

Kubota Symbol

Meng-Hsuan Wu

Advisor: Prof. Daniel Bump

Mathematics Department, Stanford University

June 15, 2008

1 Introduction

In 1964, Kubota showed in [1] the surprising result that for every $m \geq 2$ and totally complex algebraic number field F containing the m -th roots of unity, the m -th power Kubota symbol defined in Equation (1.4) is multiplicative on certain congruence subgroups Γ_M (defined in Equation (1.1)) of $SL_2(O)$, where O is the ring of integers of F . Therefore, the Kubota symbol can be used to construct a linear character of Γ_M . Furthermore, Kubota showed that this character is non-trivial.

While Kubota had shown that the Kubota symbol is multiplicative for $M = m^2$, he had not given the best possible value of M . In this thesis, we consider the cases that F is a cyclotomic field $\mathbb{Q}(\zeta_n)$, and for a few pairs of n and m we determine the best possible value of M .

For each $n, m \in \mathbb{N}$ such that $m \mid n$, let F_n be the cyclotomic field $\mathbb{Q}(\zeta_n)$, $D_n = \mathbb{Z}[\zeta_n]$ be the ring of integers of F_n , μ_m be the group of the m -th roots of unity, and $M = \prod_{i=1}^n (1 - \zeta_{p_i}^{r_i})^{k_i}$ where $p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ is the prime factorization of n in \mathbb{Z} and $k_1, k_2, \dots, k_n \in \mathbb{N}$ [3]. Let Γ_M be the set of 2×2 invertible matrices in D_n which are congruent to the identity modulo M , namely

$$\Gamma_M := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_{2 \times 2}(D_n) \mid \alpha \equiv \delta \equiv 1, \beta \equiv \gamma \equiv 0 \pmod{M}, \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1 \right\}. \quad (1.1)$$

The definition of the Kubota symbol depends on the power residue symbol, which generalizes the Legendre symbol. The power residue symbol satisfies a reciprocity law, which generalizes the quadratic reciprocity law and plays a key role in this thesis. Next we define the power residue symbol.

Definition (m -th power residue symbol). For each $\alpha, \pi \in D_n$ where π is a prime in D_n which does not divide m , define

$$\left(\frac{\alpha}{\pi}\right) = \begin{cases} 0, & \text{if } \pi \mid \alpha \\ \text{the unique value in } \mu_m \text{ such that } \left(\frac{\alpha}{\pi}\right) \equiv \alpha^{(N\pi-1)/m}(\pi), & \text{otherwise.} \end{cases} \quad (1.2)$$

Definition (Generalized m -th power residue symbol). For each $\alpha, \beta \in D$ such that $\gcd(N\beta, m) = 1$, define

$$\left(\frac{\alpha}{\beta}\right) = \prod_{i=1}^n \left(\frac{\alpha}{\pi_i}\right), \quad (1.3)$$

where $\prod_{i=1}^n \pi_i$ is the prime decomposition of β .

Now we can define the Kubota symbol:

Definition (m -th power Kubota symbol). For each $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_M$, we define

$$\mathcal{K}_m(g) = \left(\frac{\gamma}{\delta}\right) \quad (1.4)$$

where (\cdot) is the generalized m -th residue symbol defined above in Equation (1.3).

In this thesis, for each of the following cases: (i) $n = m = 3$, (ii) $n = m = 4$, (iii) $n = 4, m = 2$ we found the best value of M , i.e. for each case we determined the minimum values of k such that \mathcal{K}_m is multiplicative on $\Gamma_{(1-\zeta_n)^k}$. We also observed some preliminary results for the case $n = m = 8$.

2 Case of $n = m = 3$

In this section, we denote ζ_3 , the primitive cube root of 1, as ω .

Theorem 2.1. *The minimum value of k such that $\mathcal{K}_3(gg') = \mathcal{K}_3(g)\mathcal{K}_3(g')$ for all $g, g' \in \Gamma_{(1-\omega)^k}$ is $k = 2$.*

To prove the theorem, we first need the following results.

Definition (Primary primes in D_3). A prime $\pi \in D_3$ is called primary if $\pi \equiv 1 \pmod{3}$.

By Proposition 9.3.5 of [2] and the facts that -1 is a unit of D_3 and $(-1) \cdot 2 \equiv 1 \pmod{3}$, for each prime $\pi \in D_3$ such that $N\pi \neq 3$, exactly one of its six associates is primary.

Lemma 2.2. *For every $d \in D_3$ such that $d \equiv 1 \pmod{3}$, there exists a factorization $\pi_1\pi_2 \cdots \pi_r$ of d such that π_i is a primary prime for all $1 \leq i \leq r$. We call $\pi_1\pi_2 \cdots \pi_r$ a primary factorization of d .*

Proof. Let $\pi_1\pi_2 \cdots \pi_r$ be any prime decomposition of d . For each $1 \leq i \leq r$, let ε_i be the unique unit in d such that $\varepsilon_i\pi_i \equiv 1 \pmod{3}$ and denote $\pi'_i = \varepsilon_i\pi_i$. Then $d' = \pi'_1\pi'_2 \cdots \pi'_r$ is an associate of d since $d' = (\varepsilon_1\pi_1)(\varepsilon_2\pi_2) \cdots (\varepsilon_r\pi_r) = (\varepsilon_1\varepsilon_2 \cdots \varepsilon_r)(\pi_1\pi_2 \cdots \pi_r) = (\varepsilon_1\varepsilon_2 \cdots \varepsilon_r)d$. Note that $d' \equiv d \pmod{3}$ because $d' \equiv \prod_{i=1}^r \pi'_i \equiv 1^r = 1 \equiv d \pmod{3}$. Since the unique unit $\varepsilon \in D_3$ such that $\varepsilon d \equiv d \pmod{3}$ is $\varepsilon = 1$, we have $\varepsilon_1\varepsilon_2 \cdots \varepsilon_r = 1$, and therefore $\pi'_1\pi'_2 \cdots \pi'_r$ is a primary factorization of d . \square

Lemma 2.3 (Cubic reciprocity law). *For every $c, d \in D_3$ such that $c \equiv d \equiv 1 \pmod{3}$, we have $\left(\frac{c}{d}\right) = \left(\frac{d}{c}\right)$.*

Proof. First consider the special case that c, d are primes in D_3 . In this case, note that $\left(\frac{c}{d}\right) = \left(\frac{-c(-1)^3}{d}\right) = \left(\frac{-c}{d}\right) \left(\frac{-1}{d}\right)^3 = \left(\frac{-c}{d}\right) = \left(\frac{-c}{-d}\right)$ and similarly $\left(\frac{d}{c}\right) = \left(\frac{-d}{c}\right)$. By Theorem 1 of Section 9.3 of [2], we have $\left(\frac{c}{d}\right) = \left(\frac{-c}{-d}\right) = \left(\frac{-d}{-c}\right) = \left(\frac{d}{c}\right)$.

