1965

The law of quadratic reciprocity

Khalid Naeem
Lehigh University

THE LAW OF QUADRATIC RECIPROCITY

by
Khalid Naeem

A Thesis

Presented to the Graduate Faculty

of Lehigh University

in Candidacy for the Degree of

Master of Science

Lehigh University
1965

A CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

July 22, 1965
(date)

Gerhard Rayna
Professor in charge

Everett Pitcher
Head of the Department

Acknowledgment

The author wishes to thank Mr. Gerhard Rayna advisor, for his interest and advice in the efforts presented herein. Thanks also to Mrs. Helen Farrell for typing the manuscript.

Remarks on Notation

We borrow the following symbols.

$\rightarrow$ is to be read as "implies" thus $P(x) \rightarrow Q(x)$ reads as "P(x) implies Q(x)."

$\leftrightarrow$ is to be read as "if and only if."

$|$ is to be read as "divides."

$\{x \mid \phi(x)\}$ is to be read as "the set of x such that $\phi(x)$."

$\therefore$ is to be read as "therefore."

$\in$ is to be read as "belongs to."

i.e. is to be read as "that is."

$\| \ \|$ is to be read as "cardinality of" thus $\| S \|$ reads as "cardinality of the set S."

$\wp$ is the function defined on the integers whose value is $+1$ at even integers and -1 at odd integers.

Table of Contents

The theory of numbers, is concerned with the properties of the natural numbers 1,2,3, ... These numbers have exercised human curiosity from a very early period. The Greeks, Indians and Chinese made significant contributions prior to 1000 A.D. But as a systematic and independent science, theory of numbers is entirely a creation of modern times and can be said to date from the discoveries of Fermat.

As regards the present paper, it deals with "The Law of Quadratic Reciprocity" which is considered to be the major theorem of the theory of numbers.

The first section is devoted to the material which leads to the Gaussian Law of Quadratic Reciprocity, second section deals with the proofs of the law, while the third section deals with the Generalized Law of Quadratic Reciprocity. The range of the paper is indicated by the table of contents.

Section 1.

Theorem 1: (Gaussian Law of Quadratic Reciprocity)

If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'} \quad \text{where}$$

$$p' = \frac{p-1}{2},$$

$$q' = \frac{q-1}{2},$$ and the $(-)$ symbol is defined below (in Definition 7).

Since $p'q'$ is even when either p or q is of the form $4n+1$ and is odd when both p and q are of the form $4n+3$; we can, therefore, also state the law as follows:

If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless both p and q are of the form $4n+3$ in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Before we come to the law we deal with the following:

Definition 1: We say a is <u>congruent</u> to b (mod m) if $m \mid a-b$ or if a and b leave the same remainder when divided by m and we write

$$a \equiv b \pmod{m}.$$

Definition 2: Residue and Residue Class (mod m)(Griffin pages 53-54)

If $x \equiv a \pmod{m}$ we say that a is residue of x modulo m.

The totality of integers congruent to a given integer for the modulus m constitute a residue class modulo m.

Definition 3: Complete Residue System (mod m)

Any set of m integers selected so that no two of them belong to the same residue class modulo m forms a complete residue system modulo m.

Definition 4: Reduced Residue System (mod m)

Any set of integers prime to m and selected so that one and only one of them belongs to each of the residue classes of integers prime to m for the modulus m constitutes a reduced residue system modulo m.

Definition 5: Euler's Function $\phi(m)$ (Hardy and Wright page 52)

By $\phi(m)$ we mean the number of positive integers not greater than and prime to m, that is to say the number of integers n such that

$$0 < n \leq m \qquad (n,m) = 1$$

Lemma 1: (Hardy and Wright page 51)

If $(k,m) = d$ then

$$ka \equiv ka' \pmod{m} \rightarrow a \equiv a' \pmod{\tfrac{m}{d}}.$$

Proof: Since $(k,m) = d$ we have

$$k = k_1 d$$

$$m = m_1 d \text{ where } (k_1,m_1) = 1$$

Since $ka \equiv ka' \pmod{m}$

$\therefore m \mid k(a-a')$

or $m_1 d \mid k_1 d(a-a')$

or $m_1 d \mid k_1(a-a')$

Since $(k_1,m_1) = 1$

$\therefore m_1 \mid a-a'$

$\therefore a \equiv a' \pmod{\tfrac{m}{d}}$.

Lemma 2: (LeVeque Vol. 1 page 27)

If $\{a_1, a_2, \ldots, a_m\}$ is a complete residue system (mod m) and $(k,m) = 1$ then also $\{ka_1, ka_2, \ldots, ka_m\}$ is a complete residue system (mod m).

Proof: We need only show that the members ka_i $1 \le i \le m$ are incongruent to each other (mod m). Suppose ka_i are not incongruent then

$$ka_i \equiv ka_j \pmod{m}$$

since $(k,m) = 1$ by lemma 1 we have

$$a_i \equiv a_j \pmod{m}$$

which contradicts the hypothesis; hence ka_i $1 \le i \le m$ is a complete residue system (mod m).

Lemma 3: (LeVeque Vol 1. page 28)

If $\{a_1, \ldots, a_{\phi(m)}\}$ is a reduced residue system (mod m) and $(k,m) = 1$ then also $\{ka_1, \ldots, ka_{\phi(m)}\}$ is a reduced residue system (mod m).

Proof: Similar to that of lemma 2.

Definition 6: Quadratic residue and non residue (Hardy and Wright page 67)

Let p be an odd prime and $(a,p) = 1$ then if the congruence $x^2 \equiv a \pmod{p}$ is solvable for x we say a is quadratic residue of p written aRp; whereas if the congruence $x^2 \equiv a \pmod{p}$ is not solvable for x then a is quadratic non residue of p, written aNp.

Definition 7: Legendre's Symbol (LeVeque Vol.1 page 66)

Let p be an odd prime and $(a,p) = 1$. We define

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

For completeness we define

$$\left(\frac{a}{p}\right) = 0 \text{ if } p \mid a.$$

Lemma 4: (Niven, Zuckerman page 64)

Let p be an odd prime and let a and b denote integers prime to p.

then

(a) $a \equiv b \pmod{p} \rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(d) $\left(\frac{a^2}{p}\right) = 1 \quad \left(\frac{-1}{p}\right) = \delta\left(\frac{p-1}{2}\right)$

Proof: (a) If $a \equiv b \pmod{p}$ then the congruence $x^2 \equiv a \equiv b \pmod{p}$ is either solvable or non solvable; hence $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ (Hardy and Wright pages 67-69).

By hypothesis p is an odd prime and $(a,p) = 1$; let x be one of the members of the set

(A) $\{1,2,\ldots,p-1\}$.

Notice that the set (A) forms a reduced residue system (mod p); since $(x,p) = 1$ by lemma 3 it follows that

(B) $\{1\cdot x, 2\cdot x, \ldots, (p-1)x\}$ is also a reduced residue system (mod p).

Hence one of the members of the set (B) is congruent to a mod p; we may write

$xx' \equiv a \pmod{p}$ where $1 \leq x' \leq p-1$, and is called the associate of x.

