Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity

By *Kenneth S. Williams**) at Ottawa

Let $\zeta = \exp(2\pi i/5)$. The ring of integers

$$Z[\zeta] = \{a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 : a_1, a_2, a_3, a_4 \in Z\}$$

of the cyclotomic field $Q(\zeta)$ is a unique factorization domain (see for example [6]), all of whose units are given by $\pm\zeta^k(\zeta+\zeta^4)^n$, $k = 0, 1, 2, 3, 4$, $n \in Z$ (see for example [8], p. 99). If $a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 \in Z[\zeta]$ is not divisible by the prime $1-\zeta$, equivalently $a_1 + a_2 + a_3 + a_4 \not\equiv 0 \pmod 5$, then multiplying $a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$ by a suitable unit if necessary, we may suppose that it is normalized, that is

(1) $a_1 - a_2 - a_3 + a_4 \equiv a_1 + 2a_2 - 2a_3 - a_4 \equiv 0 \pmod 5$, $a_1 + a_2 + a_3 + a_4 \equiv 1, 2 \pmod 5$,

and thus is primary (see for example [8], p. 118).

If $\pi = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$ is a normalized prime factor of a rational prime $p \equiv 1 \pmod 5$ we set $a = a_1 + a_2 + a_3 + a_4$ so that from (1) we have

(2) $$a_1 \equiv -2a - a_4,\quad a_2 \equiv 2a - 2a_4,\quad a_3 \equiv a + 2a_4 \pmod 5$$

with $a \equiv 1$ or $2 \pmod 5$. π gives rise to a solution (x, u, v, w) of Dickson's diophantine system [1], p. 402

(3) $$16p = x^2 + 50u^2 + 50v^2 + 125w^2,\quad xw = v^2 - 4uv - u^2,\quad x \equiv 1 \pmod 5,$$

as follows: set

(4) $$\theta = b_1\zeta + b_2\zeta^2 + b_3\zeta^3 + b_4\zeta^4 = (a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4)(a_1\zeta^2 + a_2\zeta^4 + a_3\zeta + a_4\zeta^3)$$

so that

(5) $$\begin{aligned} b_1 &= a_2^2 + a_1a_4 - a_1a_2 - a_1a_3 - a_2a_4,\\ b_2 &= a_4^2 + a_2a_3 - a_1a_2 - a_2a_4 - a_3a_4,\\ b_3 &= a_1^2 + a_2a_3 - a_1a_2 - a_1a_3 - a_3a_4,\\ b_4 &= a_3^2 + a_1a_4 - a_1a_3 - a_2a_4 - a_3a_4, \end{aligned}$$

---

*) Research supported by National Research Council of Canada, Grant No. A-7233.

from which we obtain in conjunction with (2)

$$\text{(6)}\qquad \begin{cases} b_1 \equiv aa_4 \pmod 5, & b_2 \equiv a^2 + 2aa_4 \pmod 5, \\ b_3 \equiv 2a^2 - 2aa_4 \pmod 5, & b_4 \equiv -2a^2 - aa_4 \pmod 5, \end{cases}$$

which gives

$$\text{(7)}\qquad \begin{aligned} b_1 + b_2 + b_3 + b_4 &\equiv a^2 \pmod 5, & b_1 + 2b_2 - 2b_3 - b_4 &\equiv 0 \pmod 5, \\ 2b_1 - b_2 + b_3 - 2b_4 &\equiv 0 \pmod 5, & b_1 - b_2 - b_3 + b_4 &\equiv 0 \pmod 5, \end{aligned}$$

enabling us to define integers x, u, v, w (with $x \equiv 1 \pmod 5$) by

$$\text{(8)}\qquad \begin{aligned} x &= \varepsilon(b_1 + b_2 + b_3 + b_4), & 5u &= -\varepsilon(b_1 + 2b_2 - 2b_3 - b_4), \\ 5v &= -\varepsilon(2b_1 - b_2 + b_3 - 2b_4), & 5w &= -\varepsilon(b_1 - b_2 - b_3 + b_4), \end{aligned}$$

where $\varepsilon = +1$ if $a \equiv 1 \pmod 5$, $\varepsilon = -1$ if $a \equiv 2 \pmod 5$, which satisfy (3) as $\theta\bar{\theta} = p$.

