Contributions to Discrete Mathematics

Volume 7, Number 1, Pages 82–97
ISSN 1715-0868

COMPLEMENTARIES TO KUMMER'S DEGREE SEVEN RECIPROCITY LAW AND A DICKSON DIOPHANTINE SYSTEM

PERLAS CARANAY

Abstract. Let $\mathbb{Q}(\zeta)$ be the cyclotomic field obtained from $\mathbb{Q}$ by adjoining a primitive seventh root of unity ζ. Normalized primary elements of this field are characterized and related to Jacobi sums and to solutions of a system of quadratic Diophantine equations of Dickson type involving a rational prime $p \equiv 1 \pmod 7$. These objects and their connection are then used to give another formulation of the complementary laws to Kummer's reciprocity law of degree seven.

1. Introduction

Classical reciprocity laws and their accompanying complementary laws were originally used to solve problems mainly in number theory. These objects later gained more importance due to their applications in other mathematically related areas such as cryptography. They are used to compute residue symbols of the form $\left(\frac{\alpha}{\beta}\right)_l$ without factoring the modulus β in the cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi \mathbf{i}/l}$ is a primitive l-th root of unity and $l \in \mathbb{Z}$ is a prime. Cryptographic applications of these reciprocity laws and their complementaries can be found, for example, in [20], [23], and [24].

Efficient computation of residue symbols relies heavily on the use of reciprocity laws and their corresponding complementaries in $\mathbb{Q}(\zeta)$. These complementaries include those for elements which are excluded from the reciprocity law such as l, the special prime $1-\zeta$, and the units of the field. Explicit forms of the complementary laws had been known for the cases $l = 2, 3$, and 5 for quite some time now. For $l = 2$, an in-depth discussion of the quadratic reciprocity law and its complementaries can be found, for example, in [11] or [14]. The cubic case, $l = 3$, was extensively studied by Eisenstein [6, 7], and additional explicit forms of the complementaries to the cubic reciprocity law were given in [11] (pp. 112–119), [19] (pp. 78–82), and [30]. For additional treatment of the cubic reciprocity law and its complementaries, see [8] and [27]. For $l = 5$, results pertaining to the

Received by the editors March 16, 2011, and in revised form February 15, 2012.
2000 *Mathematics Subject Classification.* 11A15, 11R18, 11D09, 11D72, 11T24.
Key words and phrases. Power residues, complementary laws, cyclotomic fields, primary, Diophantine equations, Jacobi sums.

complementary laws to Kummer's quintic reciprocity law were explored in [19] (pp. 84–89), [20], and [29]. Recently, the case $l = 7$ has been examined, and the explicit forms of the complementaries to Kummer's degree seven reciprocity law appear in [2] and [3].

In this work, a different formulation of the complementaries for the case $l = 7$ is explored. This new formulation depends on a particular type of an algebraic integer, which will be called a normalized primary element, in $\mathbb{Q}(\zeta)$ with ζ a primitive seventh root of unity. Properties of these elements will be discussed here. The paper presents an interesting relationship between normalized primary elements, including Jacobi sums, in $\mathbb{Q}(\zeta)$ and solutions of a system of quadratic Diophantine equations of Dickson type. It is shown here how this relationship can be employed to obtain new formulas for the complementaries to Kummer's degree seven reciprocity law in terms of the solutions of the Dickson system. This work is inspired by an earlier paper of K. S. Williams [29] which showed that the solutions of a system of quadratic Diophantine equations involving a rational prime $p \equiv 1 \pmod 5$, due to Dickson [4, 5], can be used to obtain an explicit formulation of the complementary laws to Kummer's quintic reciprocity law.

The paper is organized as follows. Section 2 includes a brief review of some basic properties of cyclotomic fields, a discussion of the nature of primary normalized elements in $\mathbb{Q}(\zeta)$, and a presentation of Kummer's reciprocity law and its complementaries. In Section 3, we present some properties of Jacobi sums and their relation to the factorization of a prime $p \equiv 1 \pmod 7$. Then some properties of the system of quadratic Diophantine equations of Dickson type involving rational primes of the form $p = 7k + 1$, $k \in \mathbb{Z}$, are presented in Section 4. Finally, Section 5 is devoted to the derivation of the new formulas for the complementaries to Kummer's reciprocity law using the solutions of the system of equations from Section 4.

2. Cyclotomic Fields and Kummer's Reciprocity Law

We recall some properties of cyclotomic fields, give the nature of primary normalized elements in $\mathbb{Q}(\zeta)$, and revisit the reciprocity law due to Kummer and its complementaries for the case $l = 7$. For an in-depth discussion of cyclotomic fields, we refer to [22].

Suppose $l \in \mathbb{Z}$ is an odd rational prime. Let $\zeta = e^{2\pi \mathbf{i}/l}$ be a primitive l-th root of unity, so ζ satisfies

$$1 + \zeta + \cdots + \zeta^{l-1} = 0.$$

The cyclotomic field $\mathbb{Q}(\zeta)$ formed by adjoining ζ to the field of rational numbers $\mathbb{Q}$ is a Galois extension over $\mathbb{Q}$ of degree $[\mathbb{Q}(\zeta) : \mathbb{Q}] = l - 1$. Its maximal order is the ring $\mathbb{Z}[\zeta]$, so any $l - 1$ distinct powers of ζ form an integral basis of $\mathbb{Q}(\zeta)$. We will use the set $\{\zeta^i \mid 1 \leq i \leq l - 1\}$ as an integral basis of $\mathbb{Q}(\zeta)$. The $l - 1$ conjugate mappings of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are given by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq l - 1$. So the conjugates of an element

$\alpha = a_1\zeta + a_2\zeta^2 + \cdots + a_{l-1}\zeta^{l-1} \in \mathbb{Q}(\zeta)$, with $a_j \in \mathbb{Q}$, can be ordered as

$$\alpha_i = \sigma_i(\alpha) = a_1\zeta^i + a_2\zeta^{2i} + \cdots + a_{l-1}\zeta^{(l-1)i}.$$

Denote by $\overline{\alpha} = \sigma_{l-1}(\alpha)$ the complex conjugate of α. The norm and trace of α are given by $\mathbf{N}(\alpha) = \prod_{i=1}^{l-1}\sigma_i(\alpha)$ and $\mathbf{T}(\alpha) = \sum_{i=1}^{l-1}\sigma_i(\alpha)$, respectively. Since $\sigma_{l-i}(\alpha)$ is the complex conjugate of $\sigma_i(\alpha)$, $\mathbf{N}(\alpha) > 0$ for all non-zero $\alpha \in \mathbb{Q}(\zeta)$. Moreover, all the $l-1$ complex mappings are complex embeddings of $\mathbb{Q}(\zeta)$, so the unit rank of $\mathbb{Q}(\zeta)$ is $r = (l-3)/2$. Thus, the group of units of $\mathbb{Z}[\zeta]$ is of the form $\mathbb{Z}[\zeta]^* = \langle -1, \zeta\rangle \times \mathcal{E}$, where $\mathcal{E}$ is isomorphic to $\mathbb{Z}^r$. We say that two elements $\alpha, \beta \in \mathbb{Z}[\zeta]$ are associates and write $\alpha \simeq \beta$ if $\alpha\beta^{-1} \in \mathbb{Z}[\zeta]^*$.