There arise two possibilities:

Case (i) x is associated with itself, i.e. $x = x'$. In this case the congruence $x^2 \equiv a \pmod p$ has a solution; therefore aRp.

Observe that if one solution is x_1 then the other solution is $p-x_1$; for if x_1 is solution

$x_1^2 \equiv a \pmod p$ is true we check whether $(p-x_1)^2 \equiv a \pmod p$ is true

and $(p-x_1)^2 \equiv a \pmod p$ is true $\Leftrightarrow$

$$p^2 - 2px_1 + x_1^2 \equiv a \pmod p \text{ is true } \Leftrightarrow$$

$$x_1^2 \equiv a \pmod p \text{ is true}$$

hence $p-x_1$ is other solution, since quadratic equations have at most 2 solutions in a field there cannot be any other solution.

Thus when aRp there exist two solutions x_1 and $p-x_1$, and the numbers $1,2,\ldots,p-1$ may be grouped as x_1, $p-x_1$ and $\frac{1}{2}(p-3)$ pairs of unequal associated pairs.

$$\therefore\ x_1(p-x_1) \equiv -x_1^2 \equiv -a \pmod p.$$

$$xx' \equiv a \pmod p \text{ for } \tfrac{1}{2}(p-3) \text{ pairs}$$

$$\text{hence } \prod_{1 \leq x \leq p-1} x = (p-1)! \equiv -aa^{\frac{p-3}{2}} \pmod p$$

$$\text{(C)} \quad (p-1)! \equiv -a^{\frac{p-1}{2}} \pmod p.$$

Case (ii) when x is not associated with itself in this case the congruence $x^2 \equiv a \pmod p$ has no solution therefore aNp; and the numbers

$1,2,\ldots,p-1$ can be grouped into $\frac{1}{2}(p-1)$ unequal associated pairs.

$$\text{(D)} \quad \prod_{1 \leq x \leq p-1} x = (p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

by definition 7 we have

$$\left(\frac{a}{p}\right) = +1 \text{ if } aRp$$

$$\left(\frac{a}{p}\right) = -1 \text{ if } aNp$$

hence (C) and (D) can be combined into

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

Since $x^2 \equiv 1 \pmod p$ has solutions $x = \pm 1$ therefore $\left(\frac{1}{p}\right) = +1$.

Let us put $a = 1$ in (E) to obtain

$$\text{(F)} \quad (p-1)! \equiv -1 \pmod p$$

and thus incidently we have proved Wilson's Theorem:

If p is prime then

$$(p-1)! \equiv -1 \pmod p$$

Now we combine (E) and (F) to obtain

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

Since $\left(\frac{a}{p}\right)$ is just a sign ± 1, it can be placed on either side of the congruence. Thus we obtain

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

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

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

but $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$

$\therefore \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(d) $\left(\frac{a^2}{p}\right) = 1 \quad \left(\frac{-1}{p}\right) = \delta\left(\frac{p-1}{2}\right)$.

$\left(\frac{a^2}{p}\right) = 1$ is obvious from the definition of "quadratic residue" and

$\left(\frac{-1}{p}\right) = \delta\left(\frac{p-1}{2}\right)$ follows from part (b).

Definition 8: Least non negative residue (Hardy and Wright page 49)

If $x \equiv a \pmod m$ and $0 \leq a \leq m-1$ then a is called the least non negative residue of x modulo m.

Definition 9: Minimal residue (absolutely least residue) [Hardy and Wright page 73].

By the minimal residue of x (mod p) we mean that residue of x which lies between $-\frac{1}{2}p$ and $\frac{1}{2}p$. It is positive or negative according as the least non negative residue of x lies between 0 and $\frac{1}{2}p$ or between $\frac{1}{2}p$ and p.

Lemma 5:

Let $p_1 = \frac{p-1}{2}$ and let

$a \cdot 1 \equiv \varepsilon_1 r_1 \pmod p$

$a \cdot 2 \equiv \varepsilon_2 r_2$ (mod p

. . . .

. . . .

$a \cdot p_1 = \varepsilon_{p_1} r_{p_1} \pmod p$

be the set of congruences, where $\varepsilon_x r_x$ is the minimal residue of ax (mod p) and r_x is its magnitude so that $\varepsilon_x = \pm 1$; then

$$\left(\frac{a}{p}\right) = \varepsilon_1 \ \varepsilon_2 \ \ldots \ \varepsilon_{p_1} \quad \text{where } (a,p) = 1.$$

Proof: (Vinogradov page 83)

Observe that

$\{1,2,\ldots,\frac{p-1}{2}, \frac{p+1}{2}, \ldots p-1\}$ is a reduced residue system (mod p). Therefore

$\{-p_1, \ldots, -2, -1, 1,2,\ldots,p_1\}$ is also a reduced residue system (mod p). Since (a,p) = 1 hence by lemma 3 it follows that

(A) $\{-ap_1,\ldots,-2a,-a,a,2a,\ldots,p_1a\}$:

is also a reduced residue system (mod p). Therefore minimal residues of the members of the set (A) are just

$$-\varepsilon_{p_1}r_{p_1},\ldots,-\varepsilon_2r_2, -\varepsilon_1r_1, \varepsilon_1r_1, \varepsilon_2r_2,\ldots, \varepsilon_{p_1}r_{p_1}.$$

Hence these which are positive i.e. $r_1,r_2,\ldots,r_{p_1}$ must be the numbers $1,2,\ldots,p_1$.

Multiplying the set of congruences we get

$$a^{\frac{p-1}{2}} 1\cdot2\cdot \ldots p_1 \equiv \varepsilon_1 \ \varepsilon_2 \ \ldots \ \varepsilon_{p_1} r_1 r_2 \ldots r_{p_1} \pmod p$$

Since each of $1,2, \ldots, p_1$ is prime to p, hence their product $1\cdot2\cdot \ldots p_1$ is also prime to p, therefore dividing the congruence by

$1\cdot2\cdot \ldots p_1 = r_1r_2\ldots r_{p_1}$ and applying lemma 1 we get:

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \ \varepsilon_2 \ \ldots \ \varepsilon_{p_1} \pmod p$$

But by part (b) of lemma 4 we have

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

Thus from the last two congruences we obtain

$$\left(\frac{a}{p}\right) = \varepsilon_1 \ \varepsilon_2 \ldots \ \varepsilon_{p_1} .$$

Definition 10:

Let x be a real number; then [x] and {x} denote respectively the integral and fractional parts of x.

Some of the properties of [x] are the following:

(i) $[x+m] = [x]+m$, where m is an integer.

(ii) $[x] + [-x] = 0$ or -1 according as x is an integer or not.

(iii) $[x+y] \geq [x]+[y]$.

(iv) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$, if n is a positive integer.

