Quadratic Congruences

In this topic, we will learn how to know if ∃ solns for simple degree 2 modular eqns. of the form

$$x^2 \equiv n \pmod{m}.$$

where n, m are either primes & odd +ve numbers.

For this, we will use notions like Legendre symbols & tools like Quadratic Reciprocity Theorem.

We will only bother about quadratic congruences of the form

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

as of now.

Here, we immediate observe that the cases

(i) $n \equiv 0 \pmod{p}$ &

or

(ii) $p = 2$

can be handled very easily. This is because if $n \equiv 0 \pmod{p}$, then x^2 is congruent to $0 \pmod{p}$ & the eqn. $x^2 \equiv 0 \pmod{p}$ has the soln $x \equiv 0 \pmod{p}$.

In the case where p is even (i.e $p = 2$), ie. in $x^2 \equiv n \pmod{2}$, we know n is congruent to either 0 or 1 mod 2. Thus $x \equiv 0 \pmod{2}$ or $x \equiv 1 \pmod{2}$ are the solutions respectively.

What matters is the case where

p is an odd prime, & $n \not\equiv 0 \pmod{p}$.

We will assume so from now onwards.

In case $n = 1$, i.e if the eqn is $x^2 \equiv 1 \pmod{p}$, then the solns are $x_0 \equiv 1 \pmod{p}$ or $x_0 \equiv -1 \pmod{p}$. Here, the eqn. has exactly 2 solutions modulo p. However, there are other situations too.

For eg. $x^2 \equiv -1 \pmod 7$ has no solns modulo 7

$x^2 \equiv 1 \pmod 8$ has exactly four solutions.
↳ non-prime.

We will not digress to the non-prime case now. If the modulus is prime, say p, then it is a fact that

$$x^2 \equiv n \pmod p$$

has almost two solns. And it is either 0 or 2 because if x_0 is a soln, so is $p - x_0$.

Quadratic residue :-

If the congruence (1) has a soln. in x, we say that n is a quadratic residue modulo p. We denote it by nRp. or by saying n is a QR mod p.

If (1) has no soln in x, then we say that n is a quadratic non-residue modulo p & denote it by $n\bar{R}p$. or by saying n is a QNR mod p.

Eg. $x^2 \equiv -1 \pmod 5$ has 2 solns, so -1 is a QR mod 5 & is QNR mod 7.

Two problems dominate the theory of quadratic residues.

(Q1) Given a prime p, determine which n are quadratic residues mod p

(Q2) Given n, determine those primes p for which n is a QR mod p.

Q1) Find the quadratic residues modulo 11.

$1^2=1$, $2^2=4$, $3^2=9$, $4^2\equiv 5$, $5^2\equiv 3$,

$10^2\equiv 1$, $9^2\equiv 4$, $8^2\equiv 9$, $7^2\equiv 5$, $6^2\equiv 3$

Square all nos. from 1 to 10 & we get 1, 4, 9, 5 & 3 are quadratic residues mod 11 & there are no other possible squares as we have checked all possibilities.
Remaining 2, 6, 7, 8, 10 are QNR mod 11.

Theorem 1

Let p be an odd prime. Then, every reduced residue system mod p contains exactly $\frac{p-1}{2}$ quadratic residues & exactly $\frac{p-1}{2}$ quadratic non-residues.

The quadratic residues belong to the residue classes containing the nos $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$.

Idea of proof :- In general, if $1 \le k \le \frac{p-1}{2}$, then k^2 & $(p-k)^2$ are congruent modulo p. Hence, when we exhaust through all non-zero squares modulo p, only $\frac{p-1}{2}$ many of those squares are distinct

Corollary :- Given $m > 2$, $m \in \mathbb{N}$, $\{1^2, 2^2, 3^2, \dots, m^2\}$ is not a complete residue system modulo m.

Qn :- What will squaring do to a reduced residue system say modulo odd prime p? What if cubing or k^{th} power?

Primes	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
R	1	1,4	1,4,2	1,4,9,5,3	1,4,9,3,12,10
$\overline{R}$	2	2,3	3,5,6	2,6,7,8,10	2,5,6,7,8,11

Legendre symbol & its properties

Defn :- Let p be an odd prime. If $n \not\equiv 0 \pmod p$, we define Legendre's symbol $\left(\frac{n}{p}\right)$ as

$\Rightarrow (n,p) = 1$

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n R p \\ -1 & \text{if } n \overline{R} p \end{cases}$$

& if $n \equiv 0 \pmod p$, we define $\left(\frac{n}{p}\right) = 0$.

Eg- 1) $\left(\frac{0}{p}\right) = 0$; $\left(\frac{1}{p}\right) = 1$ as 1 is its own square modulo any prime p.

2) $\left(\frac{4}{p}\right) = 1$ as $4 \equiv 2^2 \pmod p$ for odd prime p.

3) If $p \nmid m$, then $\left(\frac{m^2}{p}\right) = 1$.

