(Ch-9)

(9.1) Euler's criterion

Defⁿ 9.1) Let p be an odd prime and $\gcd(a,p)=1$. If the quadratic congruence $x^2 \equiv a \pmod p$ has a solution, then 'a' is said to be quadratic residue of p. otherwise a is called a quadratic non-residue of p.

Note If $a \equiv b \pmod p$ then a is quadratic residue of p iff b is quadratic residue of p.

(Ex) 9.1) If $p = 13$.
Find how many of the integers $1, 2, 3, \ldots, 12$ are quadratic residue of 13.
i.e check $x^2 \equiv a \pmod{13}$ are solvable when a runs through the set $\{1, 2, \ldots 12\}$.

Now $1^2 \equiv 12^2 \equiv 1 \pmod{13}$
$2^2 \equiv 11^2 \equiv 4$ "
$3^2 \equiv 10^2 \equiv 9$ "
$4^2 \equiv 9^2 \equiv 3$ "
$5^2 \equiv 8^2 \equiv 12$ "
$6^2 \equiv 7^2 \equiv 10 \pmod{13}$

∴ quadratic residue of 13 are $a = 1, 3, 4, 9, 10, 12$
and non residue are $2, 5, 6, 7, 8, 11$.

Thm (9.1) Euler's criterion: Let p be odd prime & $\gcd(a,p)=1$ Then 'a' is quadratic residue of p iff $a^{(p-1)/2} \equiv 1 \pmod p$

(Pf) Suppose 'a' is quadratic residue of p.
s.t $x^2 \equiv a \pmod p$ has solution say 'x_1'
As $\gcd(a,p) = 1$ (by defⁿ of quadratic residue)
$\Rightarrow \gcd(x_1, p) = 1$ (∵ x_1 is solution)
by thm (5.1) Fermat's theorem (let p prime & $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$)
Consider $a^{(p-1)/2} \equiv (x_1^2)^{\frac{(p-1)}{2}} \equiv x_1^{p-1}$
$\equiv 1 \pmod p$ (by thm 5.1)

Conversely,

Assume that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ -①

Show: 'a' is quadratic residue of p.

Let r be primitive root of p $\Rightarrow r^{\phi(p)} \equiv 1 \pmod{p}$

~~then a = r~~ $\Rightarrow r^{p-1} \equiv 1 \pmod{p}$ -②

Using ① & ②

$a \equiv r^k \pmod{p}$ for some integer k with $1 \le k \le p-1$

Now,

$r^{\frac{k(p-1)}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ (using ①)

By theorem (8.1) The order of r (i.e p-1) must divide $k\left(\frac{p-1}{2}\right)$

$\Rightarrow$ k is an even integer say $k = 2j$

Hence $(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p}$

$\Rightarrow r^j$ is solution of congruence $x^2 \equiv a \pmod{p}$

Hence, 'a' is quadratic residue of prime 'p'.

Corollary: Let p be an odd prime & $gcd(a,p) = 1$

then 'a' is quadratic residue or non residue of p according to whether

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

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

(proof) Let p be an odd prime & $gcd(a,p) = 1$

Now, $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1$

$\equiv 0 \pmod{p}$ [by using Fermat's theorem]

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

or

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

Example(9.2) In case $p=13$, we have

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$$

thus, integer 2 is quadratic non-residue of 13

Now, $3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1 \equiv 1 \pmod{13}$

thus, integer 3 is quadratic residue of 13.

Excercise (9.1)

(Question ①) Solve the following quadratic congruences

ⓐ $x^2+7x+10 \equiv 0 \pmod{11}$

comparing with ax^2+bx+c

Since $a=1$

11 is an odd prime & $gcd(1,11)=1$

& $gcd(4,11)=1$

∴ $4(x^2+7x+10) \equiv 0 \pmod{11}$

$\Rightarrow (2x+7)^2 - (7^2 - 4\times 10) \equiv 0 \pmod{11}$

$\Rightarrow (2x+7)^2 - 9 \equiv 0 \pmod{11}$

$\Rightarrow (2x+7)^2 \equiv 9 \pmod{11}$

thus $2x+7 \equiv 3 \pmod{11}$

$\Rightarrow 2x \equiv 3-7 \pmod{11}$

$\Rightarrow 2x \equiv -4 \pmod{11}$

$\Rightarrow x \equiv -2 \pmod{11}$

(∵ $gcd(2,11)=1$)

$\Rightarrow x \equiv 9 \pmod{11}$ (∵ $11-2=9$)

or $2x+7 \equiv -3 \pmod{11}$

$\Rightarrow 2x \equiv -10 \pmod{11}$

or $x \equiv -5 \pmod{11}$

i.e $x \equiv 6 \pmod{11}$

(∵ $11-5=6$)

Hence $x \equiv 9$ or $6 \pmod{11}$

ⓑ $3x^2+9x+7 \equiv 0 \pmod{13}$

(try as excercise)

Question 2)

Prove that the quadratic congruence $6x^2+5x+1 \equiv 0 \pmod{p}$ has a solution for every prime 'p', even though the equation $6x^2+5x+1 = 0$ has no solution in the integers.

