Quadratic Residue

Zihan Yi

University of California, Santa Barbara

May 2, 2014

Definition

A nonzero square in Z/pZ is called a quadratic residue modulo n.
i.e. if there exists an integer x such that: $x^2 \equiv q$ mod(n)
Otherwise, q is called quadratic nonresidue modulo n.

Examples:

1. What is the quadratic residue modulo 11?
2. What is the quadratic residue modulo 17?

Preposition

Preposition: Half of the elements of (Z/pZ) are quadratic residues.
Prove: There are at most $\frac{p-1}{2}$ squares because:
$1^2 \equiv (p-1)^2$
$2^2 \equiv (p-2)^2$
$3^2 \equiv (p-3)^2$
...
$(\frac{p-1}{2})^2 \equiv (\frac{p+1}{2})^2$

Furthermore, these squares are all distinct because for any
$a, b \in Z/pZ$,
$a^2 = b^2 \rightarrow (a+b)(a-b)) = 0 \rightarrow b = \pm a$
So these $\frac{p-1}{2}$ squares must be distinct.
That completes the argument.

Euler's criterion

In number theory, Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime. Precisely, let p be an odd prime and a an integer coprime to p. Then $a^{\frac{p-1}{2}} \equiv 1$ (mod p) if there is an integer x such that
$a \equiv x^2 (mod p)$;
$a^{\frac{p-1}{2}} \equiv -1$ (mod p) if there is no such integer.
Euler's criterion can be concisely reformulated using the Legendre symbol:
$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$ mod p

Proof:

(1)$a \equiv x^2$

According to Fermat's little theorem (what we proved in the last semester):

If x coprime to p, $x^{p-1} \equiv 1$ mod p

$(x^2)^{\frac{p-1}{2}} \equiv 1$ mod p

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

(2)$a \not\equiv x^2$
Because of the Fermat's little theorem, $a^{p-1} \equiv 1 \text{ mod p}$
Then we can get $(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \text{ mod p}$
If there is no such an integer, $a^{\frac{p-1}{2}} \not\equiv 1$
So $a^{\frac{p-1}{2}} - 1 \not\equiv 0 \rightarrow a^{\frac{p-1}{2}} + 1 \equiv 0$
So $a^{\frac{p-1}{2}} \equiv -1$

Legendre Symbol

Legendre symbol's original definition was by means of explicit formula:

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \text{ mod p}$$

Legendre Symbol

In number theory, the legendre symbol is a multiplicative function with values 1,-1,0 that is quadratic character modulo a prime number p: its value on a (non-zero) quadratic residue mod p is 1 and on a non-quadratic residue is -1. Its value on zero is 0.

Let P be an odd prime number. An integer a is a quadratic residue mod p if it is congruent to a perfect square modulo p; otherwise, it is a quadratic non-residue modulo p.

(1)$(\frac{a}{p})$=1, if a is a quadratic residue modulo p and a $\not\equiv$ 0 mod p

(2)$(\frac{a}{p})$=-1, if a is a quadratic non-residue modulo p

(3)$(\frac{a}{p})$=0, if $a \equiv$ 0 mod p

Properties of Legendre Symbol

property 1

If $a \equiv b$ mod p, then $(\frac{a}{p}) = (\frac{b}{p})$

In other words, $(\frac{a+p}{p}) = (\frac{a}{p})$

Properties of Legendre Symbol

property 2

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

Furthermore, if $(a, p) = 1$, then $(\frac{a^2}{p}) = 1$; if $(a, p) \neq 1$, then $(\frac{a^2}{p}) = 0$

quadratic reciprocity

Let p and q be odd primes, $p \neq q$. Using the Legendre symbol, the quadratic reciprocity law can be stated concisely:

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

Supplements to the Law of Quadratic Reciprocity

The first supplement to the law of quadratic reciprocity:

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

(1) If $p \equiv 1 \bmod 4$, the $(\frac{-1}{p}) = 1$

(2) If $p \equiv 3 \bmod 4$, the $(\frac{-1}{p}) = -1$

Supplements to the Law of Quadratic Reciprocity

The second supplement to the law of quadratic reciprocity:

$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

(1) If $p \equiv 1$ or 7 (mod 8), the $(\frac{2}{p}) = 1$

(2) If $p \equiv 3$ or 5 (mod 8), the $(\frac{2}{p}) = -1$

Supplements to the Law of Quadratic Reciprocity

Special formulas for the Legendre symbol $(\frac{a}{p})$ for small values :
For an odd number prime $p \neq 3$,
$(\frac{3}{p}) = (-1)^{\frac{p+1}{6}}$
(1) If $p \equiv 1$ or 11 (mod 12), the $(\frac{3}{p}) = 1$
(2) If $p \equiv 5$ or 7 (mod 12), the $(\frac{3}{p}) = -1$

Supplements to the Law of Quadratic Reciprocity

Special formulas for the Legendre symbol $(\frac{a}{p})$ for small values
For an odd number prime $p \neq 5$,
$(\frac{5}{p}) = (-1)^{\frac{p+2}{5}}$
(1) If $p \equiv 1$ or 4 (mod 5), the $(\frac{5}{p}) = 1$
(2) If $p \equiv 2$ or 3 (mod 5), the $(\frac{5}{p}) = -1$

Computational example

Here is an example:

$(\frac{12}{47}) = (\frac{3}{47})(\frac{4}{47})$

$= (\frac{47}{3})(-1)^{\frac{47-1}{2}\frac{3-1}{2}}$

$= (\frac{2}{3})(-1)$

$= -(\frac{2}{3})$

$= -(-1)^{\frac{9-1}{8}} = 1$

So 12 is a quadratic residue modulo 47.

Computational example

Here is another example:

$$(\frac{91}{563}) = -(\frac{17}{91})$$
$$= -(\frac{6}{17})$$
$$= -(\frac{2}{17})\frac{3}{17}$$
$$= -(-1)^{\frac{17^2-1}{8}}(\frac{17}{3})(-1)^{\frac{17-1}{2}\frac{3-1}{2}}$$
$$= -(\frac{2}{3})$$
$$= (-1)^{\frac{3^2-1}{8}} = 1$$

So 91 is a quadratic residue modulo 563.

Computational example

One more example!!!

Thank you

Thanks for listening!!!