Lemma 1) If m & n are congruent modulo p, then

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right).$$

Proof :- Suppose $m R p$, ie, $\exists\ x$ s.t. $x^2 \equiv m \pmod p$.
By transitivity, $\because m \equiv n \pmod p$, we have

$$x^2 \equiv n \pmod p$$
$$\Rightarrow \quad n R p = 1$$

Clearly if one is a QR mod p, so is the other. However, if one is not a QR mod p, and the other becomes a QR, then it will lead to contradiction because of previous observation. Thus, they are either QRs simultaneously or QNRs simultaneously.

Thus, 3 is a QR mod 11 as 36 is.

Further, $\left(\frac{n+p}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{n+mp}{p}\right)$ for any $m \in \mathbb{Z}$.

The function $f_p(n) = \left(\frac{n}{p}\right)$ is a periodic function of n with period p.

$\therefore$ Elements in the same residue class modulo p have same quadratic residues (in addition to same remainders modulo p, same gcd with p.)

(If $b \equiv c \pmod m$, then $(b,m) = (c,m)$.)

Exercise :- If $(n,p) = 1$ & $x^2 = n$, then $(x,p) = 1$.

How to determine if $\left(\frac{n}{p}\right) = 1$ or -1

1) Euler's criterion :-

Let p be an odd prime. Then, for all n,

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

Properties : Let p be an odd prime. Then,

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

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ (completely multiplicative w.r.t. numerator)

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

4) If $(a,p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$ & $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

5) $\left(\frac{1}{p}\right) = 1$ & $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

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

When the numbers n & p are considerably large, properties listed above often help in answering whether $\left(\frac{n}{p}\right) = 1$ or -1 or in reducing the problem.

For. eg. $\left(\frac{8412}{647}\right) = \left(\frac{1}{647}\right) = 1$; $\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$

Quadratic reciprocity theorem

Suppose we want to check if 73 is a square (I will denote $\square$ to mean a square) mod 383, where both are primes. Now, further reductions using properties above may not work. Fortunately, we have a tool developed by Gauss called Quadratic Reciprocity theorem.

Theorem 2) : If p & q are distinct odd primes, then,

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

Think!!

It states that the two congruences $x^2 \equiv p \pmod q$ & $x^2 \equiv q \pmod p$ are either both solvable or both not solvable unless p & q are both of the form $4k+3$ in which case one of the congruences is solvable & the other is not.

Eg 1) Consider $x^2 \equiv 5 \pmod{103}$. Since 5 is not of the form $4k+3$, the results says that either $x^2 \equiv 5 \pmod{103}$ & $x^2 \equiv 103 \pmod 5$ are simultaneously solvable or simultaneously not. But since $x^2 \equiv 103 \equiv 3 \pmod 5$ has no solns, $x^2 \equiv 5 \pmod{103}$ also has no solns.

Eg. 2) Now, we will take an example which involves the properties mentioned above & QRT.

$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$. Here,

$\left(\frac{-1}{61}\right) = (-1)^{30} = 1.$

$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1$

$\left(\frac{3}{61}\right)\left(\frac{61}{3}\right) = (-1)^{\left[\left(\frac{3-1}{2}\right)\left(\frac{61-1}{2}\right)\right]} = 1$

∵ one of the primes ie, 61 is $1 \pmod 4$, clearly,

$\left(\frac{3}{61}\right)\left(\frac{61}{3}\right) = 1$. That is, equivalently, $\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)$.

III by, $\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right)$ as $61 \equiv 1 \pmod 4$

Now, $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$ as $5 \equiv 1 \pmod 4$

Now, $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$

& $\left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1$

$\Rightarrow \left(\frac{-42}{61}\right) = 1 \times -1 \times 1 \times -1 = 1$

Eg 3. Find all odd primes p such that 3 is a QR mod p.

Ans: $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\left[\left(\frac{p-1}{2}\right)\left(\frac{3-1}{2}\right)\right]} = (-1)^{\frac{p-1}{2}}$

$\Rightarrow \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)^{-1}(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$

Note that $\left(\frac{p}{3}\right)^2 = 1 \Rightarrow \left(\frac{p}{3}\right)$ is its own inverse.

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \pmod 3 \\ -1 & p \equiv 2 \pmod 3 \end{cases}$$

We don't consider the case $p \equiv 0 \pmod 3$ as it does not satisfy $(3,p) = 1$. It is an essential requirement that $(a,m) = 1$ for a to be a QR mod m (See defn).

