$ modulo p in two ways.

First:

$$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$$

$$= \prod_{i=1}^{\frac{p-1}{2}} 2i$$

$$= 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)\right)$$

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

Secondly, look at product of all even cong. classes in a different way. (mod p).

$$p-1 \equiv -1 \equiv (-1)^1 1$$

$$2 \equiv 2 \equiv (-1)^2 2$$

$$p-3 \equiv -3 \equiv (-1)^3 3$$

$$4 \equiv 4 \equiv (-1)^4 4$$

$$p-5 \equiv -5 \equiv (-1)^5 5$$

$$\vdots$$

$$S \equiv \qquad \equiv (-1)^{\frac{p-1}{2}} \quad \frac{p-1}{2}$$

$$\boxed{\prod_{i=1}^{(p-1)/2} 2i} \equiv \prod_{j=1}^{(p-1)/2} (-1)^j j$$

$$= \left[\prod_{j=1}^{(p-1)/2} (-1)^j\right] \left(\frac{p-1}{2}\right)!$$

$a^b a^c = a^{b+c}$

$$= (-1)^{\overbrace{1+2+3+\dots+\frac{p-1}{2}}} \left(\frac{p-1}{2}\right)!$$

$1+2+3+\dots+N = \frac{1}{2}N(N+1)$ Arithmetic Formula.

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

$$\boxed{= (-1)^{\frac{1}{8}(p^2-1)} \left(\frac{p-1}{2}\right)!}$$

Equating these two expressions for $\prod_{i=1}^{(p-1)/2} 2i$ we get.

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{(p^2-1)/8} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

$$\Longrightarrow \quad 2^{\frac{p-1}{2}} \equiv (-1)^{(p^2-1)/8} \pmod{p}$$

since $\gcd\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$ and so $\left(\frac{p-1}{2}\right)!$ is invertible modulo p.

So remembering Euler's criterion

$$(2|p) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{(p^2-1)/8} \mod p.$$

$$\equiv \begin{cases} +1, & (p^2-1)/8 \text{ is even.} \\ -1, & (p^2-1)/8 \text{ is odd} \end{cases}$$

$$= \begin{cases} +1, & p \equiv 1, 7 \mod 8. \\ -1, & p \equiv 3, 5 \mod 8. \end{cases}$$

$p \bmod 8 \quad p \equiv 1, 3, 5, 7 \bmod 8$

eg. $p = 8m + 7$

$$p^2 - 1 = 64m^2 + 112m + 49 - 1$$

$$= 64m^2 + 112m + 48$$

$$\frac{p^2 - 1}{8} = 8m^2 + 14m + 6.$$

which is even.

So

$$(2|p) \equiv \begin{cases} +1, & p \equiv 1, 7 \pmod 8 \\ -1, & p \equiv 3, 5 \bmod 8 \end{cases}$$

We could continue applying Euler's criterion to seek to understand $(3|p)$, $(5|p)$ etc.

Recall from yesterday.

If $n = \prod_{i=1}^{r} q_i^{a_i}$ is the prime factorization of n.

$$(n|p) = $$

$$= \left(\prod_{i=1}^{r} q_i^{a_i} \,\middle|\, p\right).$$

$$= \prod_{i=1}^{r} (q_i|p)^{a_i}$$

, since $(\cdot|p)$ is multiplicative.

$$= \prod_{\substack{i=1 \\ a_i \text{ odd}}}^{r} (q_i|p)$$

We see here that to understand $(n|p)$ we just need to understand $(q|p)$ for pairs of primes q, p.

Let's investigate $(q|p)$

From our plotting we see very systematic behaviour of the agreement/disagreement of $(p|q)$ and $(q|p)$, alternating behaviour across the odd integers. ie. pattern based on prime modulo 4.

These plots reveal the "Law of Quadratic Reciprocity" which is

$$(p|q) = \begin{cases} -(q|p), & p \equiv q \equiv 3 \pmod 4 \\ (q|p), & \text{otherwise} \end{cases}$$

Remember any odd prime p satisfies $p \equiv 1, 3 \pmod 4$

A proof based on Euler's criterion is given in the notes but many other proofs exist.

Main application of L.Q.R. is to an algorithm for calculating $(n|p)$.

L.Q.R. $(p|q) = (-1)(q|p)$ depending on p, q mod 4

FLIP

REDUCE

If $n \equiv m \bmod p$

$(n|p) = (m|p)$

FACTORIZE

$(nm|p) = (n|p)(m|p)$

Eg. Let's determine residue status of 219 modulo 383 (a prime).

i.e. $(219|383)$

$$= (3 \cdot 73 \mid 383)$$

$$= (3 \mid 383)(73 \mid 383),$$ by factoring

$$= \left(-(383 \mid 3)\right)(383 \mid 73),$$ by L.Q.R

$$= \left(-\underbrace{(2 \mid 3)}\right)(18 \mid 73)$$

$$= (18 \mid 73),$$ since $(2 \mid 3) = -1$ as 2 is the non-residue modulo 3

$$= (2 \mid 73)(3 \mid 73)^2, \quad 18 = 2 \cdot 3^2$$

$$= (2 \mid 73)$$

$$= +1,$$ by $(2 \mid p)$ result and $73 \equiv 1 \bmod 8$

So $(219 \mid 383) = +1$.

So 219 is a Quad. residue modulo 383

A second example.

461 modulo 773. A residue or not?

a prime

$$(461 | 773)$$

$$= (773 | 461), \text{ by L.Q.R. } 461 \equiv 1 \bmod 4$$

$$= (312 | 461), \text{ by reduction since } 773 \equiv 312 \bmod 461$$

$$= (2^3 \cdot 3 \cdot 13 \mid 461)$$

$$= (2 | 461)\,(3 | 461)\,(13 | 461)$$

$$= (-1)(3 | 461)(13 | 461)$$

, by $(2|p)$ result and $461 \equiv 5 \bmod 8$.

$= (-1)(461|3)(461|13)$

, by L.Q.R.

$= -(2|3)(6|13)$

, by reduction mod3 and mod 13

$= (6|13)$, since 2 is a non-residue mod3

$= (2|13)(3|13)$

$= -(13|3)$, by $(2|p)$ result and L.Q.R.

$= -(1|3)$, by reduction

$= -1$

So $(461|773) = -1$

so 461 is a non-residue modulo 773