In general case, by Lemma 2.2 there exists primary factorizations $\pi_1\pi_2 \cdots \pi_q$ and $\rho_1\rho_2 \cdots \rho_r$ of c and d , respectively. Then by the special case above we have $\left(\frac{c}{d}\right) = \left(\frac{\pi_1\pi_2 \cdots \pi_q}{\rho_1\rho_2 \cdots \rho_r}\right) = \prod_{\substack{1 \leq i \leq q \\ 1 \leq j \leq r}} \left(\frac{\pi_i}{\rho_j}\right) = \prod_{\substack{1 \leq i \leq q \\ 1 \leq j \leq r}} \left(\frac{\rho_j}{\pi_i}\right) = \left(\frac{\rho_1\rho_2 \cdots \rho_r}{\pi_1\pi_2 \cdots \pi_q}\right) = \left(\frac{d}{c}\right)$. \square

Lemma 2.4. *For every $c, d, d' \in D_3$ such that $d \equiv d' \equiv 1 \pmod{3}$, $d \equiv d' \pmod{9}$, and $d \equiv d' \pmod{c}$, we have $\left(\frac{c}{d}\right) = \left(\frac{c}{d'}\right)$.*

Proof. Let $c = c_0(-1)^s\omega^t(1-\omega)^u$ where $c_0 \equiv 1 \pmod{3}$. Then by Lemma 2.3 we have $\left(\frac{c}{d}\right) = \left(\frac{(-1)^s\omega^t(1-\omega)^u}{d}\right) \left(\frac{c_0}{d}\right) = \left(\frac{(-1)^s\omega^t(1-\omega)^u}{d}\right) \left(\frac{d}{c_0}\right)$ and similarly $\left(\frac{c}{d'}\right) = \left(\frac{(-1)^s\omega^t(1-\omega)^u}{d'}\right) \left(\frac{d'}{c_0}\right)$. Since $d \equiv d' \pmod{c_0}$, we have $\left(\frac{d}{c_0}\right) = \left(\frac{d'}{c_0}\right)$, and therefore we only need to show that $\left(\frac{(-1)^s\omega^t(1-\omega)^u}{d}\right) = \left(\frac{(-1)^s\omega^t(1-\omega)^u}{d'}\right)$.

Let $d = 1 + 3(m_0 + n_0\omega)$ and the primary factorization of d be $\pi_1 \cdots \pi_r$ where $\pi_i = 1 + 3(m_i + n_i\omega)$ for each $1 \leq i \leq r$. By the definition of the cubic residue symbol, for each $1 \leq i \leq r$ we have $\left(\frac{\omega}{\pi_i}\right) = \omega^{(N\pi_i-1)/3} =$

$\omega^{((3m_i+1)^2-(3m_i+1)(3n_i)+(3n_i)^2)/3} = \omega^{3(m_i^2-m_in_i+n_i^2+m_i)-m_i-n_i} = \omega^{-m_i-n_i}$. And by Theorem 1' of Section 9.3 of [2], $\left(\frac{1-\omega}{\pi_i}\right) = \left(\frac{1-\omega}{-\pi_i}\right) = \left(\frac{1-\omega}{(-3m_i-1)-3n_i\omega}\right) = \omega^{2(-m_i)} = \omega^{m_i}$. It can be easily checked that $m_0 \equiv \sum_{i=1}^r m_i$ (3) and $n_0 \equiv \sum_{i=1}^r n_i$ (3), thus we have $\left(\frac{\omega}{d}\right) = \prod_{i=1}^r \left(\frac{\omega}{\pi_i}\right) = \prod_{i=1}^r \omega^{-m_i-n_i} = \omega^{\sum_{i=1}^r (-m_i-n_i)} = \omega^{-m_0-n_0}$, and similarly $\left(\frac{1-\omega}{d}\right) = \omega^{m_0}$.

Let $d' = 1 + 3(m'_0 + n'_0\omega)$, then since $d \equiv d'$ (9) we have $m_0 \equiv m'_0$ (3) and $n_0 \equiv n'_0$ (3). Thus we have $\left(\frac{\omega}{d}\right) = \omega^{-m_0-n_0} = \omega^{-m'_0-n'_0} = \left(\frac{\omega}{d'}\right)$ and $\left(\frac{1-\omega}{d}\right) = \omega^{m_0} = \omega^{m'_0} = \left(\frac{1-\omega}{d'}\right)$. Together with the fact that $\left(\frac{-1}{d}\right) = \left(\frac{-1}{d'}\right) = 1$, we have $\left(\frac{(-1)^s \omega^t (1-\omega)^u}{d}\right) = \left(\frac{(-1)^s \omega^t (1-\omega)^r}{d'}\right)$. This completes the proof of this lemma. \square

Proof of Theorem 2.1. We prove the theorem by showing that \mathcal{K}_3 is multiplicative on $\Gamma_{(1-\omega)^k}$ for $k = 2$ but not for $k = 1$.

When $k = 2$, let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, g' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \Gamma_{(1-\omega)^2}$, and $g'' = gg' = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix}$. Then $g = g''(g')^{-1} = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix} \begin{pmatrix} \delta' & -\beta' \\ -\gamma' & \alpha' \end{pmatrix}$. By comparing the matrices on both sides of the equation above, we have

$$\gamma = \gamma''\delta' - \delta''\gamma'. \quad (2.1)$$

Let θ_1 be any greatest common divisor of δ' and δ'' . Since that $\delta' \equiv \delta'' \equiv 1$ (3) and that $(1-\omega) \mid 3$, we have $\delta' \equiv \delta'' \equiv 1$ (3), and therefore $(1-\omega)$ does not divide θ_1 . Thus we can pick the associate θ of θ_1 such that $\theta \equiv 1$ (3). Denote $\delta' = \delta'_0\theta$ and $\delta'' = \delta''_0\theta$, then we have $\delta' \equiv \delta'' \equiv 1$ (3). Since $\theta \mid \delta', \delta''$, we have $\theta \mid \gamma''\delta' - \delta''\gamma' = \gamma$. Let $\gamma = \gamma_0\theta$, then (2.1) can be rewritten as

$$\gamma_0\theta = \gamma''\delta'_0\theta - \delta''_0\gamma'\theta,$$

which implies

$$\gamma_0 = \gamma''\delta'_0 - \delta''_0\gamma'. \quad (2.2)$$

Thus we have

$$\left(\frac{\gamma''}{\delta''}\right) = \left(\frac{\gamma''}{\delta''_0}\right) \left(\frac{\gamma''}{\theta}\right) = \left(\frac{\gamma''\delta'_0}{\delta''_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right). \quad (2.3)$$

By (2.2) we have $\gamma_0 \equiv \gamma''\delta'_0$ (δ''_0), thus $\left(\frac{\gamma''\delta'_0}{\delta''_0}\right) = \left(\frac{\gamma_0}{\delta''_0}\right)$, and consequently (2.3) can be rewritten as

$$\left(\frac{\gamma''}{\delta''}\right) = \left(\frac{\gamma_0}{\delta''_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right). \quad (2.4)$$

Since $\delta'' = \delta\delta' + \gamma\beta' \equiv \delta\delta' \pmod{9}$ and $3 \mid \gamma, \beta'$, we have $\delta'' \equiv \delta\delta' \pmod{9}$, namely $\delta''\theta \equiv \delta\delta'_0\theta \pmod{9}$. And since we have picked θ such that $\theta \equiv 1 \pmod{3}$, we have $\gcd(\theta, 9) = 1$, and therefore $\delta''_0 \equiv \delta\delta'_0 \pmod{9}$. Furthermore, since the equation $\delta'' = \delta\delta' + \gamma\beta'$ can be rewritten as $\delta''_0\theta = \delta\delta'_0\theta + \gamma_0\theta\beta'$, we have $\delta''_0\theta \equiv \delta\delta'_0\theta \pmod{9}$, and consequently $\delta''_0 \equiv \delta\delta'_0 \pmod{9}$. By Lemma 2.4, $\left(\frac{\gamma_0}{\delta''_0}\right) = \left(\frac{\gamma_0}{\delta\delta'_0}\right) = \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma_0}{\delta'_0}\right)$, so (2.4) can be rewritten as

$$\left(\frac{\gamma''}{\delta''}\right) = \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma_0}{\delta'_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right). \quad (2.5)$$