The discriminant of $\mathbb{Q}(\zeta)$ is $(-1)^{(l-1)/2}l^{l-2}$, so the only rational prime ramified in $\mathbb{Q}(\zeta)$ is l. Let ω be the prime $1-\zeta \in \mathbb{Z}[\zeta]$. We have $l \simeq \omega^{l-1}$. The powers ω^k, with $0 \le k \le l-2$, also form an integral basis of $\mathbb{Q}(\zeta)$.

One important element in the statement of Kummer's reciprocity law is the concept of primary elements in $\mathbb{Z}[\zeta]$. The following definition can be found on p. 350 of [12] and p. 118 of [21].

Definition 2.1 (Primary elements)**.** Let $\alpha \in \mathbb{Z}[\zeta]$. Then α is said to be *primary* if there exists $B \in \mathbb{Z}$ such that the following hold:

$$\alpha \not\equiv 0 \pmod{\omega}, \quad \alpha \equiv B \pmod{\omega^2}, \quad \text{and} \quad \alpha\overline{\alpha} \equiv B^2 \pmod{l}.$$

We need to employ another crucial concept in $\mathbb{Q}(\zeta)$, which was originally introduced in [15] for the case $l = 7$. This notion is one of the key ingredients in our derivation of the reformulations of the complementary laws.

Definition 2.2. An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be *normalized* if $\alpha \equiv -1 \pmod{\omega^2}$.

We summarize some properties of primary and normalized elements in the following lemma.

Lemma 2.3.

(a) *Every conjugate of a primary element in $\mathbb{Z}[\zeta]$ is primary, and every conjugate of a normalized element in $\mathbb{Z}[\zeta]$ is normalized.*

(b) *Every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a normalized primary associate.*

(c) *If $l \le 19$, then every prime $p \equiv 1 \pmod{l}$ has a unique factorization, up to associates, of the form $p = \pi_1 \cdots \pi_{l-1}$ into normalized primary primes in $\mathbb{Z}[\zeta]$, where $\pi_i = \sigma_i(\pi_1)$ for $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $1 \le i \le l-1$.*

Proof. Note that $\sigma(\omega)$ is an associate to ω for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$. Part (a) is now straightforward to prove.

To prove part (b), recall that by Lemma 2.6 of [3], every $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha \not\equiv 0 \pmod{\omega}$ has a primary associate. So assume without loss of generality that α is primary. Let g be a primitive root modulo l. Consider the element

$$\mu = \zeta + \cdots + \zeta^g = \zeta\sigma_g(\omega)/\omega \in \mathbb{Z}[\zeta].$$

Since $\sigma_g(\omega)$ is associate to ω, μ is a unit in $\mathbb{Z}[\zeta]$. Moreover, $\mu^l \equiv g \pmod{l}$.

Let $B \in \mathbb{Z}$, $B \not\equiv 0 \pmod{l}$, such that $\alpha \equiv B \pmod{\omega^2}$ and $\alpha\overline{\alpha} \equiv B^2 \pmod{l}$. Since g is a primitive root modulo l, the elements $g^k B$, $0 \leq k \leq l-2$, are distinct. So there exists $k \in \{0, 1, \ldots, l-2\}$ such that $g^k B \equiv -1 \pmod{l}$. Note that

$$\mu^{kl} \equiv g^k \equiv -B^{-1} \pmod{l}.$$

Set $\beta = \alpha\varepsilon^{kl}$. Then $\beta \equiv -1 \pmod{\omega^2}$, so β is normalized. Also, $\beta\bar{\beta} \equiv 1 \pmod{l}$, so β is primary. Hence, β is a normalized primary associate of α.

Finally, for part (c), recall that every prime $p \equiv 1 \pmod{l}$ splits completely in $\mathbb{Q}(\zeta)$ (see Theorem 2.13 of [22], for example). Recall furthermore that if $l \leq 19$, then $\mathbb{Z}[\zeta]$ is a unique factorization domain [17]. Thus, every prime $p \equiv 1 \pmod{l}$ has a prime factorization, unique up to associates, of the form

$$p = \pi_1\pi_2\cdots\pi_{l-1},$$

with $\pi_i = \sigma_i(\pi_1)$ for $1 \leq i \leq l-1$. By part (b), π_1 has a normalized primary associate $\pi_1' = \mu\pi_1$ with $\mu \in \mathbb{Z}[\zeta]^*$. By part (a), $\pi_i' = \sigma_i(\pi_1')$ is a normalized primary associate to π_i. Since $\mathbf{N}(\mu) = 1$,

$$p = \pi_1'\pi_2'\cdots\pi_{l-1}'$$

is the desired factorization. □

For $\alpha = \sum_{i=1}^{l-1} a_i\zeta^i \in \mathbb{Z}[\zeta]$, we define the following important quantities:

$$b = b(\alpha) = \sum_{i=1}^{l-1} a_i = -\mathbf{T}(\alpha), \qquad \text{and} \qquad c = c(\alpha) = \sum_{i=1}^{l-1} i a_i \ . \tag{1}$$

These quantities satisfy the identities given in the next lemma.

Lemma 2.4. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$. Then*

(a) $b(\sigma_i(\alpha)) = b(\alpha)$ *for* $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $1 \leq i \leq l-1$.
(b) $\alpha \equiv b(\alpha) - c(\alpha)\omega \pmod{\omega^2}$.
(c) $b(\alpha\beta) \equiv b(\alpha)b(\beta) \pmod{l}$.

Proof. Write $\alpha = \sum_{i=1}^{l-1} a_i\zeta^i$ with $a_i \in \mathbb{Z}$ for $1 \leq i \leq l-1$. So $b(\alpha) = \sum_{i=1}^{l-1} a_i$. Part (a) is easy. For parts (b) and (c), see [3] Lemma 2.1 and Corollaries 2.2 and 2.3. □

Lemma 2.4(b) implies that α is normalized if and only if $b \equiv -1 \pmod{l}$ and $c \equiv 0 \pmod{l}$. Furthermore, if α is primary, then $b \not\equiv 0 \pmod{l}$ and $c \equiv 0 \pmod{l}$.

Kummer's Reciprocity Law and its Complementaries. If $\pi \in \mathbb{Z}[\zeta]$ is prime, then $\mathbb{Z}[\zeta]/\pi\mathbb{Z}[\zeta]$ is a finite field of order $\mathbf{N}(\pi)$. So $\alpha^{\mathbf{N}(\pi)-1} \equiv 1 \pmod{\pi}$ for any non-zero $\alpha \in \mathbb{Z}[\zeta]$, where α is not divisible by π. Hence, $\alpha^{(\mathbf{N}(\pi)-1)/l} \equiv \zeta^i \pmod{\pi}$ for a unique $i \in \{0, 1, \ldots, l-1\}$. The exponent i is called the *index* of α with respect to π, denoted by $\mathrm{ind}_\pi(\alpha)$. This leads to the following definition.

