A Concrete Introduction to Number Theory and Algebra–Quadratic Residue

Libin Wang

School of Computer Science, South China Normal University

December 1, 2020

First Question.

First Question.

Let p be an odd prime and a an integer relatively prime to p, is a a perfect square modulo p? Equivalently, we need to dicide whether there exists $x \in \mathbb{Z}$ such that:

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

Naive Solution.

Easy jobs.

Let $p = 11$, and $a = 5$, is a a perfect square modulo p? We write a simple program to square every number from 1 to 10. The output is :

$$1, 4, 9, 5, 3, 3, 5, 9, 4, 1$$

More data.

a	a^2
1	1
2	4
3	4
4	1

Table: $a^2 \mod 5$

More data.

a	a^2
1	1
2	4
3	2
4	2
5	4
6	1

Table: $a^i \bmod 7$

More data.

a	a^2
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Table: $a^i \bmod 13$

To find some patterns.

Pattern!

Can you find some patterns from the tables?

Some easy conclusions.

One easy conclusion.

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

Some easy conclusions.

One easy conclusion.

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

Do you see why?

Some easy conclusions.

One easy conclusion.

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

Do you see why?

Easy proof.

It is easy to prove that:

$$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}.$$

The pattern means that the congruence $x^2 \equiv 1 \pmod{p}$ has two solutions, 1 and $p-1$.

Some easy conclusions.

Another easy conclusion.

Every second columns of these tables is reflectional symmetric （反射对称） that can be described by the following formula.

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

Some easy conclusions.

Another easy conclusion.

Every second columns of these tables is reflectional symmetric （反射对称） that can be described by the following formula.

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

The proof is similar, since:

$$(p-a)^2 = p^2 + 2pa + a^2.$$

Some easy conclusions.

Another easy conclusion.

Every second columns of these tables is reflectional symmetric （反射对称） that can be described by the following formula.

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

The proof is similar, since:

$$(p-a)^2 = p^2 + 2pa + a^2.$$

This formula means the congruence $x^2 \equiv a \pmod{p}$ has two incongruent solutions, a and $p-a$.

One formally stated property.

Proposition

Let p be an odd prime and b an integer not divisible by p. Then, the congruence

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

has either no solutions or exactly two incongruent solutions modulo p.

One formally stated property.

Proof.

We know $x^2 \equiv b \pmod p$ has two incongruent solutions. Then we must show that there are no more than two incongruent solutions. Assume that x_0 and x_1 are two solutions of $x^2 \equiv b \pmod p$. Then

$$x_0^2 \equiv x_1^2 \equiv b \pmod p,$$

thus

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod p.$$

Hence, $p \mid (x_0 - x_1)$ or $p \mid (x_0 + x_1)$, which means $x_0 \equiv x_1 \pmod p$ or $x_0 \equiv -x_1 \pmod p$. Therefore, if there is a solution, there are exactly two incongruent solutions. $\square$

Quadratic Residues（二次剩余）and Quadratic Non-Residue（二次非剩余）.

Definition

Let $m, n \in \mathbb{Z}$ *with* $gcd(m, n) = 1$. *Then m is called a quadratic residue modulo n(模 n 的二次剩余) (short for* **QR***) if* $m \equiv x^2 \pmod{n}$ *for some* $x \in \mathbb{Z}$*, and m is called a quadratic nonresidue modulo n（模 n 的二次非剩余）(short for* **QNR***) otherwise.*

QR and QNR.

Example

From these tables we have showed, we know that, the **QR** *modulo* 7 *are* $\{1, 2, 4\}$*; the* **QR** *modulo* 13 *are* $\{1, 3, 4, 9, 10, 12\}$*; the* **QNR** *modulo* 7 *are* $\{3, 5, 6\}$*; the* **QNR** *modulo* 13 *are* $\{2, 5, 6, 7, 8, 11\}$*.*

QR and QNR.

Theorem

Let p be an odd prime, then there are exactly $(p-1)/2$ **QRs** *modulo p and exactly $(p-1)/2$* **QNRs** *modulo p.*

QR and QNR.

Proof.