Using (2.2) again we have $\gamma_0 \equiv -\delta''_0\gamma' \pmod{9}$, thus

$$\begin{aligned} \mathcal{K}_3(g'') &= \left(\frac{\gamma''}{\delta''}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{-\delta''_0\gamma'}{\delta'_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{-1}{\delta'_0}\right) \left(\frac{\delta''_0}{\delta'_0}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\delta''_0}{\delta'_0}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\delta'_0}{\delta''_0}\right)^{-1} \left(\frac{\gamma''}{\theta}\right) \left(\text{since } \left(\frac{-1}{\delta'_0}\right) = \left(\frac{(-1)^3}{\delta'_0}\right) = \left(\frac{-1}{\delta'_0}\right)^3 = 1\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\gamma''}{\theta}\right) \left(\text{we have } \left(\frac{\delta''_0}{\delta'_0}\right) = \left(\frac{\delta'_0}{\delta''_0}\right) \text{ by Lemma 2.3}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\delta\gamma'}{\theta}\right) \left(\text{since } \gamma'' = \gamma\alpha' + \delta\gamma' = \gamma_0\theta\alpha' + \delta\gamma' \equiv \delta\gamma' \pmod{9}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\delta}{\theta}\right) \left(\frac{\gamma'}{\theta}\right) \\ &= \left(\frac{\gamma_0}{\delta}\right) \left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\theta}{\delta}\right) \left(\frac{\gamma'}{\theta}\right) \left(\text{By Lemma 2.3}\right) \\ &= \left(\left(\frac{\gamma_0}{\delta}\right) \left(\frac{\theta}{\delta}\right)\right) \left(\left(\frac{\gamma'}{\delta'_0}\right) \left(\frac{\gamma'}{\theta}\right)\right) \\ &= \left(\frac{\gamma_0\theta}{\delta}\right) \left(\frac{\gamma'}{\delta'_0\theta}\right) \\ &= \left(\frac{\gamma}{\delta}\right) \left(\frac{\gamma'}{\delta'}\right) \\ &= \mathcal{K}_3(g)\mathcal{K}_3(g'), \end{aligned}$$

and therefore \mathcal{K}_3 is multiplicative for $k = 2$.

To conclude the proof, we propose a counterexample to show that \mathcal{K}_3 is not multiplicative for $k = 1$. Consider the matrices $g = \begin{pmatrix} 4\omega & 3\omega \\ 3\omega + 3 & 2\omega + 2 \end{pmatrix}$ and $g' = \begin{pmatrix} -2 & 3\omega \\ 3\omega + 3 & 4 \end{pmatrix}$. Although $g, g' \in \Gamma_{1-\omega}$, we have $\mathcal{K}_3(g)\mathcal{K}_3(g') = \omega^2 \cdot \omega = 1 \neq \omega = \mathcal{K}_3(gg')$. Thus $k = 2$ is the minimum value of k such that \mathcal{K}_3 is multiplicative. \square

3 Case of $n = m = 4$

Since $(1 - i)^k$ and $(1 + i)^k$ are associates, we have $\Gamma_{(1-i)^k} = \Gamma_{(1+i)^k}$. For convenience, in this and next sections we denote $\Gamma_{(1-i)^k}$ as $\Gamma_{(1+i)^k}$.

Theorem 3.1. *The minimum value of k such that $\mathcal{K}_4(gg') = \mathcal{K}_4(g)\mathcal{K}_4(g')$ for all $g, g' \in \Gamma_{(1+i)^k}$ is $k = 4$.*

To prove the theorem, we first need the following results.

Definition (Primary primes in D_4). *A prime $\pi \in D_4$ is called primary if $\pi \equiv 1 \pmod{(1+i)^3}$.*

Since the natural homomorphism $D_4^\times \rightarrow (D_4/((1+i)^3D_4))^\times$ is bijective, for each prime $\pi \in D_4$ such that $N\pi \neq 2$ exactly one of its four associates is primary.

Lemma 3.2. *For every $d \in D_4$ such that $d \equiv 1 \pmod{(1+i)^3}$, there exists a factorization $\pi_1\pi_2 \cdots \pi_r$ of d such that π_i is a primary prime for all $1 \leq i \leq r$. Furthermore, we have $\text{ord}_{1+i}(d-1) = 3$ if and only if there are an odd number of factors π_i such that $\text{ord}_{1+i}(\pi_i - 1) = 3$. We call $\pi_1\pi_2 \cdots \pi_r$ a primary factorization of d .*

Proof. Let $\pi_1\pi_2 \cdots \pi_r$ be any prime decomposition of d . For each $1 \leq i \leq r$, let ε_i be the unique unit in d such that $\varepsilon_i\pi_i \equiv 1 \pmod{(1+i)^3}$ and denote $\pi'_i = \varepsilon_i\pi_i$. Then $d' = \pi'_1\pi'_2 \cdots \pi'_r$ is an associate of d since $d' = (\varepsilon_1\pi_1)(\varepsilon_2\pi_2) \cdots (\varepsilon_r\pi_r) = (\varepsilon_1\varepsilon_2 \cdots \varepsilon_r)(\pi_1\pi_2 \cdots \pi_r) = (\varepsilon_1\varepsilon_2 \cdots \varepsilon_r)d$. Note that $d' \equiv d \pmod{(1+i)^3}$ because $d' \equiv \prod_{i=1}^r \pi'_i \equiv 1^r = 1 \equiv d \pmod{(1+i)^3}$. Since the unique unit $\varepsilon \in D_4$ such that $\varepsilon d \equiv d \pmod{(1+i)^3}$ is $\varepsilon = 1$, we have $\varepsilon_1\varepsilon_2 \cdots \varepsilon_r = 1$, and therefore $\pi'_1\pi'_2 \cdots \pi'_r$ is a primary factorization of d .

For each $1 \leq i \leq r$, since π_i is a primary prime we have $\text{ord}_{1+i}(\pi_i - 1) \geq 3$, that is $\pi_i \equiv 1 \pmod{(1+i)^3}$. This implies that $\pi_i \equiv 1$ or $3 + 2i \pmod{(1+i)^4}$ and the latter case happens precisely when $\text{ord}_{1+i}(\pi_i - 1) \geq 4$, we can infer that

$\pi_i \equiv \begin{cases} 3 + 2i ((1+i)^4), & \text{ord}_{1+i}(\pi_i - 1) = 3 \\ 1 ((1+i)^4), & \text{ord}_{1+i}(\pi_i - 1) \neq 3 \end{cases}$. Suppose that there are q primes π_i such that $\text{ord}_{1+i}(\pi_i - 1) = 3$, then since $(3 + 2i)^2 \equiv 1 ((1+i)^4)$, we have $d = \prod_{i=1}^r \pi_i \equiv (3 + 2i)^q 1^{r-q} \equiv \begin{cases} 3 + 2i ((1+i)^4) & q \text{ odd} \\ 1 ((1+i)^4) & q \text{ even} \end{cases}$, that is $\text{ord}_{1+i}(d - 1) = 3$ if q is odd and $\text{ord}_{1+i}(d - 1) \geq 4$ if q is even. \square

Lemma 3.3 (Quartic reciprocity law). *For every $c, d \in D_4$ such that $c \equiv d \equiv 1 ((1+i)^3)$, we have $\left(\frac{c}{d}\right) = \left(\frac{d}{c}\right) (-1)^{\frac{N(c)-1}{4} \cdot \frac{N(d)-1}{4}}$.*

Proof. First note that this theorem holds for the special case that c, d are primes in D_4 by Theorem 2 of Chapter 9 of [2].