Lemma 6:

Given ε_x and $\left(\frac{a}{p}\right)$ as in lemma 5 we have

$$\varepsilon_x = \delta\left(\left[\frac{2ax}{p}\right]\right) \text{ and thus}$$

$$\left(\frac{a}{p}\right) = \delta\left(\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]\right)$$

Proof: (Vinogradov page 84)

We have

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right]$$

and since $2\left[\frac{ax}{p}\right]$ is an integer we have by property (i)

$$\left[\frac{2ax}{p}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right]$$

Thus $\left[\frac{2ax}{p}\right]$ is even if the least positive residue of ax is less than $\frac{1}{2}p$ and is odd if the least positive residue is greater than $\frac{1}{2}p$ i.e. according as $\varepsilon_x = 1$ or $\varepsilon_x = -1$

$$\therefore \quad \varepsilon_x = \wp\left(\left[\frac{2ax}{p}\right]\right)$$

and thus $$\left(\frac{a}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]\right)$$

Lemma 7:

Let p and a be both odd and such that $(a,p) = 1$ where p is prime. Then

(a) $$\left(\frac{a}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]\right)$$

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

Proof: (Vinogradov page 84)

Since a and p are both odd, therefore $a+p$ is even. Since

$2a \equiv 2a + 2p \pmod{p}$.

Therefore we have by part (a) of lemma (4)

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4.\ \frac{a+p}{2}}{p}\right)$$ and by part (c) of lemma (4)

$$\left(\frac{4.\ \frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)$$

Now by lemma 6 we have

$$\left(\frac{\frac{a+p}{2}}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]\right)$$

$$= \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x\right)$$

$$= \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]\right) \cdot \wp\left(\frac{p^2-1}{8}\right)$$

$$\therefore \left(\frac{2a}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]\right) \cdot \wp\left(\frac{p^2-1}{8}\right)$$

$$\therefore \quad \text{(A)} \quad \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]\right) \cdot \wp\left(\frac{p^2-1}{8}\right)$$

putting $a = 1$ in (A) and using the fact that $\left(\frac{1}{p}\right) = 1$ and $\left[\frac{x}{p}\right] = 0$

for $1 \leq x \leq p_1$ we get:

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

and then putting (b) in (A) we obtain:

(a) $\left(\frac{a}{p}\right) = \wp\left(\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]\right)$

Lemma 8: (Gauss's Lemma) (Hardy and Wright page 74)

Let m be an integer and p an odd prime such that $(p,m) = 1$ then $\left(\frac{m}{p}\right) = \wp(\mu)$ where μ is the number of members of the set

$\{m, 2m, 3m, \ldots\ldots, \frac{1}{2}(p-1)m\}$

whose least positive residues (mod p) are greater than $\frac{1}{2}p$.

Proof: (Mathews part I page 39)

Observe that $1, 2, 3, \ldots, \frac{p-1}{2}$ are incongruent (mod p) and since $(m,p) = 1$ hence

(A) $1\cdot m, 2\cdot m, 3\cdot m, \ldots\ldots\ldots, \frac{p-1}{2}m$ are also incongruent (mod p). Hence their least positive residues (mod p) will be all incongruent; of these least positive residues a certain number, μ say, will be greater than $p' = \frac{p-1}{2}$. Denote them by $\alpha_1, \alpha_2, \ldots, \alpha_\mu$; and the others will be less than p'. Let the residues less than p' be denoted by

$$\beta_1, \beta_2, \ldots, \beta_\lambda;$$

then $\mu + \lambda = \frac{p-1}{2}$.

Now the numbers

$p-\alpha_1, p-\alpha_2, \ldots, p-\alpha_\mu$ are all less than $p'+1$. ($\leq p'$)

We observe that firstly:

the numbers $p-\alpha_i$ $1 \leq i \leq \mu$ are all incongruent (mod p) for

if they are not incongruent then

$$p-\alpha_i \equiv p-\alpha_j \pmod p \qquad 1 \leq i, j \leq \mu$$

$$\therefore \alpha_i \equiv \alpha_j \pmod p \qquad i \neq j.$$

but α_i $1 \leq i \leq \mu$ are all incongruent (mod p)

and secondly:

no $p-\alpha_i$ is congruent to β_j $\quad 1 \leq j \leq \lambda$

$1 \leq i \leq \mu$

for if some $p-\alpha_i$ is congruent to some β_j we have

$$p-\alpha_i \equiv \beta_j \pmod p$$

$$\therefore \alpha_i + \beta_j \equiv 0 \pmod p$$

but α_i and β_j are the least positive residues of the set (A)

hence there must be two numbers from the set (A) say Sm and tm

such that $Sm \equiv \alpha_i$ and

$tm \equiv \beta_j$

so that $Sm + tm \equiv 0 \pmod p$

i.e. $p \mid (S+t)m$ but $(p,m) = 1$

hence $p \mid S+t$

But S and t are both less than $\frac{1}{2}p$ hence $p \mid S+t$ is impossible.

Consequently it follows that

$(p-\alpha_1), (p-\alpha_2), \ldots (p-\alpha_\mu), \beta_1, \beta_2, \ldots, \beta_\lambda$

must be a permutation of

$1, 2, \ldots, p'$.

Hence it follows that

$$1\cdot 2\cdot 3 \ldots p' \equiv (p-\alpha_1)(p-\alpha_2) \ldots (p-\alpha_\mu)\, \beta_1 \beta_2 \ldots \beta_\lambda \pmod{p}$$

but since $p-\alpha_i \equiv -\alpha_i \pmod{p}$

we therefore have:

$$1\cdot 2\cdot 3 \ldots p' \equiv \wp(\mu)\, \alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda \pmod{p}$$

But $\alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \ldots \beta_\lambda \equiv m\cdot 2m\cdot 3m \ldots p'm \pmod{p}$

therefore $1\cdot 2\cdot 3 \ldots p' \equiv \wp(\mu)\; m\cdot 2m\cdot 3m \ldots p'm \pmod{p}$

Now since each of the numbers $1, 2, \ldots, p'$ is prime to p

hence is the product $1\cdot 2 \ldots p'$

dividing the congruence by $1\cdot 2 \ldots p'$ it follows by lemma 1 that

$$1 \equiv \wp(\mu)\, m^{p'} \pmod{p}$$

$$m^{p'} \equiv \wp(\mu) \pmod{p}$$

but by part (b) of lemma 4 we have

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

We have from the last two congruences

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

Definition 11: Lattice point.

By a lattice point we mean the point both of whose coordinates are integers.

Lemma 9: (Theorem of Eisenstein) (Hardy and Wright pages 76–77)

