Quadratic Congruences

Debdeep Mukhopadhyay

Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Quadratic Residue**
- **Primitive Element**
- **Euler's Criterion**
- **Legendre Symbol**

Practice Problem

Let C be a solution of:

$f(x) \equiv 0 (\text{mod } p^a)$ ...(1),

and let $f'(C) \neq 0 (\text{mod } p)$ ...(2)

Then prove: $f(x) \equiv 0 (\text{mod } p^{a+t})$ has exactly one solution corresponding to the solution $x = C$ of (1), for every integer $t > 0$.

Quadratic Residue

Suppose p is an odd prime and a is an integer. a is defined to be a *quadratic residue* modulo p if $a \not\equiv 0 \pmod p$ and the congruence $y^2 \equiv a \pmod p$ has a solution $y \in \mathbb{Z}_p$. a is defined to be a *quadratic non-residue* modulo p if $a \not\equiv 0 \pmod p$ and a is not a quadratic residue modulo p.

- **There are exactly (p-1)/2 QR (Quadratic Residues)**

Example

- Z_{11}
  $1^2=1$
  $2^2=4$
  $3^2=9$
  $4^2=5$
  $5^2=3$
  $6^2=3$
  $7^2=5$
  $8^2=9$
  $9^2=4$
  $10^2=1$

Note, that the QR forms a palindrome

There are exactly (11-1)/2=5 QRs.

Generalization

How many solutions are there to $x^2 \equiv a(\text{mod } p)$
for odd positive prime p?
If, $y^2 \equiv a(\text{mod } p), y \in Z_p^*$
then $(-y)^2 \equiv a(\text{mod } p)$
Note, $y \neq -y(\text{mod } p)$, as p is odd
Thus, the quadratic congruence:
$x^2 - a \equiv 0(\text{mod } p)$
can be factored into
$(x-y)(x+y) \equiv 0(\text{mod } p)$
Since, p is prime, $p \mid (x-y)$ or $p \mid (x+y)$
Thus, $x \equiv \pm y(\text{mod } p)$
Thus, there are exactly two solutions of the congruence.

The QR Problem

	Quadratic Residues
Instance:	An odd prime p, and an integer a.
Question:	Is a a quadratic residue modulo p?

- **We have a polynomial time deterministic algorithm to solve this decision problem.**

Euler comes to the rescue again

(Euler's Criterion) *Let p be an odd prime. Then a is a quadratic residue modulo p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

- **The time complexity of this check is $O(\log p)^3$ by applying square and multiply method to raise an element to a power.**
- **Note that if $a^{(p-1)/2} \equiv -1 \pmod{p}$ then a is a non-quadratic residue.**

Cyclic Group

- If p is prime, then Z_p^* is a group of order p-1 and any element in Z_p^* has an order which divides (p-1).
- In fact, if p is prime, then there exists at least one element in Z_p^* which has order equal to p-1.
  - this is called cyclic group…

Primitive Element

- If p is prime, then Z_p^* is a cyclic group.
- Any element α having order p-1 mod p is called a primitive element. Thus α is a primitive element iff:

$$\{\alpha^i : 0 \leq i \leq p-2\} = \mathbb{Z}_p^*$$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- **n=19, There are 6 primitive elements.**
- **Note the order of each element in Z_{19}^*.**
- **Is there a relation?**

Order of any element

- **Any element β in Z_p^* (where p is prime) can be written uniquely in the form $\beta=\alpha^i$, where α is a primitive element and $0 \le i \le p-2$.**
- **The order of β is:**

$$\frac{p-1}{\gcd(p-1, i)}$$

- **β is itself primitive iff gcd(p-1,i)=1. Hence, what is the number of primitive elements modulo p?**

Example

- p=13
- Thus Φ(13-1)= Φ(12)= Φ($3x2^2$)=12(1-1/3)(1-1/2)=12x(2/3)x(1/2)=4.
- Question: Is 2 a primitive element of Z_{13}^*?
  - generate all the (p-1) powers of 2.
  - lengthy process if p is large.

Theorem

THEOREM 5.8 *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod p$ for all primes q such that $q \mid (p-1)$.*

Legendre Symbol

Suppose p is an odd prime. For any integer a, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

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

Properties

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

(a) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

(c) $\left(\frac{0}{p}\right) = 0, \left(\frac{1}{p}\right) = 1, \left(\frac{a^2}{p}\right) = 1, \text{if } \gcd(a, p) = 1$

(d) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \text{ is of the form } 4k+1 \\ -1, & \text{if } p \text{ is of the form } 4k+3 \end{cases}$

(e) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8} \\ -1, & \text{else} \end{cases}$

Law of Quadratic Reciprocity

Let p, q be odd primes. Then,

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

Example

$$\left(\frac{51}{541}\right) =$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$

$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$
$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$
$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$
$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$
$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$
$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$
$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$
$$=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$

$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$

$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$

$$=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

$$=\left(\frac{7}{17}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$

$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$

$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$

$$=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

$$=\left(\frac{7}{17}\right)$$

$$=(-1)^{(7-1)(17-1)/4}\left(\frac{17}{7}\right)=\left(\frac{17}{7}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$

$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$

$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$

$$=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

$$=\left(\frac{7}{17}\right)$$

$$=(-1)^{(7-1)(17-1)/4}\left(\frac{17}{7}\right)=\left(\frac{17}{7}\right)$$

$$=\left(\frac{3}{7}\right)$$

Example

$$\left(\frac{51}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{17}{541}\right)$$

$$=(-1)^{(3-1)(541-1)/4}\left(\frac{541}{3}\right)(-1)^{(17-1)(541-1)/4}\left(\frac{541}{17}\right)$$

$$=\left(\frac{541}{3}\right)\left(\frac{541}{17}\right)$$

$$=\left(\frac{1}{3}\right)\left(\frac{14}{17}\right)=\left(\frac{14}{17}\right)$$

$$=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

$$=\left(\frac{7}{17}\right)$$

$$=(-1)^{(7-1)(17-1)/4}\left(\frac{17}{7}\right)=\left(\frac{17}{7}\right)$$

$$=\left(\frac{3}{7}\right)$$

$$=(-1)^{(3-1)(7-1)/4}\left(\frac{7}{3}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$$

Practice

- Prove $x^2 \equiv 105 (mod\ 199) has\ no\ solution.$