(Solution) If $p=2$ then $6x^2+5x+1 \equiv 0 \pmod{2}$

Since $6\cdot(1)^2+5(1)+1 = 6+6 = 12 \equiv 0 \pmod{2}$

$\therefore x \equiv 1 \pmod{2}$ is a solution

If $p=3$, then $6x^2+5x+1 \equiv 0 \pmod{3}$

Since $6(1)^2+5(1)+1 = 6+6 = 12 \equiv 0 \pmod{3}$

$\therefore x \equiv 1 \pmod{3}$ is a solution

If $p \neq 3$ & p is odd prime

Since $6 = 2 \times 3$

$\therefore \gcd(6, p) = 1$

So, $\gcd(4 \times 6, p) = 1$

Hence $24(6x^2+5x+1) \equiv 0 \pmod{p}$

$(12x+5)^2 - (25-24) \equiv 0 \pmod{p}$

$\Rightarrow (12x+5)^2 - 1 \equiv 0 \pmod{p}$

$\Rightarrow (12x+5)^2 \equiv 1 \pmod{p}$

Then $12x+5 \equiv 1 \pmod{p}$ or $12x \equiv -4 \pmod{p}$

Since $\gcd(12, p) = 1$ & $1 \mid (-4)$ & $1 \mid (-8)$

So, there exists solution

$12x+5 \equiv -1 \pmod{p}$

$12x \equiv -6 \pmod{p}$

Hence, for all prime 'p', $6x^2+5x+1 \equiv 0 \pmod{p}$ has a solution

Also,
$6x^2+5x+1=0$ equation
it has zero are
$x_1 = -\frac{1}{3}$ or $x_2 = -\frac{1}{2}$
which are not integers.

(Q-4) Show that 3 is quadratic residue of 23, but a non-residue of 31.

(Solution) Since 23 is odd prime
& $\gcd(3, 23) = 1$
& $3^{(p-1)/2} = 3^{11} = (3^3)^3 \cdot 3^2$
$\equiv 4^3 \cdot 3^2 \pmod{23}$
$\equiv 64 \cdot 9 \pmod{23}$
$\equiv -5 \cdot 9 \pmod{23}$
$\equiv -45 \pmod{23}$
$\equiv +1 \pmod{23}$
∴ 3 is quadratic residue of 13 (by corollary 9.1)

Now $p=31$, $a=3$
$3^{(p-1)/2} \equiv (3^3)^5$
$\equiv (-4)^5 \pmod{31}$
$\equiv -4^5 \pmod{31}$
$\equiv (-64) \cdot 16 \pmod{31}$
$\equiv (-1) \cdot 64 \cdot 64 \pmod{31}$
$\equiv (-1) \cdot 2 \cdot 16 \pmod{31}$
$\equiv (-1) \cdot 1 \pmod{31}$
$\equiv -1 \pmod{31}$
∴ 3 is quadratic non-residue of 31.

(9.2) The legendre symbol and its properties

(Defn 9.2) let p be an odd prime and let $\gcd(a,p)=1$.
The legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

also denoted by $\left(\frac{a}{p}\right)$ or $(a|p)$

Exp(9.3) As done in e.g 9.1
$p=13$, $x^2 \equiv a \pmod{13}$
the quadratic residues of 13 are 1, 3, 4, 9, 10, 12
and non-residues are 2, 5, 6, 7, 8, 11

$\therefore \left(\frac{1}{13}\right) = \left(\frac{a}{p}\right) = 1$ As 1 is quadratic residue of 13

$$\left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1$$

and $\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1$

(Thm 9.2) (Statement only) let p be an odd prime and let 'a' & 'b' be integers that are relatively prime to 'p'.
Then the legendre symbol has the following properties:

(a) If $a \equiv b \pmod{p}$ then $(a/p) = (b/p)$
(b) $(a^2/p) = 1$
(c) $(a/p) = a^{(p-1)/2} \pmod{p}$
(d) $(ab/p) = (a/p)(b/p)$
(e) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$

(corollary) If p is odd prime, then

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

(Thm 9.6) If p is an odd prime, then

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

(Thm 9.7) If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}$ is a primitive root of $2p+1$.