Definition 2.5. Let $\alpha, \pi \in \mathbb{Z}[\zeta]$, where $\pi \not\simeq \omega$ is a prime. Then the *l-th power residue symbol* of α modulo π is defined as

$$\left(\frac{\alpha}{\pi}\right)_l = \begin{cases} 0 & \text{if } \pi \mid \alpha\,, \\ \zeta^{\mathrm{ind}_\pi(\alpha)} & \text{if } \pi \nmid \alpha\,. \end{cases}$$

This definition may also be extended to composite moduli just like the generalization of the Legendre symbol to the Jacobi symbol. We now state Kummer's reciprocity law for an odd rational prime l (for example, see [12, 13] and [21]). The formulation of this reciprocity law for composite moduli can be found in [2, 3] and [19, 20].

Theorem 2.6 (Kummer's law of reciprocity)**.** *Let π and ψ be two distinct primary primes. Then*

$$\left(\frac{\pi}{\psi}\right)_l = \left(\frac{\psi}{\pi}\right)_l.$$

For the remainder of this section, we restrict to the case $l = 7$. Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$. We define six linear combinations of the coefficients of α as follows:

$$\begin{aligned}
b = b(\alpha) &= \sum_{i=1}^{6} a_i \;\; = a_1 + a_2 + a_3 + a_4 + a_5 + a_6, \\
c = c(\alpha) &= \sum_{i=1}^{6} i a_i \;\; = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6, \\
a = a(\alpha) &= \sum_{i=1}^{6} i^2 a_i \equiv a_1 - 3a_2 + 2a_3 + 2a_4 - 3a_5 + a_6 \pmod{7}\,, \\
d = d(\alpha) &= \sum_{i=1}^{6} i^3 a_i \equiv a_1 + a_2 - a_3 + a_4 - a_5 - a_6 \pmod{7}\,, \\
e = e(\alpha) &= \sum_{i=1}^{6} i^4 a_i \equiv a_1 + 2a_2 - 3a_3 - 3a_4 + 2a_5 + a_6 \pmod{7}\,, \\
f = f(\alpha) &= \sum_{i=1}^{6} i^5 a_i \equiv a_1 - 3a_2 - 2a_3 + 2a_4 + 3a_5 - a_6 \pmod{7}\,.
\end{aligned} \tag{2}$$

The quantities b and c were already introduced in (1). For $l = 7$, the complementaries to Kummer's reciprocity law for any primary element were

explicitly stated in [2] Theorem 4.3.1 and [3] Theorem 6.3. Here we give a version of the complementary laws using a primary prime element of $\mathbb{Z}[\zeta]$.

Theorem 2.7 (Complementary laws, $l = 7$)**.** *Let $\pi = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$ be primary prime and a, b, c, d, e, f given by* (2) *(with π in place of α). Suppose $\mathbf{N}(\pi) = p \equiv 1 \pmod 7$. Then the following hold:*

$$\left(\frac{\pm 1}{\pi}\right)_7 = 1, \qquad \left(\frac{\zeta}{\pi}\right)_7 = \zeta^{\frac{p-1}{7}},$$

$$\left(\frac{7}{\pi}\right)_7 = \zeta^{\frac{c}{7b}+\frac{3f-d}{b}+3}, \qquad \left(\frac{\omega}{\pi}\right)_7 = \zeta^{\frac{4(p+6)}{7}-\frac{c}{7b}},$$

$$\left(\frac{\zeta+\zeta^6}{\pi}\right)_7 = \zeta^{\frac{f-2d}{b}}, \qquad \left(\frac{\zeta^2+\zeta^5}{\pi}\right)_7 = \zeta^{\frac{3(d-f)}{b}}.$$

Primary and normalized elements can also be easily characterized in terms of the quantities in (2).

Lemma 2.8. *Let $\alpha = \sum_{i=1}^{6} a_i\zeta^i \in \mathbb{Z}[\zeta]$.*

(a) *α is primary if and only if $b \not\equiv 0 \pmod 7$, $c \equiv 0 \pmod 7$, and $a \equiv e \equiv 0 \pmod 7$, or equivalently, $a_1 + a_6 \equiv a_2 + a_5 \equiv a_3 + a_4 \pmod 7$.*

(b) *α is normalized if and only if $b \equiv -1 \pmod 7$ and $c \equiv 0 \pmod 7$.*

(c) *α is normalized primary if and only if $b \equiv -1 \pmod 7$, $c \equiv 0 \pmod 7$, and $a_1 + a_6 \equiv a_2 + a_5 \equiv a_3 + a_4 \equiv 2 \pmod 7$.*

Proof. For part (a), see Corollary 4.5 of [3]. Part (b) was already remarked just after the proof of Lemma 2.4. For part (c), let $a_1 + a_6 \equiv j \pmod 7$. Then

$$-1 \equiv b \equiv 3j \not\equiv 0 \pmod 7$$

if and only if $j \equiv 2 \pmod 7$. □

3. Jacobi Sums and Prime Factorization

As shown in [15], Jacobi sums play an important role in finding the solutions to a system of quadratic Diophantine equations of Dickson type involving a rational prime $p \equiv 1 \pmod 7$. These character sums can be used to write a factorization of p into two complex conjugate normalized algebraic integers, say $p = \alpha\overline{\alpha}$, where $\alpha, \overline{\alpha} \in \mathbb{Z}[\zeta]$ are Jacobi sums. This type of factorization of p will turn out to be useful in Section 5 for the derivation of Kummer's complementary laws from the solutions of the Dickson system given in the next section. We review some properties of Jacobi sums and then relate them to the factorization of the rational prime p in $\mathbb{Q}(\zeta)$. The interested reader may consult [1], [11], or [14] for additional descriptions of Jacobi sums.

Throughout this section, we assume that $l \leq 19$, so $\mathbb{Z}[\zeta]$ is a unique factorization domain. Let $p \in \mathbb{Z}$ be an odd rational prime such that $p \equiv 1 \pmod l$. A nontrivial character $\chi \pmod p$ of order l is a nontrivial multiplicative group homomorphism from $\mathbb{F}_p^*$ into the multiplicative group

of l-th roots of unity. The trivial character ε is the homomorphism on $\mathbb{F}_p^*$ satisfying $\varepsilon(\alpha) = 1$ for all $\alpha \in \mathbb{F}_p^*$. For convenience, we define $\chi(0) = 1$ if χ is the trivial character and $\chi(0) = 0$ if χ is a nontrivial character.

Definition 3.1. Let χ_1, χ_2 be characters on $\mathbb{F}_p$. The *Jacobi sum* of χ_1 and χ_2 is defined by

$$J(\chi_1, \chi_2) = \sum_{a \in \mathbb{F}_p} \chi_1(a)\chi_2(1-a).$$

The *order* n of the Jacobi sum $J(\chi_1, \chi_2)$ is the least common multiple of the orders of χ_1 and χ_2. Hence, a Jacobi sum of order n is an integer of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive n-th root of unity.

