Quadratic Residues

Concept of "square roots" in modular arithmetic.

Consider solving a quadratic equation over $\mathbb{R}$.

$$ax^2+bx+c=0.$$

By the well-known quadratic formula.

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

provided that $b^2-4ac\geqslant 0$

Proof (assuming $a\neq 0$)

$$ax^2+bx+c=0$$

$$\Longleftrightarrow \quad 4a^2x^2+4abx+4ac=0$$

$$\Longleftrightarrow \quad \underbrace{(2ax+b)^2}-b^2+4ac=0$$

$\Leftrightarrow \quad (2ax+b)^2 = b^2 - 4ac$

$\Leftrightarrow \quad 2ax + b = \pm\sqrt{b^2-4ac}$

(provided $b^2 - 4ac \geq 0$, otherwise no $x \in \mathbb{R}$ can satisfy the equation)

$$\Leftrightarrow \quad x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Can we do the same for $p>2$. congruence. (p an odd prime, and $a \not\equiv 0 \pmod p$ ie. $p \nmid a$)

$$ax^2 + bx + c \equiv 0 \mod p.$$

$$\Leftrightarrow \quad 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p$$

Note $4a$ is invertible mod p since $\gcd(4a, p) = 1$ since p is an odd prime and $p \nmid a$

$\iff (2ax+b)^2 - b^2 + 4ac \equiv 0 \pmod p$

$\iff (2ax+b)^2 \equiv b^2 - 4ac \pmod p.$

$\iff 2ax+b \equiv u \pmod p$

where $u^2 \equiv b^2 - 4ac \pmod p$

providing such a u exists

Does it?

$\iff x \equiv (u-b)(2a)^{-1} \pmod p.$

Given a congruence class mod p. Is it a square?

<u>Def 8.1</u> Let p be an odd prime ($p > 2$) and let n denote a congruence class modulo p.

$n \not\equiv 0 \mod p.$

We say n is a ~~~~ Quadratic modulo p if there are solutions to

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

n is a quadratic non-residue if there are no solutions to

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

We seek to understand residues.

Examples:

$p=7$

What are the residues mod p?

$n \equiv 1, 2, 3, 4, 5, 6$

$1 \equiv 1^2 \quad 3^2 \equiv 2 \quad 4 \equiv 2^2 \pmod{7}.$

So $1, 2, 4$ are residues mod 7

while 3, 5, 6 are non-residues mod 7.

From this and other examples.

Conjecture. For mod p, there are an equal number $\frac{p-1}{2}$ of residues and non-residues.

Observation If m is a square integer in the usual sense eg. $m = 1, 4, 9, 16, \ldots$ then m will be a quadratic residue mod p.

The main question remains.

Is n a residue mod p?

Theorem 8.1 There are $\frac{p-1}{2}$ residues and non-residues mod p.

Proof $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$.

Clearly the cong. classes.

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2 \qquad (*)$$

are all quadratic-residues. and they are all different mod p.

<u>Prof</u> Suppose $n^2 \equiv m^2 \mod p$.

where $1 \leq n, m \leq \frac{p-1}{2}$.

$$\iff p \mid n^2 - m^2$$

$$\iff p \mid (n-m)(n+m).$$

$$\iff p \mid n-m \ \underline{\text{OR}}\ p \mid n+m.$$

But $2 \leq n+m \leq p-1$

and there are no multiples of p in this range so $p \nmid n+m$.

$$\Rightarrow p \mid n-m$$

$$\Rightarrow n \equiv m \mod p.$$

$\Rightarrow n = m$

So there a least $\frac{p-1}{2}$ residues (see the list at (*))

Moreover (*) lists ~~all~~ the residues.

For suppose j^2 is a residue with $\frac{p+1}{2} \le j \le p-1$.

But then $i = p - j$

and $1 \le i \le \frac{p-1}{2}$

and $j \equiv -i \pmod{p}$.

and so $j^2 \equiv i^2 \pmod{p}$

and so j^2 is already listed in (*)

This proves there are exactly $\frac{p-1}{2}$ residues mod p and by implication there are also $\frac{p-1}{2}$ non-residues mod p

$\blacksquare$

In our motivation we connected the ideas of positive/negatives and having / ~~ha~~ not-having a square root.

residue / non-residue.

Now in $\mathbb{Z}_p^\times$ there is no immediate concept of positive/negative.

But we can salvage something. pos/negs. behave very systematically under multiplication.

pos $\times$ pos $=$ pos. pos $\times$ neg $=$ neg

neg $\times$ neg $=$ pos

Consider an example say modulo $p=71$.

eg. 44, 46 are both non-residues.

$44 \cdot 46 \equiv 36 \mod 71$

$\equiv 6^2$ which is a residue

62, 63 are non-residues.

$62 \cdot 63 \equiv 1 \mod 71$

and 1 is a residue.

