Lecture 10: Quadratic residues

Rajat Mittal

IIT Kanpur

Solving polynomial equations, $a_n x^n + \cdots + a_1 x + a_0 = 0$, has been of interest from a long time in mathematics. For equations up to degree 4, we have an explicit formula for the solutions. It has also been shown that no such explicit formula can exist for degree higher than 4.

What about polynomial equations modulo p?

Exercise 1. When does the equation $ax + b = 0 \mod p$ has a solution?

This lecture will focus on solving quadratic equations modulo a prime number p. In other words, we are interested in solving $a_2x^2+a_1x+a_0 = 0 \mod p$. First thing to notice, we can assume that every coefficient a_i can only range between 0 to $p-1$. In the assignment, you will show that we only need to consider equations of the form $x^2 + a_1x + a_0 = 0$.

Exercise 2. When will $x^2 + a_1x + a_0 = 0 \mod 2$ not have a solution?

So, for further discussion, we are only interested in solving quadratic equations modulo p, where p is an *odd* prime. For odd primes, inverse of 2 always exists.

$$x^2 + a_1x + a_0 = 0 \mod p \Leftrightarrow (x + 2^{-1}a_1)^2 = 2^{-2}a_1^2 - a_0 \mod p.$$

Taking $y = x + 2^{-1}a_1$ and $b = 2^{-2}a_1^2 - a_0$,

Exercise 3. solving quadratic equation $x^2 + a_1x + a_0 = 0 \mod p$ is same as solving $y^2 = b \mod p$.

The small amount of work we did above simplifies the original problem. We only need to solve, when a number (b) has a square root modulo p, to solve quadratic equations modulo p.

1 Quadratic residues

Given a number a, s.t., $gcd(a, p) = 1$; a is called a quadratic residue if $x^2 = a \mod p$ has a solution otherwise it is called a quadratic non-residue. From previous section, we are interested in finding out when a is a quadratic residue and if yes, what are the solutions.

The problem of finding out, whether a number is a quadratic residue or not, is easy and we will see that in this section. Problem of finding square roots modulo p is hard and we still don't have any efficient solution for it.

Before we start proving properties of quadratic residues and non-residues, let us introduce a notation.

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

The notation $\left(\frac{a}{p}\right)$ is known as the *Legendre symbol* of a modulo p. We are interested in finding out when it is 1 and when it is -1. The following theorem gives a very simple criteria to check whether a number is a quadratic residue or not.

Theorem 1. *A number a with $gcd(a, p) = 1$, where p is an odd prime, satisfies,*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p.$$

Note 1. $a^{p-1} = 1$ by Fermat's theorem, so $a^{\frac{p-1}{2}}$ is a square root of 1 modulo p. There are only two square roots of 1 modulo p, 1 and -1 (exercise).

Proof. If a is a quadratic residue, then there exist an x, s.t., $x^2 = a \mod p$. Taking power, $1 = x^{p-1} = a^{\frac{p-1}{2}} \mod p = \left(\frac{a}{p}\right)$. Hence one direction is easy.

For the other direction, if a is a quadratic non-residue, show that

Exercise 4. For every $1 \leq s \leq p-1$, there exists a unique t, s.t., $st = a \mod p$.

Clearly $s \neq t$, otherwise a will become a residue. This implies that the numbers $1, 2, \cdots, p-1$ can be divided into $\frac{p-1}{2}$ pairs, such that, every pair multiplies to a modulo p.

Taking the multiplication over all elements between 1 and $p-1$,

$$(p-1)! = a^{\frac{p-1}{2}} \mod p.$$

Using Wilson's theorem, if a is a quadratic non-residue then,

$$a^{\frac{p-1}{2}} = -1 \mod p = \left(\frac{a}{p}\right).$$

Exercise 5. Give a proof that $a^{\frac{p-1}{2}} = 1 \mod p$ for a residue a, similar to the lines of the proof for non-residue.

□

This criteria for checking residuocity gives a very important property of residues modulo p.

Theorem 2. *For two numbers a, b, both co-prime to an odd prime p,*

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

This is known as the multiplicativity of Legendre symbol. The proof is left as an exercise.

2 Quadratic reciprocity

Because of multiplicativity of Legendre symbol, it is important to find $\left(\frac{q}{p}\right)$ where q is a prime. This is a hard question, we don't know the answer to it yet. Still a beautiful theorem by Gauss, called *quadratic reciprocity*, gives the relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.

The proof of this theorem is taken from [2]. The first step is to prove Gauss's lemma.

Lemma 1. *Suppose the number of elements in set S greater than $\frac{p}{2}$ is l, where*

$$S = \{a, 2a, \cdots, \frac{p-1}{2}a\}.$$

Every number in S is considered modulo p. Then $\left(\frac{a}{p}\right) = (-1)^l$.

Proof. Remember that the set $\{a, 2a, \cdots, (p-1)a\}$ is a permutation of elements $\{1, 2, \cdots, p-1\}$. If we consider the first half of this set,

$$S = \{a, 2a, \cdots, \frac{p-1}{2}a\},$$

This is *almost* the permutation of elements $\{1, 2, \cdots, \frac{p-1}{2}\}$.

Say $r_1, r_2, \cdots, r_k$ be the elements in S less than $p/2$ and $s_1, s_2, \cdots, s_l$ be the elements greater than $p/2$. Then the set,

$$S' = \{r_1, \cdots, r_k, p - s_1, \cdots, p - s_l\},$$

has all elements between 1 and $\frac{p-1}{2}$.