Note that $J(\varepsilon, \varepsilon) = p$ and for a nontrivial character χ, $J(\varepsilon, \chi) = J(\chi, \varepsilon) = 0$. It can also be shown that for nontrivial characters χ_1 and χ_2, the modulus of the algebraic integer $J(\chi_1, \chi_2)$ is $|J(\chi_1, \chi_2)| = \sqrt{p}$, so $J(\chi_1, \chi_2)\overline{J(\chi_1, \chi_2)} = p$. Moreover, we have the following result.

Theorem 3.2. *Let χ_1 and χ_2 be characters on $\mathbb{F}_p$ of order l, where l is an odd prime. Set $\zeta = e^{2\pi \mathbf{i}/l}$. Then*

$$J(\chi_1, \chi_2) \equiv -1 \pmod{\omega^2}.$$

Proof. See [1], p. 63. □

Let π be a normalized primary prime divisor of p, and $\zeta = e^{2\pi \mathbf{i}/l}$. Consider the multiplicative character $\chi = \left(\frac{\cdot}{\pi}\right)_l$ given in Definition 2.5. Equivalently, χ is the character (mod p) such that $\chi(g) = \zeta$, where g is a primitive root modulo p with $g^{\frac{p-1}{l}} \equiv \zeta \pmod{\pi}$. We abbreviate our notation for the Jacobi sum $J(\chi^i, \chi^j)$ by $J(i, j)$.

We now consider how Jacobi sums decompose into primes in $\mathbb{Z}[\zeta]$. Let $L(a)$ be the least positive integer congruent to $a \pmod{l}$ for any integer $a \in \mathbb{Z}$ not divisible by l. As in Section 2, we order the conjugates of an element $\pi \in \mathbb{Z}[\zeta]$ as $\pi_i = \sigma_i(\pi)$ for $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $1 \leq i \leq l-1$. Assuming unique factorization, we can now present an analog of Theorem 2.1.14 in [1] pertaining to the prime factorization of Jacobi sums.

Theorem 3.3. *As above, let $p \equiv 1 \pmod{l}$. Let χ be a character on $\mathbb{Z}[\zeta]/\pi\mathbb{Z}[\zeta]$ of order l for some normalized primary prime $\pi \in \mathbb{Z}[\zeta]$ dividing p. Let $m, n \in \mathbb{Z}$ be such that $0 < m, n < l$ and $m + n \neq l$. Then $J(m, n)$ has prime factorization*

$$J(m, n) = \prod_{j \in S} \pi_{j^*},$$

where $S = \{j \mid 0 < j < l \text{ and } L(mj) + L(nj) < l\}$ and j^* is the inverse of $j \pmod{l}$.

For the remaining part of this section, let $l = 7$ and $\chi = \left(\frac{\cdot}{\pi}\right)_7$, where π is a fixed normalized prime divisor of p. We look at the prime factorization of $p \equiv 1 \pmod{7}$ in terms of normalized elements.

Lemma 3.4. *Let $\alpha \in \mathbb{Z}[\zeta]$ such that $b \not\equiv 0 \pmod 7$ and $\alpha\overline{\alpha} = p \equiv 1 \pmod 7$. Then α has a unique normalized associate.*

Proof. Existence: This follows from Lemma 2.3.

Uniqueness: Let α', and α'' be normalized associates of α with $\alpha'\overline{\alpha'} = \alpha''\overline{\alpha''} = p$. Then $\alpha' = \mu\alpha''$ for some unit $\mu \in \mathbb{Z}[\zeta]^*$. It follows that $\mu\bar{\mu} = 1$. By p. 99 of [21], $\eta_1 = \zeta + \zeta^6$ and $\eta_2 = \zeta^2 + \zeta^5$ form a system of fundamental units of $\mathbb{Q}(\zeta)$. Hence, there exist $k, m, n \in \mathbb{Z}$ such that $\mu = \pm\zeta^k\eta_1^m\eta_2^n$. Note that $\overline{\eta_1} = \eta_1$ and $\overline{\eta_2} = \eta_2$, so

$$1 = \mu\bar{\mu} = \eta_1^{2m}\eta_2^{2n}.$$

It follows that $m = n = 0$, so $\mu = \pm\zeta^k$. Now since $\alpha' \equiv \alpha'' \equiv -1 \pmod{\omega^2}$, we see that $\mu \equiv 1 \pmod{\omega^2}$, so

$$1 \equiv \pm\zeta^k \equiv \pm(1 - k\omega) \pmod{\omega^2}.$$

This forces $k \equiv 0 \pmod 7$ and the sign to be $+$, so $\mu = 1$ and hence, $\alpha' = \alpha''$ as required. □

Using normalized elements and Jacobi sums, we can now give all the factorizations of p into pairs of complex conjugates of normalized integers in $\mathbb{Z}[\zeta]$. The analog of this lemma using prime ideal factorization is given in [1], p. 146.

Lemma 3.5. *There are exactly eight distinct normalized algebraic integers $\alpha \in \mathbb{Z}[\zeta]$ such that $\alpha\overline{\alpha} = p$. These are given by $J(1,2)$, $J(3,6)$, and $J(i,i)$ for $i = 1, 2, \ldots, 6$.*

Proof. The eight listed algebraic integers are normalized by Theorem 3.2. By checking all the values m, n in Theorem 3.3, we find that there are only eight (up to associates) distinct Jacobi sums given by $J(1,2)$, $J(3,6)$, and $J(i,i)$ for $1 \le i \le 6$ with prime factorizations $\pi_1\pi_2\pi_4$, $\pi_3\pi_5\pi_6$, $\pi_1\pi_4\pi_5$, $\pi_1\pi_2\pi_3$, $\pi_1\pi_3\pi_5$, $\pi_2\pi_4\pi_6$, $\pi_4\pi_5\pi_6$, and $\pi_2\pi_3\pi_6$, respectively. For any $\alpha \in \mathbb{Z}[\zeta]$ with $\alpha\overline{\alpha} = p$, the prime factorization of α must be one of the eight listed above. Hence, α must be associate to one of the eight listed Jacobi sums. So by Lemma 3.4, the desired result follows. □

Finally, we remark that $J(i,i) = \sigma_i(J(1,1))$ for $1 \le i \le 6$. Moreover, $J(1,2)$ is easily seen to be fixed by σ_2, so $J(1,2)$ must lie in its fixed field $\mathbb{Q}(\sqrt{-7})$. Hence, $J(1,2) = t + u\sqrt{-7}$ for some $t, u \in \mathbb{Z}$. Furthermore, $\overline{J(1,2)} = \sigma_3(J(1,2)) = J(3,6)$. These observations will be used in Section 4.

