ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 16, Number 2, Spring 1986

ANOTHER PROOF OF EISENSTEIN'S LAW OF CUBIC RECIPROCITY AND ITS SUPPLEMENT

C. FRIESEN[1], B.K. SPEARMAN AND K.S. WILLIAMS[2]

ABSTRACT. A new proof is given of the law of cubic reciprocity and its supplement.

1. Introduction. The domain of Eisenstein integers $x + y\omega$, where x, y are rational integers and $\omega = (-1 + \sqrt{-3})/2$, is denoted by $Z[\omega]$. The domain $Z[\omega]$ is a unique factorization domain and its primes consist of rational primes congruent to 2 (mod 3) and their associates, complex primes of the form $a + b\omega$ with norms $N(a + b\omega) = a^2 - ab + b^2$ equal to rational primes congruent to 1 (mod 3), and $1 - \omega$ and its associates. Each prime, which is not an associate of $1 - \omega$, has exactly one of its six associates which is primary, that is, congruent to 2 (mod 3).

If λ is a prime in $Z[\omega]$, which is not an associate of $1 - \omega$, then the norm of λ is congruent to 1 (mod 3) and the cubic residue character χ_λ is defined for $\alpha \in Z[\omega]$ by

$$\chi_\lambda(\alpha) = \begin{cases} 0, \text{ if } \alpha \equiv 0 \pmod{\lambda}, \\ \omega^r, \text{ if } \alpha \not\equiv 0 \pmod{\lambda} \text{ and } \alpha^{(N(\lambda)-1)/3} \equiv \omega^r \pmod{\lambda},\ r = 0, 1, 2. \end{cases}$$

In 1844 Eisenstein [3] proved the law of cubic reciprocity.

If λ_1 and λ_2 are primary primes of $Z[\omega]$ with $N(\lambda_1) \neq N(\lambda_2)$ then

$$\chi_{\lambda_1}(\lambda_2) = \chi_{\lambda_2}(\lambda_1). \tag{1.1}$$

In a later paper [4] he proved the supplement to the law of cubic reciprocity which treats the exceptional prime $1 - \omega$.

If λ is a primary prime of $Z[\omega]$ then

Received by the editors on August 26, 1984, and in revised form on December 18, 1984

AMS *subject classification*: 10A15

Key words: Cubic reciprocity

[1] Research supported by Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Award.

[2] Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

$$(1.2) \qquad \chi_\lambda(1-\omega) = \omega^{-m},$$

where

$$m = \begin{cases} \frac{1}{3}(q+1), \text{ if } \lambda \text{ is a real prime } q \equiv 2 \pmod 3, \\ \frac{1}{3}(a+1), \text{ if } \lambda \text{ is a complex prime } a + b\omega \equiv 2 \pmod 3, \\ \qquad \text{with } N(\lambda) = p \equiv 1 \pmod 3. \end{cases}$$

A number of proofs of (1. 1) and (1. 2) have been given (for (1. 1) see for example [**2**, p. 44], [**5**], [**7**], [**8**, p. 115], [**10**, p. 218], [**11**], [**12**], [**13**], [**15**] and for (1.2) see for example [**14**], [**16**], [**19**]). The laws (1.1) and (1.2) are also special cases of more general power reciprocity laws, see for example [**1**, p. 168] and [**6**, p. 96].

In this paper we give simple new proofs of both (1.1) and (1.2) based upon ideas used by Kaplan to prove the laws of quadratic and biquadratic reciprocity [**9**] (see also [**17**]) and by Williams to prove the supplement to the law of quadratic reciprocity [**18**]. Hayashi [**7**] has also used Kaplan's ideas to prove the law of cubic reciprocity. Indeed Hayashi gives a detailed proof of the congruence (2.3) below. However although his proof is the same as the one given here for case (a) of the law of cubic reciprocity (see §2), his proof of case (b) is much more complicated than the one given here, and in addition he does not prove the supplement to the law (see §3).