	$1 \pmod 3$	$2 \pmod 3$
$p \equiv 1 \pmod 4$	$p \equiv 1 \pmod{12}$	$p \equiv 5 \pmod{12}$
$p \equiv 3 \pmod 4$	$p \equiv 7 \pmod{12}$	$p \equiv 11 \pmod{12}$

Thus, $\left(\frac{p}{3}\right)\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{12} \\ -1 & p \equiv 5 \pmod{12} \\ -1 & p \equiv 7 \pmod{12} \\ 1 & p \equiv 11 \pmod{12} \end{cases}$

$\Rightarrow \left(\frac{3}{p}\right) = 1$, ie 3 is a QR mod p iff $p \equiv \pm 1 \pmod{12}$

↙

[$p \equiv \pm 1 \pmod{12}$ means $p \equiv 1 \pmod{12}$ or $p \equiv -1 \pmod{12}$]

Exercises (Niven Zuckerman) Sec 3.2
Q2, 3, 4, 6, 7, 8, 9, 10, 11
(Hint for Q11: $x^2 \equiv 2 \pmod{15}$ has no solutions) → Done in class

* Determine whether 219 is a quadratic residue mod 383 or not.

Next, we will extend the Legendre symbols to the

case where denominator is no longer a prime.

Jacobi Symbols

Defn :- Let Q be a positive odd number such that

$$Q = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}.$$

Then, for any $n \in \mathbb{Z}$, we define

$$\left(\frac{n}{Q}\right) = \prod_{i=1}^{r} \left(\frac{n}{q_i}\right)^{\alpha_i}$$

Here, q_i-s are primes & hence, on the right, we have legendre symbols.
We also define $\left(\frac{n}{1}\right) = 1$.

To determine if a composite number is a QR or not, it is useful to study such extensions.

Theorem 3? If m & n are positive integers & P & Q are +ve integers, then

a) $\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) = \left(\frac{mn}{P}\right)$

b) $\left(\frac{n}{P}\right)\left(\frac{n}{Q}\right) = \left(\frac{n}{PQ}\right)$

Here : P & Q could be same as well ; as you will see later that by QRT for Jacobi symbols,

$$\left(\frac{n}{p^2}\right)\left(\frac{p^2}{n}\right) = (-1)^{\left[\left(\frac{n-1}{2}\right)\left(\frac{p^2-1}{2}\right)\right]}$$

Since $p^2 \equiv 1 \pmod 4$, RHS is 1 & hence,

$$\left(\frac{n}{p^2}\right) = \left(\frac{p^2}{n}\right) = 1$$

$\therefore \left(\frac{n}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{n}{p}\right)^2 = 1$ & $\left(\frac{n}{p^2}\right) = 1$ as well.

c) $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$ whenever $m \equiv n \pmod{p}$

d) $\left(\frac{a^2 n}{p}\right) = \left(\frac{n}{p}\right)$ whenever $(a, p) = 1$.

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

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

Exercise

Verify that for any p odd & positive,

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

(If p is odd, there are the possible residue classes modulo 8 for p.)

Quadratic Reciprocity Theorem

Theorem 4 :-

If p & q are positive odd integers, with $(p, q) = 1$, then

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

Q1) Determine whether 888 is a quadratic residue or non residue of the prime 1999.

Soln :- Method using Legendre symbol

$$\left(\frac{888}{1999}\right) = \left(\frac{8}{1999}\right)\left(\frac{111}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{111}{1999}\right).$$

$$\left(\frac{2}{1999}\right) = 1 \quad \text{as} \quad 1999 \equiv -1 \pmod 8.$$

Now, $\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right)$ }

Now,

$$\left(\frac{3}{1999}\right) = -\left(\frac{1999}{3}\right) \quad \text{as} \quad 1999 \equiv 3 \pmod 4.$$

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

&

$$\left(\frac{37}{1999}\right) = \left(\frac{1999}{37}\right) \quad \text{as} \quad 37 \equiv 1 \pmod 4.$$

$$= \left(\frac{1}{37}\right) = 1$$

$$\Rightarrow \left(\frac{111}{1999}\right) = -1.$$

So, $\left(\frac{888}{1999}\right) = 1 \times -1$

$\Rightarrow$ 888 is a QNR mod 1999.

An easier way that was not discussed in the class & shows the usefulness of Jacobi symbols is given now :-

here since 111 is not prime so jacobi we need to use and then work legrande wont work as denominator is not prime

$$\left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) \quad \text{as both 111 \& 1999 are } 3 \pmod 4$$

$$= -\left(\frac{1}{111}\right) = -1$$

$$\Rightarrow \left(\frac{888}{1999}\right) = 1 \times (-1)$$

The computations given in blue could be carried out in 1 step using Jacobi symbols QR7.

(Ex 2) Determine whether -104 is a quadratic residue or non-residue of the prime 997.

(Ex 3) $\left(\frac{2}{15}\right) = 1$. However, note that $x^2 \equiv 2 \pmod{15}$ has no solutions. This says that unlike Legendre symbols, if $\left(\frac{n}{p}\right) = 1$ for p odd & n, it is not necessary that $x^2 \equiv n \pmod{p}$ has solutions. However, if $\left(\frac{n}{p}\right) = -1$, then it is a fact that $x^2 \equiv n \pmod{p}$ has no solutions.