Cubic and quartic reciprocity

The laws of cubic and quartic reciprocity with a perspective towards class field theory

Rasmus Frigaard Lemvig

Bachelor project supervised by Ian Kiming

Abstract

In this paper, we explore the laws of cubic and quartic reciprocity. The theory is developed using a classical approach with Gauss and Jacobi sums. The properties of these sums, along with some basic facts of the Gaussian and Eisenstein integers, constitutes the beginning of the paper. After this background is in place, we provide proofs of the cubic and quartic reciprocity laws, establishing all necessary technical results along the way. When the proofs of the reciprocity laws are complete, we present algorithms for computing the residue symbols in an efficient manner. In the final part, we embark on a brief tour of class field theory in order to derive the cubic reciprocity law in a more high level fashion. More specifically, we do this using the Hilbert symbol and the Strong Reciprocity law.

Department of Mathematical Sciences
University of Copenhagen
Denmark
June 2021

Contents

1 The Gaussian and Eisenstein integers

We recall that the Gaussian integers are given by $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and that the Eisenstein integers are $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = e^{2\pi i/3}$. They are the number rings belonging to the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$, respectively, see for example chapter 2 in [5]. The norms are given by $N(a + bi) = a^2 + b^2$ and $N(a + b\omega) = a^2 - ab + b^2$. An element in a number ring is a unit if and only if it has norm 1, from which it follows that $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. For the Eisenstein integers, we have $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$. To see this, simply reformulate the equation $a^2 - ab + b^2 = 1$ as $(2a - b)^2 + 3b^2 = 4$ and consider cases.

Unlike most number rings, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Euclidean with respect to their norms. By general theory, they are both PIDs and UFDs. In particular, the notions of prime and irreducible coincide. A classification of the irreducibles are given in the following propositions:

Proposition 1.1. *Up to associates, the irreducible elements in $\mathbb{Z}[i]$ are:*

(i) $1 + i$.

(ii) Rational primes $q \equiv 3 \pmod 4$.

(iii) $a + bi, a - bi$ *with* $a^2 + b^2 = p$ *a prime* $p \equiv 1 \pmod 4$.

Proposition 1.2. *Up to associates, the irreducible elements in $\mathbb{Z}[\omega]$ are:*

(i) $1 - \omega$

(ii) Rational primes $q \equiv 2 \pmod 3$.

(iii) $a + b\omega, a + b\omega^2$ *with* $a^2 - ab + b^2 = p$ *a prime* $p \equiv 1 \pmod 3$

These should be well known, otherwise, consult for example [8] and [4]. Lastly, we consider the residue class rings of these number rings.

Proposition 1.3. *Let $\pi \in \mathbb{Z}[i]$ be a non-zero prime. $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field with $N\pi$ elements.*

Proof. $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a field since $\pi\mathbb{Z}[i]$ is a non-zero prime ideal hence a maximal ideal since $\mathbb{Z}[i]$ is a PID. We now note that all elements in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has a representative with norm strictly less than $N\pi$. This follows from Euclidean division. The case $\pi = 1 + i$ is easy, since the residue classes of $\pm 1, \pm i$ are all equal, so the quotient has two elements.

Now assume that $\pi = q$ with $q \equiv 3 \pmod 4$ a rational prime. We claim that a complete residue system is given by $R = \{a + bi \mid 0 \leq a, b < q\}$. Then the quotient will have $q^2 = N\pi$ elements as desired. Let $a + bi \in \mathbb{Z}[i]$. Write $a = tq + s$ and $b = t'q + s'$ for $t, t', s, s' \in \mathbb{Z}$ with $0 \leq s, s' < q$. We have $a + bi \equiv s + s'i \pmod q$, so $a + bi$ has a representative in R. Assume that $a + bi \equiv a' + b'i \pmod q$ for two representations in R. Then $(a - a')/q + ((b - b')/q)i \in \mathbb{Z}[i]$ implying that $(a - a')/q$ and $(b - b')/q$ are integers. Since $0 \leq a, a', b, b' < q$, the only possibility is $a = a'$ and $b = b'$.

Now let $N\pi = p \equiv 1 \pmod 4$. We claim that $\{0, 1, ..., p - 1\}$ is a complete set of representatives. Then $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ will have p elements. Write $\pi = a + bi$ and let $\alpha = c + di \in \mathbb{Z}[i]$ be arbitrary. Clearly, $p \nmid b$ so there is an integer k such that $kb \equiv d \pmod p$.

Thus, $\alpha - k\pi \equiv c - ka \pmod{p}$, implying $\alpha \equiv c - ka \pmod{\pi}$. This shows that every element in $\mathbb{Z}[i]$ is congruent to a rational integer modulo π. If $\alpha \equiv m \pmod{\pi}$, write $m = np + r$ with $0 \leq r < p$, then $\alpha \equiv r \pmod{\pi}$, so α is congruent to one of $0, 1, ..., p-1$ modulo π. Let $m \equiv m' \pmod{\pi}$ with $0 \leq m, m' < p$. Then $m - m' = \pi\beta$ for some $\beta \in \mathbb{Z}[i]$ and $(m - m')^2 = pN\beta$ so that p divides $m - m'$. Hence, $m = m'$, and the proof is complete. ■

A completely analogous proof goes through in the case for $\mathbb{Z}[\omega]$, so if $\pi \in \mathbb{Z}[\omega]$ is a prime, $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field with $N\pi$ elements as well. In both cases, a straightforward application of the Chinese remainder theorem shows that $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]/\alpha\mathbb{Z}[\omega]$ are rings with $N\alpha$ elements for any non-zero α in the respective ring. From proposition 1.3, we deduce:

Corollary 1.4 (**Fermat's little theorem**). *Let π be irreducible in $\mathbb{Z}[i]$ (or $\mathbb{Z}[\omega]$) and $\alpha \in \mathbb{Z}[i]$ (or $\alpha \in \mathbb{Z}[\omega]$), then:*

$$\alpha^{N\pi - 1} \equiv 1 \pmod{\pi}$$

During the project, we present some algorithms to compute certain functions. These functions (and many others) are all implemented in C++. All my code concerning the Eisenstein integers can be found here[1]. The analogous functions for the Gaussian integers are all found here[2].

2 Gauss and Jacobi sums

We first define the notion of a multiplicative character. Let p be a prime and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the finite field with p elements.

Definition 2.1. A multiplicative character on $\mathbb{F}_p$ is a homomorphism $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$. Define the trivial multiplicative character ε on $\mathbb{F}_p$ to be $\varepsilon(a) = 1$ for all $a \in \mathbb{F}_p^\times$.

From now on we omit the term "multiplicative" and simply refer to χ in the definition as a character. We extend characters to all of $\mathbb{F}_p$ by letting $\chi(0) = 0$ for $\chi \neq \varepsilon$ and $\varepsilon(0) = 1$. A well known example of a character from elementary number theory is the Legendre symbol. Let us establish some fundamental results for characters.

Proposition 2.2. *Let χ be a character and $a \in \mathbb{F}_p^\times$. We have*

(i) $\chi(1) = 1$.

(ii) $\chi(a)$ *is a* $(p-1)$*st root of unity.*

(iii) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

(iv) If $\chi \neq \varepsilon$

$$\sum_{n=0}^{p-1} \chi(n) = 0$$

and the sum is p *if* $\chi = \varepsilon$.

[1] https://github.com/RasmusFL/EisensteinIntegers
[2] https://github.com/RasmusFL/GaussianIntegers

Proof. (i) follows from $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. (ii) is just Fermat's little theorem. $a^{p-1} = 1$ gives $\chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$. To prove (iii), simply note that $1 = \chi(1) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$. $\chi(a)^{-1} = \overline{\chi(a)}$ follows from (ii). If $\chi = \varepsilon$, clearly $\sum_{n=0}^{p-1} \chi(n) = p$. Otherwise, pick $a \in \mathbb{F}_p^\times$ such that $\chi(a) \neq 1$. Then:

$$\chi(a) \sum_{n=0}^{p-1} \chi(n) = \sum_{n=0}^{p-1} \chi(an) = \sum_{n=0}^{p-1} \chi(n)$$

since $n \mapsto an$ is a bijection from $\mathbb{F}_p$ to $\mathbb{F}_p$. As $\chi(a) \neq 1$, the sum must be zero. ∎

Definition 2.3. For characters χ, λ, let $\chi\lambda$ be the character defined by $\chi\lambda(a) = \chi(a)\lambda(a)$. Define χ^{-1} to be the map $\chi^{-1}(a) = \chi(a^{-1})$.

Clearly, this makes the set of characters on $\mathbb{F}_p$ a group with identity ε. It is in fact a cyclic group of order $p-1$ generated by the character λ acting on an element $a = g^k \in \mathbb{F}_p^\times$ by $\lambda(a) = e^{2\pi i(k/(p-1))}$ where g is a generator for $\mathbb{F}_p^\times$. See [4, p. 89] for a proof. We are now ready to define the notion of a Gauss sum.

Definition 2.4. Let χ be a character on $\mathbb{F}_p$ and $a \in \mathbb{F}_p$. Define the Gauss sum for χ to be $g_a(\chi) = \sum_{n=0}^{p-1} \chi(n)\zeta^{an}$ where $\zeta = e^{2\pi i/p}$.

The following proposition says that the value of $g_a(\chi)$ for $a \neq 0$ only depends on $g_1(\chi)$ which we will denote by $g(\chi)$ from now on.

Proposition 2.5.

$$g_a(\chi) = \begin{cases} \chi(a^{-1})g(\chi), & \text{if } \chi \neq \varepsilon \text{ and } a \neq 0 \\ 0, & \text{if } \chi = \varepsilon \text{ and } a \neq 0 \text{ or } \chi \neq \varepsilon \text{ and } a = 0 \\ p, & \text{if } \chi = \varepsilon \text{ and } a = 0 \end{cases}$$

Proof. Assume $\chi \neq \varepsilon$ and $a \neq 0$. Again, since $n \mapsto an$ is a bijection:

$$\chi(a)g_a(\chi) = \chi(a) \sum_{n=0}^{p-1} \chi(n)\zeta^{an} = \sum_{n=0}^{p-1} \chi(an)\zeta^{an} = g(\chi)$$

This proves the first case. If $a \neq 0$, we may use the formula for a geometric sum as $\zeta^a \neq 1$:

$$g_a(\varepsilon) = \sum_{n=0}^{p-1} \varepsilon(n)\zeta^{an} = \sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0$$

Lastly, $g_0(\chi) = \sum_{n=0}^{p-1} \chi(n)\zeta^{0n} = \sum_{n=0}^{p-1} \chi(n)$ and this sum is zero if $\chi \neq \varepsilon$ and p otherwise by proposition 2.2. ∎

It remains to determine $g(\chi)$. The following result determines the absolute value. We start by noting the simple fact that $\sum_{k=0}^{p-1} \zeta^{k(n-m)} = p$ if $p \mid (n-m)$ and the sum is 0 otherwise.

Proposition 2.6. *For $\chi \neq \varepsilon$, we have $|g(\chi)| = \sqrt{p}$.*

Proof. To prove the proposition, we compute the sum $\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)}$ in two different ways. Using proposition 2.2, we get for $a \neq 0$:

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} = \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} = |g(\chi)|^2$$

There are $p-1$ non-zero terms in the sum, so $\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2$. On the other hand, by spelling out definitions:

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \chi(n)\overline{\chi(m)}\zeta^{an-am}$$

Define δ_{nm} by letting $\delta_{nm} = 1$ when $p \mid (n-m)$ and $\delta_{nm} = 0$ otherwise. Using the observation before the theorem:

$$\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)} = \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \chi(n)\overline{\chi(m)}\delta_{nm}p = (p-1)p$$

Cancelling $p-1$ from both sides of the equation $(p-1)|g(\chi)|^2 = (p-1)p$ completes the proof. ∎

Corollary 2.7. *For $\chi \neq \varepsilon$, we have $g(\chi)g(\overline{\chi}) = \chi(-1)p$.*

Proof. The proof follows by computing

$$\overline{g(\chi)} = \sum_{n=0}^{p-1} \overline{\chi(n)}\zeta^{-n} = \overline{\chi(-1)}\sum_{n=0}^{p-1} \overline{\chi(-n)}\zeta^{-n} = \chi(-1)g(\overline{\chi})$$

$\overline{\chi(-1)} = \chi(-1)$ follows from $\chi(-1) = \pm 1$. Multiplying both sides by $\chi(-1)g(\chi)$ and using the proposition completes the proof. ∎

This establishes the necessary results for Gauss sums. In fact, the above corollary is used to give a classical proof of the quadratic reciprocity law. We now introduce Jacobi sums.

Definition 2.8. For two characters χ and λ of $\mathbb{F}_p$, the Jacobi sum of χ and λ is defined as $J(\chi,\lambda) = \sum_{n+m=1} \chi(n)\lambda(m)$.

Proposition 2.9. *Let $\chi, \lambda \neq \varepsilon$ be characters. We have:*

(i) $J(\varepsilon,\varepsilon) = p$.

(ii) $J(\chi,\varepsilon) = 0$.