2. Proof of law of cubic reciprocity. If λ_1 and λ_2 are distinct real primary primes of $Z[\omega]$ then it is well-known that $\chi_{\lambda_1}(\lambda_2) = \chi_{\lambda_2}(\lambda_1) = 1$ (see for example [**8**, pp. 113–114]). Thus we need only treat 2 cases, namely,

(a) λ_1 a complex primary prime of $Z[\omega]$ with $N(\lambda_1) = p \equiv 1 \pmod 3$ and λ_2 a real prime $q \equiv 2 \pmod 3$,

(b) λ_1, λ_2 distinct complex primary primes of $Z[\omega]$ with $N(\lambda_1) = p \equiv 1 \pmod 3$, $N(\lambda_2) = q \equiv 1 \pmod 3$, $p \neq q$.

For both cases (a) and (b) we consider the number $N_q(p)$ of solutions $(x_1, \ldots, x_q)$ of the congruence

$$(2.1) \qquad x_1^3 + x_2^3 + \ldots + x_q^3 \equiv q \pmod p$$

in two different ways. First we note that as $p \neq q$

$$(2.2) \qquad N_q(p) \equiv 3 \pmod q$$

as each solution of (2.1) with not all the x_i equal (mod p) gives rise to q distinct solutions by a cyclic permutation. Secondly by means of standard arguments using Gauss and Jacobi sums (see for example [**8**, Chap. 8], [**17**]), we obtain

$$N_q(p) \equiv \begin{cases} 1 + p^{(q-2)/3}\,\lambda_1^{(q+1)/3}\,\chi_{\bar{\lambda}_1}(q) \\ \quad + p^{(q-2)/3}\,\bar{\lambda}_1^{(q+1)/3}\,\chi_{\lambda_1}(q) \pmod q, \text{ in case (a)}, \\ 1 + p^{(q-1)/3}\,\lambda_1^{(q-1)/3}\,\chi_{\lambda_1}(q) \\ \quad + p^{(q-1)/3}\,\bar{\lambda}_1^{(q-1)/3}\,\chi_{\bar{\lambda}_1}(q) \pmod q, \text{ in case (b)}. \end{cases} \tag{2.3}$$

In case (a), from (2.2) and (2.3), we have

$$p^{(q-2)/3}\,\lambda_1^{(q+1)/3}\,\chi_{\bar{\lambda}_1}(q) + p^{(q-2)/3}\,\bar{\lambda}_1^{(q+1)/3}\,\chi_{\lambda_1}(q) \equiv 2 \pmod q. \tag{2.4}$$

Trivially we have

$$p^{(q-2)/3}\,\lambda_1^{(q+1)/3}\,\chi_{\bar{\lambda}_1}(q) \cdot p^{(q-2)/3}\,\bar{\lambda}_1^{(q+1)/3}\,\chi_{\lambda_1}(q) \equiv 1 \pmod q. \tag{2.5}$$

From (2.4) and (2.5) we deduce

$$p^{(q-2)/3}\,\lambda_1^{(q+1)/3}\,\chi_{\bar{\lambda}_1}(q) \equiv 1 \pmod q,$$

that is

$$p^{(q-2)/3}\,\lambda_1^{(q+1)/3} \equiv \chi_{\lambda_1}(q) \pmod q. \tag{2.6}$$

Raising (2.6) to the $(q-1)^{st}$ power, we obtain

$$\lambda_1^{(q^2-1)/3} \equiv \chi_{\lambda_1}(q) \pmod q,$$

giving

$$\chi_q(\lambda_1) = \chi_{\lambda_1}(q)$$

as required.

In case (b), from (2.2) and (2.3), we have as before

$$p^{(q-1)/3}\,\lambda_1^{(q-1)/3}\,\chi_{\lambda_1}(q) \equiv 1 \pmod{\lambda_2},$$

