The Early Reciprocity Laws: From Gauss to Eisenstein

Sukumar Das Adhikari

1. Introduction. We shall start with the law of quadratic reciprocity which was guessed by Euler and Legendre and whose first complete proof was supplied by Gauss. A result central to number theory, the law of quadratic reciprocity, apart from being fascinating on its own, has led to very important generalizations.

The main aim of this article is to sketch a proof of the Eisenstein reciprocity law. Having many applications and being beautiful on its own, the Eisenstein reciprocity law related to the cyclotomic fields, is a precursor of the more general reciprocity laws. Before we move on to discuss about the Eisenstein reciprocity law, we shall have a brief discussion on cubic reciprocity as well. There we shall sketch Williams' proof [10] of Eisenstein's supplement to the law of cubic reciprocity. While for the Stickelberger relation we shall refer to the article of S. A. Katre [6] in this volume, for a deduction of some of the early reciprocity laws from Artin's we refer to that of Parvati Shastri [9]. For the proofs of some results on Gauss and Jacobi sums and, in fact, for many details about the early reciprocity laws including the biquadratic case, we refer to the beautiful book [5] of Ireland and Rosen. We also refer to the interesting expository article of Wyman: "What is a reciprocity law?"[11].

In what follows, for any prime power q, $\mathbf{F}_q$ will denote the finite field with q elements. The symbols $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{C}$ will denote respectively the set of integers, the set of rationals and the complex numbers. For a finite set S, $|S|$ will denote the number of elements of S. For a field K, K^* will denote the multiplicative group of its non-zero elements.

2. Quadratic reciprocity. The problem of solving a general polynomial congruence reduces to that of solving congruences with prime power moduli plus a set of linear congruences. The problem of solving a quadratic congruence $f(x) \equiv 0 \pmod{p}$, where $f(x)$ is a quadratic polynomial with integer coefficients and p is an odd prime, by 'completing the square' reduces to the problem of solving the congruence

$$x^2 \equiv d \pmod{p},\ d \in \mathbf{Z},\quad p \text{ a rational prime.} \tag{1}$$

The laws of quadratic reciprocity, one of the most celebrated results in all of number theory, give an algorithm for knowing the existence of solutions to the congruence (1). What we shall see is that the laws of quadratic reciprocity describe the set of primes modulo which a quadratic polynomial in $\mathbf{Z}[x]$ splits. In general, results giving similar informations (See [11], for instance) are known as reciprocity laws. However, the term reciprocity attached to the early reciprocity laws had its obvious meaning.

For a rational prime p, other than 2, and for $x \in \mathbf{F}_p^*$, the *Legendre symbol* $\left(\frac{x}{p}\right)$ is defined to be $x^{(p-1)/2}$. It is easy to see that (see Serre [8] or Adhikari [1] for instance) $\left(\frac{x}{p}\right) = 1$ or -1 according as x is a square mod p or not, i.e., $y^2 \equiv x \pmod{p}$ has a solution or not. One says that x is *quadratic residue* or *quadratic non-residue mod p* respectively.

For a rational prime p, other than 2, observing that the index of $\mathbf{F}_p^{*2}$ in $\mathbf{F}_p^*$ is 2, there are as many residues as non-residues mod p. Also, $\left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$, i.e., the Legendre symbol is a character of the mutiplicative group $\mathbf{F}_p^*$.

The definition of $\left(\frac{x}{p}\right)$ is extended to all of $\mathbf{F}_p$ by putting $\left(\frac{0}{p}\right) = 0$ and we can view $\left(\frac{x}{p}\right)$ as a function on $\mathbf{Z}$ in the obvious way.

We now state the laws of quadratic reciprocity where part (iii) is the proper reciprocity law and the first two parts are known as supplementary laws.

Theorem 2.1. (Laws of Quadratic Reciprocity). If p and l are two distinct odd primes,

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

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

iii) $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}$.

The result is amazing because there is no obvious reason to expect any connection between the symbols $\left(\frac{p}{l}\right)$ and $\left(\frac{l}{p}\right)$, or, in other words, between the congruences $x^2 \equiv p \pmod{l}$ and $x^2 \equiv l \pmod{p}$. We shall now indicate a proof of part (iii); for complete proofs one may refer to [1] or [8] mentioned above. In fact, almost any number theory text will contain one or more proofs of it. The book [5] of Ireland and Rosen mentioned above contains at least three different proofs of the theorem. We also refer to the interesting

book [2] of Cox, where for a given positive integer n, the various reciprocity laws are seen to bear upon answering the question of finding the primes p which can be expressed in the form $p = x^2 + ny^2$. In fact, Euler's discovery of quadratic reciprocity was prompted by such questions.

Let ω denote a primitive l-th root of unity in an algebraic closure Ω of $\mathbf{F}_p$. We consider the sum $S = \sum_{x \in \mathbf{F}_l^*} \left(\frac{x}{l}\right) \omega^x$.

$$\begin{aligned}
\text{We have, } S^2 &= \sum_{x,y \in \mathbf{F}_l^*} \left(\frac{xy}{l}\right) \omega^{x+y} \\
&= \sum_{y,z \in \mathbf{F}_l^*} \left(\frac{y^2 z}{l}\right) \omega^{y(z+1)} \quad (\text{Putting } \mathrm{x} = \mathrm{yz}) \\
&= \sum_{y,z \in \mathbf{F}_l^*} \left(\frac{z}{l}\right) \omega^{y(z+1)} \\
&= \sum_{y \in \mathbf{F}_l^*} \left(\frac{-1}{l}\right) \omega^0 + \sum_{z \neq -1} \left(\frac{z}{l}\right) \sum_{y \in \mathbf{F}_l^*} \omega^{y(z+1)} \\
&= \left(\frac{-1}{l}\right)(l-1) + (-1) \sum_{z \neq -1} \left(\frac{z}{l}\right)
\end{aligned}$$

(Since, $\sum_{y \in \mathbf{F}_l^*} \omega^{y(z+1)} + 1 = 1 + \omega + \cdots + \omega^{l-1} = 0$),

$$\text{so,} \quad S^2 = l\left(\frac{-1}{l}\right) - \sum_{z \in \mathbf{F}_l^*} \left(\frac{z}{l}\right).$$