4. Diophantine Equations of Dickson Type

Using cyclotomy, Dickson [4, 5] developed a system of quadratic Diophantine equations of the form

$$\begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - 4uv - u^2, \end{aligned}$$

where $x \equiv 1 \pmod 5$ and p is a rational prime such that $p \equiv 1 \pmod 5$. This system was later used by Williams to obtain certain criteria for quintic residuacity (see [28]) and an explicit formulation of the complementaries to Kummer's quintic reciprocity law (see [29]). For the purpose of the present paper, we consider a system of equations similar to the system given above. However, we now use a rational prime $p \equiv 1 \pmod 7$. We employ the system of equations (6) developed in [15]. An elementary treatment of this system is also given in [9], [25], and [26].

A summary of the results from Section 3.9 of [1], and [15] pertaining to the Diophantine system for the case $l = 7$ is presented here. Let $\zeta = e^{2\pi \mathbf{i}/7}$ be a primitive 7-th root of unity, $\omega = 1 - \zeta$, and $\mathbb{Z}[\zeta]$ the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta)$. Recall that $\mathbb{Z}[\zeta]$ is a unique factorization domain. Let $\pi \in \mathbb{Z}[\zeta]$ be a normalized primary prime divisor of p. We consider the power residue character $\chi = \left(\frac{\cdot}{\pi}\right)_7$, or equivalently, χ is a character (mod p) of order 7 with $\chi(g) = \zeta$. All throughout this section, $p \in \mathbb{Z}$ is assumed to be a rational prime such that $\alpha\overline{\alpha} = p$, where $\alpha \in \mathbb{Z}[\zeta]$ is a normalized element. So α is then one of the eight choices listed in Lemma 3.5.

Write $\alpha = \sum_{i=1}^{6} b_i \zeta^i$ with $b_i \in \mathbb{Z}$ for $1 \leq i \leq 6$. Then the coefficients of α satisfy the congruences in Lemma 2.8(c), with b_i in place of a_i. The following congruences easily follow:

$$b_1 - b_2 - b_5 + b_6 \equiv 0 \pmod 7, \tag{3}$$

$$b_1 + b_2 - 2b_3 - 2b_4 + b_5 + b_6 \equiv 0 \pmod 7. \tag{4}$$

From the coefficients of α and congruences (3) and (4), we obtain the integers $x_1, \ldots, x_6$ defined by

$$\begin{cases} x_1 = -b_1 - b_2 - b_3 - b_4 - b_5 - b_6 \\ x_2 = b_1 - b_6 \\ x_3 = b_2 - b_5 \\ x_4 = b_3 - b_4 \\ 7x_5 = b_1 + b_2 - 2b_3 - 2b_4 + b_5 + b_6 \\ 7x_6 = b_1 - b_2 - b_5 + b_6, \end{cases} \tag{5}$$

which satisfy

$$\begin{cases} 72p = 2x_1^2 + 42\left(x_2^2 + x_3^2 + x_4^2\right) + 343\left(x_5^2 + 3x_6^2\right) \\ \quad 0 = 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 \\ \qquad\qquad - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 \\ \quad 0 = 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 \\ \qquad\qquad + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6, \end{cases} \tag{6}$$

with $x_1 \equiv 1 \pmod 7$ since $x_1 = -b(\alpha) \equiv 1 \pmod 7$. The solutions of (6) are connected to certain congruences modulo p involving binomial coefficients of the form $\binom{kr}{ks}$, where $k = (p-1)/7$ and $r, s \in \mathbb{Z}$ which satisfy $1 \leq s < r \leq 6$ (see [10], for example).

It was shown in [15] that $\alpha = J(1,2) = \pi_1\pi_2\pi_4 = t + u\sqrt{-7}$, with $t, u \in \mathbb{Z}$, and its conjugate, $\overline{J(1,2)}$, give rise to four trivial solutions of (6) (trivial here means $x_5 = x_6 = 0$):

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (\pm 6t, \pm 2u, \pm 2u, \mp 2u, 0, 0).$$

Also, if $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution of (6) obtained from any of the conjugates $\sigma_i(J(1,1))$, then these six conjugates give the twelve nontrivial solutions

$$\pm(x_1, x_2, x_3, x_4, x_5, x_6) \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & -\frac{1}{2} \end{bmatrix}^i$$

where $i = 0, 1, 2, 3, 4, 5$.

Theorem 4.1. *Let p be a rational prime such that $p \equiv 1 \pmod 7$. Then the Dickson system (6) has exactly 16 integral solutions $(x_1, x_2, x_3, x_4, x_5, x_6)$, four of which are trivial and the remaining 12 are nontrivial.*

Proof. See [1], pp. 146–147. □

5. Reformulations of the Complementary Laws

We now provide a new formulation of the complementaries to Kummer's degree seven reciprocity law. As in the previous section, let ζ be a primitive 7-th root of unity, $\omega = 1 - \zeta$, and $\pi = a_1\zeta + \cdots + a_6\zeta^6 \in \mathbb{Z}[\zeta]$ a prime with $\pi \not\equiv \omega$. Suppose π divides p, where $p \equiv 1 \pmod 7$. By Lemma 2.3, we can assume that π is a normalized primary element. So $b \equiv -1 \pmod 7$ and $c \equiv 0 \pmod 7$ by Lemma 2.8, where b and c are as defined in (2) with π in place of α. Again, from Lemma 2.8 we get

$$\begin{aligned} a_1 &\equiv 2 - a_6 \pmod 7, & a_3 &\equiv 3a_5 - 2a_6 \pmod 7, \\ a_2 &\equiv 2 - a_5 \pmod 7, & a_4 &\equiv 2 - 3a_5 + 2a_6 \pmod 7. \end{aligned} \tag{7}$$

Recall that the conjugates of π can be ordered by setting $\pi_i = \sigma_i(\pi)$ for $1 \le i \le 6$, where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is determined by $\sigma_i(\zeta) = \zeta^i$. Set

$$\theta = \sum_{i=1}^{6} b_i\zeta^i = J(1,1) = \pi_1\pi_4\pi_5.$$

Then θ is normalized by Theorem 3.2 and $\theta\bar{\theta} = p$. Our goal is to express the b_i in terms of the solutions x_i of (6), then the a_i in terms of the b_i; then apply (2) and Theorem 2.7 to obtain a formula of the complementaries in terms of the x_i.