As $\varepsilon \equiv a^2 \pmod 5$ we have (using (6) and (8))

$$a_4 \equiv \varepsilon a^2(a + a_4) - a \equiv -\varepsilon a(b_2 - b_3) - a \equiv a(2u - v - 1) \pmod 5,$$

which gives on appealing to (2)

$$\text{(9)}\qquad \begin{aligned} a_1 &\equiv a(-2u + v - 1) \pmod 5, & a_2 &\equiv a(u + 2v - 1) \pmod 5, \\ a_3 &\equiv a(-u - 2v - 1) \pmod 5, & a_4 &\equiv a(2u - v - 1) \pmod 5. \end{aligned}$$

Hence from (9) we have

$$\text{(10)}\qquad \frac{a_1 - 2a_2 + 2a_3 - a_4}{a_1 + a_2 + a_3 + a_4} \equiv 2u - v \pmod 5$$

and from (5), (8), (9) we have

$$\begin{aligned} &4(a_1 + a_2 + a_3 + a_4)(a_1 + 2a_2 + 3a_3 + 4a_4) \\ &= 5\varepsilon(u - 2v) + 5(a_2^2 + 3a_3^2 + 4a_4^2 + 3a_1a_2 + 4a_1a_3 + 4a_1a_4 + 4a_2a_3 + 4a_2a_4) + 25a_3a_4 \\ &\equiv 5a^2(u - 2v) + 5a^2(u + 2v + 2) \pmod{25} \\ &\equiv 5a^2(2u + 2) \pmod{25} \end{aligned}$$

giving

$$\text{(11)}\qquad \frac{1}{5}\,\frac{a_1 + 2a_2 + 3a_3 + 4a_4}{a_1 + a_2 + a_3 + a_4} \equiv \frac{2u + 2}{4} \equiv -2u - 2 \pmod 5.$$

Now if $\left(\frac{\ }{\pi}\right)_5$ denotes the quintic residue character $(\mathrm{mod}\ \pi)$ Kummer's logarithmic differential-quotient formulae for his complementary results (see for example [3], p. 270, [2], pp. 109—113, [8], pp. 121—123) to his law of quintic reciprocity $\left(\frac{\pi_1}{\pi_2}\right)_5 = \left(\frac{\pi_2}{\pi_1}\right)_5$, where π_1, π_2 are primary primes of $Z[\zeta]$ (see for example, [8], p. 120), give after some calculation

$$\left(\frac{\zeta}{\pi}\right)_5 = \zeta^{\frac{p-1}{5}}, \quad \left(\frac{\zeta+\zeta^4}{\pi}\right)_5 = \zeta^{\frac{a_1-2a_2+2a_3-a_4}{a_1+a_2+a_3+a_4}}, \tag{12}$$

$$\left(\frac{5}{\pi}\right)_5 = \zeta^{\frac{1}{5}\frac{(a_1+2a_2+3a_3+4a_4)}{(a_1+a_2+a_3+a_4)}+\frac{3(a_1-2a_2+2a_3-a_4)}{(a_1+a_2+a_3+a_4)}+2}.$$

Thus, from (3), (10), (11), (12) and the identity $(1-\zeta)^4 = 5\zeta^2(\zeta+\zeta^4)^2$ we obtain

Theorem. *Let π be a normalized prime factor $\in Z[\zeta]$ of a rational prime $p \equiv 1 \pmod 5$ giving rise (in the manner described above) to the solution (x, u, v, w) of Dickson's diophantine system* (3). *Then we have*

$$\left(\frac{\zeta}{\pi}\right)_5 = \zeta^{\frac{2}{5}(x+4)}, \quad \left(\frac{\zeta+\zeta^4}{\pi}\right)_5 = \zeta^{2u-v},$$

$$\left(\frac{5}{\pi}\right)_5 = \zeta^{-u+2v}, \quad \left(\frac{1-\zeta}{\pi}\right)_5 = \zeta^{\frac{1}{5}(x+4)+2u}.$$