Now, there are as many squares as non-squares in $\mathbf{F}_l^*$, so $\sum_{z \in \mathbf{F}_l^*} \left(\frac{z}{l}\right) = 0$ and hence

$$S^2 = l\left(\frac{-1}{l}\right). \tag{2}$$

and

$$S^{p-1} = \left(\frac{p}{l}\right). \tag{3}$$

From (2) and (3),

$$\left(\frac{p}{l}\right) = S^{p-1} = \left(l\left(\frac{-1}{l}\right)\right)^{\frac{p-1}{2}} = \left(\frac{l}{p}\right)\left(\frac{-1}{l}\right)^{\frac{p-1}{2}} = \left(\frac{l}{p}\right)(-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}}.$$

This proves the equality in (iii) modulo p. Since p is odd, (iii) follows.

The following remark is not out of place.

Remark 2.1. In the proof above, if we replace ω by a primitive l-th root of unity in an algebraic closure of the rationals $\mathbf{Q}$, then defining S in the same way, S will again satisfy equation (2), that is, $S^2 = \pm l$. Thus, observing that $\mathbf{Q}(\sqrt{-1}) = \mathbf{Q}(\zeta_4)$ (where ζ_n is a primitive n-th root of unity in $\bar{\mathbf{Q}}$), square root of any odd prime is contained in $\mathbf{Q}(\zeta)$ for some root of unity ζ. Further, observing that $\sqrt{2} \in \mathbf{Q}(\zeta_8)$ (for $2 = -i(1+i)^2$), it follows that any quadratic extension K of $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta)$ for a root of unity ζ, thus giving an easy special case of the Kronecker-Weber theorem (see Ghate [3], in this volume).

3. Cubic reciprocity. Questions regarding solutions of the congruence $x^n \equiv a \pmod{p}$ for rational primes p for larger n's led Gauss to formulate the cubic and biquadratic reciprocities corresponding to $n = 3$ and 4 respectively. In 1844, Eisenstein was first to publish complete proofs of these theorems. In this section, we give a quick sketch of the cubic reciprocity law. On our way, we shall come across Gauss and Jacobi sums. For the details not supplied here, one may look into [5].

Writing $\omega = (-1 + \sqrt{-3})/2$, we consider the ring

$$\mathbf{Z}[\omega] = \{a + b\omega |\ a, b \in \mathbf{Z}\}.$$

For $a+b\omega \in \mathbf{Z}[\omega]$, with the norm function defined by $N(a+b\omega) = a^2-ab+b^2$, $\mathbf{Z}[\omega]$ is a Euclidean domain. The units in $\mathbf{Z}[\omega]$ are elements α with $N(\alpha) = 1$ and they are $\pm 1, \pm\omega, \pm\omega^2$. If p is a rational prime such that $p \equiv 2 \pmod{3}$, then p remains prime in $\mathbf{Z}[\omega]$. The rational primes $p \equiv 1 \pmod{3}$, split into a product of a pair of primes complex conjugate to each other. The rational prime 3 has the factorization $3 = -\omega^2(1-\omega)^2$ where $1-\omega$ is a prime in $\mathbf{Z}[\omega]$.

If $\pi \in D = \mathbf{Z}[\omega]$ is a prime, then $D/\pi D$ is a finite field with $N(\pi)$ elements and for an element $\alpha \in D$ coprime to π,

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

If the norm of π is different from 3, it is not difficult to see that the residue classes of the elements $1, \omega$ and ω^2 are distinct mod πD and therefore, $\{1, \omega, \omega^2\}$ being a subgroup of order 3 of the multiplicative group $(D/\pi D)^*$, $(N(\pi)-1)/3$ is an integer. Now, with π and α as above, $1, \omega$ and ω^2 being distinct mod πD, from the identity

$$\alpha^{N(\pi)-1} - 1 = (\alpha^{(N(\pi)-1)/3} - 1)(\alpha^{(N(\pi)-1)/3} - \omega)(\alpha^{(N(\pi)-1)/3} - \omega^2),$$

it follows that $\alpha^{(N(\pi)-1)/3}$ is congruent to exactly one of the elements $1, \omega$ or ω^2 modulo π in D.

If π is a prime in D with $N(\pi) \neq 3$, then, if π is coprime to α, the unique element to which $\alpha^{(N(\pi)-1)/3}$ is congruent modulo π, is defined to be the *cubic residue character* of α modulo π and we use the notation $(\alpha/\pi)_3$ or $\chi_\pi(\alpha)$ for it. If π divides α, we define $(\alpha/\pi)_3 = 0$.

One observes that $(\cdot/\pi)_3$ is a character of the multiplicative group $(D/\pi D)^*$, and for $\alpha \in (D/\pi D)^*$, $(\alpha/\pi)_3 = 1$ if and only if the congruence $x^3 \equiv \alpha \pmod{\pi}$ is solvable.

Because there are six units in the ring D, a non-zero element in D has six associates. For a given prime π of norm not equal to 3, we single out one among its six associates. This is done in the following way. A prime π in D, is said to be *primary* if $\pi \equiv 2 \pmod{3}$ in D. If $\pi = a + b\omega$, it amounts to say that $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$ in $\mathbf{Z}$.

It is clear that neither the prime $1-\omega$ nor any of its associates is primary. Rational primes $p \equiv 2 \pmod{3}$, which remain prime in D are primary and their other associates are not. For a prime π of norm $p \equiv 1 \pmod{3}$, again it is not difficult to see that among the associates of π, there is exactly one which is primary. With this, we are ready to state the law of cubic reciprocity.

Theorem 3.1. (The Law of Cubic Reciprocity). Consider two primes π_1 and π_2 in D such that neither of them is of norm 3 and both are primary. We also assume that $N(\pi_1) \neq N(\pi_2)$. Then

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

Remark 3.1. As in the case of quadratic reciprocity, there are supplementary laws for the cubic residue character of the units and the prime $1 - \omega$. It is easy to see that $\chi_\pi(-1) = 1$ and if π is not of norm 3, by definition, $\chi_\pi(\omega) = 1, \omega$, or ω^2 respectively for the cases $N(\pi) \equiv 1, 4$, or $7 \pmod{9}$.