We map the integers from $\mathbb{Z}_p^*$ to $\mathbf{QR}$s modulo p by squaring. since Propostion 1 tell us that, two incongruent integers map to one $\mathbf{QR}$, and we have $p-1$ squares to consider, then there are exactly $(p-1)/2$ $\mathbf{QR}$s modulo p. The remaining $(p-1)/2$ integers are $\mathbf{QNR}$s modulo p. □

Quadratic Residues Group.

Proposition

Let $\mathbb{QR}_p$ denotes the set of every $\mathbf{QR}$ modulo p, $\mathbb{QR}_p$ is a group under multiplication.

Proof.

It is easy to prove by checking every axioms of group. $\square$

Quadratic Residues Group.

The map from $\mathbb{Z}_p^*$ to $\mathbb{QR}_p$ is a group homomorphism, if we denote it as ϕ, then by earlier observation we know $ker\,\phi = \{1, p-1\}$. By using the First Isomorphism Theorem from Chapter 9, we have a new proof for last Theorem

Quadratic Residues vs Quadratic Non-Residues .

Proposition

Let p be an odd prime, then
(1.) The product of two **QR***s modulo p is a* **QR**, *denoted as*

$$\mathbf{QR} \times \mathbf{QR} = \mathbf{QR},$$

(2.) The product of a **QR** *modulo p and a* **QNR** *modulo p is a* **QNR** *modulo p, denoted as*

$$\mathbf{QR} \times \mathbf{QNR} = \mathbf{QNR},$$

(3.) The product of two **QNR***s modulo p is a* **QR**, *denoted as*

$$\mathbf{QNR} \times \mathbf{QNR} = \mathbf{QR}.$$

Quadratic Residues vs Quadratic Non-Residues .

Proof.

$$\mathbf{QR} \times \mathbf{QNR} = \mathbf{QNR},$$

Let b be a $\mathbf{QNR}$, and a be a $\mathbf{QR}$, then there exists $a_1 \in \mathbb{Z}$ such that $a \equiv a_1^2 \pmod{p}$. Assume that ab is a $\mathbf{QR}$, then there exists $c \in \mathbb{Z}$ such that

$$c^2 \equiv ab \equiv a_1^2 b \pmod{p}.$$

We know that $gcd(a_1, p) = 1$, then there exists $a_1^{-1} \in \mathbb{Z}$ such that $a_1 a_1^{-1} \equiv 1 \pmod{p}$, therefore we have

$$c^2 (a_1^{-1})^2 \equiv b \pmod{p}.$$

This means that b is a $\mathbf{QR}$ contradicting the assumtion that b is a $\mathbf{QNR}$. $\square$

Quadratic Residues vs Quadratic Non-Residues .

Proof.

$$\mathbf{QNR} \times \mathbf{QNR} = \mathbf{QR}.$$

Let a be a $\mathbf{QNR}$ and $p \nmid a$, then we know

$$a\mathbb{Z}_p^* = \mathbb{Z}_p^*.$$

We also know that there are $(p-1)/2$ $\mathbf{QR}$s and $(p-1)/2$ $\mathbf{QNR}$s in $\mathbb{Z}_p^*$. As we have proved, when we multiply a by a $\mathbf{QR}$ we get a $\mathbf{QNR}$, hence the $(p-1)/2$ products $a \times \mathbf{QR}$ give all $(p-1)/2$ $\mathbf{QNR}$s in $\mathbb{Z}_p^*$. Then when we multiply a by a $\mathbf{QNR}$, the only possibility is that it gives one of the $\mathbf{QR}$s in $\mathbb{Z}_p^*$. □

Legendre symbol.（勒让德符号）

Definition

Let p be an odd prime and let $n \in \mathbb{Z}$. The ***Legendre symbol*** *(n/p) is defined as*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue mod } p \\ -1 & \text{if } n \text{ is a quadratic nonresidue mod } p \\ 0 & \text{if } p \mid n. \end{cases}$$

Legendre symbol 的属性.

Proposition

设 p 是奇素数，$a, b \in \mathbb{Z}$ 且不被 p 整除。则有：

1. 如果 $a \equiv b \pmod{p}$，则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$；
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$；
3. $\left(\frac{a^2}{p}\right) = 1$。

Legendre symbol.

