1 (9.3) Quadratic Reciprocity

Theorem (9.9)
Quadratic Reciprocity Law: If p & q are distinct odd primes, then $(p/q)(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

(proof) Consider the rectangle in xy co-ordinate whose vertices are $(0,0)$, $(p/2, 0)$, $(0, q/2)$ & $(p/2, q/2)$.
Let R be region within the rectangle, not including any of boundary lines.
As p & q are odd, so, Lattice points in R, (lattice points whose co-ordinates are integers) consists of all points (n, m) where $1 \le n \le (p-1)/2$ & $1 \le m \le (q-1)/2$

$\therefore$ such points are $\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$

Now diagonal D from $(0,0)$ to $(p/2, q/2)$ has equation $y = (q/p)\,x$ $\left[\text{Since } y - 0 = \frac{q/2 - 0}{p/2 - 0}(x - 0) \Rightarrow y = q/p\, x\right]$

For p must divide the x-co-ordinate of any lattice point on the line $yp = qx$ & q divides its y-coordinate,
there are no such points in R.
Suppose T_1 is portion of R that is below Diagonal D.
Suppose T_2 is portion of R that is above Diagonal D.
the number of integers in interval $0 < y < kq/p$ is equal to $\left[\frac{kq}{p}\right]$
For $1 \le k \le (p-1)/2$ has $\left[\frac{kq}{p}\right]$ lattice points in T_1 contained in T_1,
$\therefore$ total number of lattice points

Scanned with CamScanner

is $\displaystyle\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$

Similarly, Number of lattice points within T_2 is

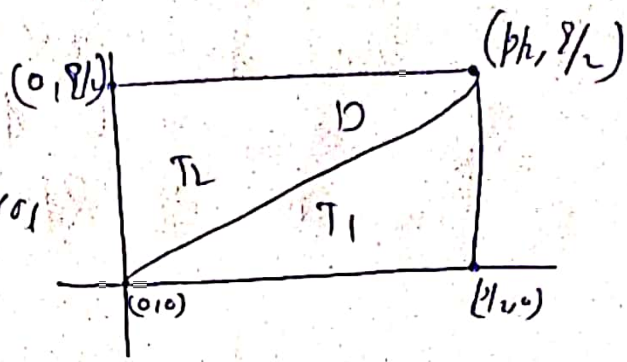
$$\sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right]$$

$\therefore$ All lattice points inside R are $\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right) = \displaystyle\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right]$

Using formula

$$\sum_{k=1}^{n-1}\left[\frac{km}{n}\right] = \frac{(m-1)(n-1)+\gcd(m,n)-1}{2}$$

where m & n are positive Integers,



Here,

$$\sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right] + \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] = \frac{\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right)+\gcd(p,q)-1}{2} + \frac{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)+\gcd(p,q)-1}{2}$$

$$= \frac{2\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right)}{2} = \frac{q-1}{2}\cdot\frac{p-1}{2} \quad (\because \gcd(p,q)=1) \quad (1)$$

By Gauss's lemma

$$(p|q)(q|p) = (-1)^{\sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right]}\cdot(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$$

$$= (-1)^{\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)} \quad (\text{Using } (1))$$

(Hence Proved)

Scanned with CamScanner

Corollary (1) If p & q are distinct odd primes, then

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

(proof) let $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$

$\Rightarrow p = 4k+1 \; (k \in \mathbb{Z})$ $\Rightarrow q = 4k+1 \; (k \in \mathbb{Z})$

$\Leftrightarrow \left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$ is even

by previous theorem $(-1)^{\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)} = (-1)^{\text{even}} = +1$

If both $4k+3$ form

$\Rightarrow \left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$ is odd $= (-1)^{\text{odd}} = -1$

(corollary (2)) If p & q are distinct odd primes, then

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

Example (9.5) Calculate Legendre symbol $(29/53)$

(Solution) Now $29 \equiv 1 \pmod 4$

$53 \equiv 1 \pmod 4$

then $\frac{29}{53} = \left(\frac{53}{29}\right)$ (by above corollary)

$= \left(\frac{24}{29}\right)$ $[\because 53 \equiv 24 \pmod{29}]$

$= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{4}{29}\right)$

$= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{2^2}{29}\right)$

$= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)(1)$ $\left[\because (a^2/p) = 1,\; a = 2,\; \gcd(2,53) = 1 \text{ by thm 9.2 (b)}\right]$

Scanned with CamScanner

Now, $\left(\frac{2}{29}\right) = -1$ (by thm 9.6)