Regarding $1 - \omega$, if $N(\pi) \neq 3$, then

$$\chi_\pi(1 - \omega) = \omega^{2m}, \tag{4}$$

where the integer m is defined as follows. If $\pi = q$ is a rational prime, then m is defined by $q = 3m - 1$. If $\pi = a + b\omega$ is a primary complex prime, then m is defined by $a = 3m - 1$.

At the end of this section, we shall sketch Williams' proof [10] of Eisenstein's supplement to the law of cubic reciprocity (equation (4) above).

Before proceeding to prove Theorem 3.1, we obtain certain results on Gauss and Jacobi sums.

Let p be a rational prime. For a finite field $\mathbf{F}_p$, characters of the multiplicative group $\mathbf{F}_p^*$, that is, homomorphisms $\mathbf{F}_p^* \to \mathbf{C}^*$ will be referred to as multiplicative characters on $\mathbf{F}_p$. We shall denote the trivial character by ϵ, that is, $\epsilon(a) = 1$ for all $a \in \mathbf{F}_p^*$. If $\chi \neq \epsilon$, we define $\chi(0) = 0$. The trivial character is extended by defining $\epsilon(0) = 1$.

If χ is a multiplicative character on $\mathbf{F}_p$, and $\zeta = e^{2\pi i/p}$, then for an element a of $\mathbf{F}_p$, the sum $\sum_{t\in\mathbf{F}_p} \chi(t)\zeta^{at}$ is called a *Gauss sum on* $\mathbf{F}_p$ and is denoted by $g_a(\chi)$. For $g_1(\chi)$, we shall simply write $g(\chi)$.

If χ_1 and χ_2 are two multiplicative characters of $\mathbf{F}_p$, then

$$\sum_{a+b=1} \chi_1(a)\chi_2(b)$$

is called a *Jacobi sum* and is denoted by $J(\chi_1, \chi_2)$.

If χ is a multiplicative character on $\mathbf{F}_p$, then we know that $\sum_{t\in\mathbf{F}_p} \chi(t) = p$ or 0, according as χ is the trivial character ϵ or not. Also, if $a \in \mathbf{F}_p^*$, then $\sum_\chi \chi(a) = p - 1$ or 0, according as a is the identity element 1 or not. We proceed to prove some results on Gauss and Jacobi sums.

Proposition 3.1.

i) If a is a non-zero element of $\mathbf{F}_p$ and χ a non-trivial multiplicative character on $\mathbf{F}_p$, then $g_a(\chi) = \chi(a^{-1})g_1(\chi)$.

ii) If a is a non-zero element of $\mathbf{F}_p$ and χ is the trivial multiplicative character ϵ, then $g_a(\epsilon) = 0$.

iii) $g_0(\chi) = p$ or 0 according as χ is the trivial character ϵ or not.

Proof: All these statements follow directly from the definition of a Gauss sum. We prove only part (i) here. To prove (i), we just observe that $\chi(a)g_a(\chi) = \chi(a)\sum_{t\in\mathbf{F}_p} \chi(t)\zeta^{at} = \sum_{t\in\mathbf{F}_p} \chi(at)\zeta^{at} = g_1(\chi)$.

Remark 3.2. In Remark 2.1, the sum S was a particular Gauss sum. This was the particular case corresponding to $a = 1$ of the *quadratic Gauss sum* $\sum_{x\in\mathbf{F}_p^*} \left(\frac{x}{p}\right) \zeta^{ax}$. We remark that for a general multiplicative character $\chi \neq \epsilon$ on $\mathbf{F}_p$, one has $g(\chi)g(\overline{\chi}) = \chi(-1)p$.

Proposition 3.2.

i) $J(\epsilon, \epsilon) = p$.

ii) If χ is a non-trivial multiplicative character on $\mathbf{F}_p$, then

$$J(\epsilon, \chi) = 0 \text{ and } \; J(\chi, \chi^{-1}) = -\chi(-1).$$

iii) If χ_1 and χ_2 are non-trivial multiplicative characters on $\mathbf{F}_p$ such that $\chi_2 \neq \chi_1^{-1}$, then

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}.$$

Proof: We prove only part (iii) here. We have

$$g(\chi_1)g(\chi_2) = \sum_{a,b\in\mathbf{F}_p} \chi_1(a)\chi_2(b)\zeta^{a+b} = \sum_{t\in\mathbf{F}_p} \left(\sum_{a+b=t} \chi_1(a)\chi_2(b) \right) \zeta^t.$$

We observe that the inner sum survives only when $t \neq 0$ and in that case, substituting $a = ta'$ and $b = tb'$, a straightforward calculation shows that the inner sum is $(\chi_1\chi_2)(t)J(\chi_1, \chi_2)$. Therefore, from the above equation we have

$$g(\chi_1)g(\chi_2) = \sum_{t\in\mathbf{F}_p} (\chi_1\chi_2)(t)J(\chi_1, \chi_2)\zeta^t = J(\chi_1, \chi_2)g(\chi_1\chi_2), \quad \text{as desired.}$$

Proposition 3.3. Let $n > 2$ be an integer. Let p be a rational prime such that $p \equiv 1 \pmod{n}$ and χ a multiplicative character of $\mathbf{F}_p$ of order n. Then

$$(g(\chi))^n = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{n-2}).$$

Proof: From part (iii) of Proposition 3.2, we have $g(\chi)^2 = J(\chi, \chi)g(\chi^2)$. Multiplying by $g(\chi)$ and applying part (iii) of Proposition 3.2 again we have $g(\chi)^3 = J(\chi, \chi)J(\chi, \chi^2)g(\chi^3)$. By repeating this process, we get

$$g(\chi)^{n-1} = J(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{n-2})g(\chi^{n-1}). \tag{5}$$

But, $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$, by Remark 3.2. Hence by (5), we obtain our result.