Proof.

It is naive by Proposition 6. $\square$

Legendre symbol.

Example

$$\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right) = 1$$

Since $10^2 \equiv 3 \pmod{97}$, *so* 3 *is a* $\mathbf{QR}$.

Legendre symbol.

Example

$$\left(\frac{75}{97}\right) = \left(\frac{3\cdot 5\cdot 5}{97}\right) = \left(\frac{3}{97}\right) = 1$$

Since $10^2 \equiv 3 \pmod{97}$, *so* 3 *is a* $\mathbf{QR}$.

Example

$$\left(\frac{269}{97}\right) = \left(\frac{2\cdot 97+75}{97}\right) = \left(\frac{75}{97}\right) = 1.$$

Euler's Criterion.（欧拉准则）

Theorem

(Euler's Criterion.) *Let p be an odd prime and let $a \in \mathbb{Z}$ with $gcd(a, p) = 1$. Then*

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

Euler's Criterion.

Proof.

We have two cases to consider. For the first case, we assume $\left(\frac{a}{p}\right) = 1$, which means that there exist $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$. By Fermat's little theorem, we have that

$$x^{(p-1)} \equiv 1 \pmod{p},$$

and

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

Hence

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

□

Euler's Criterion.

Proof.

For the second case, we assume $\left(\frac{a}{p}\right) = -1$, which means that the congruence $x^2 \equiv a \pmod{p}$ has no solutions. Using Fermat's little theorem again, we know that

$$0 \equiv a^{(p-1)} - 1 \equiv (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \pmod{p}.$$

Since $\left(\frac{a}{p}\right) = -1$, $a^{(p-1)/2} - 1 \not\equiv 0 \pmod{p}$, hence, it must be

$$a^{(p-1)/2} + 1 \equiv 0 \pmod{p}.$$

Therefore

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

$\square$

Euler's Criterion.

Example

$$\left(\frac{3}{97}\right) = 3^{(97-1)/2} \bmod 97 = 3^{48} \bmod 97 = 1.$$

Thus 3 *is a* $\mathbf{QR}$.

Euler's Criterion.

Theorem

Let p be an odd prime then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Proof.

It is easy by using Euler's criterion. $\square$

Theorem about $\left(\frac{2}{p}\right)$.

Theorem

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Theorem about primes of the form $4k+1$.

Proposition

模 4 余 1 的素数有无穷多。

Proof.

假设模 4 余 1 的素数有限，枚举之 $S=\{1,p_1,p_2,\cdots,p_n\}$。令

$$N=(2p_1p_2\cdots p_n)^2+1 \tag{1}$$

显然，N 是一个奇数（注意上式构造中嵌入的那个 2），所以必然存在一个奇素数 p 使得 $p\mid N$。也就是说：

$$(2p_1p_2\cdots p_n)^2\equiv -1 \pmod p$$

即 $\left(\frac{-1}{p}\right)=1$。根据勒让德符号的属性，可知 p 是形如 $4k+1$ 的素数，所以 $p\in S$。这说明 $p\mid(N-(2p_1p_2\cdots p_n)^2)$，即 $p\mid 1$，矛盾！ $\square$

Quadratic Reciprocity.

Theorem

(Quadratic Reciprocity, Version 1.) Let p, q be distinct odd primes.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 4; \\ -1 & \textit{if } p \equiv -1 \pmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 7 \pmod 8; \\ -1 & \textit{if } p \equiv 3 \textit{ or } 5 \pmod 8. \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \textit{if } p \equiv 1 \pmod 4 \textit{ or } q \equiv 1 \pmod 4; \\ -\left(\frac{p}{q}\right) & \textit{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Quadratic Reciprocity.

Example

$$\left(\frac{14}{137}\right) = \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) = \left(\frac{7}{137}\right) = \left(\frac{137}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Thus 14 *is a* **QR**.

Quadratic Reciprocity.

Theorem

(Quadratic Reciprocity, Version 2.) Let p, q be distinct odd primes. Then

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