Exercise 6. Show that no two elements are the same in set S'.

So, the set S' is just a permutation of $\{1, 2, \cdots, \frac{p-1}{2}\}$. Multiplying all elements in S' modulo p,

$$1.2.\cdots.\frac{p-1}{2} = r_1 r_2 \cdots r_k (p-s_1)(p-s_2)\cdots(p-s_l) = (-1)^l r_1 \cdots r_k s_1 \cdots s_l.$$

Notice that r_i's and s_i's make up set S.

$$\frac{p-1}{2}! = (-1)^l a^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p.$$

This proves that,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^l \mod p.$$

□

This lemma will help us in proving another characterization of Legendre symbol.

Theorem 3. *For an* odd *a co-prime to an odd prime p,*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor}.$$

Proof. From the proof of previous lemma 1, we need to show that l and $l' = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$ has the same parity (same value modulo 2).

Using the notation of the proof of lemma 1, let us estimate l'. Say t_j be the remainder when ja is divided by p.

$$ja = \left\lfloor \frac{ja}{p} \right\rfloor p + t_j \Rightarrow \sum_{j=1}^{\frac{p-1}{2}} ja = l'p + \sum_{j=1}^{\frac{p-1}{2}} t_j.$$

Since elements of S' are permutation of $\{1, 2, \cdots, \frac{p-1}{2}\}$,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{k} r_i + lp - \sum_{i=1}^{l} s_i.$$

Subtracting the two equations,

$$\sum_{j=1}^{\frac{p-1}{2}} (a-1)j = (l'-l)p + \sum_{j=1}^{t} t_j - \sum_{i=1}^{k} r_i + \sum_{i=1}^{l} s_i.$$

Notice that t_j's are all elements of S and hence,

$$\sum_{j=1}^{\frac{p-1}{2}} (a-1)j = (l'-l)p + 2\sum_{i=1}^{l} s_i.$$

Looking at this equation modulo 2, and the fact that a and p are odd,

$$l - l' = 0 \mod 2.$$

Hence proved. □

Exercise 7. What will be the corresponding theorem when a is even?

Now we are ready to prove the celebrated quadratic reciprocity theorem.

Theorem 4. *For two odd primes p and q,*

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

Proof. We will consider the grid made by integers in 2-dimensional plane. Look at the rectangle in Fig. 2.

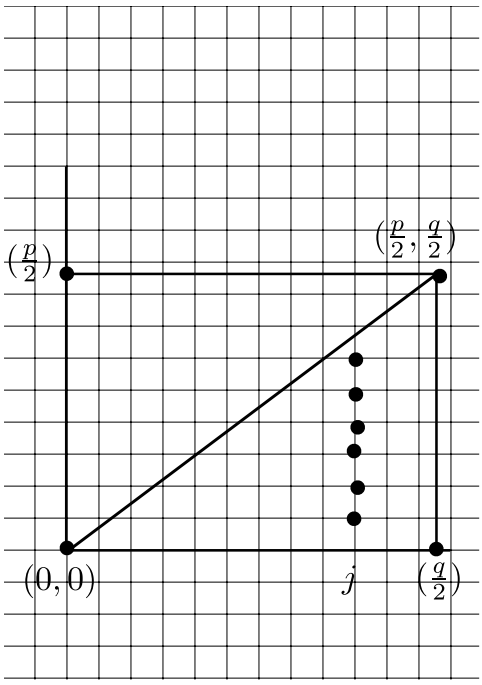

Fig. 1. Grid of integers

The number of integer points inside the rectangle is $\frac{p-1}{2}\frac{q-1}{2}$. We will show by double counting, it is also equal to

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor.$$

This will prove the theorem using Thm. 3. The first term in the summation is equal to $\left(\frac{q}{p}\right)$ and we will show that it is also equal to the number of grid points below the line L from $(0,0)$ to $(\frac{q}{2}, \frac{p}{2})$. The second term is equal to $\left(\frac{p}{q}\right)$ and by a similar argument it is equal to the number of grid points above the mentioned line L.

Exercise 8. Prove that there are no integer points on the line L before $(\frac{q}{2}, \frac{p}{2})$.

Note 2. This ensures that no point is counted twice in the argument below.

So, it is sufficient to prove that the number of points below line L in rectangle is $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$. This simply follows from the following exercise.

Exercise 9. The number of grid points in the column above $(j, 0)$ in the rectangle below L are $\left\lfloor \frac{jq}{p} \right\rfloor$.

This exercises shows that the grid points below the line, say N_1, are $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$. Hence $\left(\frac{q}{p}\right) = (-1)^{N_1}$. If the number of grid points above the line are N_2, by a similar argument, $\left(\frac{p}{q}\right) = (-1)^{N_2}$.

Since $N_1 + N_2 = \frac{p-1}{2}\frac{q-1}{2}$, the theorem follows.

□

3 Assignment

Exercise 10. Show that for solving quadratic equation modulo p, it is sufficient to solve equations of the form $x^2 + a_1 x + a_0 = 0 \mod p$.

Exercise 11. Prove Wilson's theorem.

Exercise 12. When is -1 a quadratic non-residue?

Exercise 13. Show that there are infinitely many primes of the form $4k + 1$.

Exercise 14. Using Gauss's lemma, find $\left(\frac{2}{p}\right)$.

Exercise 15. What is $\left(\frac{3}{p}\right)$?

References

1. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.
2. D. M. Burton. Elementary Number Theory. *Tata McGraw-Hill Education*, 2006.