Now we shall proceed to prove the law of cubic reciprocity. We shall need the following lemmas.

Lemma 3.1. Let π be a prime in D with $N(\pi) \neq 3$. Then

i) $\overline{\chi_\pi(\alpha)} = (\chi_\pi(\alpha))^2 = \chi_\pi(\alpha^2)$.

ii) $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$.

iii) If $\pi = q$ is a rational prime of D, $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$.

Proof: For part (i), since the squares of the numbers $1, \omega$, and ω^2 are equal to their corresponding conjugates, $\overline{\chi_\pi(\alpha)} = (\chi_\pi(\alpha))^2 = \chi_\pi(\alpha^2)$.

Next, observing that $N(\pi) = N(\overline{\pi})$, from the definition it follows that

$$\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.$$

Since $1, \omega$, and ω^2 are distinct modulo $\overline{\pi}$, we get part (ii).

Finally, for a rational prime q in D, $\overline{q} = q$ and hence from part (ii) and part (i), $\chi_q(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$.

Lemma 3.2. Let π be a complex prime in D such that $N(\pi) = p \equiv 1 \pmod 3$ in D. We also assume π to be primary. Identifying $D/\pi D$ with $\mathbf{F}_p$, and therefore considering χ_π as a multiplicative character on $\mathbf{F}_p$, if we consider the Jacobi sum $J(\chi_\pi, \chi_\pi)$, then we have

$$J(\chi_\pi, \chi_\pi) = \pi.$$

Proof: First we note that χ_π being a cubic character, $\chi_\pi(-1) = 1$. Therefore, by Proposition 3.3, we have

$$g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi). \tag{6}$$

We now claim another result on $J(\chi_\pi, \chi_\pi)$, which again is true if we replace χ_π by a general cubic character. We claim that if we write $J(\chi_\pi, \chi_\pi) = a + b\omega$ with $a, b \in \mathbf{Z}$, then we have the following congruences in $\mathbf{Z}$:

$$a \equiv 2 \pmod 3 \quad \text{and} \quad b \equiv 0 \pmod 3. \tag{7}$$

We now establish the claim (7) above.

Observing that $\chi_\pi(0) = 0$ and $\chi_\pi(t)^3 = 1$ for $t \in \mathbf{F}_p^*$, we have the following congruence in the ring of algebraic integers $\mathbf{O}$:

$$g(\chi_\pi)^3 \equiv \sum_{t \in \mathbf{F}_p^*} \zeta^{3t} \pmod 3.$$

Since the last sum is -1, by (6) above, we have

$$pJ(\chi_\pi, \chi_\pi) = g(\chi_\pi)^3 \equiv -1 \pmod 3.$$

Therefore, since $p \equiv 1 \pmod 3$,

$$a + b\omega = J(\chi_\pi, \chi_\pi) \equiv -1 \pmod 3. \tag{8}$$

Working with $\overline{\chi}_\pi$ instead of χ_π, and observing that $\overline{g(\chi_\pi)} = g(\overline{\chi}_\pi)$ one obtains

$$a + b\overline{\omega} \equiv -1 \pmod 3. \tag{9}$$

Subtracting (9) from (8),

$$\begin{aligned} & b(\omega - \overline{\omega}) && \equiv && 0 \pmod 3 \\ \Rightarrow \quad & b\sqrt{-3} && \equiv && 0 \pmod 3 \\ \Rightarrow \quad & b\sqrt{-3} && = && 3\eta, \text{ for some } \eta \in \mathbf{O} \\ \Rightarrow \quad & -3b^2 && = && 9\eta^2 \\ \Rightarrow \quad & 3 && \mid && b \end{aligned}$$

Therefore, (8) implies that

$$a + 1 = 3\theta \text{ for some } \theta \in \mathbf{O}.$$

Since $\theta \in \mathbf{Q}$ as well, θ must be a rational integer. Hence, $a \equiv -1 \pmod 3$. Therefore, claim (7) is established.

Now, from Proposition 3.2 (iii) and Remark 3.2, we have

$$J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = p$$

and therefore by (7), $J(\chi_\pi, \chi_\pi)$ is a primary prime.

Writing $J(\chi_\pi, \chi_\pi) = \gamma$, we observe that

$$\pi\overline{\pi} = p = \gamma\overline{\gamma}.$$

This gives $\pi|\gamma$ or $\pi|\overline{\gamma}$. Since all the primes involved in the above equation are primary,

$$\pi = \gamma \text{ or } \pi = \overline{\gamma}.$$

We rule out the second possibility.

We have

$$J(\chi_\pi, \chi_\pi) = \sum_{x \in \mathbf{F}_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x \in \mathbf{F}_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \pmod \pi. \tag{10}$$

Now, observing that $x^{(p-1)/3}(1-x)^{(p-1)/3}$ is a polynomial in x of degree $2(p-1)/3 < (p-1)$, and from elementary number theory, recalling the congruence

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod p, \text{ when } (p-1) \not| k,$$

we have

$$\sum_{x\in\mathbf{F}_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \equiv 0 \pmod{p}.$$

Therefore, from (10), we have $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod{\pi}$, showing thereby that the second possibility does not occur. Lemma 3.2. is thus established.

Proof of Theorem 3.1: We consider the following three possible cases:

A) Both π_1 and π_2 are rational.

B) One of them, say π_1, is rational and π_2 is complex.

C) Both π_1 and π_2 are complex.

Case A. In this case, since $\pi_1 = q_1$ and $\pi_2 = q_2$ are rational primes coprime to each other, observing that $\overline{q}_1 = q_1$ and $\overline{q}_2 = q_2$, from Lemma 3.1 above,

$$\chi_{\pi_1}(\pi_2) = \overline{\chi_{\pi_1}(\pi_2)} = \chi_{\pi_1}(\pi_2^2).$$

Since $\chi_{\pi_1}(\pi_2) \neq 0$, this implies that $\chi_{\pi_1}(\pi_2) = 1$. For the same reason, $\chi_{\pi_2}(\pi_1)$ is also 1 and therefore, Theorem 3.1 is established in this case.

Case B.

