M.S c Mathematics –SEM 2 Number Theor CC-10 Unit 3

E-content 3–**By Dr Abhik Singh**, Guest faculty, PG Department of

Mathematics, Patna University, Patna

Content: Reciprocity Law, Jacobi Symbol, Irrational Number,

Reciprocity Law

Theorem: Let P and q be two distinct odd primes then

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

Proof : We know that

$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{1/2(p-1)}[kq/2]}$, $(p/q) = (-1)^{\sum_{l=1}^{1/2(q-1)}[lp/q]}$

Then to prove the required result

$\sum_{k=1}^{1/2(p-1)}[kq/p] + \sum_{l=1}^{1/2(q-1)}[lp/q] = (p-1)/2\ (q-1)/2$ ....(1)

For this consider the p-1/2,q-1/2 integers

lp-kq

Where l=1,2..................1/2(q-1), k=1,2............................1/2(p-1).

It must be noted that there is no zero among them, because if

$lp =$ kq, then q$\nmid$ lp which is not possible.

Now we shall show that among these p-1/2.q-1/2 integers , there are $\sum_{l=1}^{1/2(q-1)}[lp/q]$ *positive integers and* $\sum_{k=1}^{1/2(p-1)}[kq/2\ ]$ negative integers

So we see that for a given l, the necessary and sufficient condition that $lp -$kq >0 is $lp/$q >k or $1 \leq k \leq lp/q$

But $lp/q < \frac{q/2p}{q}$=1/2p

$\frac{lp}{q} \leq \frac{1}{2}$(p-1)

Which gives , for any given l, the number of such k's is $\frac{lp}{q}$.

Therefore the numbers $lp -$kq , there are $\sum_{l=1}^{1/2(q-1)}[lp/q]$ positive integers .

Similarly there are $\sum_{k=1}^{1/2(p-1)}[kq/2]$ negative integers.

Hence (1) exist.

Question . (1)Find (168/11) (ii) Evaluate (-23/59)

JACOBI SYMBOL

Let P be an odd prime integer with prime factorization.

$P=p_1p_2..p_n$ (possibly $p_i=p_j$ for $i \neq j$)

$(a,p)=1$

So $\left(\frac{a}{p}\right) = \left(\frac{a}{p1}\right)\left(\frac{a}{p2}\right)................................\left(\frac{a}{pn}\right)$

Where the symbols $\left(\frac{a}{pi}\right)$on the RHS of the equality are Legendre symbols and the symbol $\left(\frac{a}{p}\right)$ on the LHS is called Jacobi symbol.

Remarks

1. When p is prime , the Jacobi symbol is the same as the Legendre symbol, hence the Jacobi symbol may be considered as a generalization of the Legendre symbol.

2. The value of Jacobi symbol is also 1 or -1.

3. When $\left(\frac{a}{p}\right)=-1$, the congruence $x2 \equiv a \pmod{p}$ has no solution

4. $\left(\frac{1}{p}\right)=1$, $\left(\frac{a.a}{p}\right)=1$

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

Theorem(1)

$\left(\frac{a}{P}\right)\left(\frac{a}{R}\right)=\left(\frac{a}{PR}\right)$ where R is an odd positive integer.

Proof : Let $R=r_1r_2$..............r_t where $r_{1,}\ r_{2,}$..........................r_t are odd primes no necessarily all distinct. Then by definition of Jacobi symbol

$$\left(\frac{a}{P}\right)\left(\frac{a}{R}\right)=\left(\frac{a}{p1}\right)\left(\frac{a}{p2}\right)\ldots\ldots\ldots\left(\frac{a}{pk}\right)\left(\frac{a}{r1}\right)\ldots\ldots\ldots\left(\frac{a}{rt}\right)$$

$$=\left(\frac{a}{p1p2\ldots\ldots r1r2r3\ldots\ldots rt}\right)=\left(\frac{a}{PR}\right)$$

Theorem(2)

Let p be an odd prime and Q any odd positive integer prime to p. then $\left(\frac{Q}{P}\right)$ =(-1)(p-1)/2 x (Q-1)/2$\left(\frac{P}{Q}\right)$