In general case, by Lemma 3.2 there exists primary factorizations $\pi_1 \pi_2 \cdots \pi_q$ and $\rho_1 \rho_2 \cdots \rho_r$ of c and d , respectively. Then by the special case above we have $\left(\frac{c}{d}\right) = \left(\frac{\pi_1 \pi_2 \cdots \pi_q}{\rho_1 \rho_2 \cdots \rho_r}\right) = \prod_{\substack{1 \leq i \leq q \\ 1 \leq j \leq r}} \left(\frac{\pi_i}{\rho_j}\right) = \prod_{\substack{1 \leq i \leq q \\ 1 \leq j \leq r}} \left(\frac{\rho_j}{\pi_i}\right) = \left(\frac{\rho_1 \rho_2 \cdots \rho_r}{\pi_1 \pi_2 \cdots \pi_q}\right) = \left(\frac{d}{c}\right)$. \square

The quartic characters for i and $1+i$ need to be handled separately.

Lemma 3.4 (quartic character for i). *For every $d \in D_4$ such that $d \equiv 1 ((1+i)^3)$, we have $\left(\frac{i}{d}\right)_4 = i^{\frac{3a-3}{2}}$.*

Proof. For the special case that $d = a + bi$ is a prime in D_4 , by Equation (1.2) we have $\left(\frac{i}{d}\right)_4 = i^{\frac{Nd-1}{4}} = i^{\frac{a^2+b^2-1}{4}}$. Examine the possibilities of a, b modulo 8, we have

a (8)	b (8)	$a^2 + b^2 - 1$ (16)	$\frac{a^2+b^2-1}{4}$ (4)
1	0, 4	0	0
3	2, 6	12	3
5	0, 4	8	2
7	2, 6	4	1

From the table above, for every a, b such that $d \equiv 1 ((1+i)^3)$ we have $\frac{a^2+b^2-1}{4} \equiv \frac{3a-3}{2} (4)$. Thus $\left(\frac{i}{d}\right)_4 = i^{\frac{a^2+b^2-1}{4}}$ can be simplified as $\left(\frac{i}{d}\right)_4 = i^{\frac{3a-3}{2}}$.

For the general case, let $\pi_1 \pi_2 \cdots \pi_r$ be a primary decomposition of d , and we prove this lemma by applying mathematical induction on r . From the special case above, this lemma holds for $r = 1$. Suppose that this lemma holds for $r = k$, namely $\left(\frac{i}{\pi_1 \pi_2 \cdots \pi_k}\right)_4 = i^{\frac{3(2a_1+1)-3}{2}}$ where $\pi_1 \pi_2 \cdots \pi_k = 1 + 2(a_1 + b_1)i$. When $r = k + 1$, let $\pi_{k+1} = 1 + 2(a_2 + b_2)i$. Since $1 + 2(a_1 + b_1)i \equiv 1 + 2(a_2 + b_2)i \equiv 1 ((1+i)^3)$, a_1 and b_1 have the same parity, and so are a_2 and b_2 . Furthermore, $\pi_1 \pi_2 \cdots \pi_{k+1} = 1 + 2(a_3 + b_3)i$ where

$a_3 = a_1 + a_2 + 2(a_1a_2 - b_1b_2)$ and $b_3 = b_1 + b_2 - 2(a_1b_2 + a_2b_1)$. By the induction assumption,

$$\begin{aligned}
\left(\frac{i}{\pi_1\pi_2\cdots\pi_{k+1}}\right)_4 &= \left(\frac{i}{\pi_1\pi_2\cdots\pi_k}\right)_4 \left(\frac{i}{\pi_{k+1}}\right)_4 \\
&= i^{\frac{3((2a_1+1)-1)}{2}} i^{\frac{3((2a_2+1)-1)}{2}} \\
&= i^{3(a_1+a_2)} \\
&= i^{3(a_1+a_2+2(a_1a_2-b_1b_2))} \\
&\quad (\text{since } a_1a_2 \text{ and } b_1b_2 \text{ have the same parity, } 4 \mid 2(a_1a_2 - b_1b_2)) \\
&= i^{3a_3} \\
&= i^{\frac{3((2a_3+1)-1)}{2}}.
\end{aligned}$$

Thus this lemma holds for $r = k + 1$ as well. \square

Lemma 3.5 (quartic character for $1 + i$). *For every $d \in D_4$ such that $d \equiv 1 \pmod{4}$, we have $\left(\frac{1+i}{d}\right)_4 = i^{\frac{a-b-b^2-1}{4}}$.*

Proof. For the special case that $d = a + bi$ is a prime in D_4 , by Exercise 9.37 of [2] we have $\left(\frac{1+i}{d}\right)_4 = i^{\frac{a-b-b^2-1}{4}}$.

For the general case, let $\pi_1\pi_2\cdots\pi_r$ be a primary decomposition of d , and we prove this lemma by applying mathematical induction on r . From the special case above, this lemma holds for $r = 1$. Suppose that this lemma holds for $r = k$, namely $\left(\frac{1+i}{\pi_1\pi_2\cdots\pi_k}\right)_4 = i^{\frac{a_1-b_1-b_1^2-1}{4}}$ where $\pi_1\pi_2\cdots\pi_k = 1 + 2(a_1 + b_1)i$. When $r = k + 1$, let $\pi_{k+1} = 1 + 2(a_2 + b_2)i$. Since $1 + 2(a_1 + b_1)i \equiv 1 + 2(a_2 + b_2)i \equiv 1 \pmod{4}$, a_1 and b_1 have the same parity, and so are a_2 and b_2 . Furthermore, $\pi_1\pi_2\cdots\pi_{k+1} = 1 + 2(a_3 + b_3)i$ where $a_3 = a_1 + a_2 + 2(a_1a_2 - b_1b_2)$ and $b_3 = b_1 + b_2 - 2(a_1b_2 + a_2b_1)$. By the induction assumption,

$$\begin{aligned}
\left(\frac{1+i}{\pi_1\pi_2\cdots\pi_{k+1}}\right)_4 &= \left(\frac{1+i}{\pi_1\pi_2\cdots\pi_k}\right)_4 \left(\frac{1+i}{\pi_{k+1}}\right)_4 \\
&= i^{\frac{(2a_1+1)-(2b_1)-(2b_1)^2-1}{4}} i^{\frac{(2a_2+1)-(2b_2)-(2b_2)^2-1}{4}} \\
&= i^{\frac{a_1-b_1-b_1^2}{2}} i^{\frac{a_2-b_2-b_2^2}{2}} \\
&= i^{\frac{(a_1-b_1)-b_1^2}{2} + \frac{(a_2-b_2)-b_2^2}{2}}.
\end{aligned}$$

Note that

$$\begin{aligned}
& \frac{a_3 - b_3}{2} - b_3^2 \\
= & \frac{(a_1 + a_2 + 2(a_1a_2 - b_1b_2)) - (b_1 + b_2 - 2(a_1b_2 + a_2b_1))}{2} + (b_1 + b_2 - 2(a_1b_2 + a_2b_1))^2 \\
\equiv & \frac{(a_1 + a_2 + 2(a_1a_2 - b_1b_2)) - (b_1 + b_2 - 2(a_1b_2 + a_2b_1))}{2} + (b_1 + b_2)^2 \\
= & \frac{(a_1 - b_1) + (a_2 - b_2)}{2} + (a_1 + b_1)(a_2 + b_2) - 2b_1b_2 + (b_1 + b_2)^2 \\
= & \frac{(a_1 - b_1)}{2} - b_1^2 + \frac{(a_2 - b_2)}{2} - b_2^2 + (a_1 + b_1)(a_2 + b_2) \\
\equiv & \frac{(a_1 - b_1)}{2} - b_1^2 + \frac{(a_2 - b_2)}{2} - b_2^2 \pmod{4}, \\
& \text{(since } a_1 + b_1 \text{ and } a_2 + b_2 \text{ are both even, } 4 \mid (a_1 + b_1)(a_2 + b_2)\text{)}
\end{aligned}$$

so

$$\begin{aligned}
\left(\frac{1+i}{\pi_1\pi_2\cdots\pi_{k+1}} \right)_4 &= i^{\frac{a_3-b_3}{2} - b_3^2} \\
&= i^{\frac{(2a_3+1)-(2b_3)-(2b_3)^2-1}{4}}.
\end{aligned}$$