Here in order to simplify notations, we write $\pi_1 = q$ and $\pi_2 = \pi$. Now, $q \equiv 2 \pmod 3$ and $N(\pi) = p \equiv 1 \pmod 3$.

From Remark 3.1, Proposition 3.3 and Lemma 3.2, we have

$$g(\chi_\pi)^3 = p\pi. \tag{11}$$

Now, (11) implies

$$\begin{aligned} g(\chi_\pi)^{q^2-1} &= (p\pi)^{(q^2-1)/3}, \\ \text{and hence,}\quad g(\chi_\pi)^{q^2-1} &\equiv \chi_q(p\pi) \pmod{q}, \quad \text{by definition.} \end{aligned}$$

Since by Lemma 3.1, $\chi_q(p) = \overline{\chi_q(p)}$ and the only real value of the character χ_q is 1, we have $\chi_q(p) = 1$ and therefore, from above,

$$g(\chi_\pi)^{q^2} = \chi_q(\pi) g(\chi_\pi) \pmod{q}. \tag{12}$$

Now, by definition

$$g(\chi_\pi)^{q^2} = \left(\sum_{t\in\mathbf{F}_p} \chi_\pi(t)\zeta^t\right)^{q^2} \equiv \sum_{t\in\mathbf{F}_p} \chi_\pi(t)^{q^2}\zeta^{q^2 t} \pmod{q}.$$

Since $q^2 \equiv 1 \pmod 3$, we have $\chi_\pi(t)^{q^2-1} = 1$.
Therefore,

$$\begin{aligned} & g(\chi_\pi)^{q^2} \equiv \sum_{t \in \mathbf{F}_p} \chi_\pi(t)\zeta^{q^2 t} \pmod q \\ \Rightarrow \quad & g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod q, \quad \text{(by definition)} \\ \Rightarrow \quad & g(\chi_\pi)^{q^2} \equiv \chi_\pi(q^{-2}) g(\chi_\pi) \pmod q \quad \text{(by Proposition 3.1 (i))} \\ \Rightarrow \quad & g(\chi_\pi)^{q^2} \equiv \chi_\pi(q) g(\chi_\pi) \pmod q. \end{aligned}$$

Hence, by (12),

$$\begin{aligned} \chi_\pi(q) g(\chi_\pi) &\equiv \chi_q(\pi) g(\chi_\pi) \pmod q \\ \Rightarrow \quad \chi_\pi(q) p &\equiv \chi_q(\pi) p \pmod q \quad \text{(multiplying both sides by } g(\overline{\chi}_\pi) \text{ and by Remark 3.2)} \\ \Rightarrow \quad \chi_\pi(q) &\equiv \chi_q(\pi) \pmod q \\ \Rightarrow \quad \chi_\pi(q) &= \chi_q(\pi). \end{aligned}$$

Case C. Write $N(\pi_1) = p_1$ and $N(\pi_2) = p_2$. Then, $p_i \equiv 1 \pmod 3$ for $i = 1, 2$.

Let $\gamma_1 = \overline{\pi}_1$ and $\gamma_2 = \overline{\pi}_2$.

Then γ_i's are primary and $p_i = \pi_i \gamma_i$ for $i = 1, 2$.

As in Case B above, we start with the relation

$$g(\chi_{\gamma_1})^3 = p_1 \gamma_1, \tag{13}$$

which implies

$$\begin{aligned} g(\chi_{\gamma_1})^{p_2-1} &= (p_1\gamma_1)^{(p_2-1)/3}, \\ \text{and hence,} \quad g(\chi_{\gamma_1})^{p_2-1} &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}, \text{ by definition.} \end{aligned}$$

Now, going back to the definition of $g(\chi_{\gamma_1})$ and proceeding as in case B, from (13) we obtain

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{14}$$

Similarly,

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{15}$$

Again, by Lemma 3.1 (i),

$$\chi_{\gamma_1}(p_2^2) = \overline{\chi_{\gamma_1}(p_2)}.$$

Therefore, by Lemma 3.1 (ii)

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2). \tag{16}$$

$$\begin{aligned}
\text{Now, } \chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) \qquad \text{(by (14))} \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) \qquad \text{(by (16))} \\
&= \chi_{\pi_1}(p_2\pi_2) \\
&= \chi_{\pi_2}(p_1^2) \qquad \text{(by (15))} \\
&= \chi_{\pi_2}(p_1\pi_1\gamma_1) \\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)
\end{aligned}$$

and hence $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$, as desired.

Williams' proof of equation (4): We extend the definition of the cubic residue character so that we are able to work with non-prime integers of D in the denominator of the symbol.

Let $\alpha, \tau \in D$. Also assume that $\tau \not\equiv 0 \pmod{(1-\omega)}$, in D.

We define $\chi_\tau(\alpha)\,(= (\alpha/\tau)_3)$

$$= \begin{cases} 1 & \text{if } \tau \text{ is a unit of } D, \\ \chi_{\tau_1}(\alpha)\chi_{\tau_2}(\alpha)\cdots\chi_{\tau_r}(\alpha) & \text{when } \tau \text{ is a non-unit and} \\ & \tau = \tau_1\tau_2\cdots\tau_r \text{ is the factorization} \\ & \text{into products of primes of } D. \end{cases}$$

Since it is easy to check that

$$\frac{N(\pi_1)-1}{3} + \frac{N(\pi_2)-1}{3} \equiv \frac{N(\pi_1\pi_2)-1}{3} \pmod 3$$

holds for any two primes π_1 and π_2 of D not of norm 3, by the above definition, for any $\tau \in D$ with $\tau \not\equiv 0 \pmod{(1-\omega)}$, we have

$$(\omega/\tau)_3 = \omega^{(N(\tau)-1)/3}. \tag{17}$$

If π is a rational prime of D, let $\pi = 3m - 1$. Now,

$$\begin{aligned}
\chi_\pi(1-\omega) &= \chi_\pi\left((1-\omega)^4\right) = \left(\chi_\pi\left((1-\omega)^2\right)\right)^2 \\
&= \left(\chi_\pi(-3\omega)\right)^2 = \left(\chi_\pi(-3)\right)^2 \left(\chi_\pi(\omega)\right)^2 \\
&= \left(\chi_\pi(\omega)\right)^2 \text{ (see Case A in the proof of Theorem 3)} \\
&= \omega^{2(N(\pi)-1)/3} = \omega^{6m^2-4m} = \omega^{2m},
\end{aligned}$$

and therefore, (4) is established when π is a rational prime of D.