Le p and q be distinct odd primes; if

$$S(q,p) = \sum_{s=1}^{p'} \left[\frac{sq}{p}\right] \quad \text{then}$$

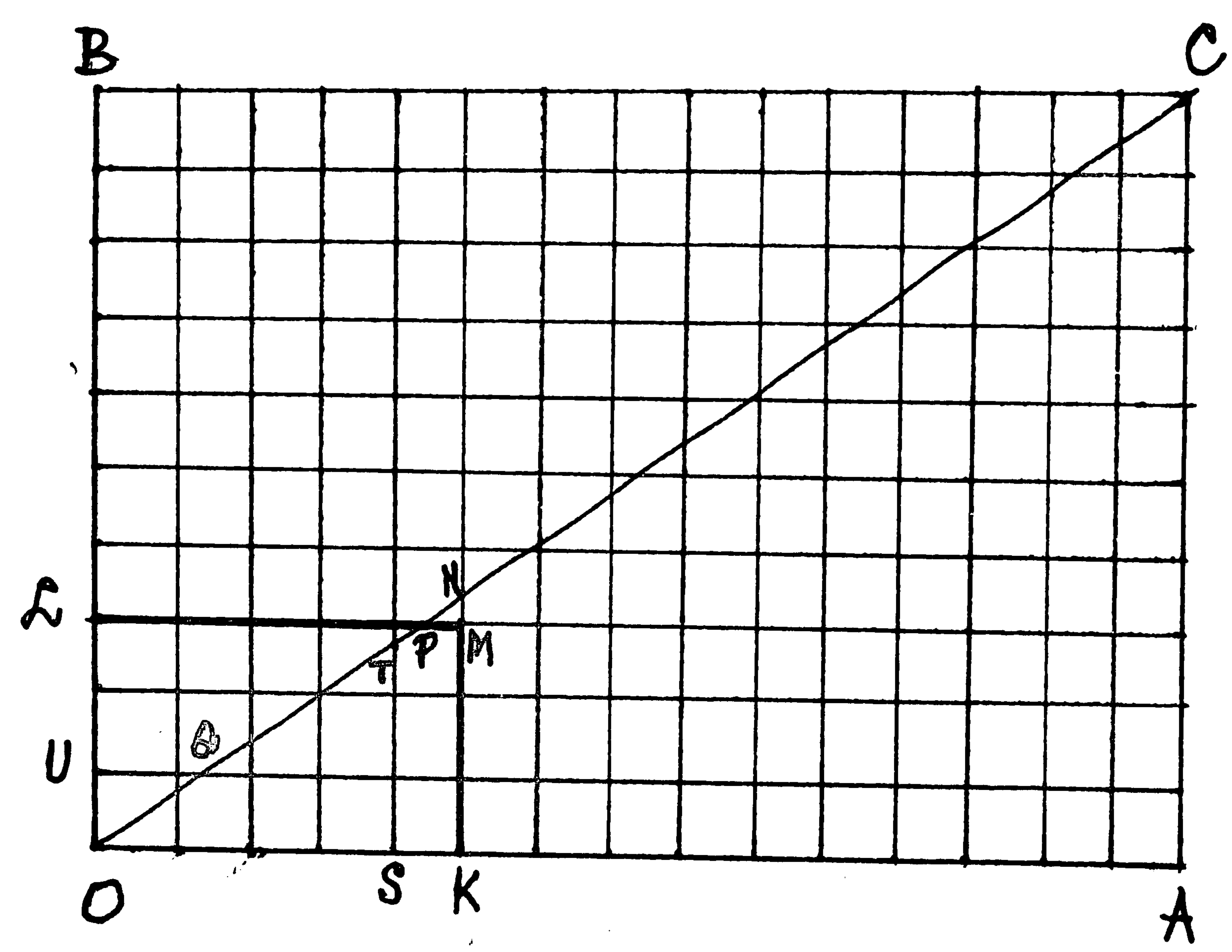
$$S(q,p) + S(p,q) = p'q' \text{ where}$$

$$p' = \frac{p-1}{2}$$

$$q' = \frac{q-1}{2} \quad .$$

We shall present two proofs.

(i) Geometric proof.



Let in the figure equations of AC and BC be

$x=p$ and $y=q$ and those of KM and LM be

$x=p'$ and $y=q'$.

If as appears in the figure $p > q$ then $p' > q'$

$$\therefore \quad \frac{q'}{p'} < \frac{q}{p} .$$

Since $q' < q\frac{p'}{p} < q'+1$ and the equation of the

diagonal OC is $\frac{y}{x} = \frac{q}{p}$.

Therefore when $x = p'$ then $y = q\,\frac{p'}{p}$; hence there is no integer

between $KM = q'$ and $KN = q\,\frac{p'}{p}$.

We now count up the number of lattice points in the rectangle OKML, where we do not count lattice points on the axes but we do count lattice points on KM and LM. In the first place this number is plainly $p'q'$; since lattice points (x,y) satisfy the conditions

$$1 \leq x \leq p' \qquad 1 \leq y \leq q'.$$

The equation of the diagonal being $y = \frac{q}{p}x$, and since $(p,q) = 1$ hence there cannot occur any lattice points on OC. Further we have already seen that there can exist no integer between M and N.

Thus there are no lattice points in the triangle PMN except possibly on PM. Hence the number of lattice points in OKML is the sum of the lattice points in the triangles OKN and OLP.

Consider now the line ST given by the equation $x = s$ the ordinate T is given by $y = \frac{q}{p} s$; hence the number of lattice points on ST are $\left[\frac{q}{p} s\right]$. Thus the number of lattice points in the triangle OKN is

$$\sum_{p=1}^{p'} \left[\frac{q}{p} s\right] = S(q,p).$$

Consider now the line UQ given by the equation $y=u$, then $x = \frac{p}{q} u$ is the abscissa of Q. Thus the number of lattice points on UQ is $\left[\frac{p}{q} u\right]$. Hence the number of lattice points in the triangle OPL is

$$\sum_{u=1}^{q'} \left[\frac{p}{q} u\right] = S(p,q).$$

Therefore $S(q,p) + S(p,q) = p'q'$.

(ii) Analytic proof: (Landau page 61)

Consider the $p'q'$ numbers defined by

$up-sq$ where $s = 1,2, \ldots, p'$ and

$u = 1,2, \ldots, q'$

We observe that none of these numbers is zero because

$$\begin{aligned} up-sq = 0 &\rightarrow up=sq \\ &\rightarrow p \mid sq \text{ but } (p,q) = 1 \\ &\therefore p \mid s \text{ which is impossible.} \end{aligned}$$

Exactly $\sum_{u=1}^{q'} \left[\frac{up}{q}\right]$ among the $p'q'$ numbers are positive

for let $s < \frac{up}{q}$ where $1 \leq s \leq \frac{p-1}{2}$;

for every $u= 1,2, \ldots, \frac{q-1}{2}$ since $\frac{up}{q}$ is not an integer. It follows that $1 \leq s < \frac{up}{q}$ has exactly $\left[\frac{up}{q}\right]$ solutions so that

$$s < \frac{q}{2}\frac{p}{q} = \frac{p}{2}$$

or $s \leq \frac{p-1}{2}$ is automatically true.

By symmetry exactly $\sum_{x=1}^{p'}\left[\frac{sq}{p}\right]$ of the $p'q'$ numbers are negative.

Therefore $\sum_{s=1}^{p'}\left[\frac{sq}{p}\right] + \sum_{u=1}^{q'}\left[\frac{up}{q}\right] = p'q'$.

Lemma 10:

Let p and q be distinct odd primes, $p' = \frac{p-1}{2}$, $q' = \frac{q-1}{2}$ and

$S_1 = \{(x,y) \mid (x,y)$ is lattice point, $1 \leq x \leq p'$, $1 \leq y < (q/p)x\}$

$S_2 = \{(x,y) \mid (x,y)$ is lattice point, $1 \leq y \leq q'$, $1 \leq x < (p/q)y\}$

then $\left\|S_1\right\| = \sum_{x=1}^{p'}\left[\frac{qx}{p}\right]$, $\left\|S_2\right\| = \sum_{y=1}^{q'}\left[\frac{py}{q}\right]$ and

$$\left\|S_1 + S_2\right\| = p'q'.$$

Proof: (Niven, Zuckerman page 68)

Let (u,v) be any lattice point such that $1 \leq u \leq \frac{p-1}{2}$

and $1 \leq v \leq \frac{q-1}{2}$; and consider the three alternatives:

(i) $v < (q/p)u$: if $v < (q/p)u$ then by definition of S_1 $(u,v) \in S_1$.