(iii) $J(\chi,\chi^{-1}) = -\chi(-1)$.

(iv) If $\chi\lambda \neq \varepsilon$, $J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

(v) If $\chi\lambda \neq \varepsilon$, $|J(\chi,\lambda)| = \sqrt{p}$.

Proof. (i) and (ii) follow by observing that the Jacobi sum becomes a Gauss sum in these cases and applying proposition 2.2. We now show (iii):

$$J(\chi,\chi^{-1}) = \sum_{n+m=1} \chi(n)\chi^{-1}(m) = \sum_{n\neq 1} \chi(n(1-n)^{-1})$$

If we denote $k = n/(1-n)$, we can solve for n by $n = k/(1+k)$. So as n runs through $\mathbb{F}_p \setminus \{1\}$, k runs through $\mathbb{F}_p \setminus \{-1\}$. Thus, the sum is equal to $-\chi(-1)$. It remains to show (iv). We first compute:

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{n=0}^{p-1} \chi(n)\zeta^n\right)\left(\sum_{n=0}^{p-1} \lambda(m)\zeta^m\right) = \sum_{n,m} \chi(n)\lambda(m)\zeta^{n+m} \\ &= \sum_{k=0}^{p-1} \left(\sum_{n+m=k} \chi(n)\lambda(m)\right)\zeta^k \end{aligned} \tag{1}$$

For $k = 0$, we get $\sum_{n+m=0} \chi(n)\lambda(m) = \sum_{n=0}^{p-1} \chi(n)\lambda(-n) = \lambda(-1)\sum_{n=0}^{p-1} \chi\lambda(n) = 0$ by our assumption that $\chi\lambda \neq \varepsilon$. When $k \neq 0$, we may find n' and m' such that $n = kn'$ and $m = km'$. Thus, $n + m = k$ gives $n' + m' = 1$. We obtain:

$$\sum_{n+m=k} \chi(n)\lambda(m) = \sum_{n'+m'=1} \chi(kn')\lambda(km') = \chi\lambda(k)J(\chi,\lambda)$$

We substitute in (1) and get the desired expression:

$$g(\chi)g(\lambda) = \sum_{k=0}^{p-1} \chi\lambda(k)J(\chi,\lambda)\zeta^k = J(\chi,\lambda)g(\chi\lambda)$$

This proves (iv). (v) follows immediately from (iv) and proposition 2.6. ∎

The final relation between the Gauss and Jacobi symbol that we need is given in the following proposition:

Proposition 2.10. *Assume that χ is a character of order $n > 2$ and $p \equiv 1 \pmod{n}$, then:*

$$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})$$

Proof. By (iv) of proposition 2.9, $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$, $g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$ and so on. Continuing up to $n-1$ gives:

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1})$$

The result follows by noting $\chi^{n-1} = \chi^{-1} = \overline{\chi}$, multiplying both sides by $g(\chi)$ and using corollary 2.7. ∎

In the next two sections, we will work with many congruences, and the following lemma will be indispensable in that regard:

Lemma 2.11. *Let $n, m \in \mathbb{Z}$ with $m > 1$, $n = s_1 \cdots s_t$, $n \equiv 1 \pmod{m}$ and $s_i \equiv 1 \pmod{m}$ for $i = 1, ..., t$. We then have:*

$$\frac{n-1}{m} \equiv \sum_{i=1}^{t} \frac{s_i - 1}{m} \pmod{m}$$

Proof. We prove the result by induction on t. For $t = 1$, there is nothing to show, so assume $t > 1$. We assume that the result holds for $k = s_1 \cdots s_{t-1}$. Note that $ks_t \equiv 1 \pmod{m}$. We have

$$\frac{k-1}{m} + \frac{s_t - 1}{m} \equiv \sum_{i=1}^{t} \frac{s_i - 1}{m} \pmod{m}$$

by the induction hypothesis. Thus, it suffices to show $(k-1)/m + (s_t - 1)/m \equiv (ks_t - 1)/m \pmod{m}$ which follows by observing that $ks_t - 1 = (k-1)(s_t - 1) + (k-1) + (s_t - 1)$ and dividing by m. ∎

3 Cubic reciprocity

3.1 The cubic residue symbol and basic properties

In this section, let $\pi \in \mathbb{Z}[\omega]$ be a prime. Our first goal is to define the cubic residue character. To do so, we first note that if $N\pi \neq 3$, the residue classes of $1, \omega$ and ω^2 are distinct. Assume $1 \equiv \omega \pmod{\pi}$. Then $\pi \mid (1 - \omega)$, so $N\pi = 3$. Similarly for $1 \equiv \omega^2 \pmod{\pi}$ and $\omega \equiv \omega^2 \pmod{\pi}$. Also note that if $N\pi \neq 3$, then $N\pi \equiv 1 \pmod{3}$. In general, $N\alpha$ is divisible by 3 precisely if $1 - \omega$ is a factor of α.

Let $\alpha \in \mathbb{Z}[\omega]$ and $\pi \nmid \alpha$. By corollary 1.4, π divides $\alpha^{N\pi - 1} - 1$, and:

$$\alpha^{N\pi-1} - 1 = (\alpha^{\frac{N\pi-1}{3}} - 1)(\alpha^{\frac{N\pi-1}{3}} - \omega)(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$$

Since π is prime, it must divide one of the three factors, and since $N\pi \neq 3$, it will divide exactly one of them. This proves that $\alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi}$ for m equal to exactly one of $0, 1, 2$. These observations allow us to make the definition:

Definition 3.1. For $N\pi \neq 3$, the *cubic residue character* of α modulo π is:

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0, & \text{if } \pi \mid \alpha \\ \omega^m, & \text{if } \alpha^{(N\pi-1)/3} \equiv \omega^m \pmod{\pi} \end{cases}$$

Let us derive some simple consequences of this definition:

Proposition 3.2. *For $\alpha, \beta \in \mathbb{Z}[\omega]$:*

(i) $(\alpha/\pi)_3 = 1$ *if and only if* $x^3 \equiv \alpha \pmod{\pi}$ *is solvable.*

(ii) $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.

(iii) $(\alpha/\pi)_3 = (\beta/\pi)_3$ *if* $\alpha \equiv \beta \pmod{\pi}$.

Proof. To prove (i), recall that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^\times$ is cyclic since $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field. Let γ be a generator. Write $x = \gamma^a$ and $\alpha = \gamma^b$, then $x^3 \equiv \alpha \pmod{\pi}$ is equivalent to $\gamma^{3a} \equiv \gamma^b \pmod{\pi}$. This equation being solvable is equivalent to $3a \equiv b \pmod{N\pi - 1}$ being solvable. From elementary number theory, this equation is solvable if and only if $\gcd(3, N\pi - 1) = 3 \mid b$, i.e. $\alpha^{\frac{N\pi-1}{3}} \equiv 1 \pmod{\pi}$. (ii) follows from a simple computation:

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{\frac{N\pi-1}{3}} \equiv \alpha^{\frac{N\pi-1}{3}}\beta^{\frac{N\pi-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$$

(iii) is proved in the same fashion:

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} \equiv \beta^{\frac{N\pi-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$$

■

Note that this proposition shows that $(-/\pi)_3$ is a cubic character. This allows us to use all the results for Gauss and Jacobi sums on $(-/\pi)_3$ whenever $N\pi = p$, a prime. From now on, we write $\chi_\pi(\alpha) = (\alpha/\pi)_3$ for convenience. The following proposition will be useful:

Proposition 3.3. *For $\alpha \in \mathbb{Z}[\omega]$, we have $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$ and $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.*

Proof. $\chi_\pi(\alpha) \in \{1, \omega, \omega^2\}$ and all of these are squares of their conjugate. This proves the first claim. For the second, note that

$$\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}, \quad \text{hence} \quad \overline{\alpha}^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$$

$N\pi = N\overline{\pi}$, so $\overline{\chi_\pi(\alpha)} \equiv \chi_{\overline{\pi}}(\overline{\alpha}) \pmod{\overline{\pi}}$ which completes the proof. ■

In order to state the cubic reciprocity law unambiguously i.e. independently of associates (note the the residue symbol is unchanged if we multiply the "denominator" by a unit), we need the notion of a *primary* element.

Definition 3.4. $\lambda \in \mathbb{Z}[\omega]$ is called *primary* if $\lambda \equiv 2 \pmod{3}$.

$\lambda = a + b\omega \in \mathbb{Z}[\omega]$ with $N\lambda \neq 3$ is primary if and only if $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$. The notion of being primary is only useful if exactly one of the six associates of λ is primary. This turns out to be the case:

Proposition 3.5. *Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ and assume $N\alpha \neq 3$. Exactly one of the associates of α is primary.*

Proof. Let us write down all the associates explicitly:

$$a + b\omega, \quad -b + (a - b)\omega, \quad (b - a) - a\omega, \quad -a - b\omega, \quad b + (b - a)\omega, \quad (a - b) + a\omega$$

We first show uniqueness. If $a+b\omega$ is primary, $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$, from which it easily follows by considering congruence classes that none of the associates are primary. The proof of existence is a straightforward check. If $a \equiv 0 \pmod{3}$ and $b \equiv 1 \pmod{3}$, the primary associate is $(a - b) + a\omega$. For $a \equiv 0 \pmod{3}$ and $b \equiv 2 \pmod{3}$, the primary associate is $(b - a) - a\omega$. We let the reader check the remaining four possible cases. Note that we cannot have the three cases with $a + b \equiv 0 \pmod{3}$, since the norm is divisible by 3 in those cases. ■

The following technical lemma shall be useful:

Lemma 3.6. *Any primary element λ in $\mathbb{Z}[\omega]$ can be written as a product $\lambda = \pm\lambda_1 \cdots \lambda_t$ with each λ_i a primary prime.*

Proof. By unique factorization, factor $\lambda = u\pi_1 \cdots \pi_m q_1 \cdots q_n$ with $u \in \mathbb{Z}[\omega]^\times$ and $N\pi_i \equiv 1 \pmod 3$, $q_i \equiv 2 \pmod 3$. For each i, let $\pi_i' = u_i\pi_i$ be the unique primary associate of π_i and $v = u \cdot \prod_i u_i$. Then $\lambda = v\pi_1' \cdots \pi_m' q_1 \cdots q_n$ is a factorization into primary primes. Reducing modulo 3, we obtain $2 \equiv v2^{m+n} \pmod 3$ implying $v = \pm 1$ since a power of 2 is either 1 or -1 modulo 3. ■

We are now ready to generalize the cubic character.

Definition 3.7. Let $\alpha \in \mathbb{Z}[\omega]$ be a nonunit such that $1 - \omega \nmid \alpha$ and let $\beta \in \mathbb{Z}[\omega]$. Write $\alpha = \prod_i \pi_i$ with all π_i irreducible. We define:

$$\chi_\alpha(\beta) = \prod_i \chi_{\pi_i}(\beta)$$

Before stating the main theorem, we have the following properties of the generalized cubic residue symbol:

Proposition 3.8. *Let $\alpha, \beta, \lambda, \rho \in \mathbb{Z}[\omega]$ with $1 - \omega \nmid \lambda, \rho$.*

(i) $\chi_\lambda(\alpha) \neq 0$ *if and only if* $(\alpha, \lambda) = 1$.

(ii) $\chi_\lambda(\alpha\beta) = \chi_\lambda(\alpha)\chi_\lambda(\beta)$.

(iii) $\chi_\lambda(\alpha) = \chi_\lambda(\beta)$ *if* $\alpha \equiv \beta \pmod \lambda$.

(iv) $\chi_{\lambda\rho}(\alpha) = \chi_\lambda(\alpha)\chi_\rho(\alpha)$.

(v) $\chi_\lambda(-1) = 1$.

(vi) $\overline{\chi_\lambda(\alpha)} = \chi_\lambda(\alpha)^2 = \chi_\lambda(\alpha^2)$.

(vii) $\overline{\chi_\lambda(\alpha)} = \chi_{\overline{\lambda}}(\overline{\alpha})$.