Now, let $\pi = a + b\omega$ be a complex prime where $a = 3m - 1$ and $b = 3n$. In this case,

$$\begin{aligned}
\chi_\pi(1-\omega) &= \chi_a(b)\chi_\pi(1-\omega) \qquad (\text{since } \chi_a(b) = 1) \\
&= \left(\chi_a(\omega)\right)^2 \chi_a(b\omega)\chi_\pi(1-\omega) \\
&= \left(\chi_a(\omega)\right)^2 \chi_a(\pi)\chi_\pi(1-\omega) \qquad (\text{since } b\omega \equiv \pi \pmod a) \\
&= \omega^{2(a^2-1)/3}\chi_a(\pi)\chi_\pi(1-\omega) \qquad (\text{by (17)}) \\
&= \omega^{6m^2-4m}\chi_a(\pi)\chi_\pi(1-\omega) \\
&= \omega^{6m^2-4m}\chi_\pi(a)\chi_\pi(1-\omega) \qquad (\text{by Theorem 3.1 and our extended definition of the cubic residue character}) \\
&= \omega^{2m}\chi_\pi(a - a\omega) \\
&= \omega^{2m}\chi_\pi(-(a+b)\omega) \qquad (\text{since } b\omega \equiv -a \pmod \pi) \\
&= \omega^{2m}\chi_\pi(\omega)\chi_\pi(a+b) \\
&= \omega^{2m+(p-1)/3}\chi_{a+b}(\pi) \\
&= \omega^{n}\chi_{a+b}(\pi) \qquad (\text{observing that } p = a^2 - ab + b^2) \\
&= \omega^{n}\chi_{a+b}(b(1-\omega)) \qquad (\text{since } b(1-\omega) \equiv -\pi \pmod{(a+b)}) \\
&= \omega^{n}\chi_{a+b}(b)\chi_{a+b}(1-\omega) \\
&= \omega^{n+2(m+n)} \\
&= \omega^{2m}.
\end{aligned}$$

4. Eisenstein reciprocity law. We shall here state and give a sketch of the proof of the Eisenstein reciprocity law. In many places, for details we shall refer to Ireland and Rosen [5]. For applications of Eisenstein reciprocity law,

we again refer to [5] as well as Ribenboim's book [7] "13 Lectures on Fermat's Last Theorem". One may also look into the recent book of Esmonde and Murty [4] for that purpose.

Let m be a positive integer and $\zeta_m = e^{2\pi i/m}$. Let D_m denote the ring of integers of $\mathbf{Q}(\zeta_m)$.

We recall some facts about the ring D_m. Ideals appearing in our discussion will be non-zero. First, $D_m = \mathbf{Z}[\zeta_m]$. Now, let P be a prime ideal in D_m not containing m and write $q = N(P) \stackrel{\text{def}}{=} |D_m/P|$. Then, $q \equiv 1 \pmod{m}$ and the elements $1, \zeta_m, \cdots, \zeta_m^{m-1}$ are distinct mod P.

We also recall that the only roots of unity in $\mathbf{Q}(\zeta_m)$ are $\pm\zeta_m^i$, $i = 1, 2, \cdots, m$.

Now, if $\alpha \in D_m$ such that $\alpha \notin P$, then

$$\alpha^{q-1} \equiv 1 \pmod{P}.$$

$$\text{Therefore, } \prod_{i=0}^{m-1} \left(\alpha^{(q-1)/m} - \zeta_m^i\right) \equiv 0 \pmod{P}.$$

Since P is a prime ideal, $\exists\ i, 0 \leq i < m$ such that

$$\alpha^{(q-1)/m} \equiv \zeta_m^i \pmod{P}. \tag{18}$$

Since $\zeta_m^i \not\equiv \zeta_m^j \pmod{P}$ for $i \not\equiv j \pmod{m}$, the integer i in (18) is unique mod m.

If $\alpha \in D_m$ is such that $\alpha \notin P$, the unique element ζ_m^i to which $\alpha^{(N(P)-1)/m}$ is congruent modulo P, is defined to be the *m-th power residue symbol* and is denoted by $(\alpha/P)_m$. This gives us a multiplicative character of the finite field D_m/P of q elements. If $\alpha \in P$, we define $(\alpha/P)_m = 0$.

Once again, it is not difficult to check that $(\alpha/P)_m = 1$ if and only if $x^m \equiv \alpha \pmod{P}$ is solvable in D_m.

Now, let $A \subset D_m$ be any proper ideal prime to m. Let $A = P_1 \cdots P_n$ be a decomposition into product of prime ideals of D_m; P_i's are not necessarily distinct. For $\alpha \in D_m$, we have the following definition.

$$(\alpha/A)_m \stackrel{\text{def}}{=} \prod_i (\alpha/P_i)_m.$$

If $\beta \in D_m$ is such that β is prime to m, then we define

$$(\alpha/\beta)_m \stackrel{\text{def}}{=} (\alpha/(\beta))_m\,,$$

where (β) denotes the principal ideal βD_m.

Let $l > 0$ be an odd prime in $\mathbf{Z}$. Then a non-zero element $\alpha \in D_l$ is called *primary* if it is prime to l and congruent to a rational integer modulo $(1-\zeta_l)^2$. We claim that for $\alpha \in D_l$ such that α prime to l there is an integer $c \in \mathbf{Z}$, unique mod l, such that $\zeta_l^c \alpha$ is primary.

We know that in D_l, the principal ideal $(l) = lD_l = (1-\zeta_l)^{l-1}$ and the principal ideal $(1-\zeta_l)$ is prime of degree 1.