(ii) $v > (q/p)u$: then $u < \left(\frac{p}{q}\right)v$ are by definition of S_2 $(u,v) \in S_2$.

(iii) $v = (q/p)u$: this alternative is impossible since this implies $p|u$ which cannot be because $1 \leq u < p$.

Thus either $(u,v) \in S_1$ or $(u,v) \in S_2$ but in no case (u,v) can belong to both S_1 and S_2 at the same time. Note that there are $\frac{p-1}{2}\ \frac{q-1}{2}$ lattice points (u,v).

Now if $(x,y) \in S_1$ then $1 \leq x \leq \frac{p-1}{2}$

$1 \leq y < (q/p)x \leq (q/p)\frac{p-1}{2} = \frac{p-1}{p}\frac{q}{2} < \frac{q}{2}$. Since q is odd and y is an integer this implies that

$$1 \leq y \leq \frac{q-1}{2}. \quad \text{Hence } (x,y) \in S_1 \text{ is a } (u,v).$$

And if $(x,y) \in S_2$ then $1 \leq y \leq \frac{q-1}{2}$

$1 \leq x < (p/q)y \leq (p/q)\frac{q-1}{2} = \frac{q-1}{q}\ \frac{p}{2} < \frac{p}{2}$. Since p is odd and x is integer we have

$$1 \leq x \leq \frac{p-1}{2}. \quad \text{Hence } (x,y) \in S_2 \text{ is a } (u,v).$$

This shows that

$$\left\| S_1 + S_2 \right\| = \frac{p-1}{2}\ \frac{q-1}{2} .$$

We now count the number of lattice points in S_1 and S_2 separately. For each $1 \leq x \leq \frac{p-1}{2}$ the pair $(x,y) \in S_1$ just for $y = 1,2,\ldots,\left[\frac{qx}{p}\right]$.

The number of these y is $\left[\frac{qx}{p}\right]$.

Thus $\left\|S_1\right\| = \sum_{x=1}^{p'}\left[\frac{qx}{p}\right]$

Similarly $\left\|S_2\right\| = \sum_{y=1}^{q'}\left[\frac{p}{q}y\right]$

We can now give a new proof of part (a) of lemma 7, which we reword as follows: (Niven, Zuckerman pages 65-66)

If p is an odd prime and (a,2p) = 1 then

$$\left(\frac{a}{p}\right) = \rho\left(\sum_{j=1}^{p'}\left[\frac{ja}{p}\right]\right)$$

$$p' = \frac{p-1}{2} .$$

Proof: Observe that

1,2,..., p' are incongruent (mod p) and since (a,2p) = 1 we have (a,p) = 1. Therefore

(A) $1\cdot a, 2\cdot a, \ldots, p'\cdot a$ are also incongruent (mod p).

Hence their least positive residues will be all incongruent. Of these a certain number μ say will be greater than p' denote them by

$\alpha_1, \ldots, \alpha_\mu$ and let the rest of them which are less than p' be denoted by

$\beta_1, \ldots, \beta_\lambda$

we have then $\mu + \lambda = p'$.

Division of the set (A) by p may be written

(B) $ja = p\left[\frac{ja}{p}\right] + u_j$

where $1 \leq j \leq p'$ and $1 \leq u_j \leq p-1$. Note that u_j are the least positive residues of ja (mod p).

Summing the equations (B) from j=1 to j=p' we get:

$$\sum_{j=1}^{p'} ja = \sum_{j=1}^{p'} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{p'} u_j .$$

$$\therefore \quad (C) \quad a\sum_{j=1}^{p'} j = \sum_{j=1}^{p'} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{\mu} \alpha_j + \sum_{j=1}^{\lambda} \beta_j .$$

Since $\lambda + \mu = p'$ hence

$p - \alpha_j \quad 1 \leq j \leq \mu$ and $\beta_j \quad 1 \leq j \leq \lambda$ are the numbers

1,2, ..., p' in same order.

Hence if $R = \sum_{j=1}^{\lambda} \beta_j$

and $R' = \sum_{j=1}^{\mu} p - \alpha_j = \mu p - \sum_{j=1}^{\mu} \alpha_j$

then $R + R' = \mu p - \sum_{j=1}^{\mu} \alpha_j + \sum_{j=1}^{\lambda} \beta_j$

but $R + R' = \sum_{j=1}^{p'} j = \frac{1}{2}\,\frac{p-1}{2}\,\frac{p+1}{2} = \frac{1}{8}(p^2-1)$.

$$\therefore \quad (D) \quad \frac{1}{8}(p^2-1) = \mu p - \sum_{j=1}^{\mu} \alpha_j + \sum_{j=1}^{\lambda} \beta_j .$$

Subtracting (D) from (C) we get:

(E) $$\frac{1}{8}(p^2-1)(a-1) = p\left(\sum_{j=1}^{p'}\left[\frac{ja}{p}\right]-\mu\right)+2\sum_{j=1}^{\mu}\alpha_j$$

Since a and p are both distinct odd numbers

$\therefore$ a−1 is even and $p^2-1 \equiv 0 \pmod 8$

$\therefore$ L.H.S. of (E) is even and the last term on the right is even hence we must have

$$2 \,\Big|\, p\left(\sum_{j=1}^{p'}\left[\frac{ja}{p}\right]-\mu\right) \quad \text{but} (2,p) = 1$$

$$\therefore \quad 2 \,\Big|\, \sum_{j=1}^{p'}\left[\frac{ja}{p}\right]-\mu .$$

$$\therefore \quad \sum_{j=1}^{p'}\left[\frac{ja}{p}\right] \equiv \mu \pmod 2 .$$

But by lemma 8

$$\left(\frac{a}{p}\right) = \delta(\mu)$$

$$\therefore \left(\frac{a}{p}\right) = \delta\left(\sum_{j=1}^{p'}\left[\frac{ja}{p}\right]\right)$$

Section 2.

We are now in a position to prove the famous theorem 1 "The Gauss Law of Reciprocity".

This theorem was discovered at different times by Euler, Legendre and Gauss, but Gauss was the first one to prove it in 1796, when he was just eighteen years old.

Carl Friedrich Gauss (1777-1855) whom his contemporaries used to call "Princeps Mathematicorum" (Prince of Mathematicians) was perhaps the greatest mathematical genius of all time, only Archimedes and Newton being comparable to him. Though Gauss contributed to almost all branches of Mathematics, number theory, or "higher arithmetic" as he called it was his favorite science; as is evident from the phrase attributed to him "Mathematics is the Queen of Sciences, but Arithmetic is the Queen of Mathematics". His interest and appraisal of the reciprocity law is manifested by the fact that he developed not less than eight different demonstrations of it and valued it so high as to call it "gem of higher arithmetic".

Among the leading mathematicians who have also proved the theorem are Cauchy, Eisentein, Jacobi,Kronecker, Kummer, Liouville and Zeller.

Indeed, the interest that it continued to arouse is evidenced by the fact that it was proved in about fifty ways during the nineteenth century, but of course the proofs are essentially not all different.

We will present a few different demonstrations of the law.

If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \wp(p'q') \quad \text{where}$$

$$p' = \frac{p-1}{2}$$

$$q' = \frac{q-1}{2} .$$

(i) By lemma 7 we have

If p and a be both odd and (a,p) = 1 then

$$\left(\frac{a}{p}\right) = \wp\left(\sum_{x=1}^{p'}\left[\frac{ax}{p}\right]\right)$$

putting q for a and s for x we get:

$$\text{(A)} \quad \left(\frac{q}{p}\right) = \wp\left(\sum_{s=1}^{p'}\left[\frac{qs}{p}\right]\right)$$

now putting p for a, q for p and u for x we get:

$$\text{(B)} \quad \left(\frac{p}{q}\right) = \wp\left(\sum_{u=1}^{q'}\left[\frac{pu}{q}\right]\right)$$

(A) and (B) give

$$\text{(C)} \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \wp\left(\sum_{u=1}^{q'}\left[\frac{pu}{q}\right] + \sum_{s=1}^{p'}\left[\frac{qs}{p}\right]\right)$$

But by lemma 9 we have

$$\sum_{u=1}^{q'}\left[\frac{pu}{q}\right]+\sum_{s=1}^{p'}\left[\frac{qs}{p}\right]=p'q'.$$

hence from (C)we obtain:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\wp(p'q')$$

(ii) We have by lemma 7

$$\left(\frac{p}{q}\right)=\wp\left(\sum_{u=1}^{q'}\left[\frac{pu}{q}\right]\right)$$

and $\left(\frac{q}{p}\right)=\wp\left(\sum_{s=1}^{p'}\left[\frac{qs}{p}\right]\right)$

and thus $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\wp\left(\sum_{u=1}^{q'}\left[\frac{pu}{q}\right]+\sum_{s=1}^{p'}\left[\frac{qs}{p}\right]\right)$

Now by lemma 10 we have

$$\sum_{u=1}^{q'}\left[\frac{pu}{q}\right]+\sum_{s=1}^{p'}\left[\frac{qs}{p}\right]=p'q'$$

Therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\wp(p'q')$

(iii) (LeVeque pages 70-71)

Consider the numbers

(A) $q, 2q, \ldots, \frac{p-1}{2}q$

(B) $p, 2p, \ldots, \frac{q-1}{2}p$

then by lemma 8 we have

$$\left(\frac{q}{p}\right) = \wp(\mu) \quad \left(\frac{p}{q}\right) = \wp(\nu)$$

where μ is the number of least positive residues (mod p) of the set (A) which are greater than $\frac{1}{2}p$ and ν is the number of least positive residues (mod q) of the set (B) which are greater than $\frac{1}{2}q$.

Since the minimal residue of a residue greater than half the modulus is negative, we can say that μ and ν are the number of minimal residues of the sets (A) and (B) with respect to mod p and mod q respectively which are negative.

We will show that $\mu+\nu \equiv \frac{p-1}{2} \frac{q-1}{2} \pmod 2$.

Choose y such that

$$-\frac{p}{2} < qx - py < \frac{p}{2} .$$

then $qx - py$ is the minimal residue of qx (mod p).

We have from the above inequality

$$\frac{qx}{p} - \frac{1}{2} < y < \frac{qx}{p} + \frac{1}{2} .$$

Thus it follows that y is unique and positive.

If $y = 0$ then $qx - py = qx > 0$. In this case, since minimal residue is positive, there is no contribution to μ.

Moreover we see that for $x \leq \frac{p-1}{2}$

$$\frac{qx}{p} - \frac{1}{2} \leq \frac{q\,\frac{p-1}{2}}{p} - \frac{1}{2} = \frac{p-1}{p}\,\frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{1}{2} = \frac{q-1}{2} .$$

and since $y < \frac{qx}{p} + \frac{1}{2}$ we have

$$y < \frac{q-1}{2} + \frac{1}{2} + \frac{1}{2} = \frac{q+1}{2}$$

so that we have $y \leq \frac{q-1}{2}$.

The number μ denotes therefore the number of combinations of x and y from the sets

(p) $1, 2, \ldots, \frac{p-1}{2}$

(q) $1, 2, \ldots, \frac{q-1}{2}$

respectively for which

$$-\frac{p}{2} < qx - py < 0$$

Likewise ν is the number of combinations of x and y from the sets (p) and (q) respectively for which

$$-\frac{q}{2} < py - qx < 0.$$

Observe that for any other pair x and y from (p) and (q) respectively either

$$py - qx > \frac{p}{2}$$

$$\text{or} \quad py - qx < -\frac{q}{2} .$$

Let there be λ of the former and ϱ of the latter.

Then clearly

$$\frac{p-1}{2}\frac{q-1}{2} = \mu + \nu + \lambda + \varrho$$

Now as x and y run through (p) and (q) respectively the numbers

$$x' = \frac{p+1}{2} - x \qquad y' = \frac{q+1}{2} - y$$

run through the same sequences (p) and (q) but in the opposite order.

Since $py' - qx' = p\left(\frac{q+1}{2} - y\right) - q\left(\frac{p+1}{2} - x\right)$

$$= \frac{p-q}{2} - (py - qx)$$

therefore if $py - qx > \frac{p}{2}$

then $py' - qx' < \frac{p-q}{2} - \frac{p}{2} = -\frac{q}{2}$.

Thus $\lambda = \rho$

$$\therefore \frac{p-1}{2}\,\frac{q-1}{2} = \mu + \nu + 2\lambda \equiv \mu + \nu \pmod 2$$

$$\therefore \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \delta\left(\frac{p-1}{2}\,\frac{q-1}{2}\right).$$

(iv) (Uspensky and Heaslet pages 289-292)

Let (A) and (B) be the same sets and μ and ν have the same meanings as in proof (iii). To prove the law it, therefore suffices to show that $\mu + \nu \equiv \frac{p-1}{2}\,\frac{q-1}{2} \pmod 2$ which we now present in the following different manner:

Observe that least positive residue (mod p) of any number belongs to one of the series:

($\mathfrak{F}$) $1, 2, \ldots, \frac{p-1}{2}$

($\mathfrak{F}'$) $\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$

while least positive residue (mod q) of any number belongs to one of the series:

(F) $1, 2, \ldots, \frac{q-1}{2}$

(F') $\frac{q+1}{2}, \frac{q+3}{2}, \ldots, q-1$

Consider now the numbers

$$(C) \quad 1, 2, \ldots, \frac{pq-1}{2}$$

We notice that the numbers (C) form least positive residues (mod pq) which are less than or equal to $\frac{pq-1}{2}$. Hence none of these is divisible by p and q simultaneously. We can, therefore, divide the numbers (C) into the following eight classes:

Class 1 contains those numbers whose least positive residues (mod p) belong to ($\mathcal{F}$) and (mod q) belong to (F). Let the cardinality of this class be α .