(viii) *Let $a \in \mathbb{Z}$ with $a \equiv 2 \pmod 3$. Then $\chi_a(\overline{\alpha}) = \chi_a(\alpha^2)$ and $\chi_a(n) = 1$ if $(a, n) = 1$ and $n \in \mathbb{Z}$.*

Proof. (i) - (iv) follow straight from the definition. $-1 = (-1)^3$ which proves (v). To show (vi) and (vii), factor λ and use the definition along with proposition 3.3. (viii) is proved as follows. $\chi_a(\overline{\alpha}) = \chi_{\overline{a}}(\overline{\alpha}) = \overline{\chi_a(\alpha)} = \chi_a(\alpha^2)$. Also, $\chi_a(n) = \overline{\chi_a(n)} = \chi_a(n)^2$, which gives $\chi_a(n) = 1$. ■

This is a proper time for an example. $1 + 6\omega$ is a prime since $N(1 + 6\omega) = 31$ is a prime. Consider $8 - 11\omega$. We wish to determine whether $x^3 \equiv 8 - 11\omega \pmod{1 + 6\omega}$ has a solution. We compute:

$$\left(\frac{8 - 11\omega}{1 + 6\omega}\right)_3 \equiv (8 - 11\omega)^{\frac{31-1}{3}} \equiv (8 - 11\omega)^{10} \pmod{1 + 6\omega}$$

The remaining computation is easily done using modular exponentiation, and this gives $(8-11\omega/1+6\omega)_3 = 1$. We conclude that $x^3 \equiv 8-11\omega \pmod{1+6\omega}$ is solvable. When π is a prime, computing $(\cdot/\pi)_3$ using modular exponentiation is fairly efficient. The algorithm works exactly as in the ordinary integers by using repeated squarings (see e.g. chapter 3 in [9]). If $n \in \mathbb{N}$, we denote the binary representation of n by $(b_{l-1}, ..., b_1, b_0)$ so that $n = b_{l-1}2^{l-1} + ... + b_1 2 + b_0$, and we define $\text{len}(n) := l$ e.g. the bitlength of n. The algorithm can thus be stated as follows:

Algorithm 1: Modular exponentiation in $\mathbb{Z}[\omega]$

Input: $\alpha, \beta \in \mathbb{Z}[\omega], n \in \mathbb{N}$
Output: $\alpha^n \pmod{\beta}$
$r \leftarrow 1$
let $(b_{l-1}, ..., b_1, b_0)$ be the binary representation of n
for $i = l-1$ *down to* 0 **do**
    $r \leftarrow r^2 \pmod{\beta}$
    if $b_i = 1$ **then**
        $r \leftarrow r \cdot \alpha \pmod{\beta}$
return r

The algorithm clearly outputs $\alpha^n \pmod{\beta}$. The for-loop runs l times, so the algorithm makes $O(\text{len}(n))$ multiplications in $\mathbb{Z}[\omega]$.

3.2 The theorem of cubic reciprocity

We are now ready to state the main theorem in full generality:

Theorem 3.9 (Law of cubic reciprocity)**.** *Let λ and ρ be relatively prime primary elements in $\mathbb{Z}[\omega]$ with $N\lambda, N\rho \neq 3$ and $N\lambda \neq N\rho$. Then*

$$\chi_\lambda(\rho) = \chi_\rho(\lambda) \tag{1}$$

For λ of the form $\lambda = 3m-1$ or $\lambda = 3m-1+3n\omega$ for integers m and n, we have the supplementary law:

$$\chi_\lambda(1-\omega) = \omega^{2m} \tag{2}$$

And for the units, we have:

$$\chi_\lambda(\omega) = \omega^{\frac{N\lambda-1}{3}} = \begin{cases} 1, & N\lambda \equiv 1 \pmod 9 \\ \omega, & N\lambda \equiv 4 \pmod 9 \\ \omega^2, & N\lambda \equiv 7 \pmod 9 \end{cases} \tag{3}$$

The strategy for proving this theorem is to first prove part (1) for two distinct primary primes. The rest is a simple application of lemma 3.6. We then turn our attention to (2) and (3).

Lemma 3.10. *Let $\pi \in \mathbb{Z}[\omega]$ be a prime with $N\pi \equiv 1 \pmod 3$. We have:*

(i) $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$.

(ii) $J(\chi_\pi, \chi_\pi) = a + b\omega \in \mathbb{Z}[\omega]$ *with* $a \equiv -1 \pmod 3$ *and* $b \equiv 0 \pmod 3$.

Proof. (i) follows immediately from proposition 2.10 and by noting that $\chi_\pi(-1) = \chi_\pi((-1)^3) = 1$. For (ii), note that $J(\chi_\pi, \chi_\pi)$ is actually an element of $\mathbb{Z}[\omega]$ since χ_π is equal to a third root of unity. Consider the congruence in the ring of algebraic integers:

$$g(\chi_\pi)^3 = \left(\sum_{n=0}^{p-1} \chi_\pi(n)\zeta^n\right)^3 \equiv \sum_{n=0}^{p-1} \chi_\pi(n)^3\zeta^{3n} \pmod 3$$

$\chi_\pi(n)^3 = 1$ for $n \neq 0$ and $\chi_\pi(0) = 0$, so the above sum is equal to $\sum_{n\neq 0} \zeta^{3n} = -1$. Thus $\overline{g(\chi_\pi)}^3 = pJ(\chi_\pi, \chi_\pi) \equiv a + b\omega \equiv -1 \pmod 3$. Recall from the proof of corollary 2.7 that $\overline{g(\chi_\pi)} = g(\overline{\chi_\pi})$ because χ_π is a cubic character. Thus, a similar computation as before gives $g(\overline{\chi_\pi})^3 \equiv pJ(\overline{\chi_\pi}, \overline{\chi_\pi}) \equiv a + b\overline{\omega} \equiv -1 \pmod 3$. Subtracting gives $b(\omega - \overline{\omega}) \equiv 0 \pmod 3$ so $b\sqrt{-3} \equiv 0 \pmod 3$. It follows that $3 \mid b$ and $a \equiv -1 \pmod 3$. ∎

Lemma 3.11. *Let $\pi \in \mathbb{Z}[\omega]$ be a primary prime with $N\pi \equiv 1 \pmod 3$. Then:*

(i) $J(\chi_\pi, \chi_\pi) = \pi$.

(ii) $g(\chi_\pi)^3 = p\pi$.

Proof. Note that (ii) is a direct consequence of (i) and lemma 3.10. $J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = p$ by proposition 2.9 (v), so $J(\chi_\pi, \chi_\pi) = \pi'$, where π' is a primary prime by (ii) of the previous lemma. As $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, we must have $\pi \mid \pi'$ or $\pi \mid \overline{\pi'}$. We show that the first possibility is indeed the case. We have:

$$J(\chi_\pi, \chi_\pi) = \sum_{n=0}^{p-1} \chi_\pi(n)\chi_\pi(1-n) \equiv \sum_{n=0}^{p-1} n^{(p-1)/3}(1-n)^{(p-1)/3} \pmod \pi$$

We claim that $1^k + 2^k + ... + (p-1)^k \equiv 0 \pmod p$ when $p - 1 \nmid k$. Let g be a primitive root of $\mathbb{Z}/p\mathbb{Z}$. Then the sum is equal to $\sum_{i=0}^{p-1} g^{ki} = (g^{pk} - 1)/(g^k - 1) = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Now note that $x^{(p-1)/3}(1-x)^{(p-1)/3}$ has degree strictly less than $p - 1$. Using the previous claim along with the binomial theorem shows that p divides $J(\chi_\pi, \chi_\pi)$, in particular, π divides $J(\chi_\pi, \chi_\pi)$. We conclude that $\pi \mid \pi'$ whence $\pi = \pi'$. ∎

We are ready to prove the law of cubic reciprocity:

Proof of theorem 3.9. We first prove the theorem for two primary primes and generalize afterwards. There are three cases to consider.
Case 1: λ and ρ are rational primes congruent to 2 modulo 3. In this case, proposition 3.8 gives $\chi_\lambda(\rho) = 1 = \chi_\rho(\lambda)$.
Case 2: $\lambda = q$ is a rational prime congruent to 2 modulo 3 and $\rho = \pi$, a prime with $N\pi = p \equiv 1 \pmod 3$. We have

$$g(\chi_\pi)^{q^2-1} = g(\chi_\pi)^{3\frac{q^2-1}{3}} = (p\pi)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi) \pmod q$$

by lemma 3.11, $\chi_q(p) = 1$ so

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi) \pmod q$$

Since $q^2 \equiv 1 \pmod 3$, we may expand the left hand side as

$$g(\chi_\pi)^{q^2} \equiv \left(\sum_{n=0}^{p-1} \chi_\pi(n)\zeta^n\right)^{q^2} \equiv \sum_{n=0}^{p-1} \chi_\pi(n)^{q^2}\zeta^{q^2 n} \equiv \sum_{n=0}^{p-1} \chi_\pi(n)\zeta^{q^2 n} \equiv g_{q^2}(\chi_\pi) \pmod q$$

Using proposition 2.5, we have $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Combining the above equations, we get $\chi_\pi(q)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi) \pmod q$. Multiplying both sides by $\overline{g(\chi_\pi)}$ and cancelling out with p, we get $\chi_\pi(q) \equiv \chi_q(\pi) \pmod q$, so the symbols are equal.
Case 3: λ and ρ are primes with $N\lambda = p_1$, $N\rho = p_2$ and $p_1, p_2 \equiv 1 \pmod 3$. Starting with the relations $g(\chi_{\overline{\lambda}})^3 = p_1\overline{\lambda}$ and $g(\chi_\rho)^3 = p_2\rho$ as above, we get in a similar way:

$$\chi_{\overline{\lambda}}(p_2^2) = \chi_\rho(p_1\overline{\lambda}), \quad \chi_\rho(p_1^2) = \chi_\lambda(p_2\rho)$$

Note also that $\chi_{\overline{\lambda}}(p_2^2) = \chi_\lambda(p_2)$ by proposition 3.8. The rest is a calculation:

$$\begin{aligned}\chi_\lambda(\rho)\chi_\rho(p_1\overline{\lambda}) &= \chi_\lambda(\rho)\chi_{\overline{\lambda}}(p_2^2) = \chi_\lambda(\rho)\chi_\lambda(p_2) = \chi_\lambda(p_2\rho) \\ &= \chi_\rho(p_1^2) = \chi_\rho(p_1\lambda\overline{\lambda}) = \chi_\rho(\lambda)\chi_\rho(p_1\overline{\lambda})\end{aligned}$$

We may cancel out the term $\chi_\rho(p_1\overline{\lambda})$ and obtain $\chi_\lambda(\rho) = \chi_\rho(\lambda)$.
The generalization to primary elements is easy. Assume λ and ρ are primary with primary factorizations $\lambda = \pm\lambda_1 \cdots \lambda_m$ and $\rho = \pm\rho_1 \cdots \rho_n$. Since the cubic residue symbol is unchanged when changing signs in both inputs, we can assume that both signs are positive. By cubic reciprocity:

$$\chi_\rho(\lambda) = \prod_{i=1}^{m}\prod_{j=1}^{n} \chi_{\rho_j}(\lambda_i) = \prod_{i=1}^{m}\prod_{j=1}^{n} \chi_{\lambda_i}(\rho_j) = \chi_\lambda(\rho)$$

This proves the more general cubic reciprocity law (1). (3) is a simple consequence of lemma 2.11 and the multiplicativity of the norm. It remains to show (2). We have two cases. First, let $\lambda = 3m - 1$ be a rational integer. For this case, we follow the elegant proof of K. S. Williams, see [10]:

$$\chi_\lambda(1-\omega) = \chi_\lambda((1-\omega)^2)^2 = \chi_\lambda(-3\omega)^2 = \chi_\lambda(-3)^2\chi_\lambda(\omega)^2 = \chi_\lambda(\omega)^2$$

by proposition 3.8. We get

$$\chi_\lambda(\omega)^2 = \omega^{\frac{2(N\lambda-1)}{3}} = \omega^{2(\lambda^2-1)/3} = \omega^{6m^2-4m} = \omega^{2m}$$

as desired. Now let $\lambda = a + b\omega$ be a complex primary element with $(a, b) = 1$. Write $a = 3m - 1$ and $b = 3n$. An easy computation gives $(N\lambda - 1)/3 \equiv -2m + n \pmod 3$ and $(a^2 - 1)/3 \equiv m \pmod 3$. We will show these claims:

(i) $\chi_\lambda(a) = \omega^m$.

(ii) $\chi_\lambda(a + b) = \omega^{2n}\chi_\lambda(1 - \omega)$.

(iii) $\chi_{a+b}(\lambda) = \chi_{a+b}(1 - \omega)$.

(iv) $\chi_{a+b}(\lambda) = \omega^{2(m+n)}$.