Thus this lemma holds for $r = k + 1$ as well. \square

Lemma 3.6. *Let $c, d, d' \in D_4$, and $c = c_0i^s(1+i)^t$ where $c_0 \equiv 1((1+i)^3)$. If $d \equiv d' \equiv 1((1+i)^3)$, $d \equiv d'((1+i)^6)$, and $d \equiv d'(c)$, we have $\left(\frac{c}{d}\right)_4 = \left(\frac{c}{d'}\right)_4(-1)^{t\frac{N(d-d')}{64}}$.*

Proof. Let $c = c_0i^s(1+i)^t$ where $c_0 \equiv 1((1+i)^3)$. Then by Lemma 3.3 we have

$$\left(\frac{c}{d}\right)_4 = \left(\frac{c_0i^s(1+i)^t}{d}\right)_4 = \left(\frac{c_0}{d}\right)_4 \left(\frac{i}{d}\right)_4^s \left(\frac{1+i}{d}\right)_4^t = (-1)^{\frac{Nc-1}{4} \cdot \frac{Nd-1}{4}} \left(\frac{d}{c_0}\right)_4 \left(\frac{i}{d}\right)_4^s \left(\frac{1+i}{d}\right)_4^t, \tag{3.1}$$

and similarly

$$\left(\frac{c}{d'}\right)_4 = (-1)^{\frac{Nc-1}{4} \cdot \frac{Nd'-1}{4}} \left(\frac{d'}{c_0}\right)_4 \left(\frac{i}{d'}\right)_4^s \left(\frac{1+i}{d'}\right)_4^t. \tag{3.2}$$

By Equations (3.1) and (3.2), it is equivalent to show that

$$(-1)^{\frac{Nc-1}{4} \cdot \frac{Nd-1}{4}} \left(\frac{d}{c_0}\right)_4 \left(\frac{i}{d}\right)_4^s \left(\frac{1+i}{d}\right)_4^t = (-1)^{\frac{Nc-1}{4} \cdot \frac{Nd'-1}{4}} \left(\frac{d'}{c_0}\right)_4 \left(\frac{i}{d'}\right)_4^s \left(\frac{1+i}{d'}\right)_4^t (-1)^{t\frac{N(d-d')}{64}}. \tag{3.3}$$

Let $d = a + bi$, then since $d \equiv d' \pmod{8}$, there exists integers k, l such that $d' = (a + 8k) + (b + 8l)i$. Thus we have

$$\begin{aligned} \frac{Nd - 1}{4} - \frac{Nd' - 1}{4} &= \frac{a^2 + b^2}{4} - \frac{(a + 8k)^2 + (b + 8l)^2}{4} \\ &= -\frac{16ak + 64k^2 + 16bl + 64l^2}{4} \\ &= -(4ak + 16k^2 + 4bl + 16l^2), \end{aligned}$$

which is divisible by 2, so $\frac{Nd-1}{4}$ and $\frac{Nd'-1}{4}$ have the same parity, and consequently

$$(-1)^{\frac{Nd-1}{4} \cdot \frac{Nd'-1}{4}} = (-1)^{\frac{Nd'-1}{4} \cdot \frac{Nd-1}{4}}. \quad (3.4)$$

And since $d \equiv d' \pmod{c_0}$, we have

$$\left(\frac{d}{c_0}\right)_4 = \left(\frac{d'}{c_0}\right)_4. \quad (3.5)$$

Furthermore, by Lemma 3.4 we have

$$\left(\frac{i}{d}\right)_4 = i^{\frac{3a-3}{2}} = i^{\frac{3a-3}{2} + 4 \cdot 3k} = i^{\frac{3(a+8k)-3}{2}} = \left(\frac{i}{d'}\right)_4. \quad (3.6)$$

By comparing Equation (3.3) with Equations (3.4), (3.5), and (3.6), we only need to show that

$$\left(\frac{1+i}{d}\right)_4^t = \left(\frac{1+i}{d'}\right)_4^t (-1)^{t \frac{N(d-d')}{64}}.$$

By Lemma 3.5, we have

$$\left(\frac{1+i}{d}\right)_4 = i^{\frac{a-b-b^2-1}{4}},$$

and

$$\begin{aligned} \left(\frac{1+i}{d'}\right)_4 &= i^{\frac{(a+8k)-(b+8l)-(b+8l)^2-1}{4}} \\ &= i^{\frac{a-b-b^2-1}{4} + 2(k-l) - 4(bl-4l^2)} \\ &= \left(\frac{1+i}{d}\right)_4 (-1)^{k-l}. \end{aligned}$$

Therefore,

$$\begin{aligned}
\left(\frac{1+i}{d}\right)_4 &= \left(\frac{1+i}{d'}\right)_4 (-1)^{-k+l} \\
&= \left(\frac{1+i}{d'}\right)_4 (-1)^{k^2+l^2} \\
&= \left(\frac{1+i}{d'}\right)_4 (-1)^{\frac{(-8k)^2+(-8l)^2}{64}} \\
&= \left(\frac{1+i}{d'}\right)_4 (-1)^{\frac{N(d-d')}{64}},
\end{aligned}$$

and consequently $\left(\frac{1+i}{d}\right)_4^t = \left(\frac{1+i}{d'}\right)_4^t (-1)^{t\frac{N(d-d')}{64}}$. This completes the proof of this lemma. \square

Proof of Theorem 3.1. We prove the theorem by showing that \mathcal{K}_4 is multiplicative on $\Gamma_{(1+i)^k}$ for $k = 4$ but not for $k = 3$.

When $k = 4$, let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $g' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \Gamma_{(1+i)^4}$, and $g'' = gg' = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix}$. Then $g = g''(g')^{-1} = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix} \begin{pmatrix} \delta' & -\beta' \\ -\gamma' & \alpha' \end{pmatrix}$. By comparing the matrices on both sides of the equation above, we have

$$\gamma = \gamma''\delta' - \delta''\gamma'. \quad (3.7)$$

Let θ_1 be any greatest common divisor of δ' and δ'' . Since that $\delta' \equiv \delta'' \equiv 1 \pmod{(1+i)^3}$ and that $(1+i) \mid (1+i)^3$, we have $\delta' \equiv \delta'' \equiv 1 \pmod{1+i}$, and therefore $(1+i)$ does not divide θ_1 . Thus we can pick the associate θ of θ_1 such that $\theta \equiv 1 \pmod{(1+i)^3}$. Denote $\delta' = \delta'_0\theta$ and $\delta'' = \delta''_0\theta$, then since $\theta \mid \delta', \delta''$, we have $\theta \mid \gamma''\delta' - \delta''\gamma' = \gamma$. Let $\gamma = \gamma_0\theta$, then (3.7) can be rewritten as

$$\gamma_0\theta = \gamma''\delta'_0\theta - \delta''_0\gamma'\theta,$$

which implies

$$\gamma_0 = \gamma''\delta'_0 - \delta''_0\gamma'. \quad (3.8)$$

Thus we have

$$\left(\frac{\gamma''}{\delta''}\right)_4 = \left(\frac{\gamma''}{\delta''_0}\right)_4 \left(\frac{\gamma''}{\theta}\right)_4 = \left(\frac{\gamma''\delta'_0}{\delta''_0}\right)_4 \left(\frac{\delta'_0}{\delta''_0}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4 = \left(\frac{\gamma_0}{\delta''_0}\right)_4 \left(\frac{\delta'_0}{\delta''_0}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4, \quad (3.9)$$

in which the last equality holds because by (3.8) we have $\gamma_0 \equiv \gamma''\delta'_0 \pmod{\delta''_0}$ and consequently $\left(\frac{\gamma''\delta'_0}{\delta''_0}\right)_4 = \left(\frac{\gamma_0}{\delta''_0}\right)_4$.

Now we check that $d = \delta''_0, d' = \delta\delta'_0$, and $c = \gamma_0$ satisfy the conditions of Lemma 3.6:

1. Since $\delta'' = \delta\delta' + \gamma\beta' \equiv \delta\delta' (\gamma\beta')$ and $(1+i)^3 \mid \gamma, \beta'$, we have $\delta'' \equiv \delta\delta' ((1+i)^6)$, namely $\delta''_0\theta \equiv \delta\delta'_0\theta ((1+i)^6)$. And since we have picked θ such that $\theta \equiv 1 ((1+i)^3)$, we have $\gcd(\theta, (1+i)^6) = 1$, and therefore $\delta''_0 \equiv \delta\delta'_0 ((1+i)^6)$.
2. Since $\delta'' = \delta''_0\theta$ and $\delta'' \equiv \theta \equiv 1 ((1+i)^3)$, we must have $\delta''_0 \equiv 1 ((1+i)^3)$. And since $(1+i)^3 \mid \delta''_0 - \delta\delta'_0$, we also have $\delta\delta'_0 \equiv 1 ((1+i)^3)$.
3. Furthermore, since the equation $\delta'' = \delta\delta' + \gamma\beta'$ can be rewritten as $\delta''_0\theta = \delta\delta'_0\theta + \gamma_0\theta\beta'$, we have $\delta''_0\theta \equiv \delta\delta'_0\theta (\gamma_0\theta)$, and consequently $\delta''_0 \equiv \delta\delta'_0 (\gamma_0)$.

Now that $d = \delta''_0, d' = \delta\delta'_0$, and $c = \gamma_0$ satisfy all the conditions of Lemma 3.6, we have $\left(\frac{\gamma_0}{\delta''_0}\right)_4 = \left(\frac{\gamma_0}{\delta\delta'_0}\right)_4 (-1)^{\text{ord}_{1+i}(\gamma_0) \frac{N(\delta''_0 - \delta\delta'_0)}{64}} = \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma_0}{\delta'_0}\right)_4 (-1)^{\text{ord}_{1+i}(\gamma_0) \frac{N(\delta''_0 - \delta\delta'_0)}{64}}$, so (3.9) can be rewritten as

$$\left(\frac{\gamma''}{\delta''}\right)_4 = \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma_0}{\delta'_0}\right)_4 \left(\frac{\delta'_0}{\delta''_0}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4 (-1)^{\text{ord}_{1+i}(\gamma_0) \frac{N(\delta''_0 - \delta\delta'_0)}{64}}. \quad (3.10)$$

In fact, the term $(-1)^{\text{ord}_{1+i}(\gamma_0) \frac{N(\delta''_0 - \delta\delta'_0)}{64}}$ can be dropped because we have a stronger result than the condition 1 above. Since $\delta'' = \delta\delta' + \gamma\beta' \equiv \delta\delta' (\gamma\beta')$ and $(1+i)^4 \mid \gamma, \beta'$, we have $\delta'' \equiv \delta\delta' ((1+i)^8)$, namely $\delta''_0\theta \equiv \delta\delta'_0\theta ((1+i)^8)$. And since we have picked θ such that $\theta \equiv 1 ((1+i)^3)$, we have $\gcd(\theta, (1+i)^8) = 1$, and therefore $\delta''_0 \equiv \delta\delta'_0 ((1+i)^8)$. This implies that $16 = (1+i)^8 \mid \delta''_0 - \delta\delta'_0$, so $256 \mid N(\delta''_0 - \delta\delta'_0)$, and therefore $\frac{N(\delta''_0 - \delta\delta'_0)}{64}$ is even. Consequently, $(-1)^{\text{ord}_{1+i}(\gamma_0) \frac{N(\delta''_0 - \delta\delta'_0)}{64}} = 1$.

Using (3.8) again we have $\gamma_0 \equiv -\delta_0''\gamma' (\delta_0')$, thus

$$\begin{aligned}
\mathcal{K}_4(g'') &= \left(\frac{\gamma''}{\delta''}\right)_4 \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{-\delta_0''\gamma'}{\delta_0'}\right)_4 \left(\frac{\delta_0'}{\delta_0''}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4 \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{-1}{\delta_0'}\right)_4 \left(\frac{\delta_0''}{\delta_0'}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\delta_0'}{\delta_0''}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4 \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\delta_0''}{\delta_0'}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\delta_0'}{\delta_0''}\right)_4^{-1} \left(\frac{\gamma''}{\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}} \\
&\quad \left(\text{since } \left(\frac{-1}{\delta_0'}\right)_4 = \left(\frac{i}{\delta_0'}\right)_4^2 = (i^{\frac{N\delta_0'-1}{4}})^2 = (-1)^{\frac{N\delta_0'-1}{4}}\right) \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\gamma''}{\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}} (-1)^{\frac{N\delta_0''-1}{4} \cdot \frac{N\delta_0'-1}{4}} \\
&\quad \left(\text{we have } \left(\frac{\delta_0''}{\delta_0'}\right)_4 = \left(\frac{\delta_0'}{\delta_0''}\right)_4 (-1)^{\frac{N\delta_0''-1}{4} \cdot \frac{N\delta_0'-1}{4}} \text{ by Lemma 3.3}\right) \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\delta\gamma'}{\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} \\
&\quad \left(\text{since } \gamma'' = \gamma\alpha' + \delta\gamma' = \gamma_0\theta\alpha' + \delta\gamma' \equiv \delta\gamma' (\theta)\right) \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\delta}{\theta}\right)_4 \left(\frac{\gamma'}{\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} \\
&= \left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\theta}{\delta}\right)_4 \left(\frac{\gamma'}{\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} (-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}} \\
&\quad \left(\text{By Lemma 3.3}\right) \\
&= \left(\left(\frac{\gamma_0}{\delta}\right)_4 \left(\frac{\theta}{\delta}\right)_4\right) \left(\left(\frac{\gamma'}{\delta_0'}\right)_4 \left(\frac{\gamma'}{\theta}\right)_4\right) (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} (-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}} \\
&= \left(\frac{\gamma_0\theta}{\delta}\right)_4 \left(\frac{\gamma'}{\delta_0'\theta}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} (-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}} \\
&= \left(\frac{\gamma}{\delta}\right)_4 \left(\frac{\gamma'}{\delta'}\right)_4 (-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} (-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}} \\
&= \mathcal{K}_4(g)\mathcal{K}_4(g')(-1)^{\frac{N\delta_0'-1}{4}(\frac{N\delta_0''-1}{4}+1)} (-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}}. \tag{3.11}
\end{aligned}$$

Note that since $\delta \equiv 1 \ ((1+i)^4)$, $\frac{N\delta-1}{4}$ is even, and therefore the term $(-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}}$ can be dropped. Furthermore, since $\delta_0' \equiv \delta_0'' \equiv 1 \ ((1+i)^3)$ and $\delta_0' \equiv \delta_0'' \ ((1+i)^4)$, $\frac{N\delta_0'-1}{4}$ and $\frac{N\delta_0''-1}{4}$ have the same parity. Therefore

exactly one of $\frac{N\delta'_0-1}{4}$ and $(\frac{N\delta''_0-1}{4} + 1)$ is even, and consequently the term $(-1)^{\frac{N\delta-1}{4} \cdot \frac{N\theta-1}{4}}$ can be dropped. Now we have

$$\mathcal{K}_4(g'') = \mathcal{K}_4(g)\mathcal{K}_4(g'),$$

thus \mathcal{K}_4 is multiplicative for $k = 4$.