Hence there exists $a \in \mathbf{Z}$ such that

$$\alpha \equiv a \pmod{(1-\zeta_l)}. \tag{19}$$

From (19),

$$\frac{\alpha - a}{1-\zeta_l} \in D_l.$$

Therefore, applying the same argument once again, there exists $b \in \mathbf{Z}$ such that

$$\frac{\alpha - a}{1-\zeta_l} \equiv b \pmod{(1-\zeta_l)}.$$

The above implies,

$$\alpha \equiv a + b(1-\zeta_l) \pmod{(1-\zeta_l)^2}. \tag{20}$$

Again, writing $\zeta_l = 1 - (1-\zeta_l)$, we observe that for $d \in \mathbf{Z}$,

$$\zeta_l^d \equiv 1 - d(1-\zeta_l) \pmod{(1-\zeta_l)^2}. \tag{21}$$

From (20) and (21),

$$\zeta_l^d \alpha \equiv a + (b - ad)(1-\zeta_l) \pmod{(1-\zeta_l)^2}. \tag{22}$$

From (19), we observe that if l divides a in $\mathbf{Z}$, then $(1-\zeta_l)$ would divide α in D_l contradicting the assumption that α is prime to l. Therefore, l does not divide a in $\mathbf{Z}$. Therefore, there exists $d \in \mathbf{Z}$ such that $ad \equiv b \pmod{l}$.

With this d, from (22) we have

$$\zeta_l^d \alpha \equiv a \pmod{(1-\zeta_l)^2}.$$

From the proof, a given α determines uniquely a and b, and hence determines a unique d mod l and our claim is established.

Now, we state the Eisenstein reciprocity law.

Theorem 4.1. (The Eisenstein Reciprocity Law). Let l be an odd prime and a $(\neq \pm 1)$ $\in \mathbf{Z}$ is such that $(l, a) = 1$. Let $\alpha \in D_l$ be such that α is a primary non-unit element of D_l and α and a are prime to each other. Then

$$(\alpha/a)_l = (a/\alpha)_l.$$

We go through a sequence of definitions and propositions before we take up the proof of Theorem 4.1.

First we set some notations. If σ is an element of the group $G = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$, for an element $\alpha \in \mathbf{Q}(\zeta_m)$, we shall write α^σ instead of $\sigma(\alpha)$. Similarly, for an ideal A of D_m, we shall use the notation A^σ to denote $\sigma(A)$. It is known that $\prod_{\sigma\in G}\sigma(A) = (N(A))$. The proof of the following proposition is straightforward.

Proposition 4.1. Let A be a proper ideal of D_m, prime to m. Let σ be an element of the group G defined above. Then

$$(\alpha/A)_m^\sigma = (\alpha^\sigma/A^\sigma)_m.$$

We start with generalizing the notion of Gauss sums. Also, we work on arbitrary finite fields. Let $\mathbf{F}$ be a finite field such that $|\mathbf{F}| = p^f$, where p is a rational prime. Let $\chi : \mathbf{F}^* \to \mathbf{C}^*$ be a character. Let the order of χ be m. Let $\psi : \mathbf{F} \to \mathbf{C}^*$ be a non-trivial additive character. Then values of χ are m-th roots of unity while those of ψ are p-th roots of unity.

As before, the trivial multiplicative character ϵ is extended by defining $\epsilon(0) = 1$ and if $\chi \neq \epsilon$, we define $\chi(0) = 0$.

We consider the *Gauss sum*

$$g(\chi,\psi) \stackrel{\text{def}}{=} \sum_{t\in\mathbf{F}} \chi(t)\psi(t).$$

We observe that $g(\chi,\psi) \in \mathbf{Q}(\zeta_m,\zeta_p)$.

We now specify the characters χ and ψ we shall be working with.

Let P be a prime ideal in D_m not containing m. Let P lie over the rational prime p, that is, $p\mathbf{Z} = P \cap \mathbf{Z}$. Let $N(P) = q = p^f$ and $\mathbf{F} = D_m/P$.

We know that $p^f \equiv 1 \pmod m$. Let t be a non-zero element of $\mathbf{F}$. Let $t = \gamma + P$ for $\gamma \in D_m$. We define

$$\chi_P(t) = (\gamma/P)_m^{-1}.$$

Now, we describe the additive character ψ. Consider the trace function $\mathrm{tr} : \mathbf{F} \to \mathbf{Z}/p\mathbf{Z}$ defined by $\mathrm{tr}(t) = t + t^p + t^{p^2} \cdots + t^{p^{f-1}}$. We define our additive character ψ by $\psi(t) = \zeta_p^{\mathrm{tr}(t)}$.

Now we consider the corresponding Gauss sum

$$g(P) \stackrel{\text{def}}{=} g(\chi_P,\psi) \stackrel{\text{def}}{=} \sum_{t\in\mathbf{F}} \chi_P(t)\psi(t).$$

We define

$$\Phi(P) \stackrel{\text{def}}{=} g(P)^m.$$

As before (see Remark 3.2),

$$|g(P)|^2 = q. \tag{23}$$

Now both $\mathbf{Q}(\zeta_m)$ and $\mathbf{Q}(\zeta_p)$ are subfields of $\mathbf{Q}(\zeta_m, \zeta_p) = \mathbf{Q}(\zeta_{mp})$ and

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{mp})/\mathbf{Q}) = \left\{\sigma_r : \zeta_{mp} \mapsto \zeta_{mp}^r,\ (r, mp) = 1\right\}.$$

We observe that σ_r leaves $\mathbf{Q}(\zeta_m)$ elementwise fixed if and only if $r \equiv 1 \pmod{m}$. Similarly, σ_r leaves $\mathbf{Q}(\zeta_p)$ elementwise fixed if and only if $r \equiv 1 \pmod{p}$.