Together, these will imply the supplementary law. By cubic reciprocity (note that a is primary) and proposition 3.8:

$$\chi_\lambda(a) = \chi_a(\lambda) = \chi_a(b\omega) = \chi_a(b)\chi_a(\omega) = \chi_a(\omega) = \omega^{\frac{Na-1}{3}} = \omega^{\frac{a^2-1}{3}} = \omega^m$$

The second claim follows using $a + b = (a + b)\omega\omega^2$:

$$\begin{aligned}\chi_\lambda(a+b) &= \chi_\lambda(\omega^2(a\omega - a)) = \chi_\lambda(-a\omega^2(1-\omega)) = \chi_\lambda(a)\chi_\lambda(\omega)^2\chi_\lambda(1-\omega) \\ &= \omega^m\omega^{\frac{2(N\lambda-1)}{3}}\chi_\lambda(1-\omega) = \omega^{m-4m+2n}\chi_\lambda(1-\omega) = \omega^{2n}\chi_\lambda(1-\omega)\end{aligned}$$

We now compute $\chi_{a+b}(\lambda)$ in two different ways as stated in the claims (note that $a + b$ is primary):

$$\chi_{a+b}(\lambda) = \chi_{a+b}(a(1-\omega)) = \chi_{a+b}(a)\chi_{a+b}(1-\omega) = \chi_{a+b}(1-\omega)$$

The last equality follows from the computation $\chi_{a+b}(a) = \chi_a(a + b) = \chi_a(b) = 1$ since $(a, b) = 1$. The final claim is proved as follows:

$$\begin{aligned}\chi_{a+b}(\lambda) &= \chi_{a+b}(1-\omega) = \chi_{a+b}((1-\omega)^2)^2 = \chi_{a+b}(-3\omega^2) = \chi_{a+b}(\omega^2) \\ &= \omega^{\frac{2((a+b)^2-1)}{3}} = \omega^{2(m+n)}\end{aligned}$$

The supplementary law now follows from cancelling ω^{2n} from both sides of the equation

$$\omega^{2m}\omega^{2n} = \chi_{a+b}(\lambda) = \chi_\lambda(a + b) = \omega^{2n}\chi_\lambda(1-\omega)$$

We now remove the restriction $(a, b) = 1$ and let $\lambda = a + b\omega$ be any primary element. Write $\lambda = k(c + d\omega)$ with $(c, d) = 1$ and $k \equiv 1 \pmod 3$. We see that $c + d\omega$ is primary. We write $a = 3m - 1$, $k = 3n + 1$ and $c = 3m' - 1$. By what we have showed:

$$\chi_\lambda(1-\omega) = \chi_{-k}(1-\omega)\chi_{c+d\omega}(1-\omega) = \omega^{2(m'-n)}$$

So we are done if we have $m' - n \equiv m \pmod 3$. Substituting $k = 3n + 1$ and $c = 3m' - 1$ in the equation $kc + 1 = 3m$ and simplifying gives $3nm' - n + m' = m$. Reducing modulo 3 finishes the proof. ■

3.3 Computing the cubic residue symbol

The fully generalized theorem of cubic reciprocity allows us to write an efficient algorithm for computing the cubic residue character. In the following, for $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, let $\alpha.a$ denote the value for a in a given iteration and likewise with $\alpha.b$. primary(α) denotes the unique primary associate of α.

Algorithm 2: Cubic residue symbol

Input: $\alpha, \beta \in \mathbb{Z}[\omega]$ with $1-\omega \nmid \beta$
Output: $\left(\frac{\alpha}{\beta}\right)_3$
$r \leftarrow 1$
while *(true)* **do**
  $\beta \leftarrow \text{primary}(\beta)$
  $\alpha \leftarrow \alpha \bmod \beta$

  if $\alpha = 0$ **then**
    if $N\beta \neq 1$ **then**
      return 0 `// α and β have a common factor`
    else
      return r

  while $1-\omega \mid \alpha$ **do**
    $\alpha \leftarrow \alpha/(1-\omega)$
    $r \leftarrow r \cdot \omega^{(2(\beta.a+1))/3}$ `// supplementary law for 1 − ω`

  $u \leftarrow \alpha/\text{primary}(\alpha)$
  $\alpha \leftarrow \text{primary}(\alpha)$ `// supplementary law for the units`
  if $u = \pm\omega$ **then**
    if $N\beta \equiv 4 \bmod 9$ **then**
      $r \leftarrow r \cdot \omega$
    if $N\beta \equiv 7 \bmod 9$ **then**
      $r \leftarrow r \cdot \omega^2$
  if $u = \pm\omega^2$ **then**
    if $N\beta \equiv 4 \bmod 9$ **then**
      $r \leftarrow r \cdot \omega^2$
    if $N\beta \equiv 7 \bmod 9$ **then**
      $r \leftarrow r \cdot \omega$
  $(\alpha, \beta) \leftarrow (\beta, \alpha)$ `// cubic reciprocity`

Proof of correctness of algorithm 2. We apply the Euclidean algorithm on α with β in each iteration. This, along with cubic reciprocity at the end, guarantees that the norm of α becomes strictly smaller in each iteration of the outer while-loop. If $\alpha = 0$ after reducing modulo β, we have two cases. If β is not a unit, α and β share a non-trivial factor, and the symbol is 0. Otherwise, we output the result r. In any case, we conclude that the algorithm terminates.

Multiplication by a unit in the denominator does not change the symbol, so we may replace β with its primary associate in the start of each iteration. The first while-loop removes all factors of $1-\omega$ and applies the supplementary law for $1-\omega$ accordingly. This

inner while-loop gives us the obvious loop-invariant that β is never divisible by $1-\omega$ at the start of each iteration. Finally, we replace α by its primary associate and compute the unit u such that $\alpha = u \cdot \text{primary}(\alpha)$. The final if-statements apply the supplementary law for the units to adjust the result r for u. This process of replacing α by primary(α) allows us to apply cubic reciprocity in the final line. Repeating all these steps until α becomes divisible by β, the algorithm will correctly output the cubic residue symbol. ■

The runtime of the above algorithm is clearly identical to the runtime of the Euclidean algorithm in $\mathbb{Z}[\omega]$. This is noticeably faster than modular exponentiation. Furthermore, the algorithm works for any β not divisible by $1-\omega$.

Lastly, we provide an example. Let $\alpha = -1165 + 2880\omega$ and $\beta = 134 - 429\omega$. One can check that $1-\omega$ does not divide β, so the cubic residue symbol is well-defined. Let us use cubic reciprocity to compute the symbol:

$$\begin{aligned}
\left(\frac{-1165+2880\omega}{134-429\omega}\right)_3 &= \left(\frac{-227-123\omega}{134-429\omega}\right)_3 = \left(\frac{227+123\omega}{134-429\omega}\right)_3 = \left(\frac{134-429\omega}{227+123\omega}\right)_3 \\
&= \left(\frac{-8+6\omega}{227+123\omega}\right)_3 = \left(\frac{8-6\omega}{227+123\omega}\right)_3 = \left(\frac{227+123\omega}{8-6\omega}\right)_3 \\
&= \left(\frac{3-5\omega}{8-6\omega}\right)_3 = \left(\frac{-\omega}{8-6\omega}\right)_3 \left(\frac{8+3\omega}{8-6\omega}\right)_3 \quad (N(8-6\omega) = 148 \equiv 4 \pmod 9) \\
&= \omega \left(\frac{9\omega}{8-6\omega}\right)_3 = \omega \left(\frac{\omega}{8-6\omega}\right)_3^2 \left(\frac{(1-\omega)^4}{8-6\omega}\right)_3 \\
&= \omega\omega^2 \left(\frac{1-\omega}{8-6\omega}\right)_3 = \omega^{2\frac{8+1}{3}} = \omega^6 = 1
\end{aligned}$$

The example illustrates an important point. The above symbol was equal to 1, but α is not a cubic residue modulo β. This can only happen when β is not a prime, and in the above case, the factorization of β is given by $\beta = \omega(1-2\omega)(5+2\omega)(-51-26\omega)$. If α was a cubic residue modulo β, α would also be a cubic residue modulo each prime factor of β. In this case however, as the reader may verify,

$$\left(\frac{\alpha}{1-2\omega}\right)_3 = \left(\frac{\alpha}{5+2\omega}\right)_3 = \left(\frac{\alpha}{-51-26\omega}\right)_3 = \omega.$$

4 Quartic reciprocity

4.1 The quartic residue symbol and basic properties

We can define the quartic residue symbol in the same manner as for the cubic residue symbol. Let $\pi \in \mathbb{Z}[i]$ be a prime. If π is not associated to $1+i$, i.e. $N\pi \neq 2$, the residue classes of $\pm 1, \pm i$ are easily seen to be distinct. Thus, they constitute all roots of $x^4 - 1 \pmod \pi$. For any $\alpha \in \mathbb{Z}[i]$ not divisible by π, $\alpha^{(N\pi-1)/4}$ is also a root of x^4-1, hence $\alpha^{(N\pi-1)/4}$ is equal to exactly one of $\pm 1, \pm i$. This makes the following well defined.

Definition 4.1. For a prime π with $N\pi \neq 2$, the quartic (or biquadratic) residue symbol of α modulo π is defined by:

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 0, & \text{if } \pi \mid \alpha \\ i^m, & \text{if } \alpha^{(N\pi-1)/4} \equiv i^m \pmod{\pi} \end{cases}$$

As before, we write χ_π instead of $(\cdot/\pi)_4$. Now assume β is a nonunit not divisible by $1+i$ and let the factorization be given by $\beta = \pi_1 \cdots \pi_m$. The general quartic residue symbol is given by:

$$\chi_\beta(\alpha) = \prod_{i=1}^{m} \chi_{\pi_i}(\alpha)$$

We also need the notion of a primary element in order to state the fundamental theorems.

Definition 4.2. A nonunit $\alpha \in \mathbb{Z}[i]$ is primary if $\alpha \equiv 1 \pmod{2+2i}$.

Lemma 4.3. *A nonunit $\alpha = a + bi \in \mathbb{Z}[i]$ is primary if and only if $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ or $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$.*

Proof. The proof follows from the computation:

$$\frac{a-1+bi}{2+2i} = \frac{(2-2i)((a-1)+bi)}{8} = \frac{(a+b-1)+(b-a+1)i}{4}$$

We see that α is primary if and only if $a+b \equiv 1 \pmod 4$ and $a-b \equiv 1 \pmod 4$. The rest is checking possible cases. ∎

Lemma 4.4. *Let $\alpha \in \mathbb{Z}[i]$ be a nonunit not divisible by $1+i$. Exactly one of the associates of α is primary. Furthermore, any primary element can be factored as a product $\pi_1 \cdots \pi_m(-q_1)\cdots(-q_n)$ of primary primes with $N\pi_i$ a rational prime congruent to 1 modulo 4 and $q_i \equiv 3 \pmod 4$.*

Proof. A straightforward calculation similar to the proofs of proposition 3.5 and lemma 3.6. ∎

We list the following useful properties of the quartic residue symbol:

Proposition 4.5. *Assume $\lambda, \rho, \pi \in \mathbb{Z}[i]$ is not divisible by $1+i$ and let $\alpha \in \mathbb{Z}[i]$ be arbitrary.*

(i) *If $\pi \nmid \alpha$ and π is prime then $\chi_\pi(\alpha) = 1$ if and only if $x^4 \equiv \alpha \pmod \pi$ has a solution in $\mathbb{Z}[i]$.*

(ii) $\chi_\lambda(\alpha\beta) = \chi_\lambda(\alpha)\chi_\lambda(\beta)$.

(iii) $\overline{\chi_\lambda(\alpha)} = \chi_{\overline{\lambda}}(\overline{\alpha})$.

(iv) *If $\alpha \equiv \beta \pmod \lambda$ then $\chi_\lambda(\alpha) = \chi_\lambda(\beta)$.*

(v) $\chi_\rho(\alpha) = \chi_\lambda(\alpha)$ *if* $(\lambda) = (\rho)$.

Proof. The proof is exactly the same as for proposition 3.8. ∎

Proposition 4.6. *Let $a \in \mathbb{Z}$.*

(i) If $q \equiv 3 \pmod 4$ is a prime, $\chi_q(a) = 1$ if a is not divisible by q.

(ii) Let $b \in \mathbb{Z}$ with $b \neq 0$. Assume a is odd and not a unit. If $(a, b) = 1$, $\chi_a(b) = 1$.

Proof. (i) follows from Fermat's little theorem:

$$\chi_q(a) \equiv a^{\frac{q^2-1}{4}} \equiv (a^{q-1})^{\frac{q+1}{4}} \equiv 1 \pmod q$$

To show (ii), factor a into positive primes as $a = p_1 \cdots p_m q_1 \cdots q_n$ with $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$ (we can assume a is positive by proposition 4.5). By (i), we have $\chi_{q_i}(b) = 1$. Write $p_i = \pi\overline{\pi}$ with π a prime, then $\chi_{p_i}(b) = \chi_\pi(b)\chi_{\overline{\pi}}(b) = \chi_\pi(b)\overline{\chi_\pi(b)} = 1$, which proves the claim. ∎

Let us now state the law of quartic reciprocity:

Theorem 4.7 (Law of quartic reciprocity)**.** *Let $\lambda = a + bi$ and $\rho = c + di$ be primary and relatively prime. Then*

$$\chi_\lambda(\rho) = \chi_\rho(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}} \tag{4}$$

We have the supplementary laws:

$$\chi_\lambda(i) = i^{\frac{1-a}{2}}, \quad \chi_\lambda(1+i) = i^{\frac{a-b-b^2-1}{4}} \tag{5}$$

It will be useful to prove the supplementary law for i before embarking on the proof of the general reciprocity law.

