

## NOTE ON THE SUPPLEMENT TO THE LAW OF CUBIC RECIPROCITY

KENNETH S. WILLIAMS<sup>1</sup>

ABSTRACT. A short proof is given of the supplement to the law of cubic reciprocity proved by Eisenstein in 1844.

Let  $\omega = (-1 + \sqrt{-3})/2$ . Let  $\pi = a + b\omega$  be a primary complex prime in the Eisenstein domain  $Z[\omega]$  so that

$$(1) \quad a \equiv 2 \pmod{3}, \quad b \equiv 0 \pmod{3},$$

say

$$(2) \quad a = 3m - 1, \quad b = 3n,$$

and

$$(3) \quad a^2 - ab + b^2 = \pi\bar{\pi} = p,$$

where  $p$  is a rational prime  $\equiv 1 \pmod{3}$  (see for example [3, Chapter 9]). The cubic residue character  $(\cdot/\pi)_3$  modulo  $\pi$  is defined by

$$(4) \quad (\alpha/\pi)_3 = \omega^r \quad \text{if } \alpha^{(p-1)/3} \equiv \omega^r \pmod{\pi},$$

where  $r = 0, 1, 2$  and  $\alpha \in Z[\omega]$  is such that  $\alpha \not\equiv 0 \pmod{\pi}$ . The supplement to the law of cubic reciprocity proved by Eisenstein [2] in 1844 states that

$$(5) \quad ((1 - \omega)/\pi)_3 = \omega^{2m}.$$

We remark that  $1 - \omega$  is a prime factor of 3 in  $Z[\omega]$ . Here is a simple proof of this result (see comment in [3, p. 115]).

Let  $(h, k)_3$  denote the number of solutions  $(r, s)$  of  $1 + g^{3r+h} \equiv g^{3s+k} \pmod{p}$ , with  $0 \leq r, s < (p-1)/3$ , where  $g$  is a primitive root  $\pmod{p}$  such that  $(g/\pi)_3 = \omega$ . (If  $g$  is such that  $(g/\pi)_3 = \omega^2$ , we can replace  $g$  by

---

Received by the editors January 31, 1974.

AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 12C20.

Key words and phrases. Supplement to law of cubic reciprocity, cubic residue character, Eisenstein domain.

<sup>1</sup>Research supported by National Research Council of Canada grant no. A-7233.

Copyright © 1975, American Mathematical Society

an appropriate power of  $g$  so that this power of  $g$  is a primitive root with cubic residue character (mod  $\pi$ ) equal to  $\omega$ .) Then it is well known (see for example [1, p. 397]) that

$$\begin{aligned}
 &9(0, 0)_3 = p - 8 + 2a - b, \\
 (6) \quad &9(0, 1)_3 = 9(1, 0)_3 = 9(2, 2)_3 = p - 2 - a + 2b, \\
 &9(0, 2)_3 = 9(2, 0)_3 = 9(1, 1)_3 = p - 2 - a - b, \\
 &9(1, 2)_3 = 9(2, 1)_3 = p + 1 + 2a - b.
 \end{aligned}$$

From the work of Muskat [4, Corollary 1 with  $e = 3$ ] we have

$$(7) \quad \text{ind}_g(3) \equiv (1, 1)_3 - (2, 2)_3 \pmod{3},$$

where, for any integer  $a \not\equiv 0 \pmod{p}$ ,  $\text{ind}_g(a)$  denotes the unique integer  $b$  such that  $a \equiv g^b \pmod{p}$ ,  $0 \leq b \leq p-2$ . Putting (2), (6) and (7) together we obtain

$$(8) \quad \text{ind}_g(3) \equiv -n \pmod{3},$$

so that  $3^{(p-1)/3} \equiv g^{-n(p-1)/3} \equiv \omega^{-n} \pmod{\pi}$ , showing that  $(3/\pi)_3 = \omega^{-n}$ . Hence

$$\left(\frac{1-\omega}{\pi}\right)_3 = \left(\frac{(1-\omega)^4}{\pi}\right)_3 = \left(\frac{3^2\omega^2}{\pi}\right)_3 = \omega^{2(p-1)/3-2n},$$

and the result follows since from (2) and (3) we have  $(p-1)/3 \equiv m+n \pmod{3}$ .

#### REFERENCES

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391-424.
2. G. Eisenstein, *Nachtrag zum kubischer Reciprocitätssatze*, J. Reine Angew. Math. **28** (1844), 28-35.
3. K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden and Quigley, Tarrytown-on-Hudson, New York, 1972.
4. J. B. Muskat, *On the solvability of  $x^e \equiv e \pmod{p}$* , Pacific J. Math. **14** (1964), 257-260. MR 28 #2997.

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA