Quadratic and Hilbert Reciprocity

Timothy Curry

B.S., Mathematics

B.S., Biological Sciences

An Undergraduate Honors Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor of Science

at the

University of Connecticut

May 2014

May 2014

APPROVAL PAGE

Bachelor of Science Honors Thesis

Quadratic and Hilbert Reciprocity

Presented by

Timothy Curry, B.S. Math, B.S., Biology

Honors Major Advisor _____
William Abikoff

Honors Thesis Advisor _____
Keith Conrad

Honors Thesis Advisor _____
Álvaro Lozano-Robledo

University of Connecticut

May 2014

ACKNOWLEDGMENTS

My most sincere appreciation and gratitude goes to both Keith Conrad and Álvaro Lozano-Robledo. Without their constant guidance and patience, this thesis would never have been completed.

Quadratic and Hilbert Reciprocity

Timothy Curry, B.S.

University of Connecticut, May 2014

Contents

Chapter 1

Introduction

The law of quadratic reciprocity provides conditions that tell whether an integer is a quadratic residue modulo primes. However, it does not treat 2 in the same manner as other primes. There is a supplementary law for 2 which details the conditions needed for it to be a quadratic residue.

In this thesis, we will recall a completion of the rational numbers $\mathbf{Q}$, called the p-adic numbers $\mathbf{Q}_p$. After exploring $\mathbf{Q}_p$, we will consider the Hilbert symbol, a particular pairing on $\mathbf{Q}_p^\times \times \mathbf{Q}_p^\times$. The Hilbert symbol satisfies the Hilbert reciprocity law, which we will show is equivalent to the law of quadratic reciprocity. However, unlike quadratic reciprocity, the Hilbert reciprocity law puts all primes on an equal footing, including 2.

For a Gaussian integer prime π, we will also discuss the π-adic completion of $\mathbf{Q}(i)$, denoted $\mathbf{Q}(i)_\pi$. Then we will examine the Hilbert symbol on $\mathbf{Q}(i)_\pi^\times$ and show that the Hilbert reciprocity law on $\mathbf{Q}(i)$ is equivalent to quadratic reciprocity in the Gaussian integers.

Chapter 2

The p-adic numbers

2.1 Useful Definitions and Properties

In this thesis, we will assume prior knowledge of the p-adic numbers $\mathbf{Q}_p$. However, in this section we will recall several important definitions and properties regarding $\mathbf{Q}_p$ that will be used frequently in this thesis.

Definition 2.1.1. Let $p \in \mathbf{Z}$ be prime. Define the *p-adic valuation* on $\mathbf{Z}$ to be the function $v_p : \mathbf{Z} - \{0\} \longrightarrow \mathbf{R}$ such that for each $n \in \mathbf{Z} - \{0\}$, $v_p(n)$ is the unique positive integer satisfying $n = p^{v_p(n)}n'$ where $p \nmid n'$. Furthermore, we extend v_p so that for $x = \frac{a}{b} \in \mathbf{Q}^\times$ with $a, b \in \mathbf{Z} - \{0\}$, we have $v_p(x) = v_p(a) - v_p(b)$. Lastly, we set $v_p(0) = \infty$.

Definition 2.1.2. Let $x \in \mathbf{Q}$. We define the *p-adic absolute value* of x by

$$|x|_p := \begin{cases} \frac{1}{p^{v_p(x)}}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases}$$

The field $\mathbf{Q}_p$ is defined as the completion of $\mathbf{Q}$ with respect to the p-adic absolute value, and we have the following theorem about the form of each element in $\mathbf{Q}_p$.

Theorem 2.1.3. *Let $x \in \mathbf{Q}_p^\times$. Then x can be written uniquely in the form*

$$x = b_{-n_0}p^{-n_0} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots = \sum_{n \geq -n_0} b_n p^n$$

with $0 \leq b_n \leq p-1$ and $-n_0 = v_p(x)$.

Proof. For a proof, see [3, p. 68, Corollary 3.3.11]. □

Definition 2.1.4. The ring of *p-adic integers* is $\mathbf{Z}_p = \{x \in \mathbf{Q}_p \ : \ |x|_p \leq 1\}$. In particular, the units of $\mathbf{Z}_p$ are $\mathbf{Z}_p^\times = \{x \in \mathbf{Q}_p \ : \ |x|_p = 1\}$.

Theorem 2.1.5. *Let $n \in \mathbf{Z}$ such that $n \geq 1$. Then the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$ induces a ring isomorphism $\mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}_p/p^n\mathbf{Z}_p$.*

Proof. See [3, p. 63, Corollary 3.3.6]. □

Theorem 2.1.6 (Hensel's Lemma). *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbf{Z}_p[x]$. Suppose that there exists a p-adic integer $\alpha_0 \in \mathbf{Z}_p$ such that*

$$f(\alpha_0) \equiv 0 \bmod p\mathbf{Z}_p$$

and

$$f'(\alpha_0) \not\equiv 0 \bmod p\mathbf{Z}_p.$$

Then there exists a unique p-adic integer $\alpha \in \mathbf{Z}_p$ *such that* $\alpha \equiv \alpha_0 \bmod p\mathbf{Z}_p$ *and* $f(\alpha) = 0$.

Proof. See [3, p. 70, Theorem 3.4.1]. □

Corollary 2.1.7. *Let* p *be an odd prime and let* $u \in \mathbf{Z}_p^\times$. *Then* $u = \square$ *in* $\mathbf{Z}_p^\times$ *if and only if* $u \equiv \square \bmod p$.

Proof. Let $u \in \mathbf{Z}_p^\times$ (in particular, $u \not\equiv 0 \bmod p$). First, if $u = \square$ in $\mathbf{Z}_p^\times$, then obviously $u \equiv \square \bmod p$. On the other hand, let $u \equiv \square \bmod p$. Then there exists some $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that $a^2 \equiv u \bmod p$. Now consider the polynomial $f(x) = x^2 - u$. We have that $f(a) \equiv a^2 - u \equiv 0 \bmod p$ and $f'(a) = 2a \not\equiv 0 \bmod p$. Thus, by Hensel's lemma there exists $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$. So $\alpha^2 = u$, meaning $u = \square$ in $\mathbf{Z}_p$ and $|\alpha|_p^2 = |u|_p = 1$, so $\alpha \in \mathbf{Z}_p^\times$. Thus, $u = \square$ in $\mathbf{Z}_p^\times$. □

Lemma 2.1.8. *Let* p *be an odd prime and let* $a, b, c \in \mathbf{Z}_p^\times$. *Then there exist* $x, y \in \mathbf{Z}/p\mathbf{Z}$ *such that* $ax^2 + by^2 \equiv c \bmod p$.

Proof. Rewrite the congruence as $ax^2 \equiv c - by^2 \bmod p$. Since there are $\frac{p+1}{2}$ squares in $\mathbf{Z}/p\mathbf{Z}$ (including $0 \bmod p$ here), $ax^2 \bmod p$ has $\frac{p+1}{2}$ values as x varies mod p, and likewise $c - by^2 \bmod p$ has $\frac{p+1}{2}$ values as y varies mod p. Since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p = |\mathbf{Z}/p\mathbf{Z}|$, by the pigeonhole principle

$$\left\{ax^2 \bmod p : x \in \mathbf{Z}/p\mathbf{Z}\right\} \cap \left\{c - by^2 \bmod p : y \in \mathbf{Z}/p\mathbf{Z}\right\} \neq \emptyset.$$

So there exist $x_0, y_0 \in \mathbf{Z}/p\mathbf{Z}$ such that $ax_0^2 \equiv c - by_0^2 \bmod p$. □

Corollary 2.1.9. *Let* p *be an odd prime and let* $a, b, c \in \mathbf{Z}_p^\times$. *Then the equation* $ax^2 + by^2 = c$ *has a solution with* $x, y \in \mathbf{Z}_p$.

Proof. By Lemma 2.1.8 there are $x_0, y_0 \in \mathbf{Z}_p$ such that $ax_0^2 + by_0^2 \equiv c \bmod p$ and either $x_0 \not\equiv 0 \bmod p$ or $y_0 \not\equiv 0 \bmod p$. The congruence is symmetric in the roles of x_0 and y_0, so without loss of generality, let $x_0 \not\equiv 0 \bmod p$. Then $\frac{c-by_0^2}{a}$ is congruent mod p to a nonzero square x_0^2, so by Hensel's lemma there exists $x \in \mathbf{Z}_p$ such that $x^2 = \frac{c-by_0^2}{a}$ and $x \equiv x_0 \bmod p$. Now let $y = y_0$. Then (x, y) is a solution to the equation $ax^2 + by^2 = c$. □

Chapter 3

The Hilbert Symbol

3.1 Definition and Basic Properties

The completions of $\mathbf{Q}$ are $\mathbf{Q}_2, \mathbf{Q}_3, \mathbf{Q}_5, ...$, and $\mathbf{R}$. To describe these with a uniform notation, let v be a place, either a prime or the symbol ∞, and define $\mathbf{Q}_\infty = \mathbf{R}$.

Definition 3.1.1. For any $a, b \in \mathbf{Q}_v^\times$, the *Hilbert symbol* of a and b relative to $\mathbf{Q}_v$ is defined as

$$(a,b)_v := \begin{cases} 1, & \text{if } ax^2 + by^2 = z^2 \text{ has a solution in } (x,y,z) \in \mathbf{Q}_v^3 - \{(0,0,0)\}, \\ -1, & \text{otherwise.} \end{cases}$$

For $a, b, c \in \mathbf{Q}_v^\times$, we will often refer to $ax^2 + by^2 = cz^2$ having a solution when we mean having a solution besides $(0,0,0)$.

Remark 3.1.2. Since we can multiply the equation $ax^2 + by^2 = z^2$ by any nonzero square without changing the existence of a solution, if v is a finite place and there is a

solution to $ax^2 + by^2 = z^2$ with $x, y, z \in \mathbf{Q}_p$, then there is a solution with $x, y, z \in \mathbf{Z}_p$ and x, y, or z in $\mathbf{Z}_p^\times$.

Example 3.1.3. We will evaluate $(2, 3)_3$. This means that we are trying to find out whether there is a solution to $2x^2+3y^2 = z^2$ with $x, y, z \in \mathbf{Q}_3$ besides $(0, 0, 0)$. If such a solution does exist, we know that one exists with $x, y, z \in \mathbf{Z}_3$ where at least one of them is a unit. With this knowledge, we can now reduce $2x^2 + 3y^2 = z^2 \bmod 3$ and obtain $2x^2 \equiv z^2 \bmod 3$. Here, if $x \equiv 0 \bmod 3$ then we would have that $z \equiv 0 \bmod 3$. Then $3|x$ and $3|z$, so $3^2|x^2$ and $3^2|z^2$. This means that $3^2|(z^2 - 2x^2)$. So $3^2|3y^2$, meaning $3|y^2$, which implies that $3|y$. Now we have that x, y, and z are not units, which is a contradiction as we had at least one of them being a unit. Thus it must be that $x \not\equiv 0 \bmod 3$. Then with $2x^2 \equiv z^2 \bmod 3$ we can divide both sides by x^2 and get that $2 \equiv \square \bmod 3$, which is a contradiction. Therefore, there is no solution to $2x^2 + 3y^2 = z^2$ in $\mathbf{Q}_3$ besides $(0, 0, 0)$ and $(2, 3)_3 = -1$.

Example 3.1.4. We will evaluate $(2, 2)_v$ for any v. Since $1, 2 \in \mathbf{Q}_v$ for all v, we can use $(x, y, z) = (1, 1, 2)$ as our solution to $2x^2 + 2y^2 = z^2$. Thus for any v we have that $(2, 2)_v = 1$.

Now that we have defined the Hilbert symbol on $\mathbf{Q}_p$, we can examine its basic properties.

Theorem 3.1.5. *For $a, b, c \in \mathbf{Q}_v^\times$,*

(*i*) $(a, b)_v = (b, a)_v$ *and* $(a, c^2)_v = 1$,

(*ii*) $(a, -a)_v = (a, 1 - a)_v = 1$,

(*iii*) $(a, b)_v = (ac^2, b)_v = (a, bc^2)_v$.

Proof. Properties (i) and (iii) follow from the definition of the Hilbert symbol, and (ii) follows from using $x = y = 1$ and $z = 0$ or $z = 1$ respectively in the equations $ax^2 - ay^2 = z^2$ and $ax^2 + (1-a)y^2 = z^2$. □

Definition 3.1.6. For $b \in \mathbf{Q}_v^\times$, let $N_{b,v} = \{x^2 - by^2 \neq 0 : x, y \in \mathbf{Q}_v\}$.

Theorem 3.1.7. *For all $b \in \mathbf{Q}_v^\times$, $N_{b,v}$ is a subgroup of $\mathbf{Q}_v^\times$ and $(\mathbf{Q}_v^\times)^2 \subset N_{b,v} \subset \mathbf{Q}_v^\times$.*

Proof. First notice that if $y = 0$ then $x^2 - by^2 = x^2$, so $(\mathbf{Q}_v^\times)^2 \subset N_{b,v}$. Any element of $N_{b,v}$ is an element of $\mathbf{Q}_v^\times$, so $N_{b,v} \subset \mathbf{Q}_v^\times$.

Now we will show that $N_{b,v}$ is a subgroup of $\mathbf{Q}_v^\times$. Using $x = 1$ and $y = 0$, we have $x^2 - by^2 = 1$, so $N_{b,v}$ contains the identity element of $\mathbf{Q}_v^\times$.

Next, let $x, y, z, w \in \mathbf{Q}_v$ such that $x^2 - by^2$ and $z^2 - bw^2$ are nonzero. Then $(x^2 - by^2)(z^2 - bw^2)$ is nonzero and

$$\begin{aligned}(x^2 - by^2)(z^2 - bw^2) &= (x + y\sqrt{b})(x - y\sqrt{b})(z + w\sqrt{b})(z - w\sqrt{b}) \\ &= (xz + byw + (xw + yz)\sqrt{b})(xz + byw - (xw + yz)\sqrt{b}) \\ &= (xz + byw)^2 - b(xw + yz)^2,\end{aligned}$$

so $(x^2 - by^2)(z^2 - bw^2) \in N_{b,v}$. Thus, $N_{b,v}$ is closed under multiplication. Lastly, $N_{b,v}$ contains multiplicative inverses since

$$\frac{1}{x^2 - by^2} = \frac{x^2 - by^2}{(x^2 - by^2)^2} = \left(\frac{x}{x^2 - by^2}\right)^2 - b\left(\frac{y}{x^2 - by^2}\right)^2.$$

□

Theorem 3.1.8. *Let $b \in \mathbf{Q}_v^\times$. If $b \in (\mathbf{Q}_v^\times)^2$, then $N_{b,v} = \mathbf{Q}_v^\times$.*

Proof. Since $b \in (\mathbf{Q}_v^\times)^2$, set $b = \beta^2$. Then for $x, y \in \mathbf{Q}_v$, $x^2 - by^2 = x^2 - (\beta y)^2 = (x + \beta y)(x - \beta y)$. With the invertible change of variables $t = x + \beta y$ and $u = x - \beta y$ (here $x = \frac{t+u}{2}$ and $y = \frac{t-u}{2\beta}$), we see that $\{x^2 - by^2 \neq 0 : x, y \in \mathbf{Q}_v\} = \{tu : t, u \in \mathbf{Q}_v^\times\} = \mathbf{Q}_v^\times$. □

Remark 3.1.9. Later on we will see that if $b \notin (\mathbf{Q}_v^\times)^2$, then $N_{b,v} \neq \mathbf{Q}_v^\times$. This will follow from Theorems 3.3.2, 3.3.3, and 3.3.4.

Theorem 3.1.10. *For $a, b \in \mathbf{Q}_v^\times$, $(a, b)_v = 1$ if and only if $a \in N_{b,v}$.*

Proof. For the direction ($\Rightarrow$), suppose $(a, b)_v = 1$. Then there exist $x, y, z \in \mathbf{Q}_v$ such that $ax^2 + by^2 = z^2$ with $(x, y, z) \neq (0, 0, 0)$. If $x \neq 0$, then we can rewrite $ax^2 + by^2 = z^2$ as $a = \frac{z^2 - by^2}{x^2}$. This gives $a = (z')^2 - b(y')^2$ for some $y', z' \in \mathbf{Q}_v$ and we're done. On the other hand, if $x = 0$ then $y \neq 0$ and $z \neq 0$, and $b = (z/y)^2$, which means that $b = \square$ in $\mathbf{Q}_v^\times$. By Theorem 3.1.8, we have $\{x^2 - by^2 \neq 0 | x, y \in \mathbf{Q}_v\} = \mathbf{Q}_v^\times$. Since $a \in \mathbf{Q}_v^\times$, we're done.

For the direction ($\Leftarrow$), suppose $a \in N_{b,v}$, so there exist $x, y \in \mathbf{Q}_v$ such that $a = x^2 - by^2$. Then, $a \cdot 1^2 + by^2 = x^2$, so $(a, b)_v = 1$. □

3.2 Square Classes

A square class in $\mathbf{Q}_v^\times$ is a coset in $\mathbf{Q}_v^\times / (\mathbf{Q}_v^\times)^2$. In this section, we will find a complete set of square class representatives for $\mathbf{Q}_v^\times$. These will be instrumental in proving the bimultiplicativity of the Hilbert symbol.

Theorem 3.2.1. *Let p be an odd prime and let $r \in \mathbf{Z}_p^\times$ such that $r \not\equiv \square \bmod p$. A set of square class representatives for $\mathbf{Q}_p^\times$ is $\{1, r, p, rp\}$.*

Proof. Since $\mathbf{Q}_p^\times = p^{\mathbf{Z}} \times \mathbf{Z}_p^\times$ and $(\mathbf{Q}_p^\times)^2 = p^{2\mathbf{Z}} \times (\mathbf{Z}_p^\times)^2$, we have

$$\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2 = \frac{p^{\mathbf{Z}} \times \mathbf{Z}_p^\times}{p^{2\mathbf{Z}} \times (\mathbf{Z}_p^\times)^2} \cong \frac{p^{\mathbf{Z}}}{p^{2\mathbf{Z}}} \times \frac{\mathbf{Z}_p^\times}{(\mathbf{Z}_p^\times)^2}.$$

Since $p^{\mathbf{Z}}/p^{2\mathbf{Z}}$ depends only on the parity of the power of p, it is represented by $\{1, p\}$. Also, by Corollary 2.1.7, if $\alpha \in \mathbf{Z}_p^\times$ then $\alpha \equiv \square \bmod p$ if and only if $\alpha \in (\mathbf{Z}_p^\times)^2$. With this, since any two nonsquare units in $\mathbf{Z}/p\mathbf{Z}$ have a square ratio, $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2$ is represented by $\{1, r\}$ where r is a nonquadratic residue in $\mathbf{Z}/p\mathbf{Z}$. Thus, $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ is represented by $\{1, p\} \times \{1, r\} = \{1, r, p, rp\}$. □

In order to find the square class representatives for $p = 2$, we will need a more general form of Hensel's lemma.

Theorem 3.2.2. *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbf{Z}_p[x]$. Suppose that there exists a p-adic integer $\alpha_0 \in \mathbf{Z}_p$ such that*

$$|f(\alpha_0)|_p < |f'(\alpha_0)|_p^2$$

Then there exists a unique p-adic integer $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| < |f'(\alpha_0)|$.

Proof. See [2, pp. 1-3, Theorem 1.4]. □

Example 3.2.3. Consider the polynomial $f(x) = x^2 - u$ where $u \in \mathbf{Z}_2^\times$. We want to use 1 as an approximate root of $f(x)$ in $\mathbf{Z}_2$. Then we want $f(x)$ to satisfy $|f(1)|_2 < |f'(1)|_2^2$. So we need $|u-1|_2 < |2|_2^2 = |4|_2$. This is equivalent to $u \equiv 1 \bmod 8\mathbf{Z}_2$. Thus Hensel's lemma says that if $u \equiv 1 \bmod 8\mathbf{Z}_2$, then u is a square in $\mathbf{Z}_2$ and thus in $\mathbf{Q}_2$.

Theorem 3.2.4. *Let $u \in \mathbf{Z}_2^\times$. Then u is a square in $\mathbf{Z}_2^\times$ if and only if $u \equiv 1 \bmod 8\mathbf{Z}_2$.*

Proof. For the direction ($\Rightarrow$), we look at the possible units mod 8, $\{1, 3, 5, 7\}$, and square them: $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. This means that any square unit r in $\mathbf{Z}_2$ is congruent to 1 mod 8. For the reverse direction, use the previous example and note that if $r = \alpha^2$ in $\mathbf{Z}_2$ with $\alpha \in \mathbf{Q}_2$ then necessarily $\alpha \in \mathbf{Z}_2^\times$ since $|\alpha|_2^2 = |r|_2 = 1$. □

Theorem 3.2.5. *A complete set of square class representatives for* $\mathbf{Q}_2^\times$ *is* $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Proof. We have that

$$\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2 = \frac{2^{\mathbf{Z}} \times \mathbf{Z}_2^\times}{2^{2\mathbf{Z}} \times (\mathbf{Z}_2^\times)^2} \cong \frac{2^{\mathbf{Z}}}{2^{2\mathbf{Z}}} \times \frac{\mathbf{Z}_2^\times}{(\mathbf{Z}_2^\times)^2}.$$

As in Theorem 3.2.1, $2^{\mathbf{Z}}/2^{2\mathbf{Z}}$ is represented by $\{1, 2\}$. Also, for $u \in \mathbf{Z}_2^\times$ we have that $2 \nmid u$. So by Theorem 2.1.3, u can be written in form $u = 1 + b_1 2 + b_2 2^2 + \cdots + b_n 2^n + \cdots$, where each $b_i \in \{0, 1\}$. Therefore, either $u \equiv 1 \bmod 4$ or $u \equiv 3 \equiv -1 \bmod 4$. As a result, $\mathbf{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$. Then $(\mathbf{Z}_2^\times)^2 = 1 + 8\mathbf{Z}_2$, and $1 + 4\mathbf{Z}_2 = (1 + 8\mathbf{Z}_2) \cup 5(1 + 8\mathbf{Z}_2)$, so $\mathbf{Z}_2^\times/(\mathbf{Z}_2^\times)^2$ is represented by $\{\pm 1\} \times \{1, 5\} = \{\pm 1, \pm 5\}$. Thus $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$ is represented by $\{1, 2\} \times \{\pm 1, \pm 5\} = \{\pm 1, \pm 2, \pm 5, \pm 10\}$. □

3.3 Bimultiplicativity of the Hilbert Symbol

A key property of the Hilbert symbol is that it is bimultiplicative. This property will be extremely useful for deriving a formula for the Hilbert symbol and proving the equivalence between the Hilbert reciprocity law and quadratic reciprocity.

Definition 3.3.1. Let p be an odd prime and let d be a nonsquare in $\mathbf{Q}_p^\times$. Then let $L_d = \mathbf{Q}_p(\sqrt{d})$. For $\alpha \in L_d$ such that $\alpha = x + y\sqrt{d}$ with $x, y \in \mathbf{Q}_p$, define $N : L_d \to \mathbf{Q}_p$ by $N(\alpha) = x^2 - dy^2$.

Theorem 3.3.2. *Let p be an odd prime and let d be a nonsquare in $\mathbf{Q}_p^\times$. If $L_d = \mathbf{Q}_p(\sqrt{d})$, then $N(L_d^\times)/(\mathbf{Q}_p^\times)^2 = \{x^2 - dy^2 \neq 0 : x, y \in \mathbf{Q}_p\}/(\mathbf{Q}_p^\times)^2$ is a subgroup of $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ with index 2.*

Proof. Since $(\mathbf{Q}_p^\times)^2 \subset N(L_d^\times) \subset \mathbf{Q}_p^\times$, to show the group $N(L_d^\times)/(\mathbf{Q}_p^\times)^2$ has index 2 in $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2 \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ it suffices to show that $N(L_d^\times)$ is neither $\mathbf{Q}_p^\times$ nor $(\mathbf{Q}_p^\times)^2$. It suffices by Theorem 3.2.1 to let $d = r, p$, and rp where $r \in \mathbf{Z}_p$ and $r \not\equiv \square \bmod p$, so we will break this proof into cases.

Case 1) Let $d = r$. We will show that only two square class representatives in $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ are elements of $N(L_r^\times)$. We will first show that p is not a norm by examining the homogenized equation $x^2 - ry^2 = pz^2$. If there is a solution other than $(0,0,0)$ to this equation where $x, y, z \in \mathbf{Q}_p$, then there is a solution where all are in $\mathbf{Z}_p$ and at least one is in $\mathbf{Z}_p^\times$. Further, reducing this equation mod p gives $x^2 - ry^2 \equiv 0 \bmod p$, which tells us x and y are either both units or both divisible by p. However, if they are both divisible by p then z must also be divisible by p. Then $x, y, z \notin \mathbf{Z}_p^\times$ and we have a contradiction. This implies that $y \not\equiv 0 \bmod p$, which in turn implies $r \equiv \square \bmod p$, a contradiction. Thus, p is not a norm from L_r. So $N(L_r^\times)/(\mathbf{Q}_p^\times)^2$ cannot have order 4. Now we will show that r is a norm. The equation $x^2 - ry^2 = r$ has a solution with $x, y \in \mathbf{Z}_p$ by Corollary 2.1.9, so r is a norm. Since 1 is clearly a norm, we have $N(L_r^\times)/(\mathbf{Q}_p^\times)^2 = \{\overline{1}, \overline{r}\}$ and has order 2.

Case 2) Let $d = \lambda p$ where $\lambda = 1$ or $\lambda = r$. To show $r \notin N(L_{\lambda p}^\times)$, consider the homogenized equation $x^2 - \lambda p y^2 = rz^2$. If this equation has a solution in $\mathbf{Q}_p$ other than $(0,0,0)$, it will have one where $x, y, z \in \mathbf{Z}_p$ and at least one is a unit. Therefore we can reduce mod p and get $x^2 \equiv rz^2 \bmod p$. So just as we saw in the previous

case, it must be that x and z are units, for otherwise p would divide x, y, and z and we would not have a unit in our solution. Since $z^2 \not\equiv 0 \bmod p$, we can divide both sides of the congruence by it and get that $r \equiv \square \bmod p$, a contradiction. Thus, r is not a norm. Next we consider the homogenized equation $x^2 - \lambda p y^2 = p z^2$. This equation has a solution in $\mathbf{Q}_p$ (other than $(0,0,0)$) if and only if $px^2 - \lambda y^2 = z^2$ has a solution in $\mathbf{Q}_p$. If there is a solution in $\mathbf{Q}_p$ then there must be one with $x, y, z \in \mathbf{Z}_p$ with at least one being a unit, so we can reduce the second equation mod p and get $-\lambda y^2 \equiv z^2 \bmod p$. Also, we can note that if y is divisible by p then z is divisible by p, which would make x divisible by p and then $x, y, z \notin \mathbf{Z}_p^\times$. This would be a contradiction, so it must be that $y \not\equiv 0 \bmod p$. This means that $-\lambda \equiv \square \bmod p$. Now, if $\lambda = 1$ we will have a contradiction unless $(\frac{-1}{p}) = 1$, and if $(\frac{-1}{p}) = 1$ then $(x, y, z) = (0, \sqrt{-1}, 1)$ is a solution to $px^2 - y^2 = z^2$. Thus for $d = p$, p is a norm if and only if $(\frac{-1}{p}) = 1$. On the other hand, if $\lambda = r$ we will have a contradiction unless $(\frac{-1}{p}) = -1$, and if $(\frac{-1}{p}) = -1$ then $-r = \square$ in $\mathbf{Z}_p$ and $(x, y, z) = (0, \sqrt{-r}, r)$ is a solution to $px^2 - ry^2 = z^2$. Therefore for $d = rp$, p is a norm if and only if $(\frac{-1}{p}) = -1$.

Lastly, we will consider the homogenized equation $x^2 - \lambda p y^2 = rpz^2$. This equation has a solution in $\mathbf{Q}_p$ if and only if $px^2 - \lambda y^2 = rz^2$ has a solution in $\mathbf{Q}_p$. And if there is a solution in $\mathbf{Q}_p$ then there must be one with $x, y, z \in \mathbf{Z}_p$ with at least one being a unit, so we can reduce the second equation mod p and get $-\lambda y^2 \equiv rz^2 \bmod p$. Using a similar argument to the one in the above paragraph, we can show that it must be that $y \not\equiv 0 \bmod p$. With this, if $\lambda = 1$ we have that $-y^2 \equiv rz^2 \bmod p$ which implies $-r \equiv \square \bmod p$. This is a contradiction unless $(\frac{-1}{p}) = -1$, and if $(\frac{-1}{p}) = -1$ then $(x, y, z) = (0, \sqrt{-r}, 1)$ is a solution to $px^2 - y^2 = rz^2$. So for $d = p$, rp is a norm if and only if $(\frac{-1}{p}) = -1$. Instead, if $\lambda = r$, then we are left with $-ry^2 \equiv rz^2 \bmod p$ which implies that $-1 \equiv \square \bmod p$. This is a contradiction unless $(\frac{-1}{p}) = 1$, and if $(\frac{-1}{p}) = 1$

then $(x, y, z) = (0, \sqrt{-1}, 1)$ is a solution to $px^2 - ry^2 = rz^2$. Thus for $d = rp$, rp is a norm if and only if $(\frac{-1}{p}) = 1$.

Overall, this gives us that

$$N(L_p^\times)/(\mathbf{Q}_p^\times)^2 = \begin{cases} \{1, p\}, & \text{if } (\frac{-1}{p}) = 1, \\ \{1, rp\}, & \text{if } (\frac{-1}{p}) = -1, \end{cases}$$

and

$$N(L_{rp}^\times)/(\mathbf{Q}_p^\times)^2 = \begin{cases} \{1, p\}, & \text{if } (\frac{-1}{p}) = -1, \\ \{1, rp\}, & \text{if } (\frac{-1}{p}) = 1. \end{cases}$$

For each value of λ, $N(L_{\lambda p}^\times)/(\mathbf{Q}_p^\times)^2$ has order 2. So for each nonsquare d in $\mathbf{Q}_p^\times$, $N(L_d^\times)/(\mathbf{Q}_p^\times)^2$ is a subgroup of $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ with index 2. □

Theorem 3.3.3. *Let $p = 2$ and let d be a nonsquare in $\mathbf{Q}_2^\times$. If $L_d = \mathbf{Q}_2(\sqrt{d})$, then $N(L_d^\times)/(\mathbf{Q}_2^\times)^2$ is a subgroup of $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$ with index 2.*

Proof. The field L_d depends on the square class of d, so we can let d run through square classes. Since $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$ has order 8 and all its elements square to 1, to show a subgroup has index 2 we show it is a proper subgroup with at least two elements besides 1. Since d would have to run through eight square classes for the entire proof, to save room we will only prove it for one unit square class and one nonunit square class. The rest of the cases are proven with similar arguments.

Let $d = -1$. First consider the equation $x^2 + y^2 = -1$. If there is a solution with $x, y \in \mathbf{Q}_2$ then we consider separately $y \in \mathbf{Z}_2$ and $y \notin \mathbf{Z}_2$. If $y \in \mathbf{Z}_2$ then $x^2 = -1 - y^2 \in \mathbf{Z}_2$, so $x \in \mathbf{Z}_2$. But $x^2, y^2 \equiv 0$ or $1 \bmod 4$, so $x^2 + y^2 \not\equiv -1 \bmod 4$, which is a contradiction, implying $y \notin \mathbf{Z}_2$. Then we can write y in the form $\frac{v}{2^m}$ where $v \in \mathbf{Z}_2^\times$ and $m \geq 1$. Then $x^2 = -1 - y^2 = \frac{-2^{2m} - v^2}{2^{2m}}$. Since v is a unit, $-2^{2m} - v^2$

is a unit and we can write x in the form $\frac{u}{2^m}$ where $u \in \mathbf{Z}_2^\times$. With this, we have $x^2 + y^2 = \frac{u^2+v^2}{2^{2m}} = \frac{u^2+v^2}{4^m} = -1$. Then $u^2 + v^2 = -4^m$ and reducing mod 4 gives us that $u^2 + v^2 \equiv 0 \bmod 4$. However, $u^2 \equiv v^2 \equiv 1 \bmod 4$ as u and v are 2-adic units. So, $u^2 + v^2 \equiv 2 \bmod 4$, a contradiction. Thus, $x^2 + y^2 = -1$ has no solution in $\mathbf{Q}_2$ and therefore -1 is not a norm. On the other hand, $2, 5 \in N(L_{-1}^\times)$ since $2 = 1^2 + 1^2$ and $5 = 1^2 + 2^2$. Thus, $2^{\{0,1\}} \times 5^{\{0,1\}} = \{1, 2, 5, 10\}$ gives us four norms that are also different square class representatives.

Let $d = 2$. We will show that 5 is not a norm by examining the homogenized equation $x^2 - 2y^2 = 5z^2$. If there is solution in $\mathbf{Q}_2$ other than $(0, 0, 0)$, then there will be one where $x, y, z \in \mathbf{Z}_2$ and at least one of x, y, or z is a unit. Additionally, if $2|x$ then $2|(x^2 - 2y^2)$, so $2|z$. Thus $4|x^2$ and $4|z^2$, which implies that $2|y^2$ and $2|y$. With this $x, y, z \notin \mathbf{Z}_2^\times$ and we have a contradiction. Thus $x \in \mathbf{Z}_2^\times$, so also $z \in \mathbf{Z}_2^\times$ and $1 - 2y^2 \equiv 5 \cdot 1 \bmod 8$. Then $y^2 \equiv 2 \bmod 4$, a contradiction. So 5 is not a norm. In contrast, $-1, 2 \in N(L_2^\times)$ since $-1 = 1^2 - 2 \cdot 1^2$ and $2 = 2^2 - 2 \cdot 1^2$. Thus, $N(L_2^\times)/(\mathbf{Q}_2^\times)^2$ has order 4 containing $(-1)^{\{0,1\}} \times 2^{\{0,1\}} = \{1, -1, 2, -2\}$.

□

Theorem 3.3.4. *A complete set of square class representatives for* $\mathbf{R}^\times$ *is* $\{-1, 1\}$. *Moreover, if* $L_{-1} = \mathbf{R}(\sqrt{-1}) = \mathbf{C}$, *then* $N(L_{-1}^\times)/(\mathbf{R}^\times)^2$ *is a subgroup of* $\mathbf{R}^\times/(\mathbf{R}^\times)^2$ *with index* 2.

Proof. Since all positive reals are squares and all negative reals are non-squares, the set $\{-1, 1\}$ is clearly a complete set of square class representatives for $\mathbf{R}^\times$. Also $N(L_{-1}^\times)/(\mathbf{R}^\times)^2 = \{x^2 + y^2 \neq 0 : x, y \in \mathbf{R}\}/(\mathbf{R}^\times)^2 = \{1\}$, as a nonzero sum of two real squares is always positive. And since $\{1\}$ is a subgroup of $\{-1, 1\}$ with index 2,

we are done. □

Lemma 3.3.5. *Let G be a finite group and let H be a subgroup of G with index 2. If $g, g' \in G$ such that $g, g' \notin H$, then $gg' \in H$.*

Proof. Since $g \in G - H$, $G = H \sqcup gH$. Now if $gg' \notin H$ then $gg' \in gH$, implying that $g' \in H$, a contradiction. Thus, $gg' \in H$. □

We now have all the information we need to prove the bimultiplicativity of the Hilbert symbol.

Theorem 3.3.6. *The Hilbert symbol is bimultiplicative. That is, for all $a, a', b, b' \in \mathbf{Q}_v^\times$, we have $(aa', b)_v = (a, b)_v(a', b)_v$ and $(a, bb')_v = (a, b)_v(a, b')_v$.*

Proof. By the symmetry of the Hilbert symbol in Theorem 3.1.5(i), it suffices to prove $(aa', b)_v = (a, b)_v(a', b)_v$. We will split this into three cases.

Case 1: $(a, b)_v = (a', b)_v = 1$. By Theorem 3.1.10, $a, a' \in N_{b,v}$. Since $N_{b,v}$ is closed under multiplication, $aa' \in N_{b,v}$ as well. Thus $(aa', b)_v = 1$ by Theorem 3.1.10.

Case 2: $(a, b)_v \neq (a', b)_v$. Without loss of generality $(a, b)_v = 1$ and $(a', b)_v = -1$. To show $(aa', b)_v = -1$, suppose by way of contradiction that $(aa', b)_v = 1$. Then by Theorem 3.1.10, a and $aa' \in N_{b,v}$, so $aaa' = a^2a' \in N_{b,v}$. This implies by Theorem 3.1.5(iii) that $(a', b)_v = (a^2a', b)_v = 1$, which contradicts our initial hypothesis. Thus, $(aa', b)_v = -1$.

Case 3: $(a, b)_v = (a', b)_v = -1$. Then $a, a' \notin N_{b,v}$. We want to show $(aa', b)_v = 1$. Since $N_{b,v}/(\mathbf{Q}_v^\times)^2$ is a subgroup of $\mathbf{Q}_v^\times/(\mathbf{Q}_v^\times)^2$ with index 2, $N_{b,v}$ is a subgroup of $\mathbf{Q}_v^\times$ with index 2. Then since $a, a' \notin N_{b,v}$, by Lemma 3.3.5 we have $aa' \in N_{b,v}$, so $(aa', b)_v = 1$. □

3.4 Formula for the Hilbert Symbol

Using the bimultiplicativity of the Hilbert symbol, we will derive a formula for it. Some texts use a different approach and find a formula for the Hilbert symbol before showing its bimultiplicativity. Then the formula is proven to be bimultiplicative, implying that the Hilbert symbol is bimultiplicative. See [4, pp. 19-22] for an example of this alternate approach.

Lemma 3.4.1. *If p is an odd prime and $a \in \mathbf{Z}_p^\times$, then $(a,p)_p = (\frac{a}{p})$.*

Proof. First we will show that $(\frac{a}{p}) = 1$ implies $(a,p)_p = 1$. Suppose $(\frac{a}{p}) = 1$. Then $a \equiv \square \bmod p$, and by Corollary 2.1.7, $a = \square$ in $\mathbf{Z}_p^\times$. Then $(a,p)_p = 1$ by Theorem 3.1.5(i). To show $(a,p)_p = 1$ implies $(\frac{a}{p}) = 1$, suppose $(a,p)_p = 1$. Then there exists $x, y, z \in \mathbf{Z}_p$ with at least one in $\mathbf{Z}_p^\times$ such that $ax^2+py^2 = z^2$. If $p|x$ then $p|(ax^2+py^2) = z^2$. With this, $p^2|(z^2 - ax^2) = py^2$ which implies that $p|y$, a contradiction since one of x, y, or z is a unit. So it must be that $x \not\equiv 0 \bmod p$. Now reducing $ax^2 + py^2 = z^2$ mod p gives $ax^2 \equiv z^2 \bmod p$. This implies that $a \equiv \square \bmod p$, so $(\frac{a}{p}) = 1$. □

Lemma 3.4.2. *If p is an odd prime, then $(p,p)_p = (\frac{-1}{p})$.*

Proof. First we will show that $(\frac{-1}{p}) = 1$ implies $(p,p)_p = 1$. Suppose $(\frac{-1}{p}) = 1$. Then $-1 \equiv \square \bmod p$, and by Corollary 2.1.7, $-1 = \square$ in $\mathbf{Z}_p^\times$. Then $(x,y,z) = (1, \sqrt{-1}, 0)$ is a solution to the equation $px^2 + py^2 = z^2$ and $(p,p)_p = 1$. To show $(p,p)_p = 1$ implies $(\frac{-1}{p}) = 1$, suppose $(p,p)_p = 1$. Then there is a solution to $px^2 + py^2 = z^2$ in $\mathbf{Q}_p$. This implies that $x^2 + y^2 = pz^2$ has a solution in $\mathbf{Q}_p$. And if it has a solution in $\mathbf{Q}_p$ then it has a solution with $x, y, z \in \mathbf{Z}_p$ where at least one of them is a unit. Also if $p|x$ then $p|y$, so we have that $p^2|(x^2 + y^2) = pz^2$. Thus $p|z$, making it so that $x, y, z \notin \mathbf{Z}_p^\times$, a

contradiction. So it must be that $x \not\equiv 0 \bmod p$. Now if we reduce $x^2 + y^2 = pz^2 \bmod p$ we get that $x^2+y^2 \equiv 0 \bmod p$, which implies that $-1 \equiv \square \bmod p$ and $(\frac{-1}{p}) = 1$. $\square$

Lemma 3.4.3. *If* $u, w \in \mathbf{Z}_2^\times$, *then* $(u, w)_2 = (-1)^{\frac{u-1}{2}\frac{w-1}{2}}$.

Proof. Note that this statement is equivalent to $(u, w)_2 = 1$ if and only if $u \equiv 1 \bmod 4$ or $w \equiv 1 \bmod 4$. We will prove this statement by dividing it into three cases.

Case 1: Let $u \equiv 1 \bmod 4$ and $w \equiv 1 \bmod 4$.

(i) Let $u \equiv 1 \bmod 8$ or $w \equiv 1 \bmod 8$. Then we have that $u = \square$ in $\mathbf{Z}_2^\times$ or $w = \square$ in $\mathbf{Z}_2^\times$, and $(u, w)_2 = 1$ by Theorem 3.1.5(i).

(ii) Let $u \equiv 5 \bmod 8$ and $w \equiv 5 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. If we let $x = 1$ and $y = 2$, then $ux^2 + wy^2 \equiv 5x^2 + 5y^2 \equiv 5 \cdot 1 + 5 \cdot 4 \equiv 25 \equiv 1 \bmod 8$. So by Theorem 3.2.4, we have proven the existence of a solution z when $x = 1$ and $y = 2$. Thus $(u, w)_2 = 1$.

Case 2: Let $u \equiv 1 \bmod 4$ and $w \equiv 3 \bmod 4$.

(i) Let $u \equiv 1 \bmod 8$. Then $u = \square$ in $\mathbf{Z}_2$ and $(u, w)_2 = 1$ by Theorem 3.1.5(i).

(ii) Let $u \equiv 5 \bmod 8$ and $w \equiv 3 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. If we let $x = 1$ and $y = 2$, then $ux^2 + wy^2 \equiv 5x^2 + 3y^2 \equiv 5 \cdot 1 + 3 \cdot 4 \equiv 17 \equiv 1 \bmod 8$. So we have proven the existence of a solution z when $x = 1$ and $y = 2$. Thus $(u, w)_2 = 1$.

(iii) Let $u \equiv 5 \bmod 8$ and $w \equiv 7 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. Again letting $x = 1$ and $y = 2$, we get that $ux^2 + wy^2 \equiv 5x^2 + 7y^2 \equiv 5 \cdot 1 + 7 \cdot 4 \equiv 33 \equiv 1 \bmod 8$ and $(u, w)_2 = 1$ as before.

Case 3: Let $u \equiv 3 \bmod 4$ and $w \equiv 3 \bmod 4$.

(*i*) Let $u \equiv 3 \bmod 8$ and $w \equiv 3 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. If a solution exists in $\mathbf{Q}_2$ we can find one in $\mathbf{Z}_2$ that includes a unit, so we can reduce this equation mod 8 and get $3x^2 + 3y^2 \equiv z^2 \bmod 8$. Here we can see that if $2|x$ and $2|y$ then $2|z$ and none of them will be a unit. But we have that one of them is a unit. So let x and y either be both units, or let one be a unit and the other be a nonunit. Since the equation is symmetric with respect to x and y, we can narrow it down to half of these cases. We let x and y run through a set of possible values mod 8 in the table below.

x^2, y^2	$3x^2 + 3y^2 \bmod 8$
$1, 1$	$3 + 3 \equiv 6$
$1, 0$	$3 + 0 \equiv 3$
$1, 4$	$3 + 12 \equiv 7$

Since $3x^2 + 3y^2$ is not congruent to any squares mod 8, we have a contradiction. So $(u, w)_2 = -1$.

(*ii*) Let $u \equiv 3 \bmod 8$ and $w \equiv 7 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. If a solution exists in $\mathbf{Q}_2$ we can find one in $\mathbf{Z}_2$ that includes a unit, so we can reduce this equation mod 8 and get $3x^2 + 7y^2 \equiv z^2 \bmod 8$, or equivalently $3x^2 \equiv z^2 + y^2 \bmod 8$. Here we can see that if $2|z$ and $2|y$ then $2|x$ and none of them will be a unit. But one of them is a unit. So let z and y either be both units, or let one be a unit and the other be a nonunit. Since the equation is symmetric with respect to z and y, we can narrow it down to half of these cases. Let z and y run through a set of values mod 8 in the table below.

z^2, y^2	$\frac{1}{3}(z^2+y^2) \bmod 8$
$1, 1$	$\frac{2}{3} \equiv 6$
$1, 0$	$\frac{1}{3} \equiv 3$
$1, 4$	$\frac{5}{3} \equiv 7$

Since $\frac{1}{3}(z^2+y^2)$ is not congruent to any squares mod 8, we have a contradiction. So $(u, w)_2 = -1$.

(*iii*) Let $u \equiv 7 \bmod 8$ and $w \equiv 7 \bmod 8$. We will consider $ux^2 + wy^2 = z^2$. If a solution exists in $\mathbf{Q}_2$ we can find one in $\mathbf{Z}_2$ that includes a unit, so we can reduce this equation mod 8 and get $7x^2 + 7y^2 \equiv z^2 \bmod 8$. If $2|x$ and $2|y$ then $2|z$ and none of them will be a unit. But one of them is a unit. So let x and y either be both units, or let one be a unit and the other be a nonunit. Since the equation is symmetric with respect to x and y, we can narrow it down to half of these cases. We let x and y run through a set of possible values mod 8 in the table below.

x^2, y^2	$7x^2 + 7y^2 \bmod 8$
$1, 1$	$7 + 7 \equiv 6$
$1, 0$	$7 + 0 \equiv 7$
$1, 4$	$7 + 28 \equiv 3$

Since $7x^2+7y^2$ is not congruent to any squares mod 8, we have a contradiction. So $(u, w)_2 = -1$.

From these three cases we have that $(u, w)_2 = 1$ if and only if $u \equiv 1 \bmod 4$ or $w \equiv 1 \bmod 4$. Thus, $(u, w)_2 = (-1)^{\frac{u-1}{2}\frac{w-1}{2}}$. □

Lemma 3.4.4. *Let $u \in \mathbf{Z}_2^\times$. Then $(u, 2)_2 = (-1)^{\frac{u^2-1}{8}}$.*

Proof. Note that this statement is equivalent to $(u, 2)_2 = 1$ if and only if $u \equiv 1 \bmod 8$ or $u \equiv 7 \bmod 8$. We will prove this statement by examining two cases.

Case 1: Let $u \equiv 1 \bmod 8$ or $u \equiv 7 \bmod 8$.

(*i*) Let $u \equiv 1 \bmod 8$. Then $u = \square$ in $\mathbf{Z}_p$ and $(u, 2)_2 = 1$ by Theorem 3.1.5(i).

(*ii*) Let $u \equiv 7 \bmod 8$. We will consider $ux^2 + 2y^2 = z^2$. If we let $x = 1$ and $y = 1$, then $ux^2 + wy^2 \equiv 7x^2 + 2y^2 \equiv 7 \cdot 1 + 2 \cdot 1 \equiv 1 \bmod 8$, implying that we can find a z. We have proven the existence of a solution, meaning $(u, 2)_2 = 1$.

Case 2: Let $u \equiv 3 \bmod 8$ or $u \equiv 5 \bmod 8$.

(*i*) Let $u \equiv 3 \bmod 8$. We will consider $ux^2 + 2y^2 = z^2$. If a solution exists in $\mathbf{Q}_2$ we can find one in $\mathbf{Z}_2$ that includes a unit, so we can reduce this equation mod 8 and get $3x^2 + 2y^2 \equiv z^2 \bmod 8$. From here, if $2|x$ then $2|3x^2 + 2y^2 = z^2$, implying $2|z$. Then we have that $2^2|x^2$ and $2^2|z^2$, so $2^2|z^2 - 3x^2 = 2y^2$, implying $2|y$. This is a contradiction as at least one of x, y, z is a unit. So it must be that x is a unit and $x^2 \equiv 1 \bmod 8$. We now let x^2 and y^2 run through all possible combinations in the table below.

x^2, y^2	$3x^2 + 2y^2 \bmod 8$
$1, 1$	$3 + 2 \equiv 5$
$1, 0$	$3 + 0 \equiv 3$
$1, 4$	$3 + 8 \equiv 3$

Since $3x^2+2y^2$ is not congruent to any squares mod 8, we have a contradiction. So $(u,2)_2 = -1$.

(ii) Let $u \equiv 5 \bmod 8$. We will consider $ux^2+2y^2 = z^2$. If a solution exists in $\mathbf{Q}_2$ we can find one in $\mathbf{Z}_2$ that includes a unit, so we can reduce this equation mod 8 and get $5x^2+2y^2 \equiv z^2 \bmod 8$. From here, if $2|x$ then $2|5x^2+2y^2 = z^2$, implying $2|z$. Then we have that $2^2|x^2$ and $2^2|z^2$, so $2^2|z^2 - 5x^2 = 2y^2$, implying $2|y$. This is a contradiction as at least one of x, y, z is a unit. So it must be that x is a unit and $x^2 \equiv 1 \bmod 8$. We now let x^2 and y^2 run through all possible combinations in the table below.

x^2, y^2	$5x^2 + 2y^2 \bmod 8$
$1, 1$	$5+2 \equiv 7$
$1, 0$	$5+0 \equiv 5$
$1, 4$	$5+8 \equiv 5$

Since $5x^2+2y^2$ is not congruent to any squares mod 8, we have a contradiction. So $(u,2)_2 = -1$.

Therefore, from these three cases we have that $(u,2)_2 = 1$ if and only if $u \equiv 1 \bmod 8$ or $u \equiv -1 \bmod 8$. Thus, $(u,2)_2 = (-1)^{\frac{u^2-1}{8}}$. □

Theorem 3.4.5. *Let $a, b \in \mathbf{Q}_v^\times$. If $v = p$ is prime, write $a = p^m u$ and $b = p^n w$ for some $m, n \in \mathbf{Z}$ and $u, w \in \mathbf{Z}_p^\times$. A formula for $(a,b)_v$ is given as follows.*

1) *When* $v = \infty$,

$$(a,b)_\infty = \begin{cases} +1, & \text{if } a > 0 \text{ or } b > 0, \\ -1, & \text{otherwise.} \end{cases}$$

2) *When* $v = p > 2$,

$$(a,b)_p = \left(\frac{-1}{p}\right)^{mn} \left(\frac{u}{p}\right)^n \left(\frac{w}{p}\right)^m.$$

3) *When* $v = p = 2$,

$$(a,b)_2 = (-1)^{\frac{u-1}{2}\frac{w-1}{2} + m\frac{w^2-1}{8} + n\frac{u^2-1}{8}}.$$

Proof.

1) If $a, b < 0$ in $\mathbf{R}$ and $ax^2 + by^2 = z^2$ with $x, y, z \in \mathbf{R}$, then $ax^2 + by^2 = 0$ and $z^2 = 0$ since $ax^2 + by^2 \leq 0$ and $z^2 \geq 0$. Since $ax^2 \leq 0$ and $by^2 \leq 0$, we have $ax^2 = 0$ and $by^2 = 0$. Thus $x = 0$, $y = 0$, and $z = 0$, so $(a,b)_\infty = -1$. On the other hand, if $a > 0$ or $b > 0$, without loss of generality suppose $a > 0$. Then $(x, y, z) = (1, 0, \sqrt{a})$ is a solution to $ax^2 + by^2 = z^2$ and thus $(a,b)_\infty = 1$.

2) Using Theorem 3.3.6, we can write $(a,b)_p = (p,p)_p^{mn}(u,p)_p^n(w,p)_p^m(u,w)_p$. Now, $(p,p)_p = (\frac{-1}{p})$ by Lemma 3.4.2. Also, $(u,p)_p = (\frac{u}{p})$ and $(w,p)_p = (\frac{w}{p})$ by Lemma 3.4.1. Lastly, $(u,w)_p = 1$ by Corollary 2.1.9. Putting these all together we have

$$(a,b)_p = (p,p)_p^{mn}(u,p)_p^n(w,p)_p^m(u,w)_p = \left(\frac{-1}{p}\right)^{mn} \left(\frac{u}{p}\right)^n \left(\frac{w}{p}\right)^m.$$

3) Using Theorem 3.3.6, we can write $(a,b)_2 = (2,2)_2^{mn}(u,2)_2^n(w,2)_2^m(u,w)_2$. First, $(2,2)_2 = 1$ as $(1,1,2)$ is a solution to $2x^2 + 2y^2 = z^2$. Next, $(u,2)_2 = (-1)^{\frac{u^2-1}{8}}$ and $(w,2)_2 = (-1)^{\frac{w^2-1}{8}}$ by Lemma 3.4.4. Lastly, $(u,w)_2 = (-1)^{\frac{u-1}{2}\frac{w-1}{2}}$ by Lemma 3.4.3.

So overall we have

$$(a,b)_2 = (-1)^{\frac{u-1}{2}\frac{w-1}{2}+m\frac{w^2-1}{8}+n\frac{u^2-1}{8}}.$$

□

3.5 Hilbert Reciprocity Law on Q

Now that we have established a formula for the Hilbert symbol and shown its bimultiplicativity, we will connect it to quadratic reciprocity.

Theorem 3.5.1. (*Quadratic Reciprocity on* $\mathbf{Z}$.) *Let* $p, q \in \mathbf{Z}^+$ *be distinct odd primes. Then we have the following:*

(*i*) (*Main Law*) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

(*ii*) (*First Supplementary Law*) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(*iii*) (*Second Supplementary Law*) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem 3.5.2. *The following are equivalent:*

(*i*) *The quadratic reciprocity law.*

(*ii*) *Hilbert reciprocity: for all* $a, b \in \mathbf{Q}^\times$ *we have* $(a,b)_v = 1$ *for all but finitely many* v *and*

$$\prod_v (a,b)_v = 1.$$

Remark 3.5.3. The bimultiplicativity of the Hilbert symbol will be very useful when proving this theorem. To see why, consider $\prod_v (6,-10)_v$. Since $(6,-10)_v = (2\cdot 3, -1\cdot$

$2 \cdot 5)_v = (2,-1)_v(2,2)_v(2,5)_v(3,-1)_v(3,2)_v(3,5)_v$, we can check that $\prod_v (6,-10)_v = 1$ by checking that $\prod_v (2,-1)_v = 1$, $\prod_v (2,2)_v = 1$, $\prod_v (2,5)_v = 1$, $\prod_v (3,-1)_v = 1$, $\prod_v (3,2)_v = 1$, and $\prod_v (3,5)_v = 1$. So we can reduce the problem down to just checking the symbols when the inputs are primes or -1.

Proof of Theorem 3.5.2.. Since a and b can be decomposed into a product of primes and -1, the Hilbert symbol can be split apart using its bimultiplicativity until the only numbers in the symbols are either primes or -1. As a result, we only need to check $\prod_v (a,b)_v = 1$ when a and b are primes or -1. Let p and q be distinct odd primes in each case.

Case 1: $\prod_v (-1,-1)_v = 1$

By Corollary 2.1.9, $(-1,-1)_v = 1$ if v is any odd prime. So we only have to check the product for $v = 2$ and $v = \infty$. We will do this by using Theorem 3.4.5. We get that $(-1,-1)_\infty = -1$ and $(-1,-1)_2 = (-1)^{\frac{-1-1}{2}\frac{-1-1}{2}} = -1$. Thus we have that $\prod_v (-1,-1)_v = 1$.

Case 2: $\prod_v (-1,2)_v = 1$

We have $(1,-2)_v = 1$ for all v since $-x^2 + 2y^2 = z^2$ has the solution $(x,y,z) = (1,1,1)$.

Case 3: $\prod_v (-1,p)_v = 1$

By Corollary 2.1.9, it suffices to compute $(-1,p)_v$ for $v = 2$, $v = p$, and $v = \infty$. Theorem 3.4.5 yields $(-1,p)_\infty = 1$, $(-1,p)_p = (\frac{-1}{p})$, and $(-1,p)_2 = (-1)^{\frac{-1-1}{2}\frac{p-1}{2}} = (-1)^{\frac{-(p-1)}{2}} = (-1)^{\frac{p-1}{2}}$. Thus $\prod_v (-1,p)_v = 1$ if and only if $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, the first supplementary for quadratic reciprocity.

Case 4: $\prod_v (2,2)_v = 1$

We have $(2,2)_v = 1$ for all v since $2x^2 + 2y^2 = z^2$ has the solution $(x,y,z) =$

$(1,1,2)$.

Case 5: $\prod_v (2,p)_v = 1$

By Corollary 2.1.9, it suffices to compute $(2,p)_v$ for $v=2$, $v=p$, and $v=\infty$. We use Theorem 3.4.5 and see that $(2,p)_\infty = 1$, $(2,p)_p = (\frac{2}{p})$, and $(2,p)_2 = (-1)^{\frac{p^2-1}{8}}$. Thus $\prod_v (2,2)_v = 1$ if and only if $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, the second supplementary law of quadratic reciprocity.

Case 6: $\prod_v (p,p)_v = 1$

By Corollary 2.1.9, it suffices to compute $(p,p)_v$ for $v=2$, $v=p$, and $v=\infty$. Using Theorem 3.4.5, we get that $(p,p)_\infty = 1$, $(p,p)_p = (\frac{-1}{p})$, and $(p,p)_2 = (-1)^{\frac{p-1}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$. Thus, $\prod_v (p,p)_v = 1$ if and only if $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, the first supplementary law of quadratic reciprocity.

Case 7: $\prod_v (p,q)_v = 1$

By Corollary 2.1.9, it suffices to compute $(p,q)_v$ for $v=2$, $v=p$, $v=q$, and $v=\infty$. Using Theorem 3.4.5, we have that $(p,q)_\infty = 1$, $(p,q)_p = (\frac{q}{p})$, $(p,q)_q = (\frac{p}{q})$, and $(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Thus $\prod_v (p,q)_v = 1$ if and only if $(\frac{p}{q})(\frac{q}{p})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$, which is equivalent to $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, the main law of quadratic reciprocity.

So by checking these seven cases we see that if Hilbert reciprocity holds, then quadratic reciprocity holds. In particular, we showed that Cases 3, 5, 6, and 7 are equivalent to the law of quadratic reciprocity (main law and supplementary laws). However, we will also prove the reverse direction for completeness.

For the other direction, assume that quadratic reciprocity holds. Then $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, so $(\frac{p}{q})(\frac{q}{p})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$. Then by Lemmas 3.4.1 and 3.4.3, we have $(p,q)_p(p,q)_q(p,q)_2 = 1$. Also, by Corollary 2.1.9, we have that $(p,q)_v = 1$ for all v except $v=2$, $v=p$, $v=q$, and $v=\infty$. Using Theorem 3.4.5, we have that $(p,q)_\infty = 1$. Thus, $\prod_v (p,q)_v = 1$ for all v.

Further, quadratic reciprocity gives us that $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Then by Lemmas 3.4.1 and 3.4.3 we have that $(-1,p)_p(-1,p)_2 = 1$. Additionally, using Theorem 3.4.5 yields $(-1,p)_\infty = 1$. So just as above, applying Corollary 2.1.9 to what we have gives $\prod_v (-1,p)_v = 1$. An almost identical argument tells us that $\prod_v (p,p)_v = 1$ as well.

Finally, quadratic reciprocity also states that $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. With this, Lemmas 3.4.1 and 3.4.4 tell us that $(2,p)_p(2,p)_2 = 1$. Using Theorem 3.4.5, we have $(2,p)_\infty = 1$. So once again, using Corollary 2.1.9 here gives us $\prod_v (2,p)_v = 1$.

Altogether, using what we showed above and what we showed in Cases 1, 2, and 4, we have shown that quadratic reciprocity implies Hilbert reciprocity. So overall we now have that Hilbert reciprocity is equivalent to quadratic reciprocity. $\square$

Chapter 4

The Hilbert Symbol on $\mathbf{Q}(i)_\pi$

4.1 Primes in $\mathbf{Z}[i]$ and completions of $\mathbf{Q}(i)$

Here we will define the notion of primality in $\mathbf{Z}[i]$. These primes will used to construct completions of $\mathbf{Q}(i)$, just as primes in $\mathbf{Z}$ were used to construct completions of $\mathbf{Q}$.

Definition 4.1.1. The *norm* of a Gaussian integer $\alpha = a + bi$ is denoted by $N(\alpha) = a^2 + b^2$.

Definition 4.1.2. A Gaussian integer $\pi = a + bi$ with $a, b \in \mathbf{Z}$ is a *Gaussian integer prime* if π is not 0 or a unit or the product of two nonunits. Further, we define $\alpha \in \mathbf{Z}[i]$ to be *odd* if $N(\alpha)$ is an odd number.

Theorem 4.1.3. *Up to multiplication by units, the primes in* $\mathbf{Z}[i]$ *are:*

(*i*) $1 + i$,

(*ii*) $\pi \in \mathbf{Z}[i]$ *such that* $\pi\bar{\pi} = p$ *where* p *is a prime integer such that* $p \equiv 1 \bmod 4$,

(iii) $p \in \mathbf{Z}^+$ *such that* p *is prime and* $p \equiv 3 \bmod 4$.

Proof. See [1, p. 33, Theorem 9.9]. □

Remark 4.1.4. Any primes in $\mathbf{Z}^+$ that are congruent to 1 mod 4 are not prime in $\mathbf{Z}[i]$. For example, $5 = (1+2i)(1-2i)$ is not prime. Also, 2 is not prime in $\mathbf{Z}[i]$ as $2 = (1+i)(1-i)$.

Definition 4.1.5. Let $\pi \in \mathbf{Z}[i]$ be a Gaussian integer prime. Define the *π-adic valuation* on $\mathbf{Z}[i]$ to be the function $v_\pi : \mathbf{Z}[i] - \{0\} \longrightarrow \mathbf{R}$ such that for each $\alpha \in \mathbf{Z}[i] - \{0\}$, $v_\pi(\alpha)$ is the unique positive integer satisfying $\alpha = \pi^{v_\pi(\alpha)}\alpha'$ where $\pi \nmid \alpha'$. Furthermore, we extend v_π so that for $\alpha = \frac{\beta}{\gamma} \in \mathbf{Q}(i)^\times$ with $\beta,\gamma \in \mathbf{Z}[i] - \{0\}$, we have $v_\pi(\alpha) = v_\pi(\beta) - v_\pi(\gamma)$. Lastly, we set $v_\pi(0) = \infty$.

Remark 4.1.6. The uniqueness of the exponent $v_\pi(\alpha)$ relies on unique factorization in $\mathbf{Z}[i]$.

Definition 4.1.7. Let π be a Gaussian integer prime and let $\alpha \in \mathbf{Q}(i)$. We define the *π-adic absolute value* on $\mathbf{Q}(i)$ as follows:

$$|\alpha|_\pi := \begin{cases} (\frac{1}{N(\pi)})^{v_\pi(\alpha)}, & \text{if } \alpha \neq 0, \\ 0, & \text{if } \alpha = 0. \end{cases}$$

Example 4.1.8. Consider the Gaussian integer prime $1+2i$. We will calculate $|25|_{1+2i}$. Since $25 = 5^2 = (1+2i)^2(1-2i)^2$ and $1+2i \nmid 1-2i$ as $\frac{1-2i}{1+2i} = \frac{-3-4i}{5} \notin \mathbf{Z}[i]$, we have that $v_{1+2i}(25) = 2$ and $|25|_{1+2i} = \frac{1}{5^2} = \frac{1}{25}$.

Example 4.1.9. Now we will calculate $|-30+40i|_{1+2i}$. Since $\frac{-30+40i}{(1+2i)^3} = 2-4i$ and $\frac{2-4i}{1+2i} = \frac{-6-8i}{5} \notin \mathbf{Z}[i]$, we have that $v_{1+2i}(-30+40i) = 3$. So, $|-30+40i|_{1+2i} = \frac{1}{5^3} = \frac{1}{125}$.

Example 4.1.10. Consider the Gaussian integer prime 3. It has norm 9, so $|6+3i|_3 = |3(2+i)|_3 = (\frac{1}{9})^1 = \frac{1}{9}$. In particular, for $\alpha \in \mathbf{Q}$, its 3-adic size in $\mathbf{Q}(i)$ is the square of its 3-adic size in $\mathbf{Q}$: $|\alpha|_{3,\mathbf{Q}(i)} = |\alpha|^2_{3,\mathbf{Q}}$.

Just as $\mathbf{Q}_p$ is a completion of $\mathbf{Q}$ with respect to the absolute value $|\cdot|_p$ with p prime, we can construct $\mathbf{Q}(i)_\pi$, a completion of $\mathbf{Q}(i)$ with respect to the absolute value $|\cdot|_\pi$ for a prime Gaussian integer π. We will define the Hilbert symbol on $\mathbf{Q}(i)_\pi$ in the exact same way that we defined it on $\mathbf{Q}_p$, and it will have all of the same basic properties of the Hilbert symbol on $\mathbf{Q}_p$ stated in Theorem 3.1.5. In addition, we will state a version of Hensel's lemma specific to $\mathbf{Q}(i)_\pi$.

Theorem 4.1.11. *Let $\alpha \in \mathbf{Q}(i)^\times_\pi$ where π is a Gaussian integer prime. Then α can be written uniquely in the form*

$$\alpha = b_{-n_0}\pi^{-n_0} + \cdots + b_0 + b_1\pi + b_2\pi^2 + \cdots + b_n\pi^n + \cdots = \sum_{n \geq -n_0} b_n\pi^n$$

with each b_i lying in a set of representatives for $\mathbf{Z}[i]/\pi\mathbf{Z}[i]$ (including 0 as the representative of $\overline{0}$), and $-n_0 = v_\pi(x)$.

Definition 4.1.12. The ring of *π-adic integers* is $\mathbf{Z}[i]_\pi = \{\alpha \in \mathbf{Q}(i)_\pi : |\alpha|_\pi \leq 1\}$. In particular, the units of $\mathbf{Z}[i]_\pi$ are $\mathbf{Z}[i]^\times_\pi = \{\alpha \in \mathbf{Q}(i)_\pi : |\alpha|_\pi = 1\}$.

Theorem 4.1.13. *Let π be a Gaussian integer prime. For $n \in \mathbf{Z}$ such that $n \geq 1$, the natural ring homomorphism $\mathbf{Z}[i] \hookrightarrow \mathbf{Z}[i]_\pi$ induces a ring isomorphism $\mathbf{Z}[i]/\pi^n\mathbf{Z}[i] \to \mathbf{Z}[i]_\pi/\pi^n\mathbf{Z}[i]_\pi$.*

Theorem 4.1.14. *Let $\alpha \in \mathbf{Z}[i]$ such that $\alpha \neq 0$. Then $\#(\mathbf{Z}[i]/\alpha\mathbf{Z}[i]) = N(\alpha)$.*

Proof. See [1, pp. 21-22, Theorem 7.14]. □

Remark 4.1.15. For any odd prime Gaussian integer π, we have that $\mathbf{Z}[i]/\pi\mathbf{Z}[i]$ is a finite field of odd order.

Theorem 4.1.16 (Hensel's Lemma). *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial whose coefficients are in $\mathbf{Z}[i]_\pi$. Suppose that there exists a π-adic integer $\alpha_0 \in \mathbf{Z}[i]_\pi$ such that*

$$f(\alpha_0) \equiv 0 \bmod \pi$$

and

$$f'(\alpha_0) \not\equiv 0 \bmod \pi,$$

where $f'(x)$ is the derivative of $f(x)$. Then there exists a unique π-adic integer $\alpha \in \mathbf{Z}[i]_\pi$ such that $\alpha \equiv \alpha_0 \bmod \pi$ and $f(\alpha) = 0$.

Corollary 4.1.17. *Let π be an odd Gaussian integer prime and let $u \in \mathbf{Z}[i]_\pi^\times$. Then $u = \square$ in $\mathbf{Z}[i]_\pi$ if and only if $u \equiv \square \bmod \pi$.*

Proof. Since $\mathbf{Z}[i]_\pi/\pi\mathbf{Z}[i]_\pi$ is a finite field of odd order, the proof is exactly like that of Corollary 2.1.7. □

Lemma 4.1.18. *Let π be an odd Gaussian integer prime. Further, let $a, b, c \in \mathbf{Z}[i]_\pi^\times$. Then there exist $x, y \in \mathbf{Z}[i]_\pi/\pi\mathbf{Z}[i]_\pi$ such that $ax^2 + by^2 \equiv c \bmod \pi$.*

Proof. Once again, since $\mathbf{Z}[i]_\pi/\pi\mathbf{Z}[i]_\pi$ is a finite field of odd order, the proof is just like proof of Lemma 2.1.8. □

Corollary 4.1.19. *Let π be an odd Gaussian integer prime and let $a, b, c \in \mathbf{Z}[i]_\pi^\times$. Then the equation $ax^2 + by^2 = c$ has a solution with $x, y \in \mathbf{Z}[i]_\pi$.*

Proof. We have that $\mathbf{Z}[i]_\pi/\pi\mathbf{Z}[i]_\pi$ is a finite field of odd order, so this proof is just like the proof of Corollary 2.1.9. □

4.2 Hilbert Symbol on $\mathbf{Q}(i)_\pi$

The completions of $\mathbf{Q}(i)$ are denoted by $\mathbf{Q}(i)_v$ where v is a place, either a Gaussian prime π or ∞. Here we have one infinite prime, ∞, and $\mathbf{Q}(i)_\infty = \mathbf{C}$.

Definition 4.2.1. For any $a, b \in \mathbf{Q}(i)_v^\times$, the *Hilbert symbol* of a and b relative to $\mathbf{Q}(i)_v$ is defined as

$$(a,b)_v := \begin{cases} +1, & \text{if } ax^2 + by^2 = z^2 \text{ has a solution in } \mathbf{Q}(i)_v^3 \text{ besides } (0,0,0), \\ -1, & \text{otherwise.} \end{cases}$$

Remark 4.2.2. Since we can multiply the equation $ax^2 + by^2 = z^2$ by any nonzero square without changing its solvability, for $v \neq \infty$ if there is a solution to $ax^2 + by^2 = z^2$ with $x, y, z \in \mathbf{Q}(i)_v$ not all zero, then there is a solution with $x, y, z \in \mathbf{Z}[i]_v$ and x, y, or z in $\mathbf{Z}[i]_v^\times$.

Example 4.2.3. We will compute $(2,3)_v$. Consider the equation $2x^2 + 3y^2 = z^2$ for $x, y, z \in \mathbf{Q}(i)_v$. This equation has the solution $(x, y, z) = (i, 1, 1)$. And since $i, 1 \in \mathbf{Q}(i)_v$ for all v, we now have that $(2,3)_v = 1$ for all v.

Theorem 4.2.4. *Let $a, b, c \in \mathbf{Q}(i)_v^\times$. We have*

(*i*) $(a,b)_v = (b,a)_v$ *and* $(a,c^2)_v = 1$,

(*ii*) $(a,-a)_v = (a,1-a)_v = 1$,

(*iii*) $(a,b)_v = (ac^2,b)_v = (a,bc^2)_v$

Proof. The proof is the same as the one for Theorem 3.1.5. □

Lemma 4.2.5. *Let $a, b \in \mathbf{Q}(i)_\infty = \mathbf{C}^\times$. Then $(a, b)_\infty = 1$.*

Proof. Since every complex number is a square in $\mathbf{C}$, we have that a and b are squares. Thus, $(a, b)_\infty = 1$ by Theorem 4.2.4 (i). □

Definition 4.2.6. For $b \in \mathbf{Q}(i)_v^\times$, set $N_{b,v} = \{x^2 - by^2 \neq 0 : x, y \in \mathbf{Q}(i)_v\}$.

Theorem 4.2.7.

(i) *For all $b \in \mathbf{Q}(i)_v^\times$, $N_{b,v}$ is a subgroup of $\mathbf{Q}(i)_v^\times$ and $(\mathbf{Q}(i)_v^\times)^2 \subset N_{b,v} \subset \mathbf{Q}(i)_v^\times$.*

(ii) *If $b \in (\mathbf{Q}(i)_v^\times)^2$, then $N_{b,v} = \mathbf{Q}(i)_v^\times$.*

Proof.

(i) The proof is the same as the one for Theorem 3.1.7.

(ii) Same as the proof in Theorem 3.1.8.

□

Remark 4.2.8. We will see in Theorems 4.4.1 and 4.4.2 that if $b \in \mathbf{Q}(i)_v^\times$ and $b \notin (\mathbf{Q}(i)_v^\times)^2$, then $N_{b,v} \neq \mathbf{Q}(i)_v^\times$.

Theorem 4.2.9. *For $a, b \in \mathbf{Q}(i)_v^\times$, $(a, b)_v = 1$ if and only if $a \in N_{b,v}$.*

Proof. The proof is the same as the one for Theorem 3.1.10. □

4.3 Square Classes

In this section, we will find a list of square class representatives of $\mathbf{Q}(i)_\pi^\times$ for each Gaussian prime π. The methods we use to do this will be very similar to the ones used when finding square class representatives for $\mathbf{Q}_p^\times$.

Theorem 4.3.1. *Let π be an odd prime Gaussian integer and let $r \in \mathbf{Z}[i]_\pi^\times$ such that $r \not\equiv \square \bmod \pi$. A complete set of square class representatives for $\mathbf{Q}(i)_\pi^\times$ is $\{1, r, \pi, r\pi\}$.*

Proof. Since $\mathbf{Q}(i)_\pi^\times = \pi^{\mathbf{Z}} \times \mathbf{Z}[i]_\pi^\times$ and $(\mathbf{Q}_\pi^\times)^2 = \pi^{2\mathbf{Z}} \times (\mathbf{Z}[i]_\pi^\times)^2$, we have

$$\mathbf{Q}(i)_\pi^\times/(\mathbf{Q}(i)_\pi^\times)^2 = \frac{\pi^{\mathbf{Z}} \times \mathbf{Z}[i]_\pi^\times}{\pi^{2\mathbf{Z}} \times (\mathbf{Z}[i]_\pi^\times)^2} \cong \frac{\pi^{\mathbf{Z}}}{\pi^{2\mathbf{Z}}} \times \frac{\mathbf{Z}[i]_\pi^\times}{(\mathbf{Z}[i]_\pi^\times)^2}.$$

Since $\frac{\pi^{\mathbf{Z}}}{\pi^{2\mathbf{Z}}}$ depends only on the parity of the power of π, it is represented by $\{1, \pi\}$. Also, $\mathbf{Z}[i]_\pi/\pi\mathbf{Z}[i]_\pi \cong \mathbf{Z}[i]/\pi\mathbf{Z}[i]$ is a finite field of odd order, so its nonzero squares are a subgroup of index 2 in the group of all nonzero elements. So $\mathbf{Z}[i]_\pi^\times/\pi\mathbf{Z}[i]_\pi^\times$ is represented by $\{1, r\}$ where $r \not\equiv \square \bmod \pi$, just like in the proof of Theorem 3.2. Thus, $\mathbf{Q}(i)_\pi^\times/(\mathbf{Q}(i)_\pi^\times)^2$ is represented by $\{1, \pi\} \times \{1, r\} = \{1, r, \pi, r\pi\}$. □

In order to classify the square class representatives for $\mathbf{Q}(i)_{1+i}$, in a way analogous to $\mathbf{Q}_2$, we will need a more general form of Hensel's lemma.

Theorem 4.3.2. *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbf{Z}[i]_{1+i}[x]$. Suppose that there exists a $(1+i)$-adic integer $\alpha_0 \in \mathbf{Z}[i]_{1+i}$ such that*

$$|f(\alpha_0)|_{1+i} < |f'(\alpha_0)|_{1+i}^2.$$

Then there exists a unique $(1+i)$-adic integer $\alpha \in \mathbf{Z}[i]_{1+i}$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| < |f'(\alpha_0)|$.

Proof. See [2, pp. 1-3, Theorem 1.4]. □

We will now do an example using this form of Hensel's lemma to determine an $m \geq 1$ such that all elements of $1 + (1+i)^m\mathbf{Z}[i]_{1+i}$ are squares, just as we determined all elements of $1 + 8\mathbf{Z}_2$ are squares in $\mathbf{Z}_2^\times$.

Example 4.3.3. We will examine the polynomial $f(x) = x^2 - u$ where $u \in \mathbf{Z}[i]^\times_{1+i}$. We want to use 1 as an approximate root. For this, we want $|f(1)|_{1+i} < |f'(1)|^2_{1+i}$, which is equivalent to $|u-1|_{1+i} < |2|^2_{1+i} = |1+i|^4_{1+i}$. This is equivalent to $u \equiv 1 \bmod (1+i)^5$. So Hensel's lemma tells us that if $u \equiv 1 \bmod (1+i)^5$, then u is a square in $\mathbf{Z}[i]^\times_{1+i}$.

It is important to note that this condition does not hold in the reverse direction. For example, $-1 = \square$ in $\mathbf{Q}(i)_{1+i}$ but $-1 \not\equiv 1 \bmod (1+i)^5$. However, this example does imply that if we want a multidirectionial statement regarding unit squares in $\mathbf{Q}(i)_{1+i}$, it would be enough to examine units mod $(1+i)^5$: if $u \equiv v \bmod (1+i)^5$ then $\frac{u}{v} = \square$, so $u = \square \iff v = \square$.

Since we'll be using $1+i$ a lot, let $\tau = 1+i$. To compute unit squares mod τ^5, we can look at numbers of the form $1 + a\tau + b\tau^2 + c\tau^3 + d\tau^4$ where $a, b, c, d \in \{0, 1\}$. Now we will square each of these mod τ^5. This information is in Table 4.3.1.

It is useful to note that $\tau^5 = -4 - 4i$, so $4i \equiv -4 \bmod \tau^5$. Additionally, since $8 = i\tau^6$, we have $-4 \equiv 4 \bmod \tau^5$ and integers only matter mod 8 when we consider them in $\mathbf{Z}[i]_\tau / \tau^5 \mathbf{Z}[i]_\tau$.

$a\ b\ c\ d$	$(1+a\tau+b\tau^2+c\tau^3+d\tau^4)^2 \mod \tau^5$
0 0 0 0	1
0 1 0 0	$-3+4i \equiv -3+4 \equiv 1$
0 0 1 0	$-3-4i \equiv -3+4 \equiv 1$
0 0 0 1	$9 \equiv 1$
0 1 1 0	$-15-8i \equiv -15+8 \equiv 1$
0 1 0 1	$5-12i \equiv 5-12 \equiv 1$
0 0 1 1	$21-20i \equiv 5-20 \equiv 1$
0 1 1 1	$9-40i \equiv 9 \equiv 1$
1 0 0 0	$3+4i \equiv 3-4 \equiv -1$
1 1 0 0	$-5+12i \equiv -5+12 \equiv -1$
1 0 1 0	$-9 \equiv -1$
1 0 0 1	$3-4i \equiv 3-4 \equiv -1$
1 1 1 0	$-25 \equiv -1$
1 1 0 1	$-5-12i \equiv -5+12 \equiv -1$
1 0 1 1	$7+24i \equiv 7+24 \equiv -1$
1 1 1 1	$-9-40i \equiv -1$

TABLE 4.3.1: The 16 unit squares of $\mathbf{Z}[i]_\tau/\tau^5$

From these calculations, we have the following theorem.

Theorem 4.3.4. *Let $u \in \mathbf{Z}[i]_\tau^\times$. Then u is a square in $\mathbf{Q}(i)_\tau^\times$ if and only if $u \equiv \pm 1 \mod \tau^5$.*

Proof. Let $u \in \mathbf{Z}[i]_\tau^\times$. First suppose $u = x^2$ in $\mathbf{Q}(i)_\tau^\times$. Then $|x|_\tau^2 = |u|_\tau = 1$, so $x \in \mathbf{Z}[i]_\tau^\times$. Thus, u is a square in $\mathbf{Q}(i)_\tau^\times$ if and only if u is a square in $\mathbf{Z}[i]_\tau^\times$, which

is equivalent to $u \equiv \square \bmod \tau^5$. By Table 4.3.1, if $u \in (\mathbf{Z}[i]_\tau^\times)^2$, then $u \equiv \pm 1 \bmod \tau^5$. On the other hand, if $u \equiv \pm 1 \bmod \tau^5$, then $u \in 1 + \tau^5\mathbf{Z}[i]_\tau$ or $u \in -(1 + \tau^5\mathbf{Z}[i]_\tau) = i^2(1 + \tau^5\mathbf{Z}[i]_\tau)$. Since all elements in $1 + \tau^5\mathbf{Z}[i]_\tau$ are squares by Example 4.3.3, u is a square in $\mathbf{Q}(i)_\tau^\times$. □

Here is a list of several numbers in $\mathbf{Z}[i]_\tau$ and their τ-adic expansions mod τ^5. We will be using this list to help simplify modular congruences later in this section.

Number	τ-adic expansion mod τ^5
-1	$1 + \tau^2 + \tau^3 + \tau^4$
i	$1 + \tau + \tau^2 + \tau^3 + \tau^4$
$-i$	$1 + \tau + \tau^3 + \tau^4$
2	$\tau^2 + \tau^3$

TABLE 4.3.2: The τ-adic expansions of some numbers mod τ^5.

We will now construct a table of the 16 units in $\mathbf{Z}[i]_\tau/\tau^5$, paired up to multiplication by -1 in each row.

1	$-1 \equiv 1+\tau^2+\tau^3+\tau^4 \bmod \ \tau^5$
$1+\tau$	$-(1+\tau) \equiv 1+\tau+\tau^2 \bmod \ \tau^5$
$1+\tau^2$	$-(1+\tau^2) \equiv 1+\tau^3+\tau^4 \bmod \ \tau^5$
$1+\tau^3$	$-(1+\tau^3) \equiv 1+\tau^2+\tau^4 \bmod \ \tau^5$
$1+\tau^4$	$-(1+\tau^4) \equiv 1+\tau^2+\tau^3 \bmod \ \tau^5$
$1+\tau+\tau^3$	$-(1+\tau+\tau^3) \equiv 1+\tau+\tau^2+\tau^3 \bmod \ \tau^5$
$1+\tau+\tau^4$	$-(1+\tau+\tau^4) \equiv 1+\tau+\tau^2+\tau^4 \bmod \ \tau^5$
$1+\tau+\tau^3+\tau^4$	$-(1+\tau+\tau^3+\tau^4) \equiv 1+\tau+\tau^2+\tau^3+\tau^4 \bmod \ \tau^5$

TABLE 4.3.3: The 8 units of $\mathbf{Z}[i]_\tau/\tau^5$ up to multiplication by ± 1.

We are now ready to list square class representatives of $\mathbf{Q}(i)_\tau^\times$.

Theorem 4.3.5. *The* 16 *square classes of* $\mathbf{Q}(i)_\tau^\times$ *are represented by*

$$\{1,\tau\} \times \{1, 1+\tau, 1+\tau^2, 1+\tau^3, 1+\tau^4, 1+\tau+\tau^3, 1+\tau+\tau^4, 1+\tau+\tau^3+\tau^4\}.$$

Proof. We have that

$$\mathbf{Q}(i)_\tau^\times/(\mathbf{Q}(i)_\tau^\times)^2 = \frac{\tau^{\mathbf{Z}} \times \mathbf{Z}[i]_\tau^\times}{\tau^{2\mathbf{Z}} \times (\mathbf{Z}[i]_\tau^\times)^2}.$$

As in Theorem 4.3.1, $\frac{\tau^{\mathbf{Z}}}{\tau^{2\mathbf{Z}}}$ is represented by $\{1,\tau\}$. Also, from Tables 4.3.1 and 4.3.3 we see that $\{1, 1+\tau, 1+\tau^2, 1+\tau^3, 1+\tau^4, 1+\tau+\tau^3, 1+\tau+\tau^4, 1+\tau+\tau^3+\tau^4\}$ represents $\mathbf{Z}[i]_\tau^\times/(\mathbf{Z}[i]_\tau^\times)^2$. Thus, $\mathbf{Q}(i)_\tau^\times/(\mathbf{Q}(i)_\tau^\times)^2 = \{1,\tau\} \times \{1, 1+\tau, 1+\tau^2, 1+\tau^3, 1+\tau^4, 1+\tau+\tau^3, 1+\tau+\tau^4, 1+\tau+\tau^3+\tau^4\}$. □

4.4 Bimultiplicativity of the Hilbert Symbol over $\mathbf{Q}(i)_v$

Here we will prove the bimultiplicativity of the Hilbert symbol over $\mathbf{Q}(i)_v$ in the same manner in which we proved it for the Hilbert symbol over $\mathbf{Q}_v$. We will show that the square classes of norms from the quadratic extensions of $\mathbf{Q}(i)_v$ are each a subgroup of $\mathbf{Q}(i)_v^\times/(\mathbf{Q}(i)_v^\times)^2$ with index 2.

Theorem 4.4.1. *Let π be an odd prime Gaussian integer and let d be a nonsquare in $\mathbf{Q}(i)_\pi^\times$. If $L_d = \mathbf{Q}(i)_\pi(\sqrt{d})$, then the group of norms $N(L_d^\times) = \{x^2 - dy^2 \neq 0 : x, y \in \mathbf{Q}(i)_\pi\}$ is a subgroup of $\mathbf{Q}(i)_\pi^\times$ with index 2.*

Proof. It suffices to prove this statement for $d = r, \pi, r\pi$ where $r \in \mathbf{Z}[i]_\pi^\times$ and $r \not\equiv \square \bmod \pi$, so we will break this proof into 3 cases. For any $d \neq \square$, we have $(\mathbf{Q}(i)_\pi^\times)^2 \subset N(L_d^\times) \subset \mathbf{Q}(i)_\pi^\times$ and $|\mathbf{Q}(i)_\pi^\times/(\mathbf{Q}(i)_\pi^\times)^2| = 4$. So it suffices to find an element of $\mathbf{Q}(i)_\pi^\times$ that is not in $N(L_d^\times)$ and an element of $N(L_d^\times)$ that is not in $(\mathbf{Q}(i)_\pi^\times)^2$. Then $N(L_d^\times)$ is strictly between $\mathbf{Q}(i)_\pi^\times$ and $(\mathbf{Q}(i)_\pi^\times)^2$, so its index is 2. First off, the equation $x^2 - dy^2 = d$ always has the solution $(x, y) = (0, i)$, so for all $d \neq \square$, we have $(\mathbf{Q}(i)_\pi^\times)^2 \subsetneq N(L_d^\times)$. It remains to show $N(L_d^\times) \subsetneq \mathbf{Q}(i)_\pi^\times$.

Case 1) Let $d = r$. Suppose the equation $x^2 - ry^2 = \pi$ has a solution in $\mathbf{Q}(i)_\pi$. Clearing denominators gives $x^2 - ry^2 = \pi z^2$ with $x, y, z \in \mathbf{Z}[i]_\pi$ and at least one is a unit. Now if we had that $\pi|x$, then we would have that $\pi|(x^2 - \pi z^2) = ry^2$. This would mean that $\pi|y$, which would imply that $\pi|z$. This would be a contradiction as x, y, and z would all be non-units. A similar situation would arise if we originally let $\pi|y$. So we must have both x and y in $\mathbf{Z}[i]_\pi^\times$. Now we can reduce mod π to get $x^2 - ry^2 \equiv 0 \bmod \pi$. Then $x^2 \equiv ry^2 \bmod \pi$ and $y \not\equiv 0 \bmod \pi$, implying that

$r \equiv \square \bmod \pi$, which is a contradiction.

Case 2) Let $d = \pi$. To show $r \notin N(L_d^\times)$, suppose $x^2 - \pi y^2 = r$ for some $x, y \in \mathbf{Q}(i)_\pi$. By clearing denominators, we get $x^2 - \pi y^2 = rz^2$ for $x, y, z \in \mathbf{Z}[i]_\pi$ and at least one is a unit. If x is not a unit, z and y also are not units, a contradiction. Thus $x \in \mathbf{Z}[i]_\pi^\times$. Reduce mod π to get $x^2 \equiv rz^2 \bmod \pi$, which implies that $r \equiv \square \bmod \pi$, which is a contradiction.

Case 3) Let $d = r\pi$. To show $r \notin N(L_d^\times)$, suppose $x^2 - r\pi y^2 = r$ for some $x, y \in \mathbf{Q}(i)_\pi$. By clearing denominators, we get $x^2 - r\pi y^2 = rz^2$ for $x, y, z \in \mathbf{Z}[i]_\pi$ and at least one is a unit. We must have x a unit, so z must also be a unit, or else $x, y, z \notin \mathbf{Z}[i]_\pi^\times$. Reduce mod π to get $x^2 \equiv rz^2 \bmod \pi$, which implies that $r \equiv \square \bmod \pi$, which is a contradiction. $\square$

Now we will show that every norm subgroup of $\mathbf{Q}(i)_\tau^\times$ has index 2.

Theorem 4.4.2. *Let $\tau = 1 + i$ and let d be a nonsquare in $\mathbf{Q}(i)_\tau^\times$. Set $L_d = \mathbf{Q}(i)_\tau(\sqrt{d})$. Then the group $N(L_d^\times) = \{x^2 - dy^2 \neq 0 : x, y \in \mathbf{Q}(i)_\tau\}$ is a subgroup of $\mathbf{Q}(i)_\tau^\times$ with index 2.*

Proof. It suffices to let d run through the square classes in $\mathbf{Q}(i)_\tau^\times$. Since $(\mathbf{Q}(i)_\tau^\times)^2 \subset N(L_d^\times) \subset \mathbf{Q}(i)_\tau^\times$ and $\mathbf{Q}(i)_\tau^\times / (\mathbf{Q}(i)_\tau^\times)^2$ has order 16, $N(L_d^\times)$ has index dividing 16 in $\mathbf{Q}(i)_\tau^\times$. Our strategy will be to first find an element of $\mathbf{Q}(i)_\tau$ that is not in $N(L_d^\times)$. This will show that the index of $N(L_d^\times)$ is less than or equal to 8. Next we will find 8 elements of $\mathbf{Q}(i)_\tau^\times$ that are in $N(L_d^\times)$ and are in different square classes, showing that the index of $N(L_d^\times)$ in $\mathbf{Q}(i)_\tau^\times$ is exactly 8. Since there are 15 cases to check, we will only showcase four of them here, two where d is a unit and two where d is a non-unit.

Case 1) Let $d = 1 + \tau$. First, we will show that $1 + \tau^2 \notin N(L_d^\times)$ using our knowledge of the unit squares in $\mathbf{Z}[i]_\tau / \tau^5 \mathbf{Z}[i]_\tau$. Since the unit squares are $\pm 1 \bmod \tau^5$,

representatives for the set of all squares mod τ^5 are $\{0, \pm 1, \pm\tau^2, \tau^4\}$. (Note that listing $\pm\tau^4$ would be redundant, as $-\tau^4 \equiv \tau^4 \bmod \tau^5$.) Now we will show that there are no solutions in $\mathbf{Q}(i)_\tau$ to $x^2-(1+\tau)y^2 = 1+\tau^2$ by viewing it as $(1+\tau)y^2+(1+\tau^2)z^2 = x^2$ with $x, y, z \in \mathbf{Z}[i]_\tau$ and at least one is a unit. Since the coefficients of the square terms are units, if there exists a solution (x, y, z) in $\mathbf{Q}(i)_\tau$ that is not $(0, 0, 0)$, then there must exist a solution where $x, y, z \in \mathbf{Z}[i]_\tau$ and at least one is a unit. Furthermore, if one variable is a unit, then exactly one of the other two variables is also a unit. If not, there would be a contradiction when the equation is reduced mod τ, as $1 + 1 \not\equiv 1 \bmod \tau$. From this, we can conclude that either both $y, z \in \mathbf{Z}[i]_\tau^\times$ or one of them is a unit while the other is not. With this knowledge, we can plug in all possible combinations for y^2 and z^2 mod τ^5. We do this in the table below. (Note: Several redundant cases are omitted from the table since we can ignore *overall* sign changes on squares as $-1 = i^2$.)

$y^2, z^2 \bmod \ \tau^5$	$(1+\tau)y^2 + (1+\tau^2)z^2 \ \bmod \ \tau^5$
$1, 1$	$\tau + 2 + \tau^2 \equiv \tau + \tau^3 + \tau^4$
$1, -1$	$\tau - \tau^2 \equiv \tau + \tau^2 + \tau^4$
$1, 0$	$1 + \tau$
$1, \tau^2$	$1 + \tau + \tau^2 + \tau^4$
$-1, \tau^2$	$-1 - \tau + \tau^2 + \tau^4 \equiv 1 + \tau$
$1, \tau^4$	$1 + \tau + \tau^4$
$0, 1$	$1 + \tau^2$
$\tau^2, 1$	$1 + \tau^3 - i\tau^4 \equiv 1 + \tau^3 + \tau^4$
$\tau^2, -1$	$-1 + \tau^3 \equiv 1 + \tau^2 + \tau^4$
$\tau^4, 1$	$1 + \tau^2 + \tau^4$

TABLE 4.4.1: Possible values of $(1+\tau)y^2 + (1+\tau^2)z^2 \ \bmod \ \tau^5$.

From the above calculations, we can see that none of the unit entries in the right-hand column are $\pm 1 \bmod \ \tau^5$ and none of the non-unit entries are divisible by an even power of τ. Therefore, we have a contradiction and $1 + \tau^2 \notin N(L_{1+\tau}^{\times})$.

Now that we have shown that $N(L_{1+\tau}^{\times})/(\mathbf{Q}(i)_{\tau}^{\times})^2$ does not have order 16, we will find 8 of its elements and then conclude it must have order 8. It is clear that τ and $1+\tau$ are norms (i.e. of the form $x^2 - (1+\tau)y^2$) using $(x, y) = (i, i)$ and $(0, i)$, respectively. Also, $1 + \tau^4$ is a norm since $(x, y) = (1, i\tau^2)$ gives $1^2 - (1+\tau)(i\tau^2)^2 = 1 + \tau^4 + \tau^5 \equiv 1 + \tau^4 \bmod \tau^5$. With this, $\tau^{\{0,1\}} \times (1+\tau)^{\{0,1\}} \times (1+\tau^4)^{\{0,1\}} = \{1, 1+\tau, 1+\tau^4, 1+\tau+\tau^4, \tau, \tau+\tau^2, \tau+\tau^5, \tau+\tau^2+\tau^5\}$ gives us eight different square class representatives of $\mathbf{Q}(i)_{\tau}^{\times}/(\mathbf{Q}(i)_{\tau}^{\times})^2$ that are elements of $N(L_{1+\tau}^{\times})/(\mathbf{Q}(i)_{\tau}^{\times})^2$.

Case 2) Let $d = 1 + \tau^3$. Similar to the previous case, we will show that $1 + \tau$ is not a norm by showing that the homogenized equation $x^2 - (1 + \tau^3)y^2 = (1 + \tau)z^2$ when $x, y, z \in \mathbf{Z}[i]_\tau$ has no solution with x,y, or z in $\mathbf{Z}[i]_\tau^\times$. Assume there is such a solution. Since the coefficients of all the square terms are units, reduce this equation mod τ^5 and plug in all combinations of y^2 and z^2 mod τ^5. We do this in the table below. We can ignore overall sign changes since $-1 = i^2$.

$y^2, z^2 \mod \tau^5$	$(1 + \tau^3)y^2 + (1 + \tau)z^2 \mod \tau^5$
$1, 1$	$2 + \tau + \tau^3 \equiv \tau + \tau^2$
$1, -1$	$-\tau + \tau^3 \equiv \tau + \tau^4$
$1, 0$	$1 + \tau^3$
$1, \tau^2$	$1 + \tau^2 + 2\tau^3 \equiv 1 + \tau^2$
$-1, \tau^2$	$-1 + \tau^2 \equiv 1 + \tau^3$
$1, \tau^4$	$1 + \tau^3 + \tau^4 + \tau^5 \equiv 1 + \tau^3 + \tau^4$
$0, 1$	$1 + \tau$
$\tau^2, 1$	$1 + \tau + \tau^2 + \tau^5 \equiv 1 + \tau + \tau^2$
$\tau^2, -1$	$-1 - \tau + \tau^2 + \tau^5 \equiv 1 + \tau + \tau^4$
$\tau^4, 1$	$1 + \tau + \tau^4 + \tau^7 \equiv 1 + \tau + \tau^4$

TABLE 4.4.2: Possible values of $(1 + \tau^3)y^2 + (1 + \tau)z^2 \mod \tau^5$.

From the above calcuations, we can see that none of the unit entries in the right-hand column of Table 4.4.2 are $\pm 1 \bmod \tau^5$ and none of the non-unit entries are divisible by an even power of τ. Thus, they cannot be squares, so $1 + \tau$ is not a norm in $L_{1+\tau^3}$. So $N(L_{1+\tau^3}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$ has order at most 8 and we will now find 8 elements. Since $1 + \tau^3 = x^2 - (1 + \tau^3)y^2$ using $(x, y) = (0, i)$, $1 + \tau^3$ is a norm. Using

$(x, y) = (1, i\tau^2)$ in $x^2 - (1+\tau^3)y^2$ gives $1 + \tau^4 + \tau^7 \equiv 1 + \tau^4 \bmod \tau^5$, so $1 + \tau^4$ is also a norm. Lastly, using $(x, y) = (1, 1)$ yields $-\tau^3 = (i\tau)^2(\tau)$, so τ is also a norm. From this, $(1+\tau^3)^{\{0,1\}} \times (1+\tau^4)^{\{0,1\}} \times (\tau)^{\{0,1\}} = \{1, 1+\tau^3, 1+\tau^4, \tau, 1+\tau^2, \tau+\tau^4, \tau+\tau^5, \tau+\tau^3\}$ gives us eight norms that are also different square class representatives.

Case 3) Let $d = \tau$. We will show that $1 + \tau^2$ is not a norm by showing that the homogenized equation $x^2 - \tau y^2 = (1 + \tau^2)z^2$ when $x, y, z \in \mathbf{Z}[i]_\tau$ has no solution with x,y, or z in $\mathbf{Z}[i]_\tau^\times$. Assume there is such a solution and reduce the equation mod τ. This gives $x^2 \equiv z^2 \bmod \tau$. If $x \equiv 0 \bmod \tau$, then $z \equiv 0 \bmod \tau$, meaning that $y \equiv 0 \bmod \tau$ and $x, y, z \notin \mathbf{Z}[i]_\tau^\times$. So we must have that x and z are units. Thus x^2 and z^2 are both congruent to $\pm 1 \bmod \tau^5$ and we can construct the table below. Once more, we can ignore overall sign changes.

$x^2, z^2 \bmod \tau^5$	$x^2 - (1+\tau^2)z^2 \bmod \tau^5$
$1, 1$	$-\tau^2 \equiv \tau^2 + \tau^4$
$1, -1$	$2 + \tau^2 \equiv \tau^3 + \tau^4$

TABLE 4.4.3: Possible values of $x^2 - (1+\tau^2)z^2 \bmod \tau^5$

Using these calculations, we see that if we divide each of the entries in the right-hand column of Table 4.4.3 by τ, none of them will be squares. Thus, $1 + \tau^2$ is not a norm from L_τ. So $N(L_\tau^\times)/(\mathbf{Q}(i)_\tau^\times)^2$ does not have order 16. We will now find its eight elements. We have that $\tau, 1+\tau$, and $1+\tau^3$ are norms, or of the form $x^2 - \tau y^2$, using $(x, y) = (0, i), (1, i)$, and $(1, i\tau)$, respectively. From this, $\tau^{\{0,1\}} \times (1+\tau)^{\{0,1\}} \times (1+\tau^3)^{\{0,1\}} = \{1, \tau, 1+\tau, 1+\tau^3, \tau+\tau^2, \tau+\tau^4, 1+\tau+\tau^3+\tau^4, \tau+\tau^2+\tau^4+\tau^5\}$ gives us eight norms that are also different square class representatives.

Case 4) Let $d = \tau + \tau^2$. We will show that $1 + \tau^3 \notin N(L_{\tau+\tau^2}^\times)$ by analyzing the

equation $x^2 - (\tau + \tau^2)y^2 = (1 + \tau^3)z^2$ in a similar manner as the previous case. If the equation is solvable, then without loss of generality there exists a solution with $x, y, z \in \mathbf{Z}[i]_\tau$ and at least one being a unit. Just like the previous case, x and z must be units. Using this knowledge and Table 4.3.2, we construct Table 4.4.4.

$x^2, z^2 \bmod \tau^5$	$x^2 - (1 + \tau^3)z^2 \bmod \tau^5$
$1, 1$	$-\tau^3 \equiv \tau^3$
$1, -1$	$2 + \tau^3 \equiv \tau^2$

TABLE 4.4.4: Possible values of $x^2 - (1 + \tau^3)z^2 \bmod \tau^5$

If we divide each entry in the right-hand column of Table 4.4.4 by $\tau + \tau^2$, the resulting numbers will not be squares. Therefore $1+\tau^3$ is not a norm from $L_{\tau+\tau^2}$. On the other hand, $\tau+\tau^2$, τ, $\tau+\tau^2+\tau^4 = x^2-(\tau+\tau^2)y^2$ using $(x, y) = (0, i), (i\tau, i)$, and (τ^2, i), respectively. So, $(\tau + \tau^2)^{\{0,1\}} \times (\tau)^{\{0,1\}} \times (\tau + \tau^2 + \tau^4)^{\{0,1\}} = \{1, \tau + \tau^2, \tau, \tau + \tau^2 + \tau^4, 1 + \tau, 1 + \tau + \tau^3, \tau + \tau^3, 1 + \tau^2\}$ gives us eight norms that are also different square class representatives.

In the table below, for each nontrivial square class representative d we list an element of $\mathbf{Q}(i)^\times_\tau$ not in $N(L^\times_d)$ and three elements t_1, t_2, and t_3 in $N(L^\times_d)$ whose images in $\mathbf{Q}(i)^\times_\tau/(\mathbf{Q}(i)^\times_\tau)^2 \cong \mathbf{F}_2^4$ are linearly independent, so they generate a subgroup of order 8.

d	Non-norm	t_1, t_2, t_3
$1+\tau$	$1+\tau^2$	$\tau,\ 1+\tau,\ 1+\tau^4$
$1+\tau^2$	$1+\tau$	$1+\tau^2,\ 1+\tau^3,\ \tau+\tau^2$
$1+\tau^3$	$1+\tau$	$1+\tau^3,\ 1+\tau^2,\ 1+\tau+\tau^3+\tau^4$
$1+\tau^4$	τ	$1+\tau^4\ , 1+\tau^2,\ 1+\tau+\tau^3$
$1+\tau+\tau^3$	$1+\tau$	$1+\tau+\tau^3,\ \tau+\tau^2,\ \tau+\tau^3$
$1+\tau+\tau^4$	$1+\tau^2$	$1+\tau+\tau^4,\ 1+\tau,\ \tau+\tau^4$
$1+\tau+\tau^3+\tau^4$	$1+\tau$	$1+\tau+\tau^3+\tau^4,\ 1+\tau+\tau^3,\ \tau+\tau^5$
τ	$1+\tau^2$	$\tau, 1+\tau,\ \ 1+\tau^3$
$\tau+\tau^2$	$1+\tau^3$	$\tau+\tau^2,\ \tau,\ \tau+\tau^2+\tau^4$
$\tau+\tau^3$	$1+\tau$	$\tau+\tau^3,\ \tau+\tau^2,\ \tau+\tau^5$
$\tau+\tau^4$	$1+\tau$	$\tau+\tau^4,\ 1+\tau+\tau^4,\ \tau$
$\tau+\tau^5$	$1+\tau^2$	$\tau+\tau^5,\ 1+\tau,\ \tau+\tau^3$
$\tau+\tau^2+\tau^4$	$1+\tau$	$\tau+\tau^2+\tau^4,\ \tau+\tau^4,\ \tau+\tau^2$
$\tau+\tau^2+\tau^5$	$1+\tau^3$	$\tau+\tau^2+\tau^5,\ \tau+\tau^5,\ \tau+\tau^2+\tau^4+\tau^5$
$\tau+\tau^2+\tau^4+\tau^5$	$1+\tau^3$	$\tau+\tau^2+\tau^4+\tau^5,\ \tau+\tau^3,\ \tau+\tau^2+\tau^5$

TABLE 4.4.5: Each $N(L_d^\times)/(\mathbf{Q}(i)_\tau^\times)^2$ has order 8.

□

Example 4.4.3. We will find a set of representatives for the eight elements of $N(L_{1+\tau^4}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$. By Table 4.4.5 we have that $1, 1+\tau^4, 1+\tau^2, 1+\tau+\tau^3 \in N(L_{1+\tau^4}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$. Now we will find the other four representatives.

We have $(1+\tau^4)(1+\tau^2) = 1+\tau^2+\tau^4+\tau^6 \equiv 1+\tau^2+\tau^4 \equiv -(1+\tau^3) \bmod \tau^5$. Thus $1+\tau^3 \in N(L_{1+\tau^4}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$.

We also have $(1+\tau^4)(1+\tau+\tau^3) = 1+\tau+\tau^3+\tau^4+\tau^5+\tau^7 \equiv 1+\tau+\tau^3+\tau^4 \bmod \tau^5$. So $1+\tau+\tau^3+\tau^4 \in N(L^\times_{1+\tau^4})/(\mathbf{Q}(i)^\times_\tau)^2$.

Since $(1+\tau^2)(1+\tau+\tau^3) = 1+\tau+\tau^2+2\tau^3+\tau^5 \equiv 1+\tau+\tau^2 \equiv -(1+\tau) \bmod \tau^5$, we have that $1+\tau \in N(L^\times_{1+\tau^4})/(\mathbf{Q}(i)^\times_\tau)^2$.

Lastly, we have $(1+\tau^4)(1+\tau^2)(1+\tau+\tau^3) = 1+\tau+\tau^2+2\tau^3+\tau^4+2\tau^5+\tau^7 \equiv 1+\tau+\tau^2+\tau^4 \equiv -(1+\tau+\tau^4) \bmod \tau^5$. Thus $1+\tau+\tau^4 \in N(L^\times_{1+\tau^4})/(\mathbf{Q}(i)^\times_\tau)^2$.

Overall we have that $N(L^\times_{1+\tau^4})/(\mathbf{Q}(i)^\times_\tau)^2$ is represented by

$$\{1, 1+\tau, 1+\tau^2, 1+\tau^3, 1+\tau^4, 1+\tau+\tau^3, 1+\tau+\tau^4, 1+\tau+\tau^3+\tau^4\}.$$

Theorem 4.4.4. *The Hilbert symbol on $\mathbf{Q}(i)_v$ is bimultiplicative. That is, for all $a, a', b, b' \in \mathbf{Q}(i)^\times_v$, $(aa', b)_v = (a,b)_v(a',b)_v$ and $(a, bb')_v = (a,b)_v(a,b')_v$.*

Proof. By Lemma 4.2.5, we have that $(a,b)_v = 1$ for $v = \infty$ for all $a, b \in \mathbf{Q}(i)^\times_\infty = \mathbf{C}^\times$. Thus the symbol is trivially multiplicative for $v = \infty$. For all other places, the proof is the same as the one for Theorem 3.3.6. □

4.5 $\mathbf{Q}(i)_\tau = \mathbf{Q}_2(i)$

We will now work towards showing that $\mathbf{Q}(i)_\tau = \mathbf{Q}_2(i)$. This fact will be useful for us in the next section.

Lemma 4.5.1. *We have that $\mathbf{Q}_2(i) \subset \mathbf{Q}(i)_\tau$. Further, let $a, b \in \mathbf{Q}_2$. Then $|a+bi|_\tau = |a^2+b^2|_2$.*

Proof. In $\mathbf{Z}[i]$, we have $2 = -i\tau^2$, so $v_\tau(2) = 2$. Thus on $\mathbf{Q}$, $|\cdot|_\tau = |\cdot|_2^2$. As a result, a sequence in $\mathbf{Q}$ is τ-adically Cauchy if and only if it is 2-adically Cauchy. Therefore

$\mathbf{Q}_2 \subset \mathbf{Q}(i)_\tau$, so $\mathbf{Q}_2(i) \subset \mathbf{Q}(i)_\tau$. Now let $a, b \in \mathbf{Q}_2$. We want to show that

$$|a + bi|_\tau = |a^2 + b^2|_2.$$

This is clear if $a = b = 0$, so assume that $a \neq 0$ or $b \neq 0$. For $r \in \mathbf{Q}$, we have that $|(ra) + (rb)i|_\tau = |r|_\tau |a + bi|_\tau = |r|_2^2 |a + bi|_\tau$ and $|(ra)^2 + (rb)^2|_2 = |r|_2^2 |a^2 + b^2|_2$. So without loss of generality, we can consider $a, b \in \mathbf{Z}_2$, and we can factor out the largest power of 2 common to a and b. Thus we can let a or b be odd (that is, in $1 + 2\mathbf{Z}_2$). If exactly one is odd, then $a + bi \equiv 1 \bmod \tau$, so $|a + bi|_\tau = 1$. We also have that $a^2 + b^2$ is odd, so $|a^2 + b^2|_2 = 1$. On the other hand, let both a and b be odd. We have that $a + bi = 1 + i + (a - 1) + (b - 1)i$. Since $(a - 1) + (b - 1)i$ is divisible by $2 = -i\tau^2$, we have that τ divides $1 + i + (a - 1) + (b - 1)i$ exactly once. Thus $|a+bi|_\tau = \frac{1}{2}$. Lastly, since a^2 and b^2 are unit squares in $\mathbf{Z}_2$, by Theorem 3.2.4 we have that $a^2 \equiv b^2 \equiv 1 \bmod 8\mathbf{Z}_2$. So $a^2 + b^2 \equiv 2 \bmod 8\mathbf{Z}_2$, implying 2 divides $a^2 + b^2$ exactly once. Thus $|a^2 + b^2|_2 = \frac{1}{2}$. So in both cases we have that $|a + bi|_\tau = |a^2 + b^2|_2$. □

Lemma 4.5.2. *Let $a, b \in \mathbf{Q}_2$ and $n \geq 1$. If $a^2 + b^2 \equiv 0 \bmod 2^{2n}$, then $a, b \equiv 0 \bmod 2^n$.*

Proof. We will prove this by induction. For the base case, suppose $n = 1$ and assume that $a^2 + b^2 \equiv 0 \bmod 4$. Working modulo 4, the only solutions to this are $(a, b) = (0, 0), (2, 0), (0, 2)$, or $(2, 2)$. In each case we have that $a, b \equiv 0 \bmod 2$, so our base case is done. For the induction case, assume that if $a^2 + b^2 \equiv 0 \bmod 2^{2n}$, then $a, b \equiv 0 \bmod 2^n$. We must show that if $a^2 + b^2 \equiv 0 \bmod 2^{2(n+1)}$, then $a, b \equiv 0 \bmod 2^{n+1}$.

Assume $a^2 + b^2 \equiv 0 \bmod 2^{2(n+1)} = 2^{2n+2}$. Then we have that $a^2 + b^2 \equiv 0 \bmod 2^{2n}$. By our induction hypothesis, this means that $a, b \equiv 0 \bmod 2^n$. Then we can write $a = 2^n a'$ and $b = 2^n b'$ for some $a', b' \in \mathbf{Z}_2$. Then $a^2 + b^2 = 2^{2n}((a')^2 + (b')^2)$, and we

have that $2^{2n}((a')^2+(b')^2) \equiv 0 \bmod 2^{2n+2}$. This implies $(a')^2+(b')^2 \equiv 0 \bmod 4$. Then by our base case, we have that $a', b' \equiv 0 \bmod 2$. Thus $a, b \equiv 0 \bmod 2^{n+1}$. □

Lemma 4.5.3. *The sequence $\{a_n+b_ni\}_{n=1}^{\infty}$ in $\mathbf{Q}_2(i)$ is τ-adically Cauchy if and only if the sequences $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ in $\mathbf{Q}_2$ are 2-adically Cauchy.*

Proof. For the forwards direction, assume $\{a_n+b_ni\}_{n=1}^{\infty}$ in $\mathbf{Q}_2(i)$ is τ-adically Cauchy. Then given $\varepsilon > 0$ we can find $k \in \mathbf{N}$ such that $\frac{1}{2^k} < \varepsilon$. Since the sequence is Cauchy, there exists $N \in \mathbf{N}$ such that for $n, m \geq N$ we have

$$|(a_n+b_ni)-(a_m+b_mi)|_\tau = |(a_n-a_m)+(b_n-b_m)i|_\tau = |(a_n-a_m)^2+(b_n-b_m)^2|_2 < \frac{1}{2^{2k}}.$$

From this we have that $(a_n-a_m)^2+(b_n-b_m)^2 \equiv 0 \bmod 2^{2k}$, and by Lemma 4.5.2 we have that $a_n - a_m \equiv 0 \bmod 2^k$ and $b_n - b_m \equiv 0 \bmod 2^k$. This implies that $|a_n-a_m|_2 < \frac{1}{2^k} < \varepsilon$ and $|b_n-b_m|_2 < \frac{1}{2^k} < \varepsilon$, so we have that $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ in $\mathbf{Q}_2$ are 2-adically Cauchy.

For the other direction, assume that $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ are 2-adically Cauchy sequences in $\mathbf{Q}_2$. Then given $\varepsilon > 0$ there exists $N \in \mathbf{N}$ such that for $n, m \geq N$ we have $|a_n-a_m|_2 < \sqrt{\varepsilon}$ and $|b_n-b_m|_2 < \sqrt{\varepsilon}$. Then we have

$$\begin{aligned}|(a_n-a_m)+(b_n-b_m)i|_\tau &= |(a_n-a_m)^2+(b_n-b_m)^2|_2 \\ &\leq max(|(a_n-a_m)^2|_2, |(b_n-b_m)^2|_2) < max(\sqrt{\varepsilon}^2, \sqrt{\varepsilon}^2) = \varepsilon,\end{aligned}$$

where the first inequality results from the strong triangle inequality. Thus $\{a_n + b_ni\}_{n=1}^{\infty}$ in $\mathbf{Q}_2(i)$ is τ-adically Cauchy. □

Lemma 4.5.4. *Let $a, b \in \mathbf{Q}_2$ and define the absolute value $|\cdot|$ on $\mathbf{Q}_2(i)$ by $|a+bi| = |a^2+b^2|_2$. Then $\mathbf{Q}_2(i)$ is complete with respect to the absolute value $|\cdot|$.*

Proof. To start, we will show that $|\cdot| : \mathbf{Q}_2(i) \to \mathbf{R}_{\geq 0}$ defined by $|a+bi| = |a^2+b^2|_2$ for $a, b \in \mathbf{Q}_2$ is an absolute value. First we will show that $|a+bi| = 0$ if and only if $a+bi = 0$. For the forward direction, assume that $|a+bi| = |a^2+b^2|_2 = 0$. Since $|\cdot|_2$ is an absolute value, we have that $a^2+b^2 = 0$. Now we must show that this implies $a = b = 0$. Suppose by way of contradiction that $a^2+b^2 = 0$ and $a \neq 0$. Then $b^2 = -a^2$, which implies that $-1 = (\frac{b}{a})^2 = \square$ in $\mathbf{Q}_2$, a contradiction. Thus $a = 0$. This implies that $b = 0$, so $a+bi = 0$. For the other direction, assume that $a+bi = 0$. Then $a = b = 0$, so $a^2+b^2 = 0$ and $|a+bi| = |a^2+b^2|_2 = |0|_2 = 0$.

Next we will show that for $\alpha, \beta \in \mathbf{Q}_2(i)$ we have $|\alpha\beta| = |\alpha||\beta|$. Since the norm function $N : \mathbf{Q}_2(i) \to \mathbf{Q}_2$ defined by $N(a+bi) = a^2+b^2$ is multiplicative, we have that

$$\begin{aligned} |\alpha\beta| = |N(\alpha\beta)|_2 &= |N(\alpha)N(\beta)|_2 \\ &= |N(\alpha)|_2|N(\beta)|_2 \\ &= |\alpha||\beta|. \end{aligned}$$

Here we used that $|\cdot|_2$ is multiplicative, as it is an absolute value.

Lastly, we will show that for $\alpha, \beta \in \mathbf{Q}_2(i)$, we have $|\alpha+\beta| \leq max(|\alpha|, |\beta|)$. If $\alpha = 0$ or $\beta = 0$ this inequality is clear, so assume $\alpha \neq 0$ and $\beta \neq 0$. Without loss of generality assume $|\alpha| \leq |\beta|$. We want to show that $|\alpha+\beta| \leq max(|\alpha|, |\beta|)$, which is true if and only if $|\frac{\alpha}{\beta}+1| \leq max(|\frac{\alpha}{\beta}|, 1) = 1$. So it suffices to show that for $\gamma \in \mathbf{Q}_2(i)$, if $|\gamma| \leq 1$, then $|\gamma+1| \leq 1$. Write $\gamma = x+yi$ for some $x, y \in \mathbf{Q}_2$. We will first show that if $|x+yi| \leq 1$, then $|x|_2 \leq 1$ and $|y|_2 \leq 1$. Assume that $|x+yi| = |x^2+y^2|_2 \leq 1$. Then suppose by way of contradiction that $|x|_2 > 1$ or $|y|_2 > 1$. Then we have two cases: $|x|_2 \neq |y|_2$ and $|x|_2 = |y|_2$. For the first case, assume without loss of generality

that $|x|_2 > |y|_2$. If $|x|_2 \neq |y|_2$, then $|x^2|_2 \neq |y^2|_2$, so $|x^2 + y^2| = max(|x^2|_2, |y^2|_2)$. Since $|x^2 + y^2|_2 \leq 1$ by assumption, we have that $|x|_2^2 \leq 1$, a contradiction. For the second case, assume $|x|_2 = |y|_2 > 1$. Then we can write $x = \frac{u}{2^n}$ and $y = \frac{v}{2^n}$ where u and v are in $\mathbf{Z}_2^\times$ and $n \in \mathbf{Z}^+$. Then $x^2 + y^2 = \frac{1}{2^{2n}}(u^2 + v^2)$. But $u^2 \equiv v^2 \equiv 1 \bmod 8\mathbf{Z}_2$ by Theorem 3.2.4, so $u^2 + v^2 \equiv 2 \bmod 8\mathbf{Z}_2$. Thus $v_2(u^2 + v^2) = 1$, implying that $|x + yi|_\tau = |x^2 + y^2|_2 = \frac{1}{2}|x|_2^2 \geq \frac{1}{2} \cdot 4 = 2 > 1$, a contradiction. So both cases lead to a contradiction, implying that $|x|_2 \leq 1$ and $|y|_2 \leq 1$. Now we will show that if $|\gamma| \leq 1$, then $|\gamma + 1| \leq 1$. Suppose that $|\gamma| = |x + yi| = |x^2 + y^2|_2 \leq 1$. Then by what we have just shown, $|x|_2 \leq 1$ and $|y|_2 \leq 1$, implying that $x, y \in \mathbf{Z}_2$. From this, $x^2+y^2+2x+1 \in \mathbf{Z}_2$ as well. Then, $|\gamma + 1| = |x + 1 + yi| = |(x + 1)^2 + y^2|_2 = |x^2 + y^2 + 2x + 1|_2 \leq 1$. Thus we have shown that for $\alpha, \beta \in \mathbf{Q}_2(i)$ we have $|\alpha + \beta| \leq max(|\alpha|, |\beta|)$. So $|\cdot|$ is an absolute value.

Now we will show that $\mathbf{Q}_2(i)$ is complete with respect to $|\cdot|$. Let $\{a_n + b_n i\}_{n=1}^\infty$ be a Cauchy sequence in $\mathbf{Q}_2(i)$. Then by Lemma 4.5.3, $\{a_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ are Cauchy sequences in $\mathbf{Q}_2$. Since $\mathbf{Q}_2$ is complete, there exist $a, b \in \mathbf{Q}_2$ such that $a_n \to a$ and $b_n \to b$. We will show that the Cauchy sequence $\{a_n + b_n i\}_{n=1}^\infty$ in $\mathbf{Q}_2(i)$ converges to $a + bi \in \mathbf{Q}_2(i)$. Given $\varepsilon > 0$ there exists $N \in \mathbf{N}$ such that for $n \geq N$ we have $|a_n - a|_2 < \sqrt{\varepsilon}$ and $|b_n - b|_2 < \sqrt{\varepsilon}$. Then we have

$$\begin{aligned} |(a_n + b_n i) - (a + bi)| &= |(a_n - a) + (b_n - b)i| \\ &= |(a_n - a)^2 + (b_n - b)^2|_2 \leq max(|(a_n - a)^2|_2, |(b_n - b)^2|_2) \\ &< max(\sqrt{\varepsilon}^2, \sqrt{\varepsilon}^2) = \varepsilon, \end{aligned}$$

where the first inequality follows from the strong triangle inequality. Thus the Cauchy sequence $\{a_n + b_n i\}_{n=1}^\infty$ in $\mathbf{Q}_2(i)$ converges to $a + bi \in \mathbf{Q}_2(i)$, and we have that $\mathbf{Q}_2(i)$

is complete with respect to the absolute value $|\cdot|$. □

Theorem 4.5.5. *We have that* $\mathbf{Q}(i)_\tau = \mathbf{Q}_2(i)$. *In particular,* $\mathbf{Z}[i]_\tau = \mathbf{Z}_2[i]$.

Proof. By Lemma 4.5.1, we have that $\mathbf{Q}_2(i) \subset \mathbf{Q}(i)_\tau$. Also, $\mathbf{Q}(i) \subset \mathbf{Q}_2(i)$ and $\mathbf{Q}(i)$ is dense in $\mathbf{Q}(i)_\tau$, so we can conclude that $\mathbf{Q}_2(i)$ is dense in $\mathbf{Q}(i)_\tau$. Lastly, by Lemma 4.5.4 we have that $\mathbf{Q}_2(i)$ is complete. Altogther this implies that $\mathbf{Q}_2(i) = \mathbf{Q}(i)_\tau$.

To show that $\mathbf{Z}[i]_\tau = \mathbf{Z}_2[i]$, we will show that for $a, b \in \mathbf{Q}_2$ we have $|a+bi|_\tau \leq 1$ if and only if $|a|_2 \leq 1$ and $|b|_2 \leq 1$. We proved the forward direction in the proof of Lemma 4.5.4. For the other direction, assume that $|a|_2 \leq 1$ and $|b|_2 \leq 1$. Then $|a+bi|_\tau = |a^2+b^2|_2 \leq max(|a^2|_2, |b^2|_2) \leq 1$. With this, we have that $|a+bi|_\tau \leq 1$ if and only if $|a|_2 \leq 1$ and $|b|_2 \leq 1$, implying that $\mathbf{Z}[i]_\tau = \mathbf{Z}_2[i]$. □

4.6 Hilbert Reciprocity on $\mathbf{Q}(i)$

Now that we have shown that the Hilbert symbol on $\mathbf{Q}(i)_v$ is bimultiplicative, we can show that Hilbert reciprocity on $\mathbf{Q}(i)_v$ is equivalent to quadratic reciprocity on $\mathbf{Z}[i]$. First we will state the law of quadratic reciprocity for $\mathbf{Z}[i]$.

Theorem 4.6.1. (*Quadratic reciprocity on* $\mathbf{Z}[i]$.) *Let* $\pi, \pi' \in \mathbf{Z}[i]$ *be distinct odd Gaussian integer primes with* $\pi \equiv \pi' \equiv 1 \bmod \tau^3$ *and let* $\pi = x + yi$ *where* $x, y \in \mathbf{Z}$. *Then we have the following:*

(*i*) $\left(\frac{\pi}{\pi'}\right) = \left(\frac{\pi'}{\pi}\right)$.

(*ii*) $\left(\frac{i}{\pi}\right) = (-1)^{\frac{N(\pi)-1}{4}}$.

(*iii*) $\left(\frac{1+i}{\pi}\right) = (-1)^{\frac{(x+y)^2-1}{8}}$.

Remark 4.6.2. Every odd Gaussian integer prime has a unit multiple that is congruent to 1 mod τ^3. We will see proof of this in the proof of Theorem 4.6.3.

Our task in the next three theorems is to compute $(\alpha, \beta)_\tau$ for $\alpha, \beta \in \mathbf{Q}(i)_\tau^\times$. In the proof of Theorem 4.6.3 we will show that $\mathbf{Q}(i)_\tau^\times = \tau^{\mathbf{Z}} \times \mathbf{Z}[i]_\tau^\times = \tau^{\mathbf{Z}} \times \langle i \rangle \times (1+\tau^3\mathbf{Z}[i]_\tau)$. We also know that $(\alpha, \alpha)_\tau = 1$. Now let $u, w \in \mathbf{Q}(i)_\tau^\times$ such that $u \equiv w \equiv 1 \bmod \tau^3$. Using the bimultiplicativity of the symbol, computing $(\alpha, \beta)_\tau$ reduces to computing the following symbols:

$$(i)\ (i, \tau)_\tau$$

$$(ii)\ (u, \tau)_\tau$$

$$(iii)\ (i, u)_\tau$$

$$(iv)\ (u, w)_\tau$$

Since $ix^2 + \tau y^2 = z^2$ has the solution $(x, y, z) = (i, 1, 1)$, we have that $(i, \tau)_\tau = 1$. The following theorems will address the other three cases.

Theorem 4.6.3. *Let $u \in \mathbf{Z}[i]_\tau^\times = \mathbf{Z}_2[i]^\times$ and let $u = x + yi$ with $x, y \in \mathbf{Z}_2$. Then we have the following:*

(*i*) *If $x \in \mathbf{Z}_2^\times$, then*

$$(u, \tau)_\tau = \begin{cases} 1, & \text{if } x + y \equiv \pm 1 \bmod 8, \\ -1, & \text{if } x + y \equiv \pm 3 \bmod 8. \end{cases}$$

(*ii*) *If* $x \in 2\mathbf{Z}_2$, *then*

$$(u,\tau)_\tau = \begin{cases} 1, & \text{if } x - y \equiv \pm 1 \bmod 8, \\ -1, & \text{if } x - y \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. First we will consider the units of $\mathbf{Z}_2[i] \bmod \tau^3$, which are represented by numbers of the form $1 + a\tau + b\tau^2$ where $a, b \in \{0, 1\}$.

a, b	$1 + a\tau + b\tau^2 \bmod \tau^3$
$0, 0$	1
$1, 0$	$1 + \tau \equiv -i$
$0, 1$	$1 + \tau^2 \equiv -1$
$1, 1$	$1 + \tau + \tau^2 \equiv i$

TABLE 4.6.1: The four units of $\mathbf{Z}_2[i] \bmod \tau^3$.

Looking at Table 4.6.1, we can see that $\mathbf{Z}_2[i]^\times = \{1, -1, i, -i\} \times (1 + \tau^3\mathbf{Z}_2[i])$. Using this direct product decomposition, for any $u \in \mathbf{Z}_2[i]^\times$, we have $u = i^k\varepsilon$ for some $k \in \mathbf{Z}$ and some $\varepsilon \in 1 + \tau^3\mathbf{Z}_2[i]$. So to compute $(u,\tau)_\tau$, we can compute $(i^k\varepsilon,\tau)_\tau = (i,\tau)_\tau^k(\varepsilon,\tau)_\tau$, with the equality coming from the bimultiplicativity of the Hilbert symbol. The equation $ix^2 + \tau y^2 = z^2$ has the solution $(i, 1, 1)$, so $(i,\tau)_\tau = 1$. Therefore, computing $(u,\tau)_\tau$ reduces to computing $(\varepsilon,\tau)_\tau$ for the appropriate ε. Furthermore, it suffices to consider ε modulo mod τ^5, so consider $\varepsilon \in (1+\tau^3\mathbf{Z}_2[i])/(1+\tau^5\mathbf{Z}_2[i])$. This has four representatives, which can be written as numbers of the form $1 + a\tau^3 + b\tau^4$ where $a, b \in \{0, 1\}$. We show these representatives in the table below.

a, b	$1 + a\tau^3 + b\tau^4$
$0, 0$	1
$1, 0$	$1 + \tau^3 = -1 + 2i$
$0, 1$	$1 + \tau^4 = -3$
$1, 1$	$1 + \tau^3 + \tau^4 = -5 + 2i$

TABLE 4.6.2: The four representatives of $(1 + \tau^3\mathbf{Z}_2[i])/(1 + \tau^5\mathbf{Z}_2[i])$.

So computing $(\varepsilon, \tau)_\tau$ has been reduced to computing the symbol for $\varepsilon \in \{1, -1 + 2i, -3, -5 + 2i\}$. Thus we have four cases.

Case 1) Let $\varepsilon = 1$. Since 1 is a square we have that $(\varepsilon, \tau)_\tau = 1$.

Case 2) Let $\varepsilon = -1 + 2i$. Since $-1 + 2i = 1 + \tau^3$ and $1 + \tau^3 \in N(L_\tau^\times)$ by Table 4.4.5, we have that $(\varepsilon, \tau)_\tau = 1$.

Case 3) Let $\varepsilon = -3$. Since $-3 = 1 + \tau^4$ and $1 + \tau^4 \notin N(L_\tau^\times)$ by our work in Case 3 of the proof of Theorem 4.4.2, we have that $(\varepsilon, \tau)_\tau = -1$.

Case 4) Let $\varepsilon = -5 + 2i$. Since $-5 + 2i = 1 + \tau^3 + \tau^4 \equiv -(1 + \tau^2) \bmod \tau^5$, and $1 + \tau^2 \notin N(L_\tau^\times)$ by our work in Case 3 of the proof of Theorem 4.4.2, we have that $(\varepsilon, \tau)_\tau = -1$.

In summary we can construct the following table.

a, b	$1 + a\tau^3 + b\tau^4$	$(1 + a\tau^3 + b\tau^4, \tau)_\tau$
$0, 0$	1	1
$1, 0$	$1 + \tau^3 = -1 + 2i$	1
$0, 1$	$1 + \tau^4 = -3$	-1
$1, 1$	$1 + \tau^3 + \tau^4 = -5 + 2i$	-1

TABLE 4.6.3: The values of $(\varepsilon, \tau)_\tau$.

From Table 4.6.3, we can clearly see that the value of $(1 + a\tau^3 + b\tau^4, \tau)_\tau$ depends on the value of b. In particular, $(1 + a\tau^3 + b\tau^4, \tau)_\tau = (-1)^b$. So for any $u \in \mathbf{Z}_2[i]^\times$ we can find the corresponding ε and value of b in order to compute $(u, \tau)_\tau$. However, this process is a bit laborious, so it would be much nicer to have a direct formula for $(u, \tau)_\tau$.

Along these lines, we can note that

$$u = 1 + a\tau^3 + b\tau^4 = 1 - 2a - 4b + 2ai \tag{4.6.1}$$

and consider the sum of the "real" and "imaginary" parts, which is $1 - 4b \equiv 1 \bmod 4$. Now set $u = x + yi$ for some $x, y \in \mathbf{Z}_2$. Since u is a unit in $\mathbf{Z}_2[i]$, it must be that $x \not\equiv y \bmod 2\mathbf{Z}_2$. So $x + y \equiv 1 \bmod 2\mathbf{Z}_2$, meaning $x + y$ is either 1 or 3 $\bmod 4\mathbf{Z}_2$. And since we can either have $x \equiv 0 \bmod 2\mathbf{Z}_2$ and $y \equiv 1 \bmod 2\mathbf{Z}_2$ or vice versa, we have two cases.

Case 1) Let $x \equiv 1 \bmod 2\mathbf{Z}_2$ and $y \equiv 0 \bmod 2\mathbf{Z}_2$. Then $y = 2A$ for some $A \in \mathbf{Z}_2$. First suppose that $x + y \equiv 1 \bmod 4\mathbf{Z}_2$. Then we have that $x \equiv 1 - 2A \bmod 4\mathbf{Z}_2$, which means that $x = 1 - 2A + 4B$ for some $B \in \mathbf{Z}_2$. With this, $x + yi = 1 - 2A + 4B + 2Ai = 1 + A\tau^3 + B\tau^4$. Also, the class of $x + yi \bmod \tau^5$ only depends on the values of A and

$B \bmod 2\mathbf{Z}_2$, so we can conclude that $(u,\tau)_\tau = (-1)^B$. So we need only to determine the parity of B. Since $x+y = 1+4B$, the parity of B depends on the value of $x+y \bmod 8\mathbf{Z}_2$. If $x+y \equiv 1 \bmod 8\mathbf{Z}_2$, then $B \equiv 0 \bmod 2\mathbf{Z}_2$ and $(u,\tau)_\tau = 1$. On the other hand, if $x+y \equiv 5 \bmod 8\mathbf{Z}_2$, then $B \equiv 1 \bmod 2\mathbf{Z}_2$ and $(u,\tau)_\tau = -1$. Next suppose that $x+y \equiv 3 \bmod 4\mathbf{Z}_2$. Then $x+y \equiv 3 \bmod 8\mathbf{Z}_2$ or $x+y \equiv 7 \bmod 8\mathbf{Z}_2$. Also, $-x-y \equiv 5 \bmod 8\mathbf{Z}_2$ or $-x-y \equiv 1 \bmod 8\mathbf{Z}_2$. Now since $(u,\tau)_\tau = (x+yi,\tau)_\tau = (-x-yi,\tau)_\tau = (-u,\tau)_\tau$, as -1 is a square, we can use the work that we did when $x+y \equiv 1 \bmod 4\mathbf{Z}_2$. By doing this we can conclude that if $x+y \equiv 3 \bmod 8\mathbf{Z}_2$, then $-x-y \equiv 5 \bmod 8\mathbf{Z}_2$, which implies that $(u,\tau)_\tau = (-u,\tau)_\tau = -1$. Additionally, we have that if $x+y \equiv 7 \bmod 8\mathbf{Z}_2$, then $-x-y \equiv 1 \bmod 8\mathbf{Z}_2$, which implies that $(u,\tau)_\tau = (-u,\tau)_\tau = 1$. In summary we now have that if $x \equiv 1 \bmod 2\mathbf{Z}_2$ then

$$(u,\tau)_\tau = \begin{cases} 1, & \text{if } x+y \equiv \pm 1 \bmod 8\mathbf{Z}_2, \\ -1, & \text{if } x+y \equiv \pm 3 \bmod 8\mathbf{Z}_2. \end{cases}$$

Case 2) Let $x \equiv 0 \bmod 2\mathbf{Z}_2$ and $y \equiv 1 \bmod 2\mathbf{Z}_2$. Then $iu = -y + xi$ is covered by Case 1 if the roles of x and y are replaced with $-y$ and x, respectively. Since $(i,\tau)_\tau = 1$, we have that if $x \equiv 0 \bmod 2\mathbf{Z}_2$ then

$$(u,\tau)_\tau = (iu,\tau)_\tau = \begin{cases} 1, & \text{if } x-y \equiv \pm 1 \bmod 8\mathbf{Z}_2, \\ -1, & \text{if } x-y \equiv \pm 3 \bmod 8\mathbf{Z}_2. \end{cases}$$

□

Theorem 4.6.4. *Let $u \in \mathbf{Z}[i]_\tau^\times$ such that $u = x + yi$ for $x, y \in \mathbf{Z}_2$. Then*

$$(i,u)_\tau = \begin{cases} 1, & \text{if } x^2 + y^2 \equiv 1 \bmod 8, \\ -1, & \text{if } x^2 + y^2 \equiv 5 \bmod 8. \end{cases}$$

.

Proof. One could prove this in a way similar to the proof for Theorem 4.6.3. However, instead of examining the sum of the real and imaginary parts of u, one would have to examine the sum of the squares of the real and imaginary parts of u. □

Theorem 4.6.5. *Let $u, w \in \mathbf{Z}[i]_\tau^\times$ such that $u \equiv w \equiv 1 \bmod \tau^3$. Then $(u,w)_\tau = 1$.*

Proof. Let $u, w \in \mathbf{Q}(i)_\tau^\times$ such that $u \equiv w \equiv 1 \bmod \tau^3$ and consider $(u,w)_\tau$. As we have seen before, the value of this symbol will only depend on u and w mod τ^5. Thus we will consider u and w in $(1+\tau^3\mathbf{Z}[i]_\tau)/(1+\tau^5\mathbf{Z}[i]_\tau)$. So u has the form $1+a\tau^3+b\tau^4$ and w has the form $1 + a'\tau^3 + b'\tau^4$ where $a, a', b, b' \in \{0, 1\}$. With this, we will now construct a table with the possible values of u and w and their corresponding symbols.

a, b	a', b'	$(u,w)_\tau$
$1, 0$	$1, 0$	$(1+\tau^3, 1+\tau^3)_\tau$
$1, 0$	$0, 1$	$(1+\tau^3, 1+\tau^4)_\tau$
$1, 0$	$1, 1$	$(1+\tau^3, 1+\tau^3+\tau^4)_\tau$
$0, 1$	$0, 1$	$(1+\tau^4, 1+\tau^4)_\tau$
$0, 1$	$1, 1$	$(1+\tau^4, 1+\tau^3+\tau^4)_\tau$
$1, 1$	$1, 1$	$(1+\tau^3+\tau^4, 1+\tau^3+\tau^4)_\tau$

Since we know that $(\alpha, \alpha)_\tau = 1$ for all $\alpha \in \mathbf{Q}(i)_\tau^\times$, we have only three nontrivial symbols to check: $(1+\tau^3, 1+\tau^4)_\tau$, $(1+\tau^3, 1+\tau^3+\tau^4)_\tau$, and $(1+\tau^4, 1+\tau^3+\tau^4)_\tau$.

We will first compute $(1+\tau^3, 1+\tau^4)_\tau$. By Example 4.4.3, we can see that $1+\tau^3 \in N(L_{1+\tau^4}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$. Thus $(1+\tau^3, 1+\tau^4)_\tau = 1$.

Next consider $(1+\tau^3, 1+\tau^3+\tau^4)_\tau$. By Table 4.3.3 we have that $1+\tau^3+\tau^4 \equiv -(1+\tau^2) \bmod \tau^5$. With this, $(1+\tau^3, 1+\tau^3+\tau^4)_\tau = (1+\tau^3, 1+\tau^2)_\tau$. In addition, Table 4.4.5 shows that $1+\tau^2 \in N(L_{1+\tau^3}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$. So $(1+\tau^3, 1+\tau^3+\tau^4)_\tau = (1+\tau^3, 1+\tau^2)_\tau = 1$.

Lastly, we will compute $(1+\tau^4, 1+\tau^3+\tau^4)_\tau$. Since $1+\tau^3+\tau^4 \equiv -(1+\tau^2) \bmod \tau^5$ by Table 4.3.3 and Table 4.4.5 tells us that $1+\tau^2 \in N(L_{1+\tau^4}^\times)/(\mathbf{Q}(i)_\tau^\times)^2$, we have $(1+\tau^4, 1+\tau^3+\tau^4)_\tau = (1+\tau^4, 1+\tau^2)_\tau = 1$.

By checking all of the above symbols, we have shown that $(u, w)_\tau = 1$. □

Remark 4.6.6. Note that this statement is much simpler than its analogue, Lemma 3.4.3, just as the main law of quadratic reciprocity over $\mathbf{Z}[i]$ is much simpler than the main law of quadratic reciprocity over $\mathbf{Z}$.

Theorem 4.6.7. *If π is an odd Gaussian integer prime and $a \in \mathbf{Z}[i]_\pi^\times$, then $(a, \pi)_\pi = (\frac{a}{\pi})$.*

Proof. The argument is just like Lemma 3.4.1. First we will show that $(\frac{a}{\pi}) = 1$ implies $(a, \pi)_\pi = 1$. Suppose $(\frac{a}{\pi}) = 1$. Then $a \equiv \square \bmod \pi$, and by Corollary 4.1.17, $a = \square$ in $\mathbf{Z}[i]_\pi^\times$. Then $(a, \pi)_\pi = 1$ by Theorem 4.2.4(i). To show $(a, \pi)_\pi = 1$ implies $(\frac{a}{\pi}) = 1$, suppose $(a, \pi)_\pi = 1$. Then there exists $x, y, z \in \mathbf{Z}[i]_\pi$ with at least one in $\mathbf{Z}[i]_\pi^\times$ such that $ax^2 + \pi y^2 = z^2$. If $\pi | x$ then $\pi | (ax^2 + \pi y^2) = z^2$. With this, $\pi^2 | (z^2 - ax^2) = \pi y^2$ which implies that $\pi | y$, a contradiction since one of x, y, or z is a unit. So $x \not\equiv 0 \bmod \pi$. Now reducing $ax^2 + \pi y^2 = z^2 \bmod \pi$ gives $ax^2 \equiv z^2 \bmod \pi$. This implies that $a \equiv \square \bmod \pi$, so $(\frac{a}{\pi}) = 1$. □

Finally, we have the Gaussian analogue of Theorem 3.5.2.

Theorem 4.6.8. *The following are equivalent:*

(i) The quadratic reciprocity law on $\mathbf{Z}[i]$.

(ii) Hilbert reciprocity on $\mathbf{Q}(i)_v$*: for all* $a, b \in \mathbf{Q}(i)_v^\times$ *we have* $(a,b)_v = 1$ *for all but finitely many* v *and*

$$\prod_v (a,b)_v = 1.$$

Proof. Since a and b can be decomposed into a product of primes and powers of i, the Hilbert symbol can be split apart using its bimultiplicativity until the only numbers in the symbols are either primes or i. As a result, we only need to check $\prod_v (a,b)_v = 1$ when a and b are primes or i. We can always ignore $v = \infty$ unlike in the rational case, since the Hilbert symbol on $\mathbf{Q}(i)_\infty = \mathbf{C}$ is trivial. Let π, π' be distinct odd Gaussian integer primes such that $\pi \equiv \pi' \equiv 1 \bmod \tau^3$.

Case 1: $\prod_v (i,i)_v = 1$

Since the equation $ix^2 + iy^2 = z^2$ has the solution $(x,y,z) = (1,i,0)$, we have that $(i,i)_v = 1$ for all v. This is an analogue of Case 1 in the proof of Theorem 3.5.2.

Case 2: $\prod_v (i,\tau)_v = 1$

Since the equation $ix^2 + \tau y^2 = z^2$ has the solution $(x,y,z) = (i,1,1)$, we have that $(i,\tau)_v = 1$ for all v. This is an analogue of Case 2 in the proof of Theorem 3.5.2.

Case 3: $\prod_v (i,\pi)_v = 1$

By Corollary 4.1.19 and Lemma 4.2.5, we only have to compute $(i,\pi)_v$ for $v = \tau$ and $v = \pi$. By Theorem 4.6.4 we have $(i,\pi)_\tau = (-1)^{\frac{N(\pi)-1}{4}}$. Also, by Theorem 4.6.7 we have $(i,\pi)_\pi = (\frac{i}{\pi})$. Thus $\prod_v (i,\pi)_v = 1$ if and only if $(\frac{i}{\pi}) = (-1)^{\frac{N(\pi)-1}{4}}$, the first

supplementary law for quadratic reciprocity on $\mathbf{Z}[i]$. This is an analogue of Case 3 in the proof of Theorem 3.5.2.

Case 4: $\prod_v (\tau, \tau)_v = 1$

Since the equation $\tau x^2 + \tau y^2 = z^2$ has the solution $(x, y, z) = (1, i, 0)$, we have that $(\tau, \tau)_v = 1$ for all v. This is an analogue of Case 4 in the proof of Theorem 3.5.2.

Case 5: $\prod_v (\tau, \pi)_v = 1$

By Corollary 4.1.19 and Lemma 4.2.5, we only have to compute $(\tau, \pi)_v$ for $v = \tau$ and $v = \pi$. Since $\pi \equiv 1 \bmod \tau^3$, by Equation 4.6.1 we have that $\pi = x + yi$ with x odd and y even. Then by Theorem 4.6.3 we have

$$(\tau, \pi)_\tau = \begin{cases} 1, & \text{if } x + y \equiv \pm 1 \bmod 8, \\ -1, & \text{if } x + y \equiv \pm 3 \bmod 8. \end{cases}$$

Also, by Theorem 4.6.7 we have $(\tau, \pi)_\pi = (\frac{\tau}{\pi})$. Thus $\prod_v (\tau, \pi)_v = 1$ if and only if

$$\left(\frac{\tau}{\pi}\right) = \begin{cases} 1, & \text{if } x + y \equiv \pm 1 \bmod 8, \\ -1, & \text{if } x + y \equiv \pm 3 \bmod 8. \end{cases}$$

This is equivalent to $(\frac{\tau}{\pi}) = (-1)^{\frac{(x+y)^2-1}{8}}$, the second supplementary law for quadratic reciprocity on $\mathbf{Z}[i]$. This is an analogue of Case 5 in the proof of Theorem 3.5.2.

Case 6: $\prod_v (\pi, \pi)_v = 1$

Since $\pi x^2 + \pi y^2 = z^2$ has the solution $(x, y, z) = (1, i, 0)$, we have that $(\pi, \pi)_v = 1$ for all v. This is an analogue of Case 6 of Theorem 3.5.2, but much simpler.

Case 7: $\prod_v (\pi, \pi')_v = 1$

By Corollary 4.1.19 and Lemma 4.2.5, we only have to compute $(\pi, \pi')_v$ for $v = \tau$,

$v = \pi$, and $v = \pi'$. By Theorem 4.6.5 we have $(\pi, \pi')_\tau = 1$. Also by Theorem 4.6.7 we have $(\pi, \pi')_\pi = (\frac{\pi'}{\pi})$ and $(\pi', \pi)_{\pi'} = (\frac{\pi}{\pi'})$. Thus $\prod_v (\pi, \pi')_v = 1$ if and only if $(\frac{\pi}{\pi'})(\frac{\pi'}{\pi}) = 1$, which is equivalent to $(\frac{\pi}{\pi'}) = (\frac{\pi'}{\pi})$, the main law of quadratic reciprocity. This is an analogue of Case 7 of Theorem 3.5.2.

So by checking these seven cases we see that if Hilbert reciprocity on $\mathbf{Q}(i)$ holds, then quadratic reciprocity on $\mathbf{Z}[i]$ holds.

For the other direction, assume that quadratic reciprocity on $\mathbf{Z}[i]$ holds. Then we have that $(\frac{\pi}{\pi'}) = (\frac{\pi'}{\pi})$ for $\pi \equiv \pi' \equiv 1 \bmod \tau^3$, which means that $(\frac{\pi}{\pi'})(\frac{\pi'}{\pi}) = 1$. Then by Theorem 4.6.7, we have that $(\pi, \pi')_{\pi'}(\pi, \pi')_\pi = 1$. From here, Theorem 4.6.5, Corollary 4.1.19, and Lemma 4.2.5 tell us that $(\pi, \pi')_v = 1$ for all v other than $v = \pi$ and $v = \pi'$. So, $\prod_v (\pi, \pi')_v = 1$.

Assuming quadratic reciprocity, we also have $(\frac{i}{\pi}) = (-1)^{\frac{N(\pi)-1}{4}}$, so $(\frac{i}{\pi})(-1)^{\frac{N(\pi)-1}{4}} = 1$. Then by Theorem 4.6.4 and Theorem 4.6.7, we have $(i, \pi)_\pi (i, \pi)_\tau = 1$. Also, Corollary 4.1.19 and Lemma 4.2.5 tell us that $(i, \pi)_v = 1$ for all v other than $v = \pi$ and $v = \tau$. With this, we have $\prod_v (i, \pi)_v = 1$.

Lastly, quadratic reciprocity tells us that for $\pi \equiv 1 \bmod \tau^3$ with $\pi = x + yi$ for $x, y \in \mathbf{Z}$,

$$\left(\frac{\tau}{\pi}\right) = \begin{cases} 1, & \text{if } x + y \equiv \pm 1 \bmod 8, \\ -1, & \text{if } x + y \equiv \pm 3 \bmod 8. \end{cases}$$

Then by Theorem 4.6.7 and Theorem 4.6.3, we have $(\tau, \pi)_\pi (\tau, \pi)_\tau = 1$. Just like before, Corollary 4.1.19 and Lemma 4.2.5 tell us that $\prod_v (\tau, \pi)_v = 1$.

Along with the bimultiplicativity of the Hilbert symbol and what we showed in Cases 1, 2, 4, and 6, we have that $\prod_v (a, b)_v = 1$ for all $a, b \in \mathbf{Q}(i)_v^\times$. Thus Hilbert reciprocity on $\mathbf{Q}(i)$ is equivalent to quadratic reciprocity on $\mathbf{Z}[i]$. $\square$

Bibliography

[1] Conrad, K., *The Gaussian Integers*, http://www.math.uconn.edu/∼kconrad/blurbs/ugradnum

[2] Conrad, K., *Hensel's Lemma*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy /hensel.pdf.

[3] Gouvea, F., *p-adic Numbers An Introduction*, Springer, New York, 2003.

[4] Serre, J-P., *A Course in Arithmetic*, Springer, New York, 1996.