Proof of the supplementary law for i. Assume first that $\lambda = a + bi$ is a primary prime. If $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$, we get:

$$\chi_\lambda(i) = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{a^2-1}{4}} = (i^{a+1})^{\frac{a-1}{4}} = (i^{-2})^{\frac{a-1}{4}} = i^{\frac{1-a}{2}}$$

In the other case, we have $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$:

$$\chi_\lambda(i) = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{a^2+4-1}{4}} = i \cdot (i^{a-1})^{\frac{a+1}{4}} = i \cdot i^{\frac{a+1}{2}} = i^{1+\frac{a+1}{2}} = i^{2+\frac{a-1}{2}} = i^{\frac{1-a}{2}}$$

The last equality follows, since $2+(a-1)/2 \equiv (1-a)/2 \pmod 4$ when $a \equiv 3 \pmod 4$. Now let λ be any primary element with factorization $\lambda = \lambda_1 \cdots \lambda_m$, where each λ_i is primary. Then $N\lambda_j \equiv 1 \pmod 4$ for all j and $N\lambda \equiv 1 \pmod 4$. Using the multiplicativity of the norm and lemma 2.11, we get:

$$\chi_\lambda(i) = \prod_{j=1}^{m} \chi_{\lambda_j}(i) = \prod_{j=1}^{m} i^{\frac{N\lambda_j - 1}{4}} = i^{\sum_{j=1}^m \frac{N\lambda_j - 1}{4}} = i^{\frac{N\lambda - 1}{4}}$$

The exact same computations as for the case with λ being prime gives the desired result. ∎

4.2 The theorem of quartic reciprocity

Proving the main theorem and the supplementary law for $1+i$ requires quite a bit of work. We now let π be a primary prime with $N\pi = p \equiv 1 \pmod 4$. As before, we can consider Gauss and Jacobi sums over $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$. To prove the reciprocity law, we need to prove a few lemmas on the Jacobi sum $J(\chi_\pi, \chi_\pi)$.

Lemma 4.8. *We have:*

(i) $J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \chi_\pi^2)$.

(ii) $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

(iii) $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = \pi$.

(iv) $g(\chi_\pi)^4 = \pi^3\overline{\pi}$.

Proof. By proposition 2.6 and 2.10, we have

$$J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\chi_\pi^2)^2} = \chi_\pi(-1)J(\chi_\pi, \chi_\pi)J(\chi_\pi, \chi_\pi^2)$$

This proves (i). (ii) follows by multiplying with $g(\chi_\pi^2)^2$ on both sides of the equation. (iii) is proved in two steps. We first show that $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ is primary. To finish the proof, it will then suffice to show that the left hand side and right hand side are associates. We write the Jacobi sum as

$$J(\chi_\pi, \chi_\pi) = 2\sum_{n=2}^{(p-1)/2} \chi_\pi(n)\chi_\pi(1-n) + \chi_\pi\left(\frac{p+1}{2}\right)^2$$

Recall that all units are congruent to 1 modulo $1+i$. Furthermore, $p \equiv 1 \pmod{2+2i}$. We may also compute:

$$\chi_\pi\left(\frac{p+1}{2}\right)^2 = \chi_\pi(2^{-1})^2 = \chi_\pi(2)^{-2} = \chi_\pi(-i(1+i)^2)^2 = \chi_\pi(-i)^2 = \chi_\pi(-1)$$

All in all, we get:

$$-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) \equiv -\chi_\pi(-1)\left(2\left(\frac{p-3}{2}\right) + \chi_\pi(-1)\right) \equiv 2\chi_\pi(-1) - 1 \equiv 1 \pmod{2+2i}$$

So $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ is a primary element. We have

$$J(\chi_\pi, \chi_\pi) = \sum_{n=0}^{p-1} \chi_\pi(n)\chi_\pi(1-n) \equiv \sum_{n=0}^{p-1} n^{\frac{p-1}{4}}(1-n)^{\frac{p-1}{4}} \pmod{\pi}$$

As in the proof of lemma 3.11, it follows that π divides $J(\chi_\pi, \chi_\pi)$. By proposition 2.9, $N(J(\chi_\pi, \chi_\pi)) = p$, so $J(\chi_\pi, \chi_\pi)$ is prime, which proves the claim. (iv) follows immediately from (ii) and (iii).

■

We now prove a series of special cases of quartic reciprocity.

Proposition 4.9. *Lad $q > 0$ be a prime $q \equiv 3 \pmod 4$, then $\chi_\pi(-q) = \chi_q(\pi)$.*

Proof. We compute (using that $q \equiv 3 \pmod 4$):

$$g(\chi_\pi)^q \equiv \sum_{n=0}^{p-1} \chi_\pi(n)^q \zeta^{qn} \equiv \sum_{n=0}^{p-1} \chi_\pi(n)^3 \zeta^{qn} \equiv g_q(\overline{\chi_\pi}) \equiv \chi_\pi(q^{-1}) g(\overline{\chi_\pi}) \equiv \chi_\pi(q) g(\overline{\chi_\pi}) \pmod q$$

Which implies

$$(g(\chi_\pi)^4)^{\frac{q+1}{4}} = g(\chi_\pi)^{q+1} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \pmod q$$

Now write $\pi = a + bi$. By Fermat's little theorem, $\pi^q = (a+bi)^q \equiv a^q + (bi)^q \equiv a - bi \equiv \overline{\pi} \pmod q$. Using corollary 2.7 and lemma 4.8, we get

$$\pi^{\frac{(q+3)(q+1)}{4}} \equiv \chi_\pi(-1)\chi_\pi(q)\pi^{q+1} \pmod q$$

In other words, $\pi^{(q^2-1)/4} \equiv \chi_\pi(-q) \pmod q$, i.e. $\chi_q(\pi) \equiv \chi_\pi(-q) \pmod q$. Both sides are units, so the proof is complete. ∎

Proposition 4.10. *Let $q \equiv 1 \pmod 4$ be a prime, then $\chi_\pi(q) = \chi_q(\pi)$.*

Proof. Since $q \equiv 1 \pmod 4$

$$g(\chi_\pi)^q \equiv \sum_{n=0}^{p-1} \chi_\pi(n)^q \zeta^{qn} \equiv \sum_{n=0}^{p-1} \chi_\pi(n) \zeta^{qn} \equiv g_q(\chi_\pi) \equiv \overline{\chi_\pi(q)} g(\chi_\pi) \pmod q$$

So $g(\chi_\pi)^{q+3} \equiv \overline{\chi_\pi(q)} g(\chi_\pi)^4$, so by lemma 4.8:

$$(\pi^3\overline{\pi})^{\frac{q+3}{4}} \equiv \overline{\chi_\pi(q)}\pi^3\overline{\pi} \pmod q$$

Since $(q, \pi) = (q, \overline{\pi}) = 1$, we may divide by $\pi^3\overline{\pi}$ on both sides and get:

$$(\pi^3)^{\frac{q-1}{4}} \overline{\pi}^{\frac{q-1}{4}} \equiv \overline{\chi_\pi(q)} \pmod q$$

Write $q = \lambda\overline{\lambda}$ with λ irreducible, then:

$$\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) \equiv \overline{\chi_\pi(q)} \pmod \lambda$$

Both sides are units and $\lambda \neq 1 + i$, so we actually have $\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi(q)}$. We may rewrite this equation as $\chi_{\overline{\lambda}}(\overline{\pi})\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi(q)}$ i.e. $\chi_q(\overline{\pi}) = \chi_\pi(q)$. We conclude that $\chi_\pi(q) = \chi_q(\pi)$. ∎

Proposition 4.11. *Let $a \in \mathbb{Z}$ and $a \equiv 1 \pmod 4$ and λ be primary. Assume $(\lambda, a) = 1$, then $\chi_a(\lambda) = \chi_\lambda(a)$.*

Proof. Factor a as $a = \pm p_1 \cdots p_s \cdot q_1 \cdots q_t$ with $p_i, q_i > 0$, $q_i \equiv 3 \pmod 4$ and $p_i \equiv 1 \pmod 4$. As λ is primary, we may factor λ as $\lambda = \pi_1 \cdots \pi_m(-q_1') \cdots (-q_n')$ with π_i, q_i' primary and irreducible with $N\pi_i \equiv 1 \pmod 4$ and $q_i' \equiv 3 \pmod 4$. Assume first that the sign of

a is positive. This implies that t is even, hence $\prod_{l=1}^{t}\chi_{\pi_i}(q_l)=\prod_{l=1}^{t}\chi_{\pi_i}(-q_l)$ for each i. Using proposition 4.9, 4.10 and 4.6:

$$\begin{aligned}\chi_\lambda(a)&=\prod_{i=1}^{m}\chi_{\pi_i}(a)\prod_{j=1}^{n}\chi_{-q_j'}(a)=\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{k=1}^{s}\prod_{l=1}^{t}\chi_{\pi_i}(p_k)\chi_{\pi_i}(q_l)\chi_{-q_j'}(p_k)\chi_{-q_j'}(q_l)\\&=\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{k=1}^{s}\prod_{l=1}^{t}\chi_{\pi_i}(p_k)\chi_{\pi_i}(-q_l)\chi_{-q_j'}(p_k)\chi_{-q_j'}(q_l)\\&=\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{k=1}^{s}\prod_{l=1}^{t}\chi_{p_k}(\pi_i)\chi_{q_l}(\pi_i)\chi_{p_k}(-q_j')\chi_{q_l}(-q_j')=\chi_a(\lambda)\end{aligned}$$

In the rare case where the reader is interested in doing the same calculation for $a<0$, note that we get the factor $\chi_{\pi_i}(-1)\chi_{-q_j'}(-1)$ in the product in the first line above. Then use that $\chi_{-q_j'}(-1)=1$ by the supplementary law for the units, and that $\chi_{\pi_i}(-1)\chi_{\pi_i}(q_l)=\chi_{\pi_i}(-q_l)$. ■

Proposition 4.12. *Let $\lambda=a+bi$ and $\rho=c+di$ be primary and relatively prime. If $(a,b)=(c,d)=1$ then*

$$\chi_\lambda(\rho)=\chi_\rho(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}$$

Proof. We start with the observations that $(a,\lambda)=(b,\lambda)=(c,\rho)=(d,\rho)=1$, $c\lambda\equiv ac+bd \pmod{\rho}$ and $a\rho\equiv ac+bd \pmod{\lambda}$. The latter relations imply $(ac+bd,\rho)=(ac+bd,\lambda)=1$. We thus have the equations:

$$\chi_\rho(c)\chi_\rho(\lambda)=\chi_\rho(ac+bd),\quad \chi_\lambda(a)\chi_\lambda(\rho)=\chi_\lambda(ac+bd)$$

Taking the conjugate of $\chi_\lambda(a)\chi_\lambda(\rho)$ and multiplying by $\chi_\rho(c)\chi_\rho(\lambda)$ gives:

$$\chi_\rho(c)\chi_{\overline{\lambda}}(a)\chi_\rho(\lambda)\overline{\chi_\lambda(\rho)}=\chi_{\rho\overline{\lambda}}(ac+bd)$$

Where we used proposition 4.5. We get:

$$\chi_\rho(\lambda)\overline{\chi_\lambda(\rho)}=\chi_{\overline{\rho}}(c)\chi_\lambda(a)\chi_{\rho\overline{\lambda}}(ac+bd) \tag{6}$$

We now assume that neither a, c nor $ac+bd$ is a unit. Let n be an odd integer and define $\varepsilon(n)=(-1)^{(n-1)/2}$. Clearly, $\varepsilon(n)n\equiv 1 \pmod 4$ and $\varepsilon(ac+bd)=\varepsilon(a)\varepsilon(c)$ because bd is divisible by 4. We write $\chi_\alpha(x)=\chi_\alpha(\varepsilon(x))\chi_\alpha(\varepsilon(x)x)$ for $\alpha\in\{\overline{\rho},\lambda,\rho\overline{\lambda}\}$ and $x\in\{a,c,ac+bd\}$. We also note that $\chi_\alpha(\varepsilon(x))=\chi_{\overline{\alpha}}(\varepsilon(x))$. These observations allow us to use proposition 4.11 and obtain:

$$\chi_\rho(\lambda)\overline{\chi_\lambda(\rho)}=\chi_c(\overline{\rho})\chi_a(\lambda)\chi_{ac+bd}(\rho\overline{\lambda})$$

The three terms on the right hand side can be computed using proposition 4.6:

$$\begin{aligned}\chi_c(\overline{\rho})&=\chi_c(c-di)=\chi_c(-di)=\chi_c(i)\\\chi_a(\lambda)&=\chi_a(a+bi)=\chi_a(bi)=\chi_a(i)\\\chi_{ac+bd}(\overline{\lambda}\rho)&=\chi_{ac+bd}((ad-bc)i)=\chi_{ac+bd}(i)\end{aligned}$$

So by the supplementary law for i:

$$\chi_\rho(\lambda)\overline{\chi_\lambda(\rho)} = \chi_{(ac+bd)ac}(i) = i^{\frac{(ac+bd)ac-1}{2}} = (-1)^{\frac{(ac+bd)ac-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}}$$

The last equality can be seen as follows. a and c are odd in any case, so $(ac)^2 \equiv 1 \pmod 8$, so it suffices to show $acbd \equiv (a-1)(c-1) \pmod 8$. If $b \equiv 0$ or $d \equiv 0 \pmod 4$, $acbd \equiv 0 \equiv (a-1)(c-1) \pmod 8$ since $a \equiv 1$ or $c \equiv 1 \pmod 4$ in these cases. One easily checks that $acbd \equiv 4 \equiv (a-1)(c-1) \pmod 8$ when $b \equiv d \equiv 2 \pmod 4$ and $a \equiv c \equiv 3 \pmod 4$. This finishes the proof when neither a, c nor $ac+bd$ is a unit.