Class 2 contains those numbers whose least positive residues (mod p) belong to ($\mathcal{F}$) and(mod q) belong to (F'). Let the cardinality of this class be β .

Class 3 contains those numbers whose least positive residues (mod p) belong to ($\mathcal{F}'$) and (mod q) belong to (F). Let the cardinality of this class be γ .

Class 4 contains those numbers whose least positive residues (mod p) belong to ($\mathcal{F}'$) and (mod q) belong to (F'). Let the cardinality of this class be δ .

Class 5 contains multiples of q whose least positive residues (mod p) belong to ($\mathcal{F}'$). Since all the multiples of q in the series (C) are q, 2q, ..., $\frac{p-1}{2}$q which form the set (A). Hence the cardinality of this class is μ .

Class 6 contains multiples of q whose least positive residues (mod p) belong to ($\mathcal{F}$). The cardinality of this class is $\frac{p-1}{2} - \mu$.

Class 7 contains multiples of p whose least positive residues (mod q) belong to (F'). Since all the multiples of p in series (C) are

$$p, 2p, \ldots, \frac{q-1}{2}p \text{ which forms the set (B).}$$

Hence the cardinality of this class is ν.

Class 8 contains multiples of p whose least positive residues (mod q) belong to (F). The cardinality of this class is $\frac{q-1}{2} - \nu$.

Observe that classes 2,4 and 7 contain all the numbers of series (C) whose least positive residues (mod q) belong to (F'). For a given residue ρ which belongs to (F'), such numbers are

$$\rho,\ q+\rho,\ 2q+\rho,\ \ldots,\ \frac{p-3}{2}q+\rho .$$

To ascertain whether there can be more numbers consider

$$tq + \rho \leq \frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2} .$$

$$\text{or} \quad tq \leq \frac{p-3}{2}q + \left(q + \frac{q-1}{2} - \rho\right)$$

thus the inequality can hold for $t = \frac{p-3}{2}$ and not for $t = \frac{p-1}{2}$. Hence with a given value of ρ we have $\frac{p-1}{2}$ numbers and since number of residues in (F') is $\frac{q-1}{2}$; ρ therefore can have $\frac{q-1}{2}$ values. Hence it follows that classes 2,4 and 7 comprise $\frac{p-1}{2}\frac{q-1}{2}$ numbers.

$$\therefore (1) \qquad \beta+\sigma+\nu = \frac{p-1}{2}\frac{q-1}{2} .$$

Now consider the classes 3,4 and 5 which contain all the numbers of series (C) whose least positive residues (mod p) belong to $(\mathcal{J}')$.

For a given residue η which belongs to $(\mathcal{F}')$, such numbers are

$$\eta,\ p+\eta\ ,\ 2p+\eta\ ,\ \dots\ ,\ \frac{q-3}{2}p+\eta$$

Thus with a given value of η we have $\frac{q-1}{2}$ numbers and since η can have $\frac{p-1}{2}$ values. It follows that the classes 3,4 and 5 contain $\frac{p-1}{2}\ \frac{q-1}{2}$ numbers.

$$\therefore (2) \qquad \gamma+\delta+\mu = \frac{p-1}{2}\ \frac{q-1}{2}$$

Now consider the series

$$(D) \qquad \frac{pq+1}{2}\ ,\ \frac{pq+3}{2}\ ,\ \dots\ ,\ pq-1$$

Notice that none of these numbers is divisible by p and q simultaneously and to each number a in the series (C) which belongs to the class 3, there corresponds the number pq−a in the series (D) such that the least positive residues of the numbers pq−a with respect to moduli p and q belong to $(\mathcal{F})$ and (F') respectively and vice versa. Therefore we notice that in the class 3, there are exactly as many numbers as there are numbers in series (D) whose least positive residues (mod p) belong to $(\mathcal{F})$ and (mod q) belong to (F').

Union of series (C) and (D) is the series

(E) 1,2, ... , pq−1.

Thus it follows that the cardinality of classes 2 and 3 is the same as the number of terms in series (E) whose least positive residues (mod p) belong to $(\mathcal{F})$ and (mod q) belong to (F'). Notice that the number of such pairs of residues is $\frac{p-1}{2}\frac{q-1}{2}$, and to any such pair there corresponds a unique number in series (E). It follows therefore, that the classes 2 and 3 contain $\frac{p-1}{2}\frac{q-1}{2}$ numbers.

$$\therefore (3) \quad \beta+\gamma = \frac{p-1}{2}\frac{q-1}{2} .$$

adding (1) and (2) we get

$$\beta+\gamma+2\delta+\mu+\nu = 2\,\frac{p-1}{2}\frac{q-1}{2} .$$

subtracting (3) we get:

$$\mu+\nu+2\delta = \frac{p-1}{2}\frac{q-1}{2} .$$

$$\therefore \quad \mu+\nu \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod 2 .$$

Applications:

By combining the law of quadratic reciprocity with the properties of Legendre's symbol mentioned in lemma 4; it is easy to evaluate $\left(\frac{q}{p}\right)$

Example: $\left(\frac{2819}{4177}\right)$ observe that 2819 and 4177 are both primes and

$4177 \equiv 1 \pmod 4$

$$\therefore \left(\frac{2819}{4177}\right) = \left(\frac{4177}{2819}\right) = \left(\frac{1358}{2819}\right) = \left(\frac{2\cdot 7\cdot 97}{2819}\right)$$

$$= \left(\frac{2}{2819}\right)\left(\frac{7}{2819}\right)\left(\frac{97}{2819}\right) = -1\cdot - \left(\frac{2819}{7}\right)\left(\frac{2819}{97}\right)$$

$$= \left(\frac{5}{7}\right)\left(\frac{6}{97}\right) = \left(\frac{2}{5}\right)\left(\frac{1}{3}\right) = -1$$

Thus 2819 is not a quadratic residue of 4177. Moreover, the quadratic reciprocity law can be used to determine the primes p of which a given prime q is a quadratic residue.

Example: 5 is a quadratic residue of primes of the form $10n \pm 1$ and a quadratic non residue of primes of the form $10n \pm 3$.

Let $p = 10n + k$ where $k = 1, 3, 7$ or 9.

Since $5 \equiv 1 \pmod 4$ we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{10\,n+k}{5}\right) = \left(\frac{k}{5}\right).$$

The residues of 5 are 1 and 4. Hence 5 is a residue of primes $5n+1$ and $5n+4$, that is of primes $10n+1$ and $10n+9$; and it is a non residue of all other odd primes.

Section 3

We now come to Jacobi Law of Quadratic Reciprocity, also known as the Generalized Quadratic Reciprocity Law. The law will be dealt with as Theorem 2.

We first deal with the following:

Note that if P is an integer, positive and odd then either $P = 1$ or $P = p_1 p_2 \dots p_r$ where $p_1, p_2, \dots, p_r$ are odd primes not necessarily distinct.