Proof : Let Q=q1q2................................qn are all odd primes and not necessarily all distinct. Then $\left(\frac{Q}{P}\right)=\left(\frac{q1}{p}\right)\left(\frac{q2}{p}\right)$.........................$\left(\frac{qn}{p}\right)$

By law of quadratic reciprocity we know that it is equal to

(-1)(p-1)/2 .(q-1)/2$\left(\frac{p}{q1}\right)$(-1)(p-1)/2.(q2-1)/2$\left(\frac{p}{q2}\right)$.................................(-1)p-1/2.qn-1/2$\left(\frac{p}{qn}\right)$

= (-1)(p-1)2{(q1-1)/2+(q2-1)/2+.......................................(.qn-1)/2)}$\left(\frac{P}{Q}\right)$

=(-1)p-1/2{(Q-1)/2+2u)$\left(\frac{P}{Q}\right)$

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

Proved

Irrational Number

An irrational number as a real number which cannot be expressed in the form $\frac{a}{b}$ where a and b stand for integers.

Example- e, π, $\sqrt{2}$, $\sqrt[7]{11}$, e^{π}, π^{e}, etc

1. **Prove $\sqrt{2}$ is irrational**

Soln : Let us assume that $\sqrt{2}=\frac{a}{b}$ for some integers a, b such that (a, b)=1....................................(i)

It follows that $a^2=2b^2$....................................... (ii)

This implies that a^2 is even .consequently a is even because if a is odd , a^2 would also be odd.

Let us then put a=2a ,for some integer a_1.Then we obtain from (2)

$4a_1^2=2b^2$ or $b^2=2a_1^2$.

Thus both a and b are even .But This contradicts our assumption (1).It follows that $\sqrt{2}$ cannot be expressed in the form $\frac{a}{b}$.

This proves the theorem.

Theorem (1)

If k is a positive integer then e^k is irrational.

Proof Assume that the theorem is false. Hence $e^k=\frac{a}{b}$ for some positive integers a,b .

Let us now consider the definite integral

$I = b\, k^{2n+1} \int_0^1 e^{kx} f(x)\, dx$

Where $f(x) = x^n(1-x)^n/n!$

Integrating by parts we get

$I = b\, k^{2n+1}[\, (e^{kx}/k\, f(x) - e^{kx}/k^2 f'(x) + e^{kx}/k^3 f''(x) - \ldots\ldots$

$. + e^{kx}/k^{2n+1} f^{(2n)}(x)]_0^1$

Since $f^{(2n+1)}(x) = 0$ for $k > 0$. The general term on the right of the above equality is numerically of the form

$b\, k^{2n+1}(e^{kx}/k^{r+1} f^{(r)}(x))^1{}_0$ where $0 \leq r \leq 2n$

$= b\, k^{2n+1}(a/b\; 1/k^{r+1}\; f^{(r)}(1) - 1/k^{r+1} f^{(r)}(0)\}$

$= k^{2n+1}/k^{r+1}\{(a\, f^{(r)}(1) - b f^{(r)}(o)\}$

=an integer

Because $r+1 \leq 2n+1$, and $f^{(r)}(1), f^{(r)}(0)$ are integers

Hence I is an integer for all n .... (1)

On the other hand $0 < f(x) < 1/n!$, $0 < x < 1$.Therefore

$0 < e^{kx} f(x) < e^{kx}/n!$

$0 < b\, k^{2n+1} \int_0^1 e^{kx} f(x) dx < b k^{2n+1}/n! \int_0^1 e^{kx} dx$

$0 < I < b k^{2n+1}/n!\; e^k - 1/k$

$0 < I < b\, e^k (k^2)^n/n!$

But we know that $(k^2)^n/n! \to 0$ as $n \to \infty$.

Hence $I < 1$ for all sufficiently large value of n.

But this contradicts (1).

It follows that e^k is an irrational.

Assignment: (i) **Prove π^2 is irrational. (ii)Prove π is irrational**