

This page is here to make the page numbers come out correctly.

Do not print this page.

*Finding the Unit Structure in a Factor
Ring of a Quadratic Number Field*

A Thesis Presented to
The Faculty of the Mathematics Program
California State University Channel Islands

In (Partial) Fulfillment
of the Requirements for the Degree
Masters of Science

by

Marina Morales

August, 2016

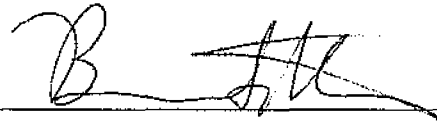
© 2016

Marina Morales

ALL RIGHTS RESERVED

Signature page for the Masters in Mathematics Thesis of Marina Morales

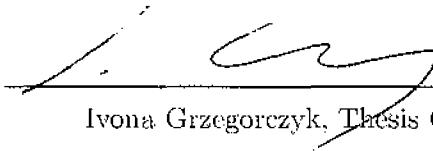
APPROVED FOR THE MATHEMATICS PROGRAM



Brian Sittinger, Thesis Advisor

16 Aug. 2016

Date



Ivona Grzegorzcyk, Thesis Committee

Aug 16, 2016

Date

APPROVED FOR THE UNIVERSITY



Dr. Gary A. Berg, AVP Extended University Date

8-16-16

Acknowledgements

First, I would like to thank my advisor Dr. Brian Sittinger for the encouragement he displayed while writing this thesis. He continually conveyed an adventure to exploring mathematical concepts and without his teachings, this thesis would not have been possible. In particular, the results in the final part of the thesis we have achieved collaboratively. In addition, I would like thank my committee member, Dr. Ivona Grzegorzcyk for guiding and helping me to make this study an achievement. I would also like to thank my parents and friends for the constant support they gave. Lastly, I give a big thanks to the Mathematics Department at California State University Channel Islands for their amazing program to build my future.

Abstract

Finding the Unit Structure in a Factor Ring of a Quadratic Number Field

by Marina Morales

The unit group structure of \mathbb{Z}_m is well-known in Number Theory, largely due to the significance of primitive roots modulo m whenever they exist. We investigate the analogous problem for a quadratic number ring \mathcal{O} , determining the unit group structure and a set of generators of the quotient ring \mathcal{O}/\mathfrak{a} for some fixed ideal \mathfrak{a} in \mathcal{O} .

CONTENTS

1. Introduction	1
2. Background and Terminology	6
2.1. Quadratic Number Fields	6
2.2. Basic Ideas Concerning Quotient Rings of \mathcal{O}	12
3. Unit group structure theorems	19
3.1. Splitting Case	19
3.2. Inert Case	20
3.3. Ramifying Case	28
4. Primitive Roots in Quadratic Number Rings	45
5. Appendix: Eisenstein Integers	48
References	56

1. INTRODUCTION

A useful and descriptive way to represent a finite abelian group is as a direct product of cyclic groups. With this description, it is easy to deduce many important properties of the group, such as its order, subgroups, and rank. In this thesis, we investigate the structure of the group of units in any factor ring of a quadratic number ring.

As a motivating example we start with \mathbb{Z}_m , the ring of integers modulo m . This is a finite commutative ring whose units (elements having multiplicative inverses) form a multiplicative group which is denoted by $(\mathbb{Z}_m)^*$. It is a standard fact that an element $x \in (\mathbb{Z}_m)^*$ is a unit if and only if $\gcd(x, m) = 1$. Moreover, the order of $(\mathbb{Z}_m)^*$ is given by the classic Euler phi-function $\phi(m)$.

We want to know the group structure of $(\mathbb{Z}_m)^*$. To help us with this, we invoke the Chinese Remainder Theorem.

Theorem 1. *Chinese Remainder Theorem.*

Let $m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ be a prime factorization for m . Then,

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

As a consequence, this induces the isomorphism

$$(\mathbb{Z}_m)^* \cong (\mathbb{Z}_{p_1^{n_1}})^* \times (\mathbb{Z}_{p_2^{n_2}})^* \times \cdots \times (\mathbb{Z}_{p_k^{n_k}})^*.$$

Therefore, it suffices to understand the structure of $(\mathbb{Z}_{p^n})^*$ for any prime p . This is given in the following theorem, whose proof can be found in many places, such as [9].

Theorem 2. *Unit Structure of $(\mathbb{Z}_{p^n})^*$.*

(1) *For any odd prime p , we have*

$$(\mathbb{Z}_{p^n})^* = \langle g \rangle \cong \mathbb{Z}_{p^n - p^{n-1}} \text{ for some } g \in \mathbb{Z}_{p^n}.$$

$$(2) (\mathbb{Z}_{2^n})^* = \begin{cases} \{1\} & \text{if } n = 1 \\ \{\pm 1\} \cong \mathbb{Z}_2 & \text{if } n = 2 \\ \{\pm 1\} \times \langle 5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} & \text{if } n \geq 3. \end{cases}$$

If $(\mathbb{Z}_m)^*$ is cyclic, then any of its generators is called a **primitive root** modulo m . For example, when p is odd, g is a primitive root modulo $m = p^n$ for any $n \in \mathbb{N}$. We can say more; by using this theorem in conjunction with the Chinese Remainder Theorem, it is straightforward to deduce that a primitive root modulo m exists if and only if $m = 2, 4, p^n, 2p^n$ for any odd prime p and positive integer n .

When primitive roots exist, it is often very convenient to use them in proofs and explicit constructions; for instance, given a primitive root modulo an odd prime p , the quadratic residues mod p are precisely the even

powers of the primitive root. Primitive roots are also important in cryptological applications involving the discrete log problem, most notably the Diffie-Hellman key exchange, El Gamal public-key cryptosystem, and the Schnorr identification scheme. Finding quadratic non-residues modulo a prime is another interesting problem in number theory. Applications relying on generating quadratic non-residues include the Tonelli-Shanks algorithm and Cippola-Lehmer algorithm for computing square roots modulo a prime as well as the Goldwasser-Micali probabilistic encryption scheme. Further details can be found in [10].

Our second example is the ring of **Gaussian integers**

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Note that $\mathbb{Z}[i]$ has similar arithmetic properties reminiscent of \mathbb{Z} , such as divisibility, primes, and being a UFD (and PID).

The primes in $\mathbb{Z}[i]$ are different from those in \mathbb{Z} and are described in the following theorem.

Theorem 3. *Primes in $\mathbb{Z}[i]$.*

- (1) *If p is prime in \mathbb{N} and $p \equiv 3 \pmod{4}$, then p is still prime in $\mathbb{Z}[i]$.*
- (2) *If p is prime in \mathbb{N} and $p \equiv 1 \pmod{4}$, then $p = \pi\bar{\pi}$ for some distinct primes $\pi \in \mathbb{Z}[i]$.*

(3) $2 = -i(1+i)^2$ and $1+i$ is prime in $\mathbb{Z}[i]$.

For example, 7 is still prime in $\mathbb{Z}[i]$, but 5 is not prime in $\mathbb{Z}[i]$ since $5 = (2+i)(2-i)$. Instead, $2+i$ and $2-i$ are primes in $\mathbb{Z}[i]$ that “replace” 5.

As in \mathbb{Z} , we can do modular arithmetic in $\mathbb{Z}[i]$. We now approach this from a ring-theoretic point of view. Observe that since $\mathbb{Z}_m \cong \mathbb{Z}/\langle m \rangle$, arithmetic of \mathbb{Z} modulo m is essentially the same as performing arithmetic in $\mathbb{Z}/\langle m \rangle$. Also observe that since \mathbb{Z} is a PID, any ideal in \mathbb{Z} can be written in the form $\langle m \rangle$ for some $m \in \mathbb{Z}_{\geq 0}$.

Now, we apply these ideas to $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, any ideal in $\mathbb{Z}[i]$ can be written in the form $\langle \gamma \rangle$ for some $\gamma \in \mathbb{Z}[i]$. Then fixing $\gamma \in \mathbb{Z}[i]$, we study the quotient ring $\mathbb{Z}[i]/\langle \gamma \rangle$.

Reminiscent of the case with modular arithmetic in \mathbb{Z} , given $\gamma \in \mathbb{Z}[i]_{\neq 0}$, what is the group structure of $(\mathbb{Z}[i]/\langle \gamma \rangle)^*$? To help us with this, we use the following variant of the Chinese Remainder Theorem for $\mathbb{Z}[i]$ which can be found in [2].

Theorem 4. *Chinese Remainder Theorem for $\mathbb{Z}[i]$.*

Let $\gamma = \pi_1^{n_1} \pi_2^{n_2} \cdots \pi_k^{n_k}$ be a prime factorization for $\gamma \in \mathbb{Z}[i]$ where $\pi_1, \pi_2, \dots, \pi_k$ are distinct primes in $\mathbb{Z}[i]$. Then,

$$\mathbb{Z}[i]/\langle \gamma \rangle \cong \mathbb{Z}[i]/\langle \pi_1^{n_1} \rangle \times \mathbb{Z}[i]/\langle \pi_2^{n_2} \rangle \times \cdots \times \mathbb{Z}[i]/\langle \pi_k^{n_k} \rangle.$$

As a consequence, the Chinese Remainder Theorem induces the isomorphism

$$(\mathbb{Z}[i]/\langle\gamma\rangle)^* \cong (\mathbb{Z}[i]/\langle\pi_1^{n_1}\rangle)^* \times (\mathbb{Z}[i]/\langle\pi_2^{n_2}\rangle)^* \times \dots \times (\mathbb{Z}[i]/\langle\pi_k^{n_k}\rangle)^*.$$

Therefore, to understand $(\mathbb{Z}[i]/\langle\gamma\rangle)^*$ it suffices to study the structure of $(\mathbb{Z}[i]/\langle\pi^n\rangle)^*$ where π is a prime in $\mathbb{Z}[i]$. Cross [1] studied this problem; we summarize his results below.

Theorem 5. *Group Structure for $(\mathbb{Z}[i]/\langle\pi^n\rangle)^*$.*

(1) *Suppose $\pi = p \equiv 3 \pmod{4}$. Let g be a primitive root modulo p^n and $h \in \mathbb{Z}_{p^2-1} \subseteq (\mathbb{Z}[i]_{p^n})^*$ have order $p^2 - 1$. Then,*

$$(\mathbb{Z}[i]_{p^n})^* = \langle 1 + pi \rangle \times \langle g \rangle \times \langle h \rangle \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

(2) *Suppose $p \equiv 1 \pmod{4}$ such that $p = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[i]$. Let g be a primitive root modulo p^n . Then,*

$$(\mathbb{Z}[i]/\langle\pi^n\rangle)^* = \langle g \rangle \cong \mathbb{Z}_{p^n - p^{n-1}}.$$

(3) *For $\pi = 1 + i$, $(\mathbb{Z}[i]/\langle 1 + i \rangle)^* = \{1\}$ and $(\mathbb{Z}[i]/\langle (1 + i)^2 \rangle)^* = \langle i \rangle \cong \mathbb{Z}_2$.*

For $n > 2$, we have

$$(\mathbb{Z}[i]/\langle(1+i)^n\rangle)^* = \begin{cases} \langle 1 + 2i \rangle \times \langle 5 \rangle \times \langle i \rangle \cong \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_4 & \text{if } n = 2m \\ \langle 1 + 2i \rangle \times \langle 5 \rangle \times \langle i \rangle \cong \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_4 & \text{if } n = 2m + 1. \end{cases}$$

For our next example, we can consider the Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. This is another example of a ring that possesses arithmetic properties similar to \mathbb{Z} and $\mathbb{Z}[i]$. As this is a special case of the results that follow, we will place its results in an appendix.

We instead consider the more general problem of finding the group structure and the generators for a quotient ring in any quadratic number field over \mathbb{Q} . The results on the group structure exist in the literature; Kohler ([4]) recently compiled them together (so he could use these results to explicitly compute characters on these groups), proving these results via intricate counting arguments *without giving the generators*. We follow Cross' [1] approach to find the generators in any such quotient ring. We first review the pertinent facts about quadratic number fields in the next section. Then, we spend the remainder of the thesis deriving the group structure for a quotient ring in any quadratic number field.

2. BACKGROUND AND TERMINOLOGY

2.1. Quadratic Number Fields. Here, we first will give a quick review of some basic concepts from algebraic number theory, as found in [6] and [9].

Definition 1. An *algebraic number* (over \mathbb{Q}) is a complex number that is a root of a polynomial with rational coefficients.

Any algebraic number α yields an associated **algebraic number field** $K = \mathbb{Q}(\alpha)$. Classic examples of such algebraic number fields are the quadratic number fields $\mathbb{Q}(\sqrt{d})$ for any square-free integer d and the cyclotomic number fields $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ for some integer $n \geq 3$.

Definition 2. An *algebraic integer* is a complex number that is a root of a monic polynomial with integer coefficients.

Remark: $\sqrt{5}$ is an algebraic integer since it is a root of the monic polynomial $x^2 - 5$. This definition provides a generalization of the set of integers, because any $n \in \mathbb{Z}$ is a root of the monic polynomial $x - n$. Meanwhile, $\frac{1}{2}$ is not an algebraic integer since $2x - 1$ is not monic, and there is no monic polynomial with integer coefficients that has $\frac{1}{2}$ as a root.

Any algebraic number field K has a corresponding **ring of (algebraic) integers (algebraic number ring)** \mathcal{O}_K , which is the set of algebraic integers in K . Whenever K is implied without any confusion, we will write \mathcal{O} for its algebraic number ring.

Now we define the ring of integers to a quadratic field $\mathbb{Q}(\sqrt{d})$. This is given in the definition.

Definition 3. Fix a square-free integer d . Then the **quadratic number ring** \mathcal{O} associated to $\mathbb{Q}(\sqrt{d})$ is the set

$$\{a + b\omega : a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Remark: The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is the set of algebraic integers in the quadratic field $\mathbb{Q}(i)$ (here, $d = -1$). Similarly, the ring of Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, is the set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{-3})$.

Next, we discuss the problem of factoring in \mathcal{O} .

Definition 4. Given an algebraic number ring \mathcal{O} , we say that a nonzero nonunit $\alpha \in \mathcal{O}$ is **irreducible** if its only factors are units and associates of α .

In \mathbb{Z} , one often says that an irreducible integer is *prime*; but in a number ring, we define this term differently as follows:

Definition 5. Given an algebraic number ring \mathcal{O} , we say that a nonzero nonunit $\pi \in \mathcal{O}$ is **prime** if for any $\alpha, \beta \in \mathcal{O}$ such that $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

Note: Hereafter, we refer to the primes in \mathbb{N} as **rational primes** to distinguish these from primes in an algebraic number ring \mathcal{O} .

Remark: In any algebraic number ring possessing the unique factorization property into irreducibles, such as \mathbb{Z} and $\mathbb{Z}[i]$, the previous definitions are equivalent. However, this is not always the case. For example, if we take $K = \mathbb{Q}(\sqrt{-5})$, then we have the following factorizations into irreducibles in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Since the factors above are all irreducible in $\mathbb{Z}[\sqrt{-5}]$ and none of these factors are associates to one another, $\mathbb{Z}[\sqrt{-5}]$ does not possess the unique factorization property into irreducibles. This introduces an important question: How can we assess primality when we do not have unique factorization into irreducibles for each element? The key idea is to introduce prime ideals.

Definition 6. *Given an algebraic number ring \mathcal{O} , we say that a proper ideal $\mathfrak{p} \subsetneq \mathcal{O}$ is **prime** if, whenever \mathfrak{q} and \mathfrak{r} are ideals in \mathcal{O} such that $\mathfrak{q}\mathfrak{r} \subseteq \mathfrak{p}$, then $\mathfrak{q} \subseteq \mathfrak{p}$ or $\mathfrak{r} \subseteq \mathfrak{p}$.*

It is an important result of Dedekind that all ideals in a given algebraic number ring possess unique factorization into prime ideals. To illustrate

this point, let us return to our example in $\mathbb{Z}[\sqrt{-5}]$, where we saw that

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

It can be shown that $\mathfrak{p}_1 = \langle 3, 2 + \sqrt{-5} \rangle$, $\mathfrak{p}_2 = \langle 3, 2 - \sqrt{-5} \rangle$, $\mathfrak{p}_3 = \langle 7, 3 + \sqrt{-5} \rangle$ and $\mathfrak{p}_4 = \langle 7, 3 - \sqrt{-5} \rangle$ are prime ideals in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, $\langle 3 \rangle = \mathfrak{p}_1\mathfrak{p}_2$, $\langle 7 \rangle = \mathfrak{p}_3\mathfrak{p}_4$, $\langle 1 + 2\sqrt{-5} \rangle = \mathfrak{p}_1\mathfrak{p}_4$, and $\langle 1 - 2\sqrt{-5} \rangle = \mathfrak{p}_2\mathfrak{p}_3$.

Therefore, we see that the two factorizations into irreducibles give rise to the same prime *ideal* factorization of $\langle 21 \rangle$, namely $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.

Next, we give a description of the prime ideals in \mathcal{O} . We first introduce the following terminology.

Definition 7. Let p be a rational prime and \mathcal{O} be a quadratic number ring.

(1) We say that p **splits** in \mathcal{O} if $\langle p \rangle = \mathfrak{p}\bar{\mathfrak{p}}$ for some distinct prime ideals $\mathfrak{p}, \bar{\mathfrak{p}}$ in \mathcal{O} .

Note that $\bar{\mathfrak{p}}$ is the ideal whose elements are conjugates to those in \mathfrak{p} .

(2) We say that p is **inert** in \mathcal{O} if $\langle p \rangle$ is a prime ideal in \mathcal{O} .

(3) We say that p **ramifies** in \mathcal{O} if $\langle p \rangle = \mathfrak{p}^2$ for some prime ideal \mathfrak{p} in \mathcal{O} .

The resulting primes ideals are said to **lie above** p .

For example, we saw in the set of Gaussian integers $\mathbb{Z}[i]$, a rational prime p is inert when $p \equiv 3 \pmod{4}$, splits when $p \equiv 1 \pmod{4}$, and ramifies when $p = 2$.

In the spirit of the Gaussian integers, we want to characterize the prime ideals in a quadratic number rings more precisely. For a quadratic number ring, we define the **discriminant** Δ as follows:

$$\Delta = \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Now, we can state this theorem about prime ideals in a quadratic number ring (see [6] for a proof).

Theorem 6. *Behavior of rational primes in a quadratic number ring.*

(a) *For an odd rational prime p :*

(1) *p is inert in \mathcal{O} if $\left(\frac{d}{p}\right) = -1$.*

(2) *p splits in \mathcal{O} if $\left(\frac{d}{p}\right) = 1$.*

(3) *p ramifies in \mathcal{O} if $p \mid \Delta$.*

(b) *For the rational prime 2:*

(1) *2 is inert in \mathcal{O} if $d \equiv 5 \pmod{8}$.*

(2) *2 splits in \mathcal{O} if $d \equiv 1 \pmod{8}$.*

(3) *2 ramifies in \mathcal{O} if d is even, or $d \equiv 3$ or $7 \pmod{8}$.*

Mimicking the properties of \mathbb{Z} we have a notion of ‘divides’ in the context of ideals (which reduces to the usual definition of divisibility of element in the case that all ideals are principal).

Definition 8. *Given ideals $\mathfrak{a}, \mathfrak{b}$ in \mathcal{O} , we say that \mathfrak{a} **divides** \mathfrak{b} , written $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$ for some ideal \mathfrak{c} in \mathcal{O} .*

For example, any prime ideal in \mathcal{O} divides the rational prime over which it lies. Moreover, it follows immediately from this definition that $\mathfrak{a} \mid \mathfrak{b}$ iff $\mathfrak{a} \supseteq \mathfrak{b}$.

2.2. Basic Ideas Concerning Quotient Rings of \mathcal{O} . We now consider quotient rings in \mathcal{O} . We fix a nonzero ideal \mathfrak{a} in \mathcal{O} and consider \mathcal{O}/\mathfrak{a} . (Note that \mathfrak{a} need not be principal.)

Again, we have a version of the Chinese Remainder Theorem for \mathcal{O} (as any two distinct prime ideals are comaximal in \mathcal{O} ; see [2] for a proof):

Theorem 7. *Chinese Remainder Theorem for \mathcal{O} .*

Let $\mathfrak{a} = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_k^{n_k}$ be a prime factorization for the ideal \mathfrak{a} in \mathcal{O} where $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k$ are distinct prime ideals in \mathcal{O} . Then,

$$\mathcal{O}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{p}_1^{n_1} \times \mathcal{O}/\mathfrak{p}_2^{n_2} \times \dots \times \mathcal{O}/\mathfrak{p}_k^{n_k}.$$

As we will be interested in the unit group $(\mathcal{O}/\mathfrak{a})^*$, the Chinese Remainder Theorem again induces the isomorphism

$$(\mathcal{O}/\mathfrak{a})^* \cong (\mathcal{O}/\mathfrak{p}_1^{n_1})^* \times (\mathcal{O}/\mathfrak{p}_2^{n_2})^* \times \dots \times (\mathcal{O}/\mathfrak{p}_k^{n_k})^*.$$

Hence, it suffices to study $(\mathcal{O}/\mathfrak{p}^n)^*$ for some fixed prime ideal \mathfrak{p} in \mathcal{O} and $n \in \mathbb{N}$.

We first find a complete set of equivalence classes to $\mathcal{O}/\mathfrak{p}^n$. To assist us in this endeavor, we introduce the norm of an ideal.

Definition 9. *The **norm** of a nonzero ideal \mathfrak{a} in \mathcal{O} is defined as $\mathfrak{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.*

Remark 1: Note that the norm is always finite. It can be shown that the norm is completely multiplicative: if $\mathfrak{a}, \mathfrak{b}$ are nonzero ideals in \mathcal{O} , then $\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

Remark 2: Since any prime ideal \mathfrak{p} is always maximal in an algebraic number ring \mathcal{O} , we know that \mathcal{O}/\mathfrak{p} is a field. In the case of a quadratic number ring, this implies that $\mathfrak{N}(\mathfrak{p}) = p^2$ if p is inert, and $\mathfrak{N}(\mathfrak{p}) = p$ if p is not inert.

The following is a generalization of one of Cross' results: [1]

Theorem 8. *The complete set of equivalence classes to \mathcal{O} modulo a power of a prime ideal \mathfrak{p} are given as follows:*

(1) If p splits and \mathfrak{p} lies above p , then $\mathcal{O}/\mathfrak{p}^n = \{0, 1, 2, \dots, p^n - 1\}$.

(2) If p is inert, then $\mathcal{O}/\mathfrak{p}^n = \{a + b\omega \mid a, b = 0, 1, 2, \dots, p^n - 1\}$.

(3) If p ramifies and \mathfrak{p} lies above p , then

- $\mathcal{O}/\mathfrak{p}^{2m} = \{a + b\omega \mid a, b = 0, 1, 2, \dots, p^m - 1\}$.
- $\mathcal{O}/\mathfrak{p}^{2m+1} = \{a + b\omega \mid b = 0, 1, 2, \dots, p^{m+1} - 1, a = 0, 1, 2, \dots, p^m - 1\}$.

Proof. By Remarks 1 and 2, along with $\mathfrak{N}(\mathfrak{p}^n) = \mathfrak{N}(\mathfrak{p})^n$, we have the right number of equivalence classes for $\mathcal{O}/\mathfrak{p}^n$. Hence, it suffices to establish that the given equivalence classes of $\mathcal{O}/\mathfrak{p}^n$ are distinct.

(1) Suppose that p splits and \mathfrak{p} lies above p .

If $a = b$ in $\mathcal{O}/\mathfrak{p}^n$ with $a, b \in \{0, 1, \dots, p^n - 1\}$, then $\mathfrak{p}^n \mid \langle a - b \rangle$, and by conjugation we have $\bar{\mathfrak{p}}^n \mid \langle a - b \rangle$. Since $\gcd(\mathfrak{p}, \bar{\mathfrak{p}}) = \langle 1 \rangle$, we have $\mathfrak{p}^n \bar{\mathfrak{p}}^n = \langle p^n \rangle \mid \langle a - b \rangle$, which is equivalent to $p^n \mid (a - b)$. Since $a, b \in \{0, 1, \dots, p^n - 1\}$, we conclude that $a = b$.

(2) Next, suppose that p is inert (and thus $\mathfrak{p} = \langle p \rangle$).

Suppose that $a + b\omega = c + d\omega$ in $\mathcal{O}/\mathfrak{p}^n$ for some $a, b, c, d \in \{0, 1, \dots, p^n - 1\}$. Then, $(a - c) + (b - d)\omega = 0$ in $\mathcal{O}/\mathfrak{p}^n$. This, in turn, implies that $p^n \mid (a - c)$ and $p^n \mid (b - d)$. Since a, b, c, d are between 0 and $p^n - 1$ inclusive, we conclude that $a = c$ and $b = d$.

(3) Finally, suppose that p ramifies and \mathfrak{p} lies above p .

If $n = 2m$, then the distinctness of the given equivalence classes is proved as in the inert case. Now, suppose that $n = 2m + 1$ and $a + b\omega = c + d\omega$ in $\mathcal{O}/\mathfrak{p}^n$, where $a, c \in \{0, 1, \dots, p^{m+1} - 1\}$ and $b, d \in \{0, 1, \dots, p^m - 1\}$. Since $\mathfrak{p}^n = \langle p^m \rangle \mathfrak{p}$, it follows that $p^m \mid (b - d)$ and thus $b = d$. Therefore, $\langle p^m \rangle \mathfrak{p} \mid \langle a - c \rangle$, or equivalently $a - c = p^m \cdot k$ for some integer k , since the only rational elements in \mathcal{O} are integers. Then, $\mathfrak{p} \mid \langle k \rangle$. Taking norms, we find that $p \mid k^2$ and thus $p \mid k$. Hence, $p^{m+1} \mid (a - c)$ and by the choices of a and c , we conclude that $a = c$.

□

Next, we generalize the Euler phi function of elementary number theory to algebraic number rings.

Definition 10. *The **phi function** defined on a nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}$ is defined as $\Phi(\mathfrak{a}) = |(\mathcal{O}/\mathfrak{a})^*|$.*

Remark: It can be shown that the Φ is multiplicative; if $\mathfrak{a}, \mathfrak{b}$ are relatively prime ideals in \mathcal{O} , then $\Phi(\mathfrak{a}\mathfrak{b}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b})$. Hence, it