Definition 12: (Jacobi Symbol) (Dickson pages 42-45)

If n is an integer prime to P we define

$$\left(\frac{n}{1}\right) = 1 \quad \text{and}$$

$$\left(\frac{n}{P}\right) = \left(\frac{n}{p_1}\right) \cdots\cdots \left(\frac{n}{p_r}\right)$$

without loss of generality from now on we will take $P > 1$ i.e.

$$P = p_1 p_2 \dots p_r = \prod_{1 \leq i \leq r} p_i$$

Lemma 11: If n is quadratic residue of P then $\left(\frac{n}{p}\right) = 1$

Proof: If n is quadratic residue of P then the congruence $x^2 \equiv n$ (mod $P = p_1 \dots p_r$) is solvable so that $x^2 \equiv n \pmod{p_i}$ is solvable for each $1 \leq i \leq r$. Hence by definition 7

$$\left(\frac{n}{p_i}\right) = 1 \quad \text{for} \quad 1 \leq i \leq r \text{ so that } \left(\frac{n}{P}\right) = 1.$$

Lemma 12:

If P is positive and odd and if both m and n are prime to P then

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

Proof: By definition 12

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_r}\right)$$

$$\left(\frac{n}{P}\right) = \left(\frac{n}{p_1}\right) \cdots \left(\frac{n}{p_r}\right)$$

$$\left(\frac{mn}{P}\right) = \left(\frac{mn}{p_1}\right) \cdots \left(\frac{mn}{p_r}\right) .$$

but by part C of lemma 4

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

$$\therefore \left(\frac{mn}{P}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_r}\right)\left(\frac{n}{p_1}\right) \cdots \left(\frac{n}{p_r}\right)$$

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

Lemma 13:

If n is prime to odd integer $P > 0$ then

$$\left(\frac{n}{P}\right) = \left(\frac{m}{P}\right) \quad \text{if } n \equiv m \pmod{P}$$

Proof: $n \equiv m \pmod{P = p_1 \ldots p_r}$

hence $n \equiv m \pmod{p_i} \qquad 1 \le i \le r.$

By part (a) of lemma 4 we have

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

$$\therefore \prod\left(\frac{n}{p_i}\right) = \prod\left(\frac{m}{p_i}\right)$$

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

Lemma 14:

If P is positive and odd then

$$\frac{P-1}{2} \equiv \sum_i \tfrac{1}{2}(p_i-1) \pmod 2$$

Proof:

Let $P = \prod_{1 \le i < r} p_i = \prod (1 + p_i - 1)$

and since the product of two even integers p_i-1 and p_j-1 is divisible by 4; we have

$$P \equiv 1 + \sum_i (p_i - 1) \pmod 4$$

$$\therefore P-1 \equiv \sum_i (p_i-1) \pmod 4.$$

$$\therefore \frac{P-1}{2} \equiv \sum_i \tfrac{1}{2}(p_i-1) \pmod 2.$$

Lemma 15:

If P is positive and odd then

$$\left(\frac{-1}{P}\right) = \wp\left(\frac{P-1}{2}\right)$$

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

Proof: We have by lemma 14

$$\frac{P-1}{2} \equiv \sum \tfrac{1}{2}(p_i-1) \pmod 2$$

By definition 12

$$\left(\frac{-1}{P}\right) = \prod\left(\frac{-1}{p_i}\right)$$ but by part (d) of lemma 4

$$\left(\frac{-1}{p_i}\right) = \wp\left(\frac{p_i-1}{2}\right)$$

$$\therefore \text{ we have } \left(\frac{-1}{P}\right) = \prod \wp\left(\frac{p_i-1}{2}\right) = (-1)^{\sum_1 \frac{p_i-1}{2}}$$

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

we have

$$P^2 = \prod\left\{1 + (p_i^2-1)\right\}$$

and since p_i^2-1 is divisible by 8 we have

$$P^2 \equiv 1 + \sum(p_i^2-1) \pmod{64}$$

$$\therefore \quad \frac{P^2-1}{8} \equiv \sum \frac{1}{8}(p_i^2-1) \pmod{8}$$

By definition 12

$\left(\frac{2}{P}\right) = \prod\left(\frac{2}{p_i}\right)$ but by part (b) of lemma 7 we have

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

$$\therefore \left(\frac{2}{P}\right) = \prod(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum\frac{p_i^2-1}{8}}$$

$$\therefore \quad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} .$$

We now come to theorem 2:

Theorem 2: Let P and Q be integers, positive, odd and relatively prime. Then

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

Proof: (Landau page 68)

Without loss of generality let $P > 1$, $Q > 1$ and let their decompositions into prime factors be denoted by

$$P = \prod p$$
$$Q = \prod q$$

then $\left(\frac{P}{Q}\right) = \left(\frac{\prod p}{\prod q}\right)$. By lemma 12 we have

$$\left(\frac{P}{Q}\right) = \left(\frac{\prod p}{\prod q}\right) = \prod_p \left(\frac{p}{\prod q}\right).$$

Now by definition 12 we have

$$\left(\frac{P}{Q}\right) = \prod_p \left(\frac{p}{\prod q}\right) = \prod_p \prod_q \left(\frac{p}{q}\right).$$

Likewise $\left(\frac{Q}{P}\right) = \prod_q \prod_p \left(\frac{q}{p}\right)$.

Thus $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{p,q} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. Applying Theorem 1 we obtain

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{p,q} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

$$\therefore \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\sum_{p,q}\left(\frac{p-1}{2}\frac{q-1}{2}\right)} = (-1)^{\left(\sum_p \frac{p-1}{2}\right)\left(\sum_q \frac{q-1}{2}\right)}$$

By lemma 14 we have

$$\sum_p \frac{p-1}{2} \equiv \frac{P-1}{2} \pmod 2.$$

$$\sum_q \frac{q-1}{2} \equiv \frac{Q-1}{2} \pmod 2.$$

Thus $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$

References

1. G.H. Hardy and E.M. Wright, "An Introduction to the Theory of Numbers" Aberdeen 1954.

2. I.M. Vinogradov, "Elements of Number Theory". First English translation of the fifth Russian edition of 1949.

3. William Judson LeVeque, "Topics in Number Theory" Vol. 1 Ann Arbor, Michigan 1955.

4. Ivan Niven and Herbert S. Zuckerman, "An Introduction to the Theory of Numbers" 1960.

5. Harriet Griffin, "Elementary Theory of Numbers" 1954.

6. G.B. Mathews, "Theory of Numbers" Part I, Bangor N. Wales, 1927.

7. Uspensky and Heaslet, "Elementary Number Theory" Stanford 1939.

8. Dickson, "Modern Elementary Theory of Numbers" 1939.

9. Landau, "Elementary Number Theory" Göttingen 1927.

10. Nagell, "Introduction to Number Theory" Uppsala 1951.

Vita

Khalid Naeem was born in Abbottabad West Pakistan on 12th February 1936. He is son of Mr. and Mrs. Mohammad Khurshid Ahmad.

He matriculated from No.1 Government High School Abbottabad in 1951. He then joined Government College Abbottabad and studied for the periods 1951-1953 and 1954-1956 to get B.Sc.

During the years 1953-1954 and 1956-1959 he worked as a teacher.

He joined University of Peshawar West Pakistan in 1959 and got his M.Sc. (Mathematics) in 1961.

He served as a lecturer in the Engineering College University of Peshawar for the period 1961-1963.

In 1963, he came to Lehigh University on assistantship and completed his work for M.S. (Mathematics) in 1965.