Let $c \in \mathbf{Z}$ be such that $c \equiv 1 \pmod{m}$.

$$\begin{aligned}
\sigma_c(g(P)) &= \sigma_c\left(\sum_{t\in\mathbf{F}} \chi_P(t)\psi(t)\right) \\
&= \sum_{t\in\mathbf{F}} \chi_P(t)\psi(t)^c \qquad (\text{since, } \chi_P(t) \in \mathbf{Q}(\zeta_m),\ \sigma_c(\chi_P(t)) = \chi_P(t)) \\
&= \sum_{t\in\mathbf{F}} \chi_P(t)\psi(ct) \\
&= \chi_P(c)^{-1} g(P)
\end{aligned}$$

Therefore,

$$\sigma_c\left(\Phi(P)\right) = \sigma_c\left((g(P)^m\right) = g(P)^m = \Phi(P).$$

Thus, $\Phi(P)$ is invariant under σ_c and hence the following proposition.

Proposition 4.2.

$$\Phi(P) \in \mathbf{Q}(\zeta_m).$$

Now, we state the following result, and, as had been mentioned already, we refer to [5] or [6] for its proof.

Proposition 4.3. (Stickelberger) Let P be a prime ideal in D_m such that $m \notin P$. Then the principal ideal

$$(\Phi(P)) = (g(P)^m) = P^{\sum t\sigma_t^{-1}},$$

where the sum is over all $1 \le t < m$ which are relatively prime to m.

Let $A \subset D_m$ be a proper ideal prime to m. Let $A = P_1P_2\cdots P_n$ where P_i's are prime ideals. Then we define

$$\Phi(A) \stackrel{\text{def}}{=} \Phi(P_1)\Phi(P_2)\cdots\Phi(P_n).$$

If $A = (\alpha)$ is a principal ideal, we write $\Phi(\alpha)$ for $\Phi((\alpha))$.

Proposition 4.4. Let A, B be proper ideals of D_m, both prime to m. Let $\alpha \in D_m$ be prime to m. Let $\gamma = \sum t\sigma_t^{-1}$, where the sum is over all $1 \leq t < m$ which are relatively prime to m. Then

i) $\Phi(A)\Phi(B) = \Phi(AB)$.

ii) $|\Phi(A)|^2 = N(A)^m$.

iii) The principal ideal $(\Phi(A))$ is equal to A^γ.

iv) $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$ for some unit $\epsilon(\alpha)$ of D_m.

Proof: Whereas (i) follows directly from definition, (ii) follows from (23). Part (iii) follows from Proposition 4.3 (Stickelberger).

Now, by Part (iii), we get that the principal ideal $(\Phi(\alpha)) = (\alpha)^\gamma = (\alpha^\gamma)$. That is, $\Phi(\alpha)$ and α^γ generate the same principal ideal and that implies (iv).

If $\alpha \in D_m$ is as in Proposition 4.4, we now proceed to have more precise informations about $\epsilon(\alpha)$ appearing in part (iv). By part (ii) of the above proposition, $|\Phi(\alpha)|^2 = |N(\alpha)|^m$. On the other hand, it is not very difficult to see (see [5]) that $|(\alpha)^\gamma|^2 = |N(\alpha)|^m$. It then follows that $|\epsilon(\alpha)| = 1$. Similarly, by using Proposition 4.1, one derives that $|\epsilon(\alpha)^\sigma| = 1$ for all $\sigma \in G$. Therefore, $\epsilon(\alpha)$ is a root of unity. Since $\epsilon(\alpha) \in \mathbf{Q}(\zeta_m)$, we have the following proposition.

Proposition 4.5. $\epsilon(\alpha) = \pm\zeta_m^i$ for some i.

Let $m = l$, an odd prime and $\alpha \in D_l$ be primary. Then one can obtain (see [5]) the following more precise information.

Proposition 4.6. $\epsilon(\alpha) = \pm 1$.

Now, let $\alpha \in D_l$ be primary and a non-unit and B a proper ideal of D_l such that B is prime to l and $N(B)$ is prime to α. Since l is odd, -1 is not an l-th root of unity and hence by the above proposition

$$(\epsilon(\alpha)/B)_l = 1. \tag{24}$$

For prime ideals P, P' of D_l, both prime to l, such that $N(P)$ and $N(P')$ are relatively prime, it is not very difficult (see [5]) to observe that

$$(\Phi(P)/P')_l = (N(P')/P)_l.$$

From this, using part (iv) of Proposition 4.4 and Proposition 4.1 one derives

$$(\epsilon(\alpha)/B)_l(\alpha/N(B))_l = (N(B)/\alpha)_l.$$

Therefore, by (24),

$$(\alpha/N(B))_l = (N(B)/\alpha)_l \tag{25}$$

Proof of Theorem 4.1: Let p be a rational prime other than l such that p is prime to α. Let P be a prime ideal of D_l containing p. Then $N(P) = p^f$ and therefore, by (25),

$$(\alpha/p)_l^f = (p/\alpha)_l^f.$$

Since f divides the degree of the extension $\mathbf{Q}(\zeta_l)$ over $\mathbf{Q}$, which is $l-1$, l does not divide f and hence from the above,

$$(\alpha/p)_l = (p/\alpha)_l$$

and the theorem follows by multiplicativity.

Acknowledgements. I would like to thank Professors M. Ram Murty and D. S. Nagaraj for carefully going through the manuscript.

REFERENCES

1. S. D. Adhikari, *An Introduction to Commutative Algebra and Number Theory*, Narosa Publishing House, (1999).
2. David A. Cox, *Primes of the form x^2+ny^2*, John Wiley & Sons, (1989).
3. Eknath Ghate, *The Kronecker-Weber Theorem*, This volume.
4. Jody Esmonde and M. Ram Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, (1999).
5. Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Springer-Verlag, (1990).

6. S. A. Katre, *Gauss-Jacobi sums and Stickelberger's Theorem*, This volume.

7. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, (1979).

8. J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, (1973).

9. Parvati Shastri, *Reciprocity laws: Artin - Hilbert*, This volume.

10. Kenneth S. Williams, *On Eisenstein's supplement to the law of cubic reciprocity*, Bull. Cal. Math. Soc., **69**, 311–314 (1977).

11. B. F. Wyman, *What is a reciprocity law?*, Am. Math. Monthly, **79**, 571–586 (1972).

Sukumar Das Adhikari
Mehta Research Institute
Chhatnag Road, Jhusi
Allahabad 211 019, India
e-mail: adhikari@mri.ernet.in