First, we show that π gives rise to a solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of Dickson's Diophantine system (6). We explicitly compute (via MAPLE) the product $\pi_1\pi_4\pi_5$ to obtain expressions for the coefficients b_i in terms of the a_i:

$$
\begin{aligned}
b_1 &= a_5^3 + a_1^2a_4 - a_1^2a_5 + a_1a_2^2 - a_1a_4^2 - a_1a_6^2 - a_2^2a_3 \\
&\quad - a_2^2a_5 + a_2^2a_6 + a_2a_3^2 - a_2a_5^2 - a_2a_6^2 - a_3^2a_4 - a_3^2a_6 - a_3a_5^2 \\
&\quad + a_3a_6^2 - a_4a_5^2 + a_4a_6^2 - a_5a_6^2 - a_1a_2a_3 + a_1a_2a_4 - a_1a_3a_4 \\
&\quad + a_1a_3a_5 + a_1a_3a_6 + a_1a_4a_5 + a_2a_3a_4 - a_2a_4a_6 + 2a_2a_5a_6 \\
&\quad + 2a_3a_4a_5 + a_3a_5a_6 - a_4a_5a_6, \\
b_2 &= a_3^3 - a_1^2a_2 + a_1a_2^2 - a_1a_3^2 + a_1a_5^2 - a_1a_6^2 - a_2^2a_3 \\
&\quad + a_2a_4^2 - a_2a_5^2 - a_3^2a_4 - a_3^2a_6 - a_3a_4^2 - a_3a_5^2 + a_4^2a_5 - a_4^2a_6 \\
&\quad - a_4a_5^2 + a_4a_6^2 - a_5a_6^2 + a_5^2a_6 + a_1a_2a_3 + a_1a_2a_4 - a_1a_2a_6 \\
&\quad - a_1a_3a_5 + 2a_1a_3a_6 - a_1a_4a_5 + a_1a_4a_6 + a_2a_3a_6 - a_2a_4a_6 \\
&\quad + a_2a_5a_6 + 2a_3a_4a_5 + a_3a_5a_6, \\
b_3 &= a_1^3 - a_1^2a_2 - a_1^2a_5 - a_1^2a_6 - a_1a_3^2 - a_1a_4^2 - a_1a_6^2 \\
&\quad - a_2^2a_4 - a_2^2a_5 + a_2^2a_6 + a_2a_4^2 - a_2a_6^2 + a_3^2a_5 - a_3a_4^2 - a_3a_5^2 \\
&\quad + a_3a_6^2 + a_4^2a_5 - a_4^2a_6 + a_4a_6^2 + a_1a_2a_3 + a_1a_2a_4 + 2a_1a_2a_5 \\
&\quad + a_1a_3a_5 + 2a_1a_4a_6 - a_1a_4a_5 + a_2a_3a_4 - a_2a_3a_5 - a_2a_3a_6 \\
&\quad + a_2a_5a_6 + a_3a_5a_6 - a_4a_5a_6, \\
b_4 &= a_6^3 + a_1^2a_3 + a_1^2a_4 - a_1^2a_5 - a_1^2a_6 - a_1a_3^2 + a_1a_5^2 \\
&\quad - a_1a_6^2 - a_2^2a_4 + a_2a_3^2 + a_2a_4^2 - a_2a_5^2 - a_2a_6^2 - a_3^2a_4 + a_3^2a_5 \\
&\quad - a_3^2a_6 - a_3a_5^2 - a_4^2a_6 - a_5a_6^2 - a_1a_2a_3 + a_1a_2a_4 + a_1a_2a_5 \\
&\quad + 2a_1a_3a_6 - a_1a_4a_5 - a_2a_3a_6 - a_2a_4a_5 + a_2a_4a_6 + 2a_2a_5a_6 \\
&\quad + a_3a_4a_5 + a_3a_5a_6 + a_4a_5a_6, \\
b_5 &= a_4^3 - a_1^2a_2 + a_1^2a_3 - a_1^2a_6 + a_1a_2^2 - a_1a_3^2 - a_1a_4^2 \\
&\quad - a_2^2a_3 - a_2^2a_4 - a_2^2a_5 + a_2^2a_6 + a_2a_3^2 - a_3^2a_4 + a_3^2a_5 - a_3a_4^2 \\
&\quad - a_4^2a_6 - a_4a_5^2 + a_5^2a_6 - a_5a_6^2 + a_1a_2a_4 + a_1a_2a_5 - a_1a_3a_5 \\
&\quad + a_1a_3a_6 + a_1a_4a_5 + 2a_1a_4a_6 - a_1a_5a_6 + 2a_2a_3a_4 - a_2a_3a_6 \\
&\quad - a_2a_4a_6 + a_3a_5a_6 + a_4a_5a_6, \\
b_6 &= a_2^3 - a_1^2a_2 + a_1^2a_3 + a_1^2a_4 - a_1^2a_5 - a_1^2a_6 - a_1a_4^2 \\
&\quad + a_1a_5^2 - a_2^2a_3 - a_2^2a_4 - a_2^2a_5 - a_2a_5^2 - a_2a_6^2 - a_3^2a_6 - a_3a_4^2 \\
&\quad + a_3a_6^2 + a_4^2a_5 - a_4a_5^2 + a_5^2a_6 - a_1a_2a_3 + a_1a_2a_4 + 2a_1a_2a_5 \\
&\quad - a_1a_3a_5 + a_1a_4a_6 + 2a_2a_3a_4 + a_2a_3a_6 + a_2a_4a_6 - a_3a_4a_6 \\
&\quad + a_3a_4a_5 + a_3a_5a_6 - a_4a_5a_6.
\end{aligned}
\tag{8}
$$

Then we use (7) to reduce the b_i modulo 7 to obtain

$$(9)\qquad \begin{cases} b_1 \equiv 2 + 2a_5 - 3a_6 \pmod 7 \\ b_2 \equiv 2 + 3a_5 + 3a_6 \pmod 7 \\ b_3 \equiv 2a_5 - a_6 \pmod 7 \\ b_4 \equiv 2 - 2a_5 + a_6 \pmod 7 \\ b_5 \equiv -3a_5 - 3a_6 \pmod 7 \\ b_6 \equiv -2a_5 + 3a_6 \pmod 7 . \end{cases}$$

By using (8), just like in Section 4, we can define the integers x_1, x_2, x_3, x_4, x_5, and x_6 as given in (5) with the first of those equations implying $x_1 \equiv 1 \pmod 7$. These x_i satisfy (6) since $\theta\overline{\theta} = p$. Solving (5) for b_1, b_2, b_3, b_4, b_5, and b_6 gives

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \end{bmatrix} = \frac{1}{12} \begin{bmatrix} -2 & 6 & 0 & 0 & 1 & 3 \\ -2 & 0 & 6 & 0 & 1 & -3 \\ -2 & 0 & 0 & 6 & -2 & 0 \\ -2 & 0 & 0 & -6 & -2 & 0 \\ -2 & 0 & -6 & 0 & 1 & -3 \\ -2 & -6 & 0 & 0 & 1 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ 7x_5 \\ 7x_6 \end{bmatrix}.$$

So

$$(10)\qquad \begin{cases} 12b_1 = -2x_1 + 6x_2 + 7x_5 + 21x_6 \\ 12b_2 = -2x_1 + 6x_3 + 7x_5 - 21x_6 \\ 12b_3 = -2x_1 + 6x_4 - 14x_5 \\ 12b_4 = -2x_1 - 6x_4 - 14x_5 \\ 12b_5 = -2x_1 - 6x_3 + 7x_5 - 21x_6 \\ 12b_6 = -2x_1 - 6x_2 + 7x_5 + 21x_6. \end{cases}$$

Hence,

$$(11)\qquad \begin{aligned} &b_1 \equiv x_1 - 3x_2 \pmod 7, \quad && b_4 \equiv x_1 + 3x_4 \pmod 7, \\ &b_2 \equiv x_1 - 3x_3 \pmod 7, && b_5 \equiv x_1 + 3x_3 \pmod 7, \\ &b_3 \equiv x_1 - 3x_4 \pmod 7, && b_6 \equiv x_1 + 3x_2 \pmod 7. \end{aligned}$$