To conclude the proof, we propose a counterexample to show that \mathcal{K}_4 is not multiplicative for $k = 3$. Consider the matrices $g = \begin{pmatrix} 19 + 14i & 26 + 34i \\ 4 & 7 + 2i \end{pmatrix}$ and $g' = \begin{pmatrix} 19 + 6i & 68 + 32i \\ 4 & 15 + 2i \end{pmatrix}$. Although $g, g' \in \Gamma_{(1+i)^3}$, we have $\mathcal{K}_4(g)\mathcal{K}_4(g') = (-1) \cdot (-1) = 1 \neq -1 = \mathcal{K}_4(gg')$. Thus $k = 4$ is the minimum value of k such that \mathcal{K}_4 is multiplicative. \square

4 Case of $n = 4, m = 2$

In this section we consider the case that $n = 4$ and $m = 2$. As we will show in Theorem 4.1, we can pick a better level of M than in the case of $n = m = 4$ so that the Kubota symbol is multiplicative.

Theorem 4.1. *The minimum value of k such that $\mathcal{K}_2(gg') = \mathcal{K}_2(g)\mathcal{K}_2(g')$ for all $g, g' \in \Gamma_{(1+i)^k}$ is $k = 3$.*

To prove this theorem, we need the fact that in D_4 the quadratic Kubota symbol \mathcal{K}_2 is the square of the quadratic Kubota symbol \mathcal{K}_4 .

Lemma 4.2. *For every $g \in \Gamma_{(1+i)}$, $\mathcal{K}_2(g) = \mathcal{K}_4(g)^2$.*

Proof. First note that in D_4 the quadratic residue symbol is the square of the quartic residue symbol. Let α be any element in D_4 and π be any primary prime in D_4 . If $\pi \nmid \alpha$, let $(\frac{\alpha}{\pi})_4 = i^t$, then since the element $(-1)^t$ in μ_2 satisfies that $(-1)^t = (i^t)^2 = (\frac{\alpha}{\pi})_4^2 \equiv (\alpha^{\frac{N\pi-1}{4}})^2 = \alpha^{\frac{N\pi-1}{2}} (\pi)$, we must have $(\frac{\alpha}{\pi})_2 = (-1)^t = (\frac{\alpha}{\pi})_4^2$. If $\pi \mid \alpha$, then clearly we have $(\frac{\alpha}{\pi})_2 = 0 = 0^2 = (\frac{\alpha}{\pi})_4^2$. Thus in D_4 the quadratic residue symbol is the square of the quartic residue symbol.

For each $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_{(1+i)}$, let $\pi_1\pi_2 \cdots \pi_r$ be the prime factoriza-

tion of δ . Then by the above property,

$$\begin{aligned}
\mathcal{K}_2(g) &= \left(\frac{\gamma}{\delta}\right)_2 \\
&= \prod_{i=1}^r \left(\frac{\gamma}{\pi_i}\right)_2 \\
&= \prod_{i=1}^r \left(\frac{\gamma}{\pi_i}\right)_4^2 \\
&= \left(\prod_{i=1}^r \left(\frac{\gamma}{\pi_i}\right)_4\right)^2 \\
&= \left(\frac{\gamma}{\delta}\right)_4^2 \\
&= \mathcal{K}_4(g)^2.
\end{aligned}$$

□

Proof of Theorem 4.1. By Lemma 4.2, it is equivalent to show that 3 is the least value of k such that $\mathcal{K}_4(gg')^2 = \mathcal{K}_4(g)^2\mathcal{K}_4(g')^2$ for all $g, g' \in \Gamma_{(1+i)^k}$.

In the proof of Theorem 3.1, we showed in Equation (3.11) that for all $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, g' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \Gamma_{(1+i)^4}$ and $gg' = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix}$ we have

$$\mathcal{K}_4(gg') = \mathcal{K}_4(g)\mathcal{K}_4(g')(-1)^{\frac{N\delta'_0-1}{4}(\frac{N\delta''_0-1}{4}+1)}(-1)^{\frac{N\delta-1}{4}\cdot\frac{N\theta-1}{4}},$$

where θ is a greatest common divisor of δ' and δ'' such that $\theta \equiv 1 \pmod{(1+i)^3}$, and δ'_0, δ''_0 are such that $\delta' = \delta'_0\theta, \delta'' = \delta''_0\theta$. Note that during the process of deriving Equation (3.11), we have only used the fact that $g, g' \in \Gamma_{(1+i)^3} \supset \Gamma_{(1+i)^4}$, except in the paragraph after Equation (3.10) we used the fact that $g, g' \in \Gamma_{(1+i)^4}$ to drop the term $(-1)^{\text{ord}_{1+i}(\gamma_0)\frac{N(\delta''_0-\delta\delta'_0)}{64}}$ in the right hand side of Equation (3.10). Therefore, Equation (3.11) would be true for $g, g' \in \Gamma_{(1+i)^3}$ if the term $(-1)^{\text{ord}_{1+i}(\gamma_0)\frac{N(\delta''_0-\delta\delta'_0)}{64}}$ is added in the right hand side, namely

$$\mathcal{K}_4(gg') = \mathcal{K}_4(g)\mathcal{K}_4(g')(-1)^{\frac{N\delta'_0-1}{4}(\frac{N\delta''_0-1}{4}+1)}(-1)^{\frac{N\delta-1}{4}\cdot\frac{N\theta-1}{4}}(-1)^{\text{ord}_{1+i}(\gamma_0)\frac{N(\delta''_0-\delta\delta'_0)}{64}} \quad (4.1)$$

is true for $g, g' \in \Gamma_{(1+i)^3}$.

By squaring both sides of Equation (4.1), we have

$$\begin{aligned}
\mathcal{K}_4(gg')^2 &= \left(\mathcal{K}_4(g)\mathcal{K}_4(g')(-1)^{\frac{N\delta'_0-1}{4}(\frac{N\delta''_0-1}{4}+1)}(-1)^{\frac{N\delta-1}{4}\cdot\frac{N\theta-1}{4}}(-1)^{\text{ord}_{1+i}(\gamma_0)\frac{N(\delta''_0-\delta\delta'_0)}{64}} \right)^2 \\
&= \mathcal{K}_4(g)^2\mathcal{K}_4(g')^2 \cdot 1^{\frac{N\delta'_0-1}{4}(\frac{N\delta''_0-1}{4}+1)} \cdot 1^{\frac{N\delta-1}{4}\cdot\frac{N\theta-1}{4}} \cdot 1^{\text{ord}_{1+i}(\gamma_0)\frac{N(\delta''_0-\delta\delta'_0)}{64}} \\
&= \mathcal{K}_4(g)^2\mathcal{K}_4(g')^2,
\end{aligned}$$

thus \mathcal{K}_2 is multiplicative on $\Gamma_{(1+i)^3}$. \square

5 Case of $n = m = 8$

To study the case of $n = 8$, it would be convenient if we can form the octic reciprocity law first. In this section, we denote ζ_8 , the primitive octic root of 1, as θ .