giving

$$\chi_{\lambda_2}(p\lambda_1)\,\chi_{\lambda_1}(q) = 1. \tag{2.7}$$

Replacing λ_1 by $\bar{\lambda}_1$ we obtain

$$\chi_{\lambda_2}(p\bar{\lambda}_1)\,\chi_{\bar{\lambda}_1}(q) = 1, \tag{2.8}$$

and interchanging the roles of λ_1 and λ_2 we have

$$\chi_{\lambda_1}(q\lambda_2)\,\chi_{\lambda_2}(p) = 1. \tag{2.9}$$

From (2.8) and (2.9) we deduce

$$\begin{aligned}\chi_{\lambda_1}(\lambda_2)\,\chi_{\lambda_2}(p\bar{\lambda}_1) &= \chi_{\lambda_1}(\lambda_2)\,\chi_{\bar{\lambda}_1}(q)^{-1}\\ &= \chi_{\lambda_1}(\lambda_2)\,\chi_{\lambda_1}(q)\\ &= \chi_{\lambda_1}(q\lambda_2)\\ &= \chi_{\lambda_2}(p)^2\\ &= \chi_{\lambda_2}(\lambda_1)\,\chi_{\lambda_2}(p\bar{\lambda}_1),\end{aligned}$$

and dividing by $\chi_{\lambda_2}(p\bar{\lambda}_1)$ we obtain the required result

$$\chi_{\lambda_1}(\lambda_2) = \chi_{\lambda_2}(\lambda_1).$$

This completes the proof of the law of cubic reciprocity.

3. Proof of supplement to law of cabic reciprocity. If λ is a real prime $q \equiv 2 \pmod 3$, we have

$$\begin{aligned}\chi_q(1-\omega) &= \chi_q^{-2}(1-\omega) = \chi_q^{-1}((1-\omega)^2)\\ &= \chi_q^{-1}(-3\omega) = \chi_q^{-1}(\omega)\\ &= \omega^{-(q^2-1)/3} = \omega^{-(q+1)/3},\end{aligned}$$

as required. Hence we need only consider the case when λ is a complex primary prime $\pi = a + b\omega$ in $Z[\omega]$. We have

$$a = 3m - 1,\ b = 3n, \tag{3.1}$$

for integers m and n, and

$$a^2 - ab + b^2 = \pi\,\bar{\pi} = p, \tag{3.2}$$

where p is a rational prime $\equiv 1 \pmod 3$.

We prove (1.2) in this case by proving the following equivalent result

$$\chi_\pi(3) = \omega^{-n}. \tag{3.3}$$

This is accomplished by counting the number $N_3(p)$ of solutions (x, y, z) of the congruence

$$x^3 + y^3 + z^3 \equiv 3 \pmod p \tag{3.4}$$

in two different ways.

Using Gauss and Jacobi sums we can prove

$$N_3(p) = p^2 + 3p(\chi_\pi(3) + \chi_\pi^2(3)) - (2a - b). \tag{3.5}$$

On the other hand the solutions of (3.4) can be grouped as shown in the left-hand column of Table 1 with the number in each group indicated in the right-hand column.

Table 1

2 of $x^3, y^3, z^3 \equiv 0 \pmod p$	$3(1+\chi_\pi(3)+\chi_\pi^2(3))$
exactly 1 of $x^3, y^3, z^3 \equiv 0 \pmod p$ and other 2 cubes are congruent $\pmod p$	$9\left(1+\chi_\pi\left(\frac{3}{2}\right)+\chi_\pi^2\left(\frac{3}{2}\right)\right)$
exactly 1 of $x^3, y^3, z^3 \equiv 0 \pmod p$ and other 2 cubes are distinct $\pmod p$	$3(p-2)+3(\chi_\pi^2(3)\pi+\chi_\pi(3)\bar{\pi})$ $-6(1+\chi_\pi(3)+\chi_\pi^2(3))$ $-9\left(1+\chi_\pi\left(\frac{3}{2}\right)+\chi_\pi^2\left(\frac{3}{2}\right)\right)$
$x^3 \equiv y^3 \equiv z^3 \not\equiv 0 \pmod p$	27
x^3, y^3, z^3 nonzero $\pmod p$ and exactly 2 cubes congruent $\pmod p$	$9p-9(\chi_\pi(2)+\chi_\pi^2(2))$ $+9(\chi_\pi^2(6)\pi+\chi_\pi(6)\bar{\pi})$ $-9(1+\chi_\pi(3)+\chi_\pi^2(3))$ $-9\left(1+\chi_\pi\left(\frac{3}{2}\right)+\chi_\pi^2\left(\frac{3}{2}\right)\right)-81$
x^3, y^3, z^3 nonzero and distinct $\pmod p$	multiple of 162

The numbers of solutions in the groups are easily obtained using the following three results.

(i) the number of solutions x of

$$x^3 \equiv C \pmod p \qquad (p \nmid C)$$

is

$$1+\chi_\pi(C)+\chi_\pi^2(C);$$

(ii) the number of solutions x, y of

$$Ax^3+By^3 \equiv C \pmod p \qquad (p \nmid ABC)$$

is

$$p-(\chi_\pi(AB^2)+\chi_\pi^2(AB^2))+(\chi_\pi(ABC)\bar{\pi}+\chi_\pi^2(ABC)\pi);$$

(iii) each solution (x, y, z) in the last group gives rise to $3^3 \times 3!$ distinct solutions by replacing x, y, z by $k^r x, k^s y, k^t z$, where $r, s, t = 0, 1, 2$ and $k^3 \equiv 1 \pmod p$, $k \not\equiv 1 \pmod p$, and then permuting them.

From (3.5) and Table 1 we obtain

$$\begin{aligned} &p^2-12p+81-(2a-b)+(3p+12)(\chi_\pi(3)+\chi_\pi^2(3)) \\ (3.6)\qquad &-3(\chi_\pi^2(3)\pi+\chi_\pi(3)\bar{\pi})+9(\chi_\pi(2)+\chi_\pi^2(2)) \\ &-9(\chi_\pi^2(6)\pi+\chi_\pi(6)\bar{\pi})+9\left(\chi_\pi\left(\frac{3}{2}\right)+\chi_\pi^2\left(\frac{3}{2}\right)\right) \equiv 0 \pmod{162}. \end{aligned}$$

From the trivial congruences

and
$$(1 + \chi_\pi(2) + \chi_\pi^2(2))\,(1 + \chi_\pi(3) + \chi_\pi^2(3)) \equiv 0 \pmod 9$$
$$b(1 + \omega\chi_\pi^2(6) + \omega^2\chi_\pi(6)) \equiv 0 \pmod 9,$$

we obtain, as $-a \equiv 1 \pmod 3$,

$$\begin{aligned}&-a(1 + \chi_\pi(6) + \chi_\pi^2(6)) + (\chi_\pi(2) + \chi_\pi^2(2))\\ &+ (\chi_\pi^2(2)\chi_\pi(3) + \chi_\pi(2)\,\chi_\pi^2(3)) + (\chi_\pi(3) + \chi_\pi^2(3))\\ &- b(1 + \omega\chi_\pi^2(6) + \omega^2\chi_\pi(6)) \equiv 0 \pmod 9,\end{aligned}$$

which gives

$$\tag{3.7}\begin{aligned}&(\chi_\pi(2) + \chi_\pi^2(2)) - (\chi_\pi^2(6)\pi + \chi_\pi(6)\bar{\pi}) + \left(\chi_\pi\left(\frac{3}{2}\right) + \chi_\pi^2\left(\frac{3}{2}\right)\right)\\ &\equiv (a + b) - (\chi_\pi(3) + \chi_\pi^2(3)) \pmod 9.\end{aligned}$$

Using (3.7) in (3.6) we obtain

$$\tag{3.8}\begin{aligned}&p^2 - 12p + 7a + 10b + 3(p + 1)(\chi_\pi(3) + \chi_\pi^2(3))\\ &- 3(\chi_\pi^2(3)\pi + \chi_\pi(3)\bar{\pi}) \equiv 0 \pmod{81}.\end{aligned}$$

From (3.1) and (3.2) we have

$$\tag{3.9} p = 9m^2 - 9mn + 9n^2 - 6m + 3n + 1,$$

so that

$$\tag{3.10} p^2 - 12p \equiv 27m^2 - 27mn + 33m + 24n - 11 \pmod{81}.$$

Making use of (3.1), (3.9) and (3.10) in (3.8) we obtain, after dividing by 9,

$$\tag{3.11}\begin{aligned}&(3m^2 - 3mn + 3n^2 - 3m + n + 1 - n\omega)\,\chi_\pi^2(3)\\ &+ (3m^2 - 3mn + 3n^2 - 3m + n + 1 - n\omega^2)\chi_\pi(3)\\ &+ (3m^2 - 3mn + 6m + 6n - 2) \equiv 0 \pmod 9.\end{aligned}$$