(Thm 9.8) There are infinitely many primes of the form $8k-1$

(Lemma) If p is an odd prime and 'a' an odd integer with $\gcd(a,p) = 1$ then

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$$

$[ka/p]$ → greatest integer function

(Exs. 9.2)

(9-1) Find the value of following legendre symbols:

(d) $\left(\frac{28}{43}\right) = \left(\frac{9\times 2}{43}\right)$ (by Thm 9.2 (d))

$= \left(\frac{9}{43}\right)\left(\frac{2}{43}\right)$

$= \left(\frac{3^2}{43}\right)\left(\frac{2}{43}\right)$ (by Thm 9.2 (b))

$= 1 \cdot \left(\frac{2}{43}\right)$

$= \left(\frac{2}{43}\right)$

p is 43 odd prime

$\gcd(9,43) = 1$

$(2,43) = 1$

Now $\left(\frac{2}{43}\right)$ $(a,p)=1$, $(2,43)=1$

$2^{(43-1)/2} = 2^{21}$

Now [show whether (check) $2^{21} \equiv -1$ or $1 \pmod{43}$]

Section (9.1)

by corollary let p ($0 < a < p$) $\gcd(a,p)=1$ then a is quadratic residue already $a^{(p-1)/2} \equiv 1 \pmod p$

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

2^{21}

$2^7 = 128 \equiv (-1) \pmod{43}$

$(2^7)^3 = (-1)^3 \equiv -1 \pmod{43}$

$\therefore \left(\frac{2}{43}\right) = -1$

$2^{21} \equiv -1 \pmod{43}$

$\therefore$ 2 is quadratic non-residue of 43

$\therefore \left(\frac{2}{43}\right) = -1$

$\therefore \left(\frac{18}{43}\right) = -1$

(4) $\left(\frac{-72}{131}\right) = \left(\frac{-1}{131}\right)\left(\frac{8^2}{131}\right) \times \left(\frac{2}{131}\right)$

$\left(\frac{-1}{131}\right) = \left(\frac{-1}{p}\right) = -1$ $\left[\because \begin{array}{l} p \equiv 3 \pmod 4 \\ 131 \equiv 3 \pmod 4 \\ \text{corollary proved} \end{array}\right]$

$\left(\frac{8^2}{131}\right) = 1$ (since 131 is odd prime) [Thm 9.2 (b)]

$\left(\frac{2}{131}\right) = -1$ [Thm 9.6 $131 \equiv 3 \pmod 8$]

$\therefore \left(\frac{-72}{131}\right) = -1 \times 1 \times (-1) = 1$

(Gauss's lemma) (Statement)

Let p be an odd prime and let $\gcd(a, p) = 1$

If 'n' denotes the number of integers in the set

$S = \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\}$

whose remainders upon division by p exceeds $p/2$

then $(a/p) = (-1)^n$

(Q-2) Use Gauss lemma, find legendre symbol

$a = 8,\ p = 11$

(a) $\left(\frac{8}{11}\right)$

$S = \{a, 2a, 3a \cdots \left(\frac{p-1}{2}\right)a\}$

$S = \{8, 2\times 8, 3\times 8, \cdots \left(\frac{11-1}{2}\right)8\}$

$S = \{8, 16, 24, 32, 40\}$ $\quad > \frac{p}{2}$

Now, no. of elt in S which leave remainder $> \frac{11}{2}$

when divide by 11

$8 \equiv 8 \pmod{11}$ and $8 > 5.5$

$16 \equiv 5 \pmod{11}$ but $5 \not> 5.5$

$24 \equiv 2 \pmod{11}$ but $2 \not> 5.5$

$32 \equiv 10 \pmod{11}$ and $10 > 5.5$

$40 \equiv 7 \pmod{11}$ and $7 > 5.5$

No. of elt in S whose remainder $> \frac{11}{2}$

$\Rightarrow n = 3 \quad (8, 32, 40)$

$\therefore \left(\frac{8}{11}\right) = (-1)^n = (-1)^3 = -1$

(b) $\left(\frac{7}{13}\right)$ $\quad S = \{7, 14, 21, 28, 35, 42\}$

on modulo (13) $\quad S = \{7, 1, 8, 2, 9, 3\}$

rem $> \frac{13}{2}$ $\quad \Rightarrow n = 3 \quad \therefore \left(\frac{7}{13}\right) = (-1)^3 = -1$

$r > 6.5$