Next, we need to express the coefficients $a_1, a_2, a_3, a_4, a_5, a_6$ of π in terms of the solutions $x_1, x_2, x_3, x_4, x_5, x_6$ of the given Diophantine system (6). It follows from (9) that $b_5 \equiv 4a_5 + 4a_6 \pmod 7$ and $b_6 \equiv 5a_5 + 3a_6 \pmod 7$. So

$$(12)\qquad a_5 \equiv -3b_5 - 3b_6 \pmod 7 \quad \text{and} \quad a_6 \equiv 3b_6 - 2b_5 \pmod 7 .$$

Now we substitute the values of b_5 and b_6 from (11) into (12) to obtain expressions for a_5 and a_6, which we then substitute into (7) to get the

values of the remaining a_i. We find

$$\begin{aligned} a_1 &\equiv 2 - x_1 - 2x_2 - x_3 \pmod 7 \\ a_2 &\equiv 2 - x_1 + 2x_2 + 2x_3 \pmod 7 \\ a_3 &\equiv x_1 - 3x_2 - x_3 \pmod 7 \\ a_4 &\equiv 2 - x_1 + 3x_2 + x_3 \pmod 7 \\ a_5 &\equiv x_1 - 2x_2 - 2x_3 \pmod 7 \\ a_6 &\equiv x_1 + 2x_2 + x_3 \pmod 7 . \end{aligned} \tag{13}$$

Note that in these formulas, we chose to express the a_i in terms of x_1, x_2, and x_3. But they could be expressed in terms of any three among the x_i.

We can now express the values of d/b, f/b, $c/7b$ and $(p-1)/7$, which were used in the explicit forms of Kummer's complementary laws in Theorem 2.7, in terms of the x_i. From (13), using $b \equiv -1 \pmod 7$ we get

$$-d \equiv -a_1 - a_2 + a_3 - a_4 + a_5 + a_6 \equiv 1 - x_1 + x_2 + 3x_3 \pmod 7 \tag{14}$$

and

$$-f \equiv -a_1 + 3a_2 + 2a_3 - 2a_4 - 3a_5 + a_6 \equiv -3x_2 + 3x_3 \pmod 7 . \tag{15}$$

Next, the value of $c/7b$ is computed from the product $6b^2c$ as shown below. We add and subtract products of the a_i to the expanded form of the expression $6b^2c$ so that it can be expressed as a linear combination of the b_i plus a multiple of 7 and a multiple of 49. Then

$$\begin{aligned} 6b^2c &= 6(a_1 + a_2 + a_3 + a_4 + a_5 + a_6)^2(a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6) \\ &= 2b_1 + 4b_2 + 6b_3 + b_4 + 3b_5 + 5b_6 + 7A + 49B \\ &\equiv 2b_1 + 4b_2 + 6b_3 + b_4 + 3b_5 + 5b_6 + 7A \pmod{49} , \end{aligned}$$

where

$$\begin{aligned} A = {} & a_2^3 + 2a_3^3 + 3a_4^3 + 4a_5^3 + 5a_6^3 + 6a_1^2a_2 + 3a_1^2a_3 + 4a_1^2a_4 + a_1^2a_5 \\ & + 2a_1^2a_6 + 3a_1a_2^2 + a_1a_3^2 + 3a_1a_4^2 + a_1a_5^2 + 6a_1a_6^2 + a_2^2a_3 + 2a_2^2a_4 \\ & + 3a_2^2a_5 + 6a_2a_3^2 + 5a_2a_5^2 + 3a_3^2a_4 + a_3^2a_5 + 5a_3^2a_6 + 5a_3a_4^2 \\ & + 6a_3a_5^2 + 4a_3a_6^2 + 2a_4^2a_5 + 5a_4a_6^2 + 5a_5^2a_6 + 2a_5a_6^2 + 3a_1a_2a_3 \\ & + 2a_1a_2a_4 + 3a_1a_2a_5 + 2a_1a_2a_6 + 2a_1a_3a_5 + a_1a_3a_6 + 4a_1a_4a_5 \\ & + a_1a_4a_6 + 5a_2a_3a_4 + 4a_2a_3a_5 + 5a_2a_3a_6 + 5a_2a_4a_5 + 6a_2a_5a_6 \\ & + 4a_3a_4a_5 + 2a_3a_4a_6 + 6a_4a_5a_6. \end{aligned}$$

From (10) we get

$$\begin{aligned} 2b_1 + 4b_2 + 6b_3 + b_4 + 3b_5 + 5b_6 & \\ &= -\frac{7}{2}x_1 - \frac{3}{2}x_2 + \frac{1}{2}x_3 + \frac{5}{2}x_4 \\ &\equiv -28x_1 - 26x_2 + 25x_3 + 27x_4 \\ &\equiv -2(14x_1 + 13x_2 + 12x_3 + 11x_4) \pmod{49} . \end{aligned}$$

Next, substitute the values of the a_i from (13) into A so that

$$A \equiv -(2x_1 + 4x_2 - 5x_3 + 4) \pmod{7}.$$

Hence,

$$6b^2c \equiv -2(14x_1 + 13x_2 + 12x_3 + 11x_4) - 7(2x_1 + 4x_2 - 5x_3 + 4) \pmod{49}.$$

It follows that

$$-\frac{c}{7} \equiv \frac{6c}{7} \equiv -2\left(2x_1 + \frac{13x_2 + 12x_3 + 11x_4}{7}\right) - (2x_1 + 4x_2 - 5x_3 + 4) \pmod{7}.$$

It is an easy exercise to show that $(13x_2 + 12x_3 + 11x_4)/7$ is an integer. Therefore,

$$-\frac{c}{7} \equiv x_1 + \frac{37x_2 + 95x_3 + 55x_4}{7} - 4 \pmod{7}. \tag{16}$$

Next we express $(p-1)/7$ in terms of the x_i. From (6), it follows that

$$\begin{aligned} 23p &\equiv 2x_1^2 + 42\left(x_2^2 + x_3^2 + x_4^2\right) \\ p &\equiv 15x_1^2 + 21\left(x_2^2 + x_3^2 + x_4^2\right) \\ p - 1 &\equiv 15x_1^2 - 1 + 21\left(x_2^2 + x_3^2 + x_4^2\right) \pmod{49}, \end{aligned}$$

so

$$\frac{p-1}{7} \equiv \frac{15x_1^2 - 1}{7} + 3\left(x_2^2 + x_3^2 + x_4^2\right) \pmod{7}. \tag{17}$$

Hence, we can now substitute (14), (15), (16), and (17) into the complementary laws in Theorem 2.7. The connection between the complementary laws and Dickson's Diophantine system is summarized in the following theorem.