Now $\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right)$ (by above corollary ~~[illegible]~~

$= \left(\frac{2}{3}\right)$ $\because 29 \equiv 2 \pmod 3$)

$= -1$ [by thm 9.6 $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3 \pmod 8$

$\Rightarrow \frac{2}{3} \equiv -1$ if $3 \equiv 3 \pmod 8$]

$\therefore \left(\frac{29}{53}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$

$= (-1)(-1) = 1$

Theorem (9.10) If $p \neq 3$, is an odd prime, then

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Example (9.6) Solution of quadratic congruence with a composite modulus. (Composite are numbers with have atleast one factor other than number itself & 1)

(Solution) consider

$x^2 \equiv 196 \pmod{1357}$

check whether $x^2 \equiv 196 \pmod{1357}$ is solvable or Not

Now, $1357 = 23 \times 59$

the given congruence is solvable iff both

$x^2 \equiv 196 \pmod{23}$

& $x^2 \equiv 196 \pmod{59}$

are solvable

Consider, (find value of legendre symbols)

$\left(\frac{196}{23}\right)$ & $\left(\frac{196}{59}\right)$

Scanned with CamScanner

Now, $\left(\frac{196}{23}\right) = \left(\frac{12}{23}\right) = \left(\frac{3}{23}\right) = 1$ (by thm 9.10)

[& $12 = 2^2 \times 3$

$\left(\frac{12}{23}\right) = \left(\frac{2^2}{23}\right) \times \left(\frac{3}{23}\right)$

$= 1 \times \left(\frac{3}{23}\right)$]

$\therefore \left(\frac{196}{23}\right) = 1$

thus, congruence $x^2 \equiv 196 \pmod{23}$ admits a solution

Now, $\left(\frac{196}{59}\right) = \left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right)$ (by corr (2))

$= -\left(\frac{2}{19}\right) = -(-1) = 1$ (by thm 9.6)

$\therefore \left(\frac{196}{59}\right) = 1$

$x^2 \equiv 196 \pmod{59}$ has a solution

$\therefore$ $x^2 \equiv 196 \pmod{1357}$ has solution.

$\therefore$ Congruence $x^2 \equiv 196$.

Exp (9.7) If $F_n = 2^{2^n} + 1$; $n > 1$, is a prime then 2 is not a primitive root of F_n. (done already)

But 3 is a primitive root of any prime of above type.

(Solution) $F_n = 2^{2^n} + 1$, where 2 is Not primitive root (done in section 8.3)

Do as exercise.

Scanned with CamScanner

Ex(9.3)

(Q-1) Evaluate the following legendre symbols

(a) $(71/73)$

$\because 71 \equiv -1 \pmod 4,\ 73 \equiv 1 \pmod 4$

($\because$ By cor. 2 section 9.3), we have

$$\left(\frac{71}{73}\right) = \left(\frac{73}{71}\right)$$

& $73 \equiv 2 \pmod{71}$

$\therefore (73/71) = (2/71)$

& $71 \equiv 7 \pmod 8$

Hence $(2/71) = 1$ (by thm 9.6)

$\therefore (71/73) = 1$

(Q-4) Verify that if p is an odd prime, then

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

(Solution) $(-2/p) = (-1/p)(2/p)$

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad \text{(corr. 9.2 section 9.2)}$$

& (By thm 9.6)

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

$\therefore$ if $p \equiv 1 \pmod 8$

then $p \equiv 1 \pmod 4$ & $4 \mid 8$

[Using if $a \equiv b \pmod m$ & $n \mid m$ $\Rightarrow a \equiv b \pmod n$ where $a, b \in \mathbb{Z}$ & $m, n \in \mathbb{Z}^+$]

$\Rightarrow (-2/p) = (-1/p)(2/p)$

$= 1 \cdot 1 = 1$

If $p \equiv 3 \pmod 8$ then $p \equiv 3 \pmod 4$

So $(-2/p) = (-1/p)(2/p) = (-1)(-1) = 1$

Scanned with CamScanner

If $p \equiv 5 \pmod 8$

then $p \equiv 5 \pmod 4$

$\equiv 1 \pmod 4$

$\therefore (-2/p) = (-1/p)(2/p) = 1 \times (-1) = -1$

if $p \equiv 7 \pmod 8$ then $p \equiv 7 \pmod 4$

$\equiv 3 \pmod 4$

$\therefore (-2/p) = (-1/p)(2/p) = (-1) \times (-1) = -1$

Hence, we get

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

Scanned with CamScanner