We now consider the case where a, c or $ac+bd$ is a unit. If $a = \pm 1$, $c = \pm 1$ or $ac + bd = \pm 1$, we can skip the process of switching numerator and denominator in the residue symbol in (6) and instead, if necessary, apply the supplementary law for i to obtain the same congruence as before. ■

We finally have all the necessary tools to give a proof of the quartic reciprocity law.

Proof of quartic reciprocity. Write the primary elements λ and ρ as $\lambda = m(a+bi)$ and $\rho = n(c+di)$ so that $m \equiv n \equiv 1 \pmod 4$ and $(a,b) = (c,d) = 1$. To see why this is possible, simply factor out the greatest common divisor from λ and ρ. If this is congruent to 3 modulo 4, multiply by -1 twice to get the desired form. Using all the previous propositions, we get:

$$\begin{aligned}\chi_\lambda(\rho) &= \chi_\lambda(n)\chi_\lambda(c+di) = \chi_n(\lambda)\chi_m(c+di)\chi_{a+bi}(c+di)\\ &= \chi_n(\lambda)\chi_{c+di}(m)\chi_{c+di}(a+bi)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}\\ &= \chi_\rho(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}\end{aligned}$$

■

It remains to prove the supplementary law for $1+i$. An elementary proof is harder than one would expect. First we shall prove a handful of useful lemmas.

Lemma 4.13. *Let p be a prime $p \equiv 1 \pmod 4$ and q a positive prime with $q \equiv 3 \pmod 4$. Then:*

(i) $\chi_p(1+i) = i^{\frac{p-1}{4}}$.

(ii) $\chi_q(1+i) = i^{\frac{-q-1}{4}}$.

Proof. To prove (i), write $p = \pi\overline{\pi}$ with π irreducible. We calculate:

$$\begin{aligned}\chi_p(1+i) = \chi_\pi(1+i)\chi_{\overline{\pi}}(1+i) = \chi_\pi(1+i)\overline{\chi_\pi(1-i)} = \chi_\pi(1+i)\chi_\pi(1-i)^3\\ = \chi_\pi(i(1-i))\chi_\pi(1-i)^3 = \chi_\pi(i)\chi_\pi(1-i)^4 = \chi_\pi(i) = i^{\frac{p-1}{4}}\end{aligned}$$

To prove (ii), we note that $(1+i)^{q-1} \equiv -i \pmod q$. This is because $(1+i)^q \equiv 1+i^q \equiv 1-i \pmod q$, hence $(1+i)^{q-1} \equiv (1-i)/(1+i) \equiv -i \pmod q$. The rest is an easy calculation:

$$\chi_q(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} \equiv ((1+i)^{q-1})^{\frac{q+1}{4}} \equiv (-i)^{\frac{q+1}{4}} \equiv i^{\frac{-q-1}{4}} \pmod q$$

■

Corollary 4.14. *The above results hold when p is replaced by any integer $a \equiv 1 \pmod 4$ and q is replaced by any positive integer $a \equiv 3 \pmod 4$.*

Proof. Let $a \equiv 1 \pmod 4$ and factor $a = p_1 \cdots p_m q_1 \cdots q_n$ with $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$. We may assume $a > 0$ (a potential negative sign is killed since $\chi_{-p_i}(1+i) = \chi_{p_i}(1+i)$), so by lemma 2.11:

$$\begin{aligned}\chi_a(1+i) &= \prod_{i=1}^{m}\prod_{j=1}^{n}\chi_{p_i}(1+i)\chi_{q_j}(1+i) = \prod_{i=1}^{m}\prod_{j=1}^{n} i^{\frac{p_i-1}{4}} i^{\frac{-q_j-1}{4}} \\ &= i^{\sum_{i=1}^{m}\frac{p_i-1}{4}+\sum_{j=1}^{n}\frac{-q_j-1}{4}} = i^{\frac{a-1}{4}}\end{aligned}$$

The last equality follows because n is even. When $a \equiv 3 \pmod 4$, n will be odd (by assumption, a is positive in this case), so we get $\chi_a(1+i) = i^{(-a-1)/4}$. ∎

Lemma 4.15. *Let $\pi = a + bi \in \mathbb{Z}[i]$ be a primary prime. Then:*

(i) $\chi_\pi(a) = i^{\frac{a-1}{2}}$ *when* $\pi \equiv 1 \pmod 4$.

(ii) $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$ *when* $\pi \equiv 3 + 2i \pmod 4$.

(iii) $\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}$.

Proof. We start by noting that irreducibility of π guarantees $(a, b) = 1$. Assume $\pi \equiv 1 \pmod 4$ i.e. $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$. By proposition 4.11, 4.6 and the supplementary law:

$$\chi_\pi(a) = \chi_a(\pi) = \chi_a(bi) = \chi_a(b)\chi_a(i) = \chi_a(i) = i^{\frac{1-a}{2}} = i^{\frac{a-1}{2}}$$

The last equality follows from $a \equiv 1 \pmod 4$ and $2 \equiv -2 \pmod 4$. This shows (i). To show (ii), assume $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$. We compute:

$$\begin{aligned}\chi_\pi(a) &= \chi_\pi(-1)\chi_\pi(-a) = (-1)^{\frac{a-1}{2}}\chi_{-a}(\pi) = -\chi_{-a}(bi) \\ &= -\chi_{-a}(b)\chi_{-a}(i) = -\chi_{-a}(i) = -i^{\frac{-a-1}{2}}\end{aligned}$$

Now let π be an arbitrary primary prime. Using the corollary above and the simple observations $a + b \equiv 1 \pmod 4$ and $a + ai = a + b + i\pi$, (iii) follows from a somewhat lengthy computation:

$$\begin{aligned}\chi_\pi(a)\chi_\pi(1+i) &= \chi_\pi(a(1+i)) = \chi_\pi(a+b+i\pi) = \chi_\pi(a+b) \\ &= \chi_{a+b}(\pi) = \chi_{a+b}(a-ai) = \chi_{a+b}(a)\chi_{a+b}(1-i) \\ &= \chi_{a+b}(1-i) = \overline{\chi_{a+b}(1+i)} = \chi_{a+b}(1+i)^3 = i^{\frac{3(a+b-1)}{4}}\end{aligned}$$

The final equality is just the above corollary. ∎

If the reader has not yet been discouraged by these endless series of congruences, the final proof on quartic reciprocity is in sight at long last.

Proof of the supplementary law for $1+i$. We first assume that π is a prime and use the previous lemma. If $\pi \equiv 1 \pmod 4$, we get:

$$\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}} \cdot (i^{\frac{a-1}{2}})^{-1} = i^{\frac{3a+3b-3-2a-2}{4}} = i^{\frac{a+3b-1}{4}} = i^{\frac{a-b-b^2-1}{4}}$$

And if $\pi \equiv 3+2i \pmod 4$, we compute:

$$\begin{aligned}\chi_\pi(1+i) &= i^{\frac{3(a+b-1)}{4}}(-i^{\frac{-a-1}{2}})^{-1} = -i^{\frac{3(a+b-1)}{4}} i^{\frac{a+1}{2}} = -i^{\frac{5a+3b-1}{4}} \\ &= i^{2+a+b+\frac{a-b-1}{4}} = i^{-1+\frac{a-b-1}{4}} = i^{\frac{a-b-b^2-1}{4}}\end{aligned}$$

Hence the formula holds in both cases. We now prove the law for general primary elements. By a simple induction argument, it suffices to show that for primary $\pi_1 = a_1 + b_1 i$ and $\pi_2 = a_2 + b_2 i$, we have:

$$\frac{a_1 - b_1 - b_1^2 - 1}{4} + \frac{a_2 - b_2 - b_2^2 - 1}{4} \equiv \frac{a - b - b^2 - 1}{4} \pmod 4$$

where $a = a_1 a_2 - b_1 b_2$ and $b = a_1 b_2 + a_2 b_1$. We multiply through by four and consider the relation modulo 16. We have four cases, two of them being symmetric. If $b_1 \equiv 0 \pmod 4$ and $b_2 \equiv 2 \pmod 4$, we have the following relations modulo 16:

$$a_2 b_1 \equiv 3b_1, \quad a_1 b_1 \equiv 2(a_1 - 1) + b_2, \quad b_1 b_2 \equiv 2b_1, \quad a_1 a_2 \equiv 3(a_1 - 1) + a_2 \pmod{16}$$

We now do the calculation (we let the reader fill in the details of calculating $(2(a_1-1) + b_2 + 3b_1)^2$ with the proper reductions):

$$\begin{aligned}a - b - b^2 - 1 &\equiv 3(a_1 - 1) + a_2 - 2b_1 - 2(a_1 - 1) - b_2 - 3b_1 - (2(a_1 - 1) + b_2 + 3b_1)^2 - 1 \\ &\equiv a_1 - 1 + a_2 - 5b_1 - b_2 - (4 + 8(a_1 - 1) + 4b_2 + b_2^2 - 8a_1 - 8 + 4) - 1 \\ &\equiv a_1 - b_1 - b_1^2 - 1 + a_2 - b_2 - b_2^2 - 1 \pmod{16}\end{aligned}$$

Which is what we wanted to show. The case $b_1 \equiv 2 \pmod 4$ and $b_0 \equiv 0 \pmod 4$ follows by symmetry, and the other cases follow a similar strategy. Determine relations for $a_1 a_2$, $b_1 b_2$, $a_1 b_2$ and $a_2 b_1$ modulo 16 and simplify. ■

4.3 Computing the quartic residue symbol

We can now write an algorithm completely analogous to algorithm 2. Let $\Re(\alpha)$ and $\Im(\alpha)$ denote the real and imaginary part of α in a given iteration, respectively:

Algorithm 3: Quartic residue symbol

Input: $\alpha, \beta \in \mathbb{Z}[i]$ with $1+i \nmid \beta$
Output: $\left(\frac{\alpha}{\beta}\right)_4$
$r \leftarrow 1$
while ***(true)*** **do**
  $\beta \leftarrow \text{primary}(\beta)$
  $\alpha \leftarrow \alpha \bmod \beta$

  if $\alpha = 0$ **then**
    if $N\beta \neq 1$ **then**
      return 0 `// α and β have a common factor`
    else
      return r

  while $1+i \mid \alpha$ **do**
    $\alpha \leftarrow \alpha/(1+i)$
    $r \leftarrow r \cdot i^{(\Re(\beta)-\Im(\beta)-\Im(\beta)^2-1)/4}$ `// supplementary law for 1+i`

  $u \leftarrow \alpha/\text{primary}(\alpha)$
  $\alpha \leftarrow \text{primary}(\alpha)$ `// supplementary law for the units`
  if $u = -1$ **then**
    $r \leftarrow r \cdot i^{1-\Re(\beta)}$
  if $u = i$ **then**
    $r \leftarrow r \cdot i^{(1-\Re(\beta))/2}$
  if $u = -i$ **then**
    $r \leftarrow r \cdot i^{3(1-\Re(\beta))/2}$
  if $\Re(\alpha) = 3 \bmod 4$ **and** $\Re(\beta) = 3 \bmod 4$ **then**
    $r \leftarrow -r$ `// quartic reciprocity`
  $(\alpha, \beta) \leftarrow (\beta, \alpha)$

Let us compute the symbol $(-7/11+6i)_4$:

$$\begin{aligned}\left(\frac{-7}{11+6i}\right)_4 &= \left(\frac{11+6i}{-7}\right)_4 = \left(\frac{-3-i}{-7}\right)_4 = \left(\frac{1+i}{-7}\right)_4 \cdot \left(\frac{-2+i}{-7}\right)_4 \\ &= i^{\frac{-7-1}{4}} \cdot \left(\frac{-i}{-7}\right)_4 \left(\frac{-1-2i}{-7}\right)_4 \\ &= (-1) \cdot \left(\frac{-1}{-7}\right)_4 \cdot \left(\frac{i}{-7}\right)_4 \cdot \left(\frac{-7}{-1-2i}\right)_4 \\ &= (-1) \cdot i^{1-(-7)} i^{\frac{1-(-7)}{2}} = (-1) \cdot \left(\frac{-i}{-1-2i}\right)_4 \\ &= (-1) \cdot \left(\frac{-1}{-1-2i}\right)_4 \cdot \left(\frac{i}{-1-2i}\right)_4 = (-1) \cdot i^{1-(-1)} i^{\frac{1-(-1)}{2}} = i\end{aligned}$$

Since $N(11+6i) = 157$ is a prime, so is $11+6i$, so we may conclude that -7 is a quartic non-residue modulo $6+11i$. This example is found in a table in Gauss' second thesis on biquadratic residues, see [2, p. 572]. In the table, it is listed as though $(-7/11+6i)_4 = 1$. However, it is likely that -7 was simply printed slightly off, since the correct placement is just below its place in the document. So whether Gauss made a calculation error or the error was made in print will likely remain a mystery. The astute reader may verify that all 148 other entries in the table are correct.

5 Class field theory and the Hilbert symbol

In this section, we introduce some notions of class field theory, including the Hilbert symbol, which we will utilize to give an alternate proof of cubic reciprocity. We follow the exposition in [6] unless stated otherwise.