We remark that as a consequence of this theorem, 5 is a quintic residue of $p \equiv 1 \pmod 5$ if and only if $u - 2v \equiv 0 \pmod 5$, a result due to Muskat [7]. As the only solutions of (3) are (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$ and $(x, -v, u, -w)$, the congruence $u - 2v \equiv 0 \pmod 5$ is independent of the choice of solution (x, u, v, w) of (3).

Example. The primary prime factor $\pi = 5\zeta + \zeta^2 + 2\zeta^3 + 3\zeta^4$ of $p = 61$ leads to $(x, u, v, w) = (1, 4, -1, 1)$ so that by the theorem we have

$$\left(\frac{\zeta}{\pi}\right)_5 = \zeta^2, \quad \left(\frac{\zeta+\zeta^4}{\pi}\right)_5 = \zeta^4, \quad \left(\frac{5}{\pi}\right)_5 = \zeta^4, \quad \left(\frac{1-\zeta}{\pi}\right)_5 = \zeta^4.$$

Using $\zeta \equiv -3 \pmod \pi$ as necessary we can check these results as follows:

$$\left(\frac{\zeta}{\pi}\right)_5 \equiv \zeta^{\frac{61-1}{5}} = \zeta^{12} = \zeta^2 \pmod \pi,$$

$$\left(\frac{\zeta+\zeta^4}{\pi}\right) \equiv (\zeta+\zeta^4)^{12} \equiv (78)^{12} \equiv 17^{12} \equiv (4913)^4 \equiv 33^4$$

$$\equiv 1089^2 \equiv (-9)^2 \equiv 3^4 \equiv \zeta^4 \pmod \pi,$$

$$\left(\frac{5}{\pi}\right)_5 \equiv 5^{12} \equiv 125^4 \equiv 3^4 \equiv \zeta^4 \pmod \pi,$$

$$\left(\frac{1-\zeta}{\pi}\right)_5 \equiv (1-\zeta)^{12} \equiv 4^{12} \equiv 64^4 \equiv 3^4 \equiv \zeta^4 \pmod \pi.$$

We close by remarking that in all likelihood the ideas of this paper can be used to obtain corresponding explicit forms for the complementary theorems to Kummer's law of septic reciprocity. The appropriate diophantine system is discussed in [5] (see also [9]). Presumably the necessary and sufficient condition for 7 to be a septic residue of $p \equiv 1 \pmod 7$ given in [4] would follow as a corollary.

References

[1] *L. E. Dickson*, Cyclotomy, higher congruences, and Waring's problem, Amer. J. Math. **57** (1935), 391—424.
[2] *H. Hasse*, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II, Reziprozitätsgesetz, Würzburg 1965.
[3] *E. Kummer*, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen, J. reine angew. Math. **56** (1858), 270.
[4] *P. A. Leonard* and *K. S. Williams*, The septic character of 2, 3, 5 and 7, Pacific J. Math. **52** (1974), 143—147.
[5] *P. A. Leonard* and *K. S. Williams*, A diophantine system of Dickson, Atti Accad. Nazionale dei Lincei **56** (1974), 145—150.
[6] *J. Masley*, Solution of class number one problem for cyclotomic fields, Abstracts of Communications, 1974 International Congress of Mathematicians, Vancouver, B.C. p. 46.
[7] *J. B. Muskat*, On the solvability of $x^e \equiv e \pmod{p}$, Pacific J. Math. **14** (1964), 257—260.
[8] *H. J. S. Smith*, Report on the Theory of Numbers, New York 1964.
[9] *K. S. Williams*, Elementary treatment of a quadratic partition of primes $p \equiv 1 \pmod 7$, Illinois J. Math. **18** (1974), 608—621.

Carleton University, Ottawa, Ontario, Canada

Eingegangen 24. März 1975