Theorem 5.1. *Let $\pi \in \mathbb{Z}[\zeta]$ be a normalized primary prime factor of a rational prime $p \equiv 1 \pmod{7}$ which gives rise to the solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of Dickson's Diophantine system* (6). *Then*

$$\begin{aligned} \left(\frac{\zeta}{\pi}\right)_7 &= \zeta^{\frac{15x_1^2-1}{7}+3(x_2^2+x_3^2+x_4^2)}, \\ \left(\frac{\zeta+\zeta^6}{\pi}\right)_7 &= \zeta^{2x_1+2x_2-3x_3-2}, \\ \left(\frac{\zeta^2+\zeta^5}{\pi}\right)_7 &= \zeta^{3-3x_1-2x_2}, \\ \left(\frac{7}{\pi}\right)_7 &= \zeta^{2(x_1-1)+\frac{65x_2+88x_3+55x_4}{7}}, \\ \left(\frac{1-\zeta}{\pi}\right)_7 &= \zeta^{6x_1+5(x_2^2+x_3^2+x_4^2)+\frac{60x_1^2+5x_2+38x_3+22x_4+24}{7}-3}. \end{aligned}$$

It was shown in [16] that $(\frac{7}{p})_7 = 1$ if and only if the solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of (6) satisfies the congruence $x_2 - 19x_3 - 18x_4 \equiv 0 \pmod{49}$. This result also follows easily from Theorem 5.1 as shown in Corollary 5.3.2 of [2].

Finally, this section concludes with an example to illustrate the results above. PARI/GP [18] was used for the computations in $\mathbb{Q}(\zeta)$. We computed norms of all normalized primary elements $\sum_{i=0}^{6} a_i\zeta^i$, with small coefficients $-3 \leq a_i \leq 3$, to find some elements which do not have too large rational primes as their norms. For instance, the primes 631, 673, and 701 are norms of some normalized primary elements in $\mathbb{Z}[\zeta]$ with such small coefficients.

Example 5.2. Let $p = 631$ with the normalized primary prime factor $\pi = 2\zeta - \zeta^2 + 2\zeta^3 + 3\zeta^5$, which yields $(b_1, b_2, b_3, b_4, b_5, b_6) = (15, -3, -15, 3, -9, 1)$. Then $(x_1, x_2, x_3, x_4, x_5, x_6) = (8, 14, 6, -18, 4, 4)$, and from Theorem 5.1 it follows that

$$\left(\frac{\zeta}{\pi}\right)_7 = \zeta^6,\ \left(\frac{7}{\pi}\right)_7 = \zeta,\ \left(\frac{\zeta+\zeta^6}{\pi}\right)_7 = \zeta^3,\ \left(\frac{\zeta^2+\zeta^5}{\pi}\right)_7 = 1,\ \left(\frac{1-\zeta}{\pi}\right)_7 = \zeta^3.$$

Acknowledgement

I would like to express my deepest gratitude to Dr. Renate Scheidler for her invaluable comments and suggestions for the improvement of this work.

References

1. B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. Series of Monographs and Advanced Texts, vol. 21, John Wiley and Sons, Inc., New York, USA, 1998.
2. P. Caranay, *On Residue Symbols and Kummer's Reciprocity Law of Degree Seven*, Master's thesis, University of Calgary, Canada, 2009.
3. P. Caranay and R. Scheidler, *An efficient seventh power residue symbol algorithm*, Int. J. Number Theory **6** (2010), no. 8, 1831–1853.
4. L. E. Dickson, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. **37** (1935), 363–380.
5. ———, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
6. G. Eisenstein, *Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahen*, J. Reine Angew. Math. **27(4)** (1844), 289–310.
7. ———, *Nachtrag zum cubischen Reciprocitätssatzes für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahen. Criterien des cubischen Characters der Zahl 3 und ihrer Theiler.*, J. Reine Angew. Math. **28(1)** (1844), 28–35.
8. C. Friesen, B. K. Spearman, and K. S. Williams, *Another proof of Eisenstein's law of cubic reciprocity and its supplement*, Rocky Mountain J. Math. **16** (1986), no. 2, 395–402.
9. R. H. Hudson and K. S. Williams, *A new criterion for 7 to be a fourth power* (mod p), Israel J. Math. **38** (1981), no. 3, 221–230.
10. ———, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), no. 2, 431–505.

11. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., GTM 84, Springer Science + Business Media LLC, New York, USA, 1990.
12. E. E. Kummer, *Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste*, Collected Papers, vol. I, Springer-Verlag, Berlin, Germany, 1975, Edited by André Weil., pp. 345–357.
13. _____, *Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Collected Papers, vol. I, Springer-Verlag, Berlin, Germany, 1975, Edited by André Weil., pp. 699–839.
14. F. Lemmermeyer, *Reciprocity Laws from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, Germany, 2000.
15. P. A. Leonard and K. S. Williams, *A Diophantine system of Dickson*, Atti. Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. **56** (1974), no. 8, 145–150.
16. _____, *The septic character of 2, 3, 5, and 7*, Pacific Journal of Mathematics **52** (1974), no. 1, 143–147.
17. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286–287** (1976), 248–256.
18. The PARI Group, Bordeaux, *PARI/GP, version* `2.3.3`, 2008, Avalaible from `http://pari.math.u-bordeaux.fr/`.
19. R. Scheidler, *Applications of Algebraic Number Theory to Cryptography*, Ph.D. thesis, University of Manitoba, Winnipeg, Canada, 1993.
20. R. Scheidler and H. C. Williams, *A public-key cryptosystem utilizing cyclotomic fields*, Designs, Codes, and Cryptography **6** (1995), 117–131.
21. H. J. S. Smith, *Report on the Theory of Numbers*, Collected Mathematical Papers, vol. I, Chelsea Publishing Company, New York, USA, 1979.
22. L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., GTM 83, Springer-Verlag, New York, USA, 1997.
23. H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Trans. Inf. Theory **IT-26** (1980), no. 6, 726–7290.
24. _____, *An M^3 public-key encryption scheme*, Lecture Notes in Computer Science: Advances in Cryptology–CRYPTO '85 Proceedings, vol. 218, Springer, Berlin, 1986, pp. 358–368.
25. K. S. Williams, *Elementary treatment of a quadratic partition of primes $p \equiv 1 (\mathrm{mod}\ 7)$*, Illinois J. of Math. **18** (1974), no. 4, 608–621.
26. _____, *A quadratic partition of primes $p \equiv 1 (\mathrm{mod}\ 7)$*, Math. Comp. **28** (1974), 1133–1136.
27. _____, *Note on the supplement to the law of cubic reciprocity*, Proc. Amer. Math. Soc. **47** (1975), 333–334.
28. _____, *Explicit criteria for quintic residuacity*, Math. Comp. **30** (1976), 847–853.
29. _____, *Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity*, J. Reine Angew. Math. **288** (1976), 207–210.
30. _____, *On Eisenstein's supplement to the law of cubic reciprocity*, J. Reine Angew. Math. **288** (1977), 207–210.

Department of Mathematics and Statistics, University of Calgary
2500 University Drive NW, Calgary AB, Canada, T2N 1N4
E-mail address: `pcaranay@ucalgary.ca`