In the following, whenever we have an infinite Galois extension L/K, the Galois group $G(L/K)$ is endowed with the Krull topology, i.e. the topology with basis around 1 equal to all cosets $G(L/M)$, where M runs through all finite subextensions of L/K. If L/K is finite, $G(L/K)$ simply has the discrete topology. In any case, this makes $G(L/K)$ a topological group, as is readily checked:

Lemma 5.1. *$G(L/K)$ is a topological group in the Krull topology and the basis of subgroups around 1 $\{G(L/M) \mid M/K$ a finite subextension$\}$ consists of normal subgroups.*

Proof. The multiplication $G \times G \to G$, $(\sigma, \tau) \mapsto \sigma\tau$ is continuous since the preimage of the basis neighbourhood $\sigma\tau G(M/K)$ contains the open subset $\sigma G(M/K) \times \tau G(M/K)$. The inverse map $\sigma \mapsto \sigma^{-1}$ is also continuous as the preimage of the basis neighbourhood $\sigma^{-1}G(M/K)$ contains $\sigma G(M/K)$. For any finite Galois subextension M/K, M is a splitting field of some polynomial f. Any $\sigma \in G(L/K)$ will permute the roots of f and hence $\sigma(M) = M$. Let $\tau \in G(L/M)$. Then for any $x \in M$, we have $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$. This proves that $G(L/M) \trianglelefteq G(L/K)$ as claimed. ∎

If L/K is a Galois extension, we can consider maps $f : G(L/K) \to L^\times$ satisfying $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$. These are called *crossed homomorphisms*. A special case of crossed homomorphisms are the maps $f_a : G(L/K) \to L^\times$ given by $f_a(\sigma) = \sigma a/a$ for some $a \in L^\times$. We state the following important theorem for later use (for a proof, we refer to [6, p. 14]):

Theorem 5.2 (Hilbert's Satz 90)**.** *Let L/K be a finite Galois extension. Any crossed homomorphism $f : G(L/K) \to L^\times$ is of the form $f = f_a$ for some $a \in L^\times$.*

5.1 Kummer theory

Definition 5.3. Let K be a field containing the n'th roots of unity and assume $(\mathrm{char}K, n) = 1$. A Kummer extension of K is an extension of the form $L = K(\sqrt[n]{\Delta})$ where Δ is a subgroup of $K^\times$ containing the group $K^{\times n}$ of n-th powers.

The definition means that L is generated by all n-th roots $\sqrt[n]{a}$ for $a \in \Delta$.

Lemma 5.4. *A Kummer extension L/K is abelian of exponent n, i.e. $G(L/K)$ is abelian and $\sigma^n = 1$ for all $G(L/K)$. Conversely, if L/K is abelian of exponent n, then $L = K(\sqrt[n]{\Delta})$ for $\Delta = L^{\times n} \cap K^\times$.*

Proof. Let L/K be a Kummer extension, $L = K(\sqrt[n]{\Delta})$. L/K is the composite of all its finite subextensions and, by construction, each of these finite subextensions are themselves composites of cyclic subextensions of the form $K(\sqrt[n]{a})/K$ for $a \in \Delta$. These are all Galois with Galois group a subgroup of μ_n (if b is a root of $x^n - a$, the homomorphism $G(L/K) \to \mu_n$, $\sigma \mapsto \sigma b/b$ is an injection), hence L/K is abelian. Let $\sigma \in G(L/K)$. Then we have $\sigma^n = 1$ when σ is restricted to any finite cyclic subextension of the form $K(\sqrt[n]{a})/K$, hence we have $\sigma^n = 1$ on L.
Conversely, let L/K be abelian of exponent n and $\Delta = L^{\times n} \cap K^\times$. Obviously, $K(\sqrt[n]{\Delta}) \subseteq L$. Again, L/K is the composite of its cyclic subextensions. It thus suffices to prove $M \subseteq K(\sqrt[n]{\Delta})$ for any cyclic subextension M/K. $G(M/K)$ has order dividing n (this follows from $\sigma^n = 1$). Thus, M is of the form $M = K(\sqrt[n]{a})$ with $a \in L^{\times n} \cap K^\times$, so $M \subseteq K(\sqrt[n]{\Delta})$, and the proof is complete. ∎

The following result is essential in Kummer theory, simplified for our purposes:

Theorem 5.5. *If $L = K(\sqrt[n]{\Delta})$ is a Kummer extension, then $\Delta = L^{\times n} \cap K^\times$ and we have an isomorphism*

$$\mathrm{Hom}(G(L/K), \mu_n) \cong \Delta/K^{\times n}$$

given by

$$\Delta/K^{\times n} \to \mathrm{Hom}(G(L/K), \mu_n), \quad a \pmod{K^{\times n}} \mapsto \chi_a \text{ with } \chi_a(\sigma) = \frac{\sigma\sqrt[n]{a}}{\sqrt[n]{a}}$$

Proof. Let L/K be a Kummer extension. Then $L = K(\sqrt[n]{\Delta})$ with $\Delta = L^{\times n} \cap K^\times$ by the previous lemma. Define the homomorphism

$$\Delta \to \mathrm{Hom}(G(L/K), \mu_n), \quad a \mapsto \chi_a$$

with $\chi_a(\sigma) = \sigma\sqrt[n]{a}/\sqrt[n]{a}$. We have $\chi_a = 1$ if and only if $\sigma\sqrt[n]{a} = \sqrt[n]{a}$ for all $\sigma \in G(L/K)$ if and only if $\sqrt[n]{a} \in K^\times$ i.e. $a \in K^{\times n}$. Thus, the kernel of the map is $K^{\times n}$ and we have an injective homomorphism

$$\Delta/K^{\times n} \to \mathrm{Hom}(G(L/K), \mu_n)$$

For surjectivity, there are two cases. Assume first that $G(L/K)$ is finite. Let $\chi \in \mathrm{Hom}(G(L/K), \mu_n)$, then $\chi : G(L/K) \to L^\times$ is a crossed homomorphism, since $\chi(\sigma\tau) =$

$\chi(\sigma)\chi(\tau) = \chi(\sigma)\sigma\chi(\tau)$ as $\chi(\tau) \in \mu_n \subseteq K$. By Hilbert's Satz 90, there exists a $b \in L^\times$ such that

$$\chi(\sigma) = \frac{\sigma b}{b} \quad \text{for all} \quad \sigma \in G(L/K)$$

Since $\sigma(b^n) = \sigma(b)^n = \chi(\sigma)^n b^n = b^n$ for all $\sigma \in G(L/K)$, we must have $b^n = a \in K^\times \cap L^{\times n} = \Delta$, so $\chi = \chi_a$, proving surjectivity in the finite case. Now assume L/K is an infinite extension. In this case, we regard $\mathrm{Hom}(G(L/K), \mu_n)$ as the set of all continuous homomorphisms $\chi : G(L/K) \to \mu_n$. We let $\{\Delta_i/K^{\times n}\}$ denote the set of all finite subgroups of $\Delta/K^{\times n}$, and we set $L_i = K(\sqrt[n]{\Delta_i})$. We then have $\Delta/K^{\times n} = \bigcup_i \Delta_i/K^{\times n}$ and $L = \bigcup_i L_i$. Thus, the groups $G(L/L_i)$ form a basis of open neighbourhoods of 1 in $G(L/K)$. Let $\chi : G(L/K) \to \mu_n$ be a continuous homomorphism, then the kernel is open and hence must contain a subgroup $G(L/L_i)$. χ induces a homomorphism $\tilde{\chi} : G(L_i/K) \to \mu_n$ such that $\chi(\sigma) = \tilde{\chi}(\sigma|_{L_i})$. By the proof we just gave of the finite case, we have $\tilde{\chi} = \tilde{\chi}_a$ for some $a \in \Delta_i$. Then $\chi(\sigma) = \tilde{\chi}_a(\sigma|_{L_i}) = \sigma\sqrt[n]{a}/\sqrt[n]{a} = \chi_a(\sigma)$, hence $\chi = \chi_a$, and the proof is complete. ■

5.2 The reciprocity map and the norm residue symbol

We quickly recall the definition of a local field and the local reciprocity law. In particular, the norm-residue symbol will be needed to define the Hilbert symbol. A field K is called a *local field* if it is complete with respect to a discrete valuation and it has a finite residue class field. It can be shown that any local field is either a finite extension of the p-adic numbers $\mathbb{Q}_p$ (local fields of this form are called p-adic number fields) or the field $\mathbb{F}_p(t)$ of formal Laurent series over $\mathbb{F}_p$ (see chapter II, §5 in [7]).

Let K be a local field and let $\tilde{K}/K$ be the maximal unramified extension of K. This is equal to the composite of each finite unramified extension of K. Let L/K be a finite extension so that L is itself a local field. If $\mathfrak{p}_K$ and $\mathfrak{p}_L$ denote the maximal ideals of the valuation rings $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively, we have an extension (Galois) of the residue fields $L/\mathfrak{p}_L$ over $K/\mathfrak{p}_K$. The Galois group is cyclic of order f, called the *inertia degree* (see chapter 4 in [5]). It has a generator, denoted by ϕ, satisfying

$$\phi(a) \equiv a^{|K/\mathfrak{p}_K|} \pmod{\mathfrak{p}_L} \text{ for all } a \in \mathcal{O}_L$$

This generator is called the *Frobenius automorphism*. For an infinite extension, the Frobenius automorphism becomes a so called topological generator. For a local field K, $\phi_K \in G(\tilde{K}/K)$ denotes the Frobenius automorphism of the maximal unramified extension $\tilde{K}$ of K. Consider a finite extension L/K and fix some Galois extension M of K containing L. If $n = [L : K]$ and H is the subgroup of $G(M/K)$ with fixed field L, let $\sigma_1, ..., \sigma_n$ be a system of left coset representatives of H in $G(M/K)$. We define the *norm-map*

$$N_{L/K} : L \to K \quad \text{by} \quad N_{L/K}(a) = \prod_{i=1}^{n} \sigma_i(a).$$

We then have $N_{L/K}L = \{N_{L/K}(a) \mid a \in L\}$. We can now state

Theorem 5.6 (The local reciprocity law)**.** *For every Galois extension L/K of local fields, we have a canonical isomorphism*

$$r_{L/K} : G(L/K)^{ab} \to K^\times/N_{L/K}L^\times$$

given as follows: Let $\sigma \in G(L/K)$ and let $\tilde{\sigma} \in G(\tilde{L}/K)$ be a lift of σ (i.e. $\tilde{\sigma}|_L = \sigma$) satisfying $\tilde{\sigma}|_{\tilde{K}} = \phi_K^n$ for some $n \in \mathbb{N}$ (called a Frobenius lift *of σ). If M is the fixed field of $\tilde{\sigma}$ and π_M is a prime element of M (i.e. π_M generates the maximal ideal in $\mathcal{O}_M$), then*

$$r_{L/K}(\sigma) = N_{M/K}(\pi_M) \pmod{N_{L/K}L^\times}$$

That this map is even well-defined is a rather lengthy and technical argument. A full exposition can be found in chapter II of [6]. The map has an inverse, from which we obtain a map called the *local norm residue symbol*:

$$(\cdot, L/K) : K^\times \to G(L/K)^{ab}$$

with kernel $N_{L/K}L^\times$. Another theorem we shall use is the following:

Theorem 5.7. *If K is a local field which contains the n-th roots of unity and $L = K(\sqrt[n]{K^\times})$, then*

$$G(L/K) \cong K^\times/K^{\times n} \text{ with } K^\times \ni a \mapsto (a, L/K) \in G(L/K)$$

5.3 The Hilbert symbol

Now let K be a local field containing μ_n with $(\mathrm{char}K, n) = 1$. Let $L = K(\sqrt[n]{K^\times})$ be the maximal Kummer extension of K of exponent n, then

$$\mathrm{Hom}(G(L/K), \mu_n) \cong K^\times/K^{\times n},$$

but by class field theory, we also have

$$G(L/K) \cong K^\times/K^{\times n},$$

so the bilinear map

$$G(L/K) \times \mathrm{Hom}(G(L/K), \mu_n) \to \mu_n, \quad (\sigma, \chi) \mapsto \chi(\sigma)$$

defines a nondegenerate bilinear (in the multiplicative sense) pairing

$$\left(\frac{\cdot, \cdot}{\mathfrak{p}}\right)_n : K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

called the *Hilbert symbol*. We go through the basic properties of the Hilbert symbol.