Theorem 5.1. *The greatest value of k such that the natural homomorphism $D_8^\times \rightarrow (D_8/((1-\theta)^k D_8))^\times$ is surjective is $k = 5$.*

Proof. Since $1-\theta$ is a prime in D_8 and $N(1-\theta) = 2$, there are $(1-\frac{1}{2}) \cdot 2^k = 2^{k-1}$ elements in $(D_8/((1-\theta)^k D_8))^\times$.

On the other hand, the units of D_8^\times are precisely the elements of the form $\theta^a(\theta + \theta^{-1} - 1)^b$ where $0 \leq a \leq 7, b \in \mathbb{Z}$. Therefore, the range of the natural homomorphism is the set $\{\overline{\theta^a(\theta + \theta^{-1} - 1)^b} \mid 0 \leq a \leq 7, 0 \leq b \leq B\}$ where B is the least positive integer such that $\{\overline{\theta^a(\theta + \theta^{-1} - 1)^b} \mid 0 \leq a \leq 7, 0 \leq b \leq B\} = \{\overline{\theta^a(\theta + \theta^{-1} - 1)^b} \mid 0 \leq a \leq 7, 0 \leq b \leq B+1\}$.

We ran the following sage program,

```

k.<theta> = CyclotomicField(8)

u0=theta+theta^7-1

for pow in range(1,21):
    rc=[]
    i=0
    newUnits=true
    while(newUnits==true):
        newUnits=false
        for j in range(0,8):
            newRes=true
            m=0
            u=u0^i*theta^j
            while(newRes==true and m<len(rc)):
                if((u-rc[m])/((1-theta)^pow)).is_integral():
                    newRes=false
                    m+=1

```

```

        if(newRes==true):
            rc.append(u0^i*theta^j)
            newUnits=true
        i+=1
    print len(rc), "of the", 2^(pow-1),"units of (D_8 / ((1-theta)^(pow-1)))^X occurred."

```

and obtained the following result:

k	$ (D_8/((1-\theta)^k D_8))^\times $	elements of $(D_8/((1-\theta)^k D_8))^\times$ in the range of the homomorphism
1	1	1
2	2	2
3	4	4
4	8	8
5	16	16
6	32	16
7	64	32
8	128	32
9	256	32
10	512	32
11	1024	64
12	2048	64
13	4096	64
14	8192	64
15	16384	128
16	32768	128
17	65536	128
18	131072	128
19	262144	256
20	524288	256

Thus $k = 5$ is the greatest value of k such that the natural homomorphism $D_8^\times \rightarrow (D_8/((1-\theta)^k D_8))^\times$ is surjective. \square

Hypothesis 5.2. *The minimum value of k such that $\left(\frac{\pi}{\rho}\right) = \left(\frac{\rho}{\pi}\right)$ for all primes $\pi, \rho \in D_8$ satisfying $\pi \equiv \rho \equiv 1 \pmod{(1-\theta)^k}$ is $k = 8$, where (\cdot) is the octic residue symbol.*

Reasoning. For each $k = 1, 2, \dots$, we generate the set S_k of all primes in D_8 which are congruent to 1 modulo $(1-\theta)^k$ with norms less than 40000, then we randomly pick 100 pairs of primes π, ρ from S_k and observe the number of pairs of primes π, ρ satisfying that $\left(\frac{\pi}{\rho}\right)_8 = \left(\frac{\rho}{\pi}\right)_8$. This is done through the following sage program:

```

k.<theta> = CyclotomicField(8)

def gm(a, b, c, d):
    return matrix(2, [a,b,c,d])

def kubota(matr):
    return symbol(matr[1][0], matr[1][1])

def factorization(g):
    return [[x[0].gens_reduced()[0], x[1]] for x in k.factor(g)]

def symbol(a, b):
    return prod(primesymbol(k(a),gen)^mult for [gen,mult] in factorization(k(b)))

def primesymbol(a,p):
    for x in [1,theta,theta^2,theta^3,theta^4,theta^5,theta^6,theta^7]:
        if((a^((norm(k(p))-1)/8)-x)/p).is_integral():
            return x

def kprimes(n):
    return flatten([[y[0] for y in factorization(x)] for x in list(primes(n))])

def kprimesmall(n):
    v = kprimes(n)
    w = []
    for i in range(0,len(v)):
        if(norm(v[i]) <= n):
            w.append(v[i])
    return w

def isprime(a):
    if(len(factorization(a))==1 and factorization(a)[0][1]==1):
        return true
    return false

maxnorm = 40000
minpow = 1
maxpow = 10
samples = 100
maxFailedC = 0
maxFailedD = 0

w=kprimesmall(maxnorm)
print "(power, primary primes, samples, samples that reciprocity holds, success rate %)"
for pow in range(minpow,maxpow+1):
    primaryprimes = []
    for i in range(0,len(w)):
        if((w[i]-1)/((1-theta)^pow)).is_integral():
            primaryprimes.append(w[i])
    if(len(primaryprimes)>=10):
        succ=0
        for i in range(0,samples):
            c = primaryprimes[ZZ(ntl.ZZ_random(len(primaryprimes)))]
            d = primaryprimes[ZZ(ntl.ZZ_random(len(primaryprimes)))]
            if(primesymbol(c,d)==primesymbol(d,c)):
                succ+=1

```

```

else:
    maxFailedC = c
    maxFailedD = d
    print (pow,len(primaryprimes),samples,succ,100.0*succ/samples)
print (maxFailedC, maxFailedD)

```

We obtained the following result:

k	$ S_k $	pairs of π, ρ picked from S_k	pairs of π, ρ such that $\left(\frac{\pi}{\rho}\right)_8 = \left(\frac{\rho}{\pi}\right)_8$	probability that $\left(\frac{\pi}{\rho}\right)_8 = \left(\frac{\rho}{\pi}\right)_8$
1	4190	100	14	14%
2	2058	100	14	14%
3	1030	100	15	15%
4	518	100	36	36%
5	253	100	40	40%
6	142	100	57	57%
7	70	100	69	69%
8	34	100	100	100%
9	16	100	100	100%
10	14	100	100	100%

When $k = 7$, there exist counterexamples, e.g. when $\pi = -2\theta^3 - 2\theta^2 + 10\theta + 3$, $\rho = -6\theta^3 + 2\theta^2 - 10\theta + 3$ we have $\left(\frac{\pi}{\rho}\right)_8 = \theta^7 \neq \theta^3 = \left(\frac{\rho}{\pi}\right)_8$. On the other hand, all 300 samples of π, ρ chosen when $k \geq 8$ satisfy that $\left(\frac{\pi}{\rho}\right)_8 = \left(\frac{\rho}{\pi}\right)_8$. Thus we conjecture that the octic reciprocity law holds for primes congruent to 1 modulo $(1 - \theta)^8$. \square

References

- [1] T. Kubota. Ein arithmetischer Satz über eine Matrizen­gruppe. *Journal für die reine und angewandte Mathematik*, **222** (1966), 55–57.
- [2] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. New York: Springer, 2000.
- [3] W. Stein (2004). Quadratic Extensions. In *A Brief Introduction to Classical and Adelic Algebraic Number Theory* Section 13.2.1. Retrived June 12, 2008, from <http://modular.fas.harvard.edu/papers/ant/html/node48.html>