38 is a residue, 47 is a non-residue

$38 \cdot 47 \equiv 11 \mod 71$

which is a non-residue

and $40 \cdot 31 \equiv 33 \pmod{71}$

a non-residue

$24 \cdot 25 \equiv 32 \pmod{71}$

a residue.

So from inspecting examples we can form a conjecture.

① res × res = res

② non-res × non-res = res.

③ non-res × res = non-res.

Proofs

① Let a, b be residues mod p.

say $a \equiv \alpha^2$, $b \equiv \beta^2 \pmod p$

$$ab \equiv \alpha^2 \beta^2 \mod p$$
$$\equiv (\alpha\beta)^2 \mod p.$$

So ab is also a residue. ☒

③ Let a be a residue and b a non-residue mod p.

Say $a \equiv \alpha^2 \pmod p$

Assume ab is residue

say $ab \equiv \gamma^2 \mod p$.

$$\Rightarrow \alpha^2 b \equiv \gamma^2$$
$$\Rightarrow b \equiv (\alpha^{-1})^2 \gamma^2$$
$$\Rightarrow b \equiv (\alpha^{-1}\gamma)^2 \mod p$$

$\Rightarrow$ b is residue (mod p)

This contradicts the above.

So by "proof by contradiction" principle we get that ab is a non-residue modulo p.

non-res × non-res = residue.

(2) Seems harder to get a handle on

~~So~~ we assume a, b are both non-residues. What of ab?

Let $r_1, \dots, r_{\frac{p-1}{2}}$ be the residues mod p.

we've prove that $a r_i$ is always a non-residue. $ar_1, ar_2, \dots, ar_{\frac{p-1}{2}}$

Suppose ab is a non-residue, this means

$$ab \equiv a r_i \pmod p$$

$\Rightarrow$ $b \equiv r_i$, a residue.

But this contradicts the ~~[illegible]~~ assumption that b is a non-residue.

So therefore ab must be a residue modulo p. ∎

Def 8.2 Legendre symbol.

We define a symbol/notation for n modulo p to indicate whether or not n is a quadratic residue mod p.

$$(n|p) = \begin{cases} +1, & \text{if } n \text{ is a res.} \\ -1, & \text{if } n \text{ is a non-res.} \end{cases}$$

So eg.

$$(1|7) = (2|7) = (4|7) = +1$$

$$(3|7) = (5|7) = (6|7) = -1.$$

Notice that our proofs of the conjectures on how residues/non-residues multiply, tells us that $(\cdot|p)$ is a multiplicative function of the first argument. Namely,

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

So let's try and extract the values for $(n|p)$ based on the prime factorization of n.

$$n = \prod_{i=1}^{r} q_i^{a_i}$$, for distinct primes q_i

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

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

, by multiplicative prop.

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

So general problem of deciding if n is a residue mod p reduces to the problem of understanding whether a prime q is a residue modulo another prime p.

<u>Quadratic Reciprocity</u> is a governing principle over the answers to $(q|p)$.

Get more insight into evaluating $(n|p)$.

Recall Fermat's Little Theorem.

$$n^{p-1} \equiv 1 \mod p.$$

for $n \in \mathbb{Z}_p^\times$. ie. $n \not\equiv 0 \mod p$.

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

So $n^{\frac{p-1}{2}}$ is a solution to

$$x^2 \equiv 1 \mod p.$$

i.e. $x \equiv -1, +1 \mod p$.

the only two solutions by Lagranges theorem from chapter 7.

$$\implies n^{\frac{p-1}{2}} \equiv -1 \text{ or } +1 \pmod{p}.$$

Is this connected to $(n|p)$??

In fact they're the same.

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

Theorem 8.4. (Eulers Criterion).

<u>Proof</u> <u>Assume $(n|p) = +1$</u>

i.e. n is a quadratic residue mod p.

ie. $n \equiv u^2 \pmod p$

for none u.

But now.

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

$$\equiv u^{p-1}$$

$$\equiv +1 \pmod p \text{ by F.L.T.}$$

So $(n|p) \equiv n^{\frac{p-1}{2}}$ in this case.

Secondly, assume $\boxed{(n|p) = -1}$

ie. n is a non-residue mod p.

Let $r_1, \ldots, r_{\frac{p-1}{2}}$ be the residues mod p.

these are all solutions to

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

and by Lagrange's theorem these are <u>all</u> the solutions.

$$\Rightarrow n^{\frac{p-1}{2}} \not\equiv +1 \pmod p$$

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

So again in this case, $(n|p)$ and $n^{\frac{p-1}{2}}$ both agree modulo p.

So overall

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

Two applications.

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

by Euler's criterion.

$$= \begin{cases} +1 & \text{if } \frac{p-1}{2} \text{ is even.} \\ -1 & \text{if } \frac{p-1}{2} \text{ is odd.} \end{cases}$$

$$= \begin{cases} +1, & p-1 \equiv 0 \bmod 4. \\ -1, & \text{if } p-1 \equiv 2 \bmod 4. \end{cases}$$

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

Euler's criterion also quickly settles.

$(2|p)$

Can show

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