Lemma 5.8. *For $a, b \in K^\times$, the Hilbert symbol $(a, b/\mathfrak{p})_n$ is given by*

$$(a, K(\sqrt[n]{b})/K)\,\sqrt[n]{b} = \left(\frac{a, b}{\mathfrak{p}}\right)_n \sqrt[n]{b}$$

Proof. Under the isomorphism $K^\times/K^{\times n} \cong G(L/K)$, the image of a is the norm residue symbol $\sigma = (a, L/K)$. The isomorphism $K^\times/K^{\times n} \cong \mathrm{Hom}(G(L/K), \mu_n)$ maps b to the map $\chi_b : G(L/K) \to \mu_n$ given by $\chi_b(\tau) = \tau\sqrt[n]{b}/\sqrt[n]{b}$. Spelling out the definition of the Hilbert symbol, we have

$$\left(\frac{a, b}{\mathfrak{p}}\right)_n = \chi_b(\sigma) = \frac{\sigma\sqrt[n]{b}}{\sqrt[n]{b}},$$

and so $(a, K(\sqrt[n]{b})/K)\,\sqrt[n]{b} = (a, b/\mathfrak{p})_n\,\sqrt[n]{b}$. ∎

Proposition 5.9. *We have the following properties of the Hilbert symbol:*

(i) $\left(\frac{aa',b}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{a',b}{\mathfrak{p}}\right)_n$

(ii) $\left(\frac{a,bb'}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{a,b'}{\mathfrak{p}}\right)_n$

(iii) $\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^{-1}$

(iv) $\left(\frac{a,-a}{\mathfrak{p}}\right)_n = 1$

(v) $\left(\frac{a,1-a}{\mathfrak{p}}\right)_n = 1$

Proof. (i) and (ii) is just bilinearity of the Hilbert symbol. If $b \in K^\times$ and $x \in K$ such that $x^n - b \neq 0$ and ζ is a primitive n-th root of unity, we have

$$x^n - b = \prod_{i=0}^{n-1} (x - \zeta^i \beta), \quad \beta^n = b.$$

Write $n = d \cdot m$, where d is the greatest divisor of n such that $y^d = b$ has a solution in K. $K(\beta)/K$ is a cyclic extension of degree m, and the conjugates of $x - \zeta^i\beta$ are the elements $x - \zeta^j\beta$ with $j \equiv i \pmod{d}$. Therefore

$$x^n - b = \prod_{i=0}^{d-1} N_{K(\beta)/K}(x - \zeta^i \beta),$$

implying that $x^n - b$ is a norm of $K(\sqrt[n]{b})/K$. This is the case if and only if $(x^n - b, K(\sqrt[n]{b})/K) = 1$, and by lemma 5.8, this is the case if and only if

$$\left(\frac{x^n - b, b}{\mathfrak{p}}\right)_n = 1$$

Letting $x = 0$ and $b = -a$, we get (iv). Choosing $x = 1$ and $b = 1 - a$, we get (v). It only remains to show (iii):

$$\begin{aligned}\left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{b,a}{\mathfrak{p}}\right)_n &= \left(\frac{a,-a}{\mathfrak{p}}\right)_n \left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{b,a}{\mathfrak{p}}\right)_n \left(\frac{b,-b}{\mathfrak{p}}\right)_n \\ &= \left(\frac{a,-ab}{\mathfrak{p}}\right)_n \left(\frac{b,-ab}{\mathfrak{p}}\right)_n = \left(\frac{ab,-ab}{\mathfrak{p}}\right)_n = 1\end{aligned}$$

■

5.4 Cubic reciprocity revisited

We are now almost ready to tackle cubic reciprocity from a new approach. We will need one more theorem, but before presenting it, we fix some notation. For a number field K containing μ_n, an element $a \in K$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $na \notin \mathfrak{p}$, we

may define the n-th power Legendre symbol $(a/\mathfrak{p})_n$ to be the unique n-th root of unity satisfying

$$a^{\frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}$$

See [1, p. 165] for details.

Theorem 5.10 (Strong Reciprocity)**.** *Let K be a number field containing μ_n and assume $\alpha, \beta \in \mathcal{O}_K$ are relatively prime to each other and n. Then*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{p|n\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n$$

where ∞ is the product of the real infinite primes of K, which only occur for $n = 2$.

Proof. We refer to chapter III in [3] for a proof. ■

We can now give our alternate proof of cubic reciprocity. Let $K = \mathbb{Q}(\omega)$ for $\omega = e^{2\pi i/3}$, and let $\mathcal{O}_K$ denote the ring of integers i.e. $\mathcal{O}_K = \mathbb{Z}[\omega]$. In this case, $n = 3$ and the only prime in $\mathbb{Z}[\omega]$ dividing 3 is $\lambda = 1 - \omega$. So Strong Reciprocity in this case is just

$$\left(\frac{\alpha}{\beta}\right)_3 \left(\frac{\beta}{\alpha}\right)_3^{-1} = \left(\frac{\alpha, \beta}{\lambda}\right)_3.$$

So proving cubic reciprocity amounts to showing:

$$\alpha, \beta \text{ primary in } \mathcal{O}_K \Rightarrow \left(\frac{\alpha, \beta}{\lambda}\right)_3 = 1$$

α, β primary means that $\alpha, \beta \equiv -1 \pmod{3\mathcal{O}_K}$. The residue symbol is unchanged when the denominator is replaced by one of its associates, so we may assume $\alpha, \beta \equiv -1 \pmod{\lambda^2\mathcal{O}_K}$ (λ^2 is associated to 3). Let K_λ be the completion at λ and $\mathcal{O}_\lambda$ the corresponding valuation ring. Proving cubic reciprocity thus amounts to proving:

$$\alpha, \beta \equiv -1 \pmod{\lambda^2\mathcal{O}_\lambda} \Rightarrow \left(\frac{\alpha, \beta}{\lambda}\right)_3 = 1$$

We follow the proof outlined in exercise 8.9 of [1]:

Second proof of cubic reciprocity. Claim 1: If $\alpha \equiv -1 \pmod{\lambda^4\mathcal{O}_\lambda}$, there exists $u \in \mathcal{O}_\lambda$ such that $\alpha = u^3$ for some $u \in \mathcal{O}_\lambda$. We prove this by inductively constructing a coherent sequence (u_n) in $\mathcal{O}_\lambda$ with $\alpha \equiv u_n^3 \pmod{\lambda^n\mathcal{O}_\lambda}$ for all $n \geq 4$. The case $n = 4$ holds by assumption since $-1 = (-1)^3$. If u_n is defined for $n > 4$, let $u_{n+1} = u_n + a\lambda^{n-2}$ for $a \in \mathcal{O}_\lambda$ to be determined. Then

$$u_{n+1}^3 = u_n^3 + 3u_n^2 a\lambda^{n-2} + 3u_n a^2\lambda^{2n-4} + a^3\lambda^{3n-6}$$

Note that $2n-4, 3n-6 \geq n+1$ as $n > 4$. Thus, we have $u_{n+1}^3 \equiv u_n^3 + 3u_n^2 a\lambda^{n-2} \pmod{\lambda^{n+1}\mathcal{O}_\lambda}$. Write $\alpha = u_n^3 + b\lambda^n$, then we have (recall that $3 = -\omega^2\lambda^2$):

$$u_{n+1}^3 \equiv \alpha - b\lambda^n + u_n^2(-\omega^2 a)\lambda^n \pmod{\lambda^{n+1}\mathcal{O}_\lambda}$$

If we furthermore write $u_n = c+d\lambda^n$, we get $u_n^2 = c^2+d^2\lambda^{2n}+2cd\lambda^n \equiv c^2+2cd\lambda^n \pmod{\lambda^{n+1}\mathcal{O}_\lambda}$. Substituting this into the previous equation gives:

$$\begin{aligned} u_{n+1}^3 &\equiv \alpha - b\lambda^n + (c^2+2cd\lambda^n)(-\omega^2 a)\lambda^n \equiv \alpha - b\lambda^n - c^2\omega^2 a\lambda^n - 2cda\omega^2\lambda^{2n} \\ &\equiv \alpha - b\lambda^n - c^2\omega^2 a\lambda^n \equiv \alpha - \lambda^n(b+c^2\omega^2 a) \pmod{\lambda^{n+1}\mathcal{O}_\lambda} \end{aligned}$$

So our task amounts to solving $b + c^2\omega^2 a \equiv 0 \pmod{\lambda\mathcal{O}_\lambda}$ i.e. $c^2\omega^2 a \equiv -b \pmod{\lambda\mathcal{O}_\lambda}$ for a. The condition $u_n \equiv u_{n-1} \pmod{\lambda^{n-1}\mathcal{O}_\lambda}$ shows that $\lambda \nmid c$ (otherwise we could not have $u_4 \equiv -1 \pmod{\lambda^4\mathcal{O}_\lambda}$). In other words, c is a unit and therefore $c^2\omega^2$ is also a unit. This proves that the equation has a solution for a, and we have constructed the desired sequence (note that $u_{n+1} \equiv u_n \pmod{\lambda^n\mathcal{O}_\lambda}$). By completeness of $\mathcal{O}_\lambda$, (u_n) converges to some element $u \in \mathcal{O}_\lambda$ with $\alpha = u^3$.

Claim 2: If $\alpha, \alpha' \in \mathcal{O}_\lambda^\times$ and $\alpha \equiv \alpha' \pmod{\lambda^4\mathcal{O}_\lambda}$, then $(\alpha, \beta/\lambda)_3 = (\alpha', \beta/\lambda)_3$ for all $\beta \in K_\lambda^\times$. Note that $-1 \equiv -\alpha\alpha^{-1} \equiv -\alpha'\alpha^{-1} \pmod{\lambda^4\mathcal{O}_\lambda}$, so applying the first claim, we have $-\alpha'\alpha^{-1} = u^3$ for some $a \in \mathcal{O}_\lambda$:

$$\left(\frac{-\alpha'\alpha^{-1}}{\lambda}\right)_3 = \left(\frac{u,\beta}{\lambda}\right)_3^3 = 1 \quad \text{i.e.} \quad \left(\frac{\alpha'\alpha^{-1}}{\lambda}\right)_3 = 1$$

Using the simple fact that $(-1, \beta/\lambda)_3 = 1$ as $-1 = (-1)^3$. We conclude:

$$\begin{aligned} \left(\frac{\alpha',\beta}{\lambda}\right)_3 \cdot \left(\frac{\alpha^{-1},\beta}{\lambda}\right)_3 = 1 \quad &\text{i.e.} \quad \left(\frac{\alpha',\beta}{\lambda}\right)_3 \cdot \left(\frac{\alpha\alpha^{-1},\beta}{\lambda}\right)_3 = \left(\frac{\alpha,\beta}{\lambda}\right)_3 \\ &\text{i.e.} \quad \left(\frac{\alpha',\beta}{\lambda}\right)_3 = \left(\frac{\alpha,\beta}{\lambda}\right)_3 \end{aligned}$$

as claimed.

Finally, assume that $\alpha \equiv \beta \equiv -1 \pmod{\lambda^2\mathcal{O}_\lambda}$. Write $\alpha = -1 + a\lambda^2$ and $\beta = -1 + b\lambda^2$ for $a, b \in \mathcal{O}_\lambda$. Note that:

$$-1 + a\beta\lambda^2 = -1 + a(-1+b\lambda^2)\lambda^2 = -1 - a\lambda^2 + ab\lambda^4 \equiv -1 - a\lambda^2 \pmod{\lambda^4\mathcal{O}_\lambda}$$

In other words, $1 + a\lambda^2 \equiv 1 - a\beta\lambda^2 \pmod{\lambda^4\mathcal{O}_\lambda}$. Using properties (i), (v) and the previous claim:

$$\left(\frac{\alpha,\beta}{\lambda}\right)_3 = \left(\frac{-\alpha,\beta}{\lambda}\right)_3 \cdot \left(\frac{-\alpha,a\lambda^2}{\lambda}\right)_3 = \left(\frac{-\alpha,a\beta\lambda^2}{\lambda}\right)_3$$

By noting that $-\alpha(1+a\lambda^2) \equiv 1 \pmod{\lambda^4\mathcal{O}_\lambda}$, we can continue the computation as follows:

$$\begin{aligned} \left(\frac{-\alpha,a\beta\lambda^2}{\lambda}\right)_3 &= \left(\frac{-\alpha,a\beta\lambda^2}{\lambda}\right)_3 \cdot \left(\frac{1-a\beta\lambda^2,a\beta\lambda^2}{\lambda}\right)_3 \\ &= \left(\frac{-\alpha,a\beta\lambda^2}{\lambda}\right)_3 \cdot \left(\frac{1+a\lambda^2,a\beta\lambda^2}{\lambda}\right)_3 = 1 \end{aligned}$$

And the proof is complete.

■

References

[1] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, Inc., 1989. ISBN 0-471-50654-0.

[2] Carl F. Gauss. *Untersuchungen über höhere Arithmetik*. Verlag von Julius Springer, 1889. URL `https://hdl.handle.net/2027/gri.ark:/13960/t8pc60281`.

[3] Helmut Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper Teil II: Reziprozitätsgesetz*. Physica-Verlag, 1965.

[4] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 2 edition, 1990. ISBN 0-387-97329-X.

[5] Daniel A. Marcus. *Number fields*. Springer, 2 edition, 2018. ISBN 978-3-319-90232-6.

[6] Jürgen Neukirch. *Class Field Theory*. Springer-Verlag, 1986.

[7] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992. ISBN 3-540-65399-6.

[8] Morten S. Risager. *Introduction to number theory*. University of Copenhagen, 2020. URL `http://web.math.ku.dk/~risager/introtal/main`.

[9] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2 edition, 2008.

[10] Kenneth S. Williams. *On Eisenstein's supplement to the law of cubic reciprocity*. Number 69. Bull. Cal. Math. Soc., 1977. URL `https://people.math.carleton.ca/~williams/papers/pdf/093.pdf`.