Now subtracting

$$(3m^2 - 3mn + 3n^2 - 3m)\,(1 + \chi_\pi(3) + \chi_\pi^2(3)) \equiv 0 \pmod 9,$$

from (3.11), we obtain

$$(-3n^2 - 3n - 2) + \chi_\pi(3)(n + 1 - n\omega^2) + \chi_\pi^2(3)(n + 1 - n\omega) \equiv 0 \pmod 9.$$

Now $\chi_\pi(3) = 1$ yields

$$-3n^2 \equiv 0 \pmod 9, \quad \text{i.e., } n \equiv 0 \pmod 3;$$

$\chi_\pi(3) = \omega$ yields

$$-3n^2 + 3n - 3 \equiv 0 \pmod 9, \text{ i.e., } n \equiv 2 \pmod 3;$$

and $\chi_\pi(3) = \omega^2$ yields

$$-3n^2 - 3n - 3 \equiv 0 \pmod 9, \text{ i.e., } n \equiv 1 \pmod 3.$$

This shows that $\chi_\pi(3) = \omega^{-n}$, completing the proof of the supplement to the law of cubic reciprocity.

The authors would like to thank the referee whose suggestions enabled then to simplify some of the arguments.

REFERENCES

1. E. Artin and J. Tate, *Class field theory*, W.A. Benjamin, Inc., New York, 1967.

2. G. Cooke, Notes *Lectures on the power reciprocity laws of algebraic number theory*, Cornell University, 1974.

3. G. Eisenstein, *Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen*, J. Reine Angew. Math. **27** (1844), 289–310.

4. G. Eisenstein, *Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Criterien des cubischen Characters der Zahl* 3 *und ihrer Theiler*, J. Reine Angew. Math. **28** (1844), 28–35.

5. W. Habicht, *Ein elementarer Beweis des kubischen Reziprozitatsgesetzes*, Math. Ann. **139** (1960), 343–365.

6. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil* II: *Reziprozitätsgesetz*, Physica-Verlag, Würzburg-Wien, 1970.

7. H. Hayashi, *On a simple proof of Eisenstein's reciprocity law*, Mem. Fac. Sci. Kyushu Univ. Ser. A, **28** (1974), 93–99.

8. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

9. P. Kaplan, *Démonstration des lois de reciprocité quadratique et biquadratique*, J. Fac. Sci. Univ. Tokyo Sect. 1 **16** (1969), 115–145.

10. P. Kaplan, *Cours d'Arithmétique*, Université de Nancy I.

11. T. Kubota, *Reciprocities in Gauss' and Eisenstein's number fields*, J. Reine Angew. Math. **208** (1961), 35–50.

12. K. Shiratani, *Die Diskriminante der Weierstaßschen elliptischen Funktionen und das Reziprozitätsgesetz in besonderen imaginärquadratischen Zahlkörpern*, Abh. Math. Sem. Univ. Hamberg **31** (1967), 51-61.

13. Th. Skolen, *Remarks on proofs by cyclotomic formulas of reciprocity laws for power residues*, Math. Scand. **9** (1961), 229–242.

14. Th. Skolen, *A proof of the quadratic law of reciprocity with proofs of two so-called "Ergänzungssätze"*, Norske Vid. Selsk. Forh. Trondheim **34** (1961), 18–24.

15. H.J.S. Smith, *Report on the Theory of Numbers*, Chelsea Publ. Co., New York, 1964.

16. K.S. Williams, *Note on the supplement to the law of cubic reciprocity*, Proc. Amer. Math. Soc. **47** (1975), 333–334.

17. K.S. Williams, *Note on a result of Kaplan*, Proc. Amer. Math. Soc. **56** (1976), 34–36.

18. K.S. Williams, *The quadratic character of* 2 mod p, Math. Mag. **49** (1976), 89–90.

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NEW BRUNSWICK, FREDERICTON, NEW BRUNSWICK, CANADA E3B 5A3

DEPARTMENT OF MATHEMATICS, COLLEGE OF NEW CALEDONIA, PRINCE GEORGE, BRITISH COLUMBIA, CANADA V2N 1P8

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA K1S 5B6