Quadratic Residues

COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
SRI CITY, INDIA

Groups

$2 +_5 4 = 6 \bmod 5 = 1$

1) Closure: $a +_n b \in Z_n$
2) Associative
3) Existence of identity
4) Existence of inverse

$(a +_n b) +_n c$
$= a +_n (b +_n c)$

Additive Group: $+_n$

- $\mathbf{Z_n}$ = {0, 1, …, n-1} forms a group under addition modulo n.

Multiplicative Group:

- Z_n^* = {x | 1 <= x < n and gcd(x,n) = 1} forms a group under multiplication modulo n. $\times_n$
  - For prime p, Z_p^* includes all elements [1,p-1].
  - E.g., Z_6^* = {1, 5} ✓
  - E.g., Z_7^* = {1, 2, 3, 4, 5, 6} ✓

$2 \times_5 4 = 8 \bmod 5$
$= 3$

Order and Generator

Order of x: smallest t such that $x^t = 1 \bmod n$
- E.g., in Z_{11}^*, ord(3) = 5, ord(2) = 10

Generator: an element whose order = group size.
- E.g., 3 is the generator of Z_7^*

Subgroup: generated from an element of order t < Φ(n)
- $\{1,3,3^2=9,3^3=5,3^4=4\} = \{1,3,4,5,9\}$ is a subgroup of Z_{11}^*

A group is cyclic if it has a generator.

For any prime p, the group Z_p^* is cyclic, i.e, every Z_p^* has a generator, say g.
- $Z_p^* = \{1, g, g^2, g^3, \ldots, g^{p-2}\}$

$\boxed{a \times 1 = 1 \times a = a}$

$a + 0 = 0 + a = a$

$3^2 = 9 \bmod 11 = 9$

$3^3 = 5 \bmod 11$

$3^4 = 81 \bmod 11 = 4$

$3^5 = 4 \times 3 \bmod 11 = 1$

$3^4 \times 3$ 5

$(3^5)^2 = 1$

$(3^5)^3 = 1$

$3^1 = 3$

$3^2 = 9 \bmod 7 = 2$

$3^3 = 6$

$3^4 = 4$

$3^5 = 5$

$3^6 = 1$

Quadratic Residue

$\boxed{x^2+1=0}$ has no solution in $\mathbb{R}$

$\Rightarrow \boxed{x^2=-1}$ in $\mathbb{C}$

$x = \pm\sqrt{-1}$

$= \pm i$

- y is a quadratic residue (mod n) if there exists x in Z_n^* such that $x^2 = y \pmod n$

  i.e., y has a square root in Z_n^*

- **Claim:** For any prime p, every quadratic residue has exactly two square roots x, -x mod p.

- **Proof:** if $x^2 = u^2 \pmod p$, then $(x-u)(x+u) = 0 \pmod p$,

  so, either p divides x-u (i.e., x=u), or p divides x+u (i.e., x=-u)

  It implies if $x^2 = 1 \pmod p$, x = 1 or -1.

Quadratic Residue

Theorem: For any prime p, and g is generator,

$\boxed{g^k \text{ is a quadratic residue iff k is even}}$.

Given $Z_p^* = \{1, g, g^2, g^3, \ldots, g^{p-2}\}$

- Even powers of g are quadratic residues
- Odd powers of g are not quadratic residues

Legendre symbol:

- $\left(\frac{a}{p}\right)$ = 1 if a is a quadratic residue mod p,

  -1 if a is not a quadratic residue mod p,

  0 if p divides a.

Euler's Criteria

$x^2 = 1 \Rightarrow x = \pm 1$

Theorem: **For prime p>2 and a in Z_p^*, $\boxed{\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p}$.**

- Z_p^* is cyclic, a = g^k for some k.
- If k is even, let k = 2m, $a^{(p-1)/2} = g^{(p-1)m} = 1$.
- If k is odd, let k = 2m+1, $a^{(p-1)/2} = g^{(p-1)/2} = -1$.
- Reasons:
  - This is a square root of 1.
  - $g^{(p-1)/2} = 1$ since ord(g) = (p-1)/2.
  - But 1 has two square roots. Thus, the only solution is -1.

$(g^{p-1})^{1/2} = \sqrt{1} \bmod p$

$x = \sqrt{1}$

$\Rightarrow x^2 = 1 \bmod p$

If n is prime, $a^{(n-1)/2}$= 1 or -1.

If we find $a^{(n-1)/2}$ is $\boxed{\text{not 1 and -1,}}$ n is composite.

$$\left(\frac{3}{5}\right) = 3^{(5-1)/2} \pmod 5 = -1 \text{ QNR}$$

large

$3^2 \bmod 5 = 4 \bmod 5 = -1$

$\nexists$ no $y \in Z_5^*$

$y^2 = 3$

$\sqrt{3} \notin Z_5^*$

$Z_5^* = \{1, 2, 3, 4\}$

$1^2 = 1 \bmod 5$

$2^2 = 4 \bmod 5$

$3^2 = 9 \bmod 5 = 4$

$4^2 = 16 \bmod 5 = 1$

$Q_5 = \{1, 4\}$

$\left(\frac{4}{5}\right) = ?$

$= 4^{(5-1)/2} \bmod 5$

$= 4^2 \bmod 5$

$= 16 \bmod 5$

$= 1$

$\therefore$ 4 is QR mod 5

Cippolla's Algorithm

- Let y is a quadratic residue modulo p
- Choose t such that $u = t^2 - y$ is quadratic non-residue
- Then $x = (t+w)^{(p+1)/2}$ gives a square root of y, where $w = \sqrt{u}$
  that is, $x^2 = y \bmod p$, if y is quadratic residue.

Quadratic Residue: $\exists y$ such that $x^2 = y \; mod \; p$

Example: find $\sqrt{2} \; mod \; 17$

Sol: Is 2 quadratic residue mod 17 ? $\rightarrow$ yes 2 is QR mod 17.

$$\left(\frac{2}{17}\right) \stackrel{?}{=} 1 \Rightarrow 2^{(17-1)/2} \bmod 17$$

$$= 2^8 \bmod 17 = \underline{1}$$

Let y is a quadratic residue modulo p

Choose t such that $\mathrm{u} = t^2 - y$ is quadratic non-residue

Then $\mathrm{x} = (t + w)^{(p+1)/2}$ gives a square root of y, where $\mathrm{w} = \sqrt{u}$

that is, $x^2 = y \bmod p$, if y is quadratic residue.

Example: find $\sqrt{2} \bmod 17$

$t = 0, \quad u = t^2 - y = 0^2 - 2 \bmod 17 = 15$

$15^{(17-1)/2} = 1 \bmod 17 \quad QR \quad \times$

$t = 3, \quad u = 3^2 - 2 = 7 \bmod 17$

$7^8 \bmod 17 = -1 \quad QNR$

$w = \sqrt{7}, \quad x = (3 + \sqrt{7})^{(17+1)/2} = (3 + \sqrt{7})^9 \bmod 17$

$(3+\sqrt{7})^9$:

$$(3+\sqrt{7})^2 = (3+\sqrt{7})(3+\sqrt{7})$$
$$= 16 + 6\sqrt{7}$$

$$(3+\sqrt{7})^4 = (3+\sqrt{7})^2 \times (3+\sqrt{7})^2$$
$$= (16+6\sqrt{7})(16+6\sqrt{7})$$
$$= 15 + 5\sqrt{7}$$

Check

$$\boxed{6^2 \equiv 2 \mod 17}$$

$$\sqrt{2} = \begin{cases} 6 \mod 17 \\ -6 \mod 17 \\ 11 \mod 17 \end{cases}$$

$$(3+\sqrt{7})^8 = (3+\sqrt{7})^4 (3+\sqrt{7})^4$$
$$= (15+5\sqrt{7})(15+5\sqrt{7})$$
$$= 9 + 14\sqrt{7}$$

$$(3+\sqrt{7})^9 = (3+\sqrt{7})^8 (3+\sqrt{7})^1$$
$$= (9+14\sqrt{7})(3+\sqrt{7})$$
$$= 6 \mod 17$$

Q: find $\sqrt{2} \pmod{23}$? Q: find $\sqrt{3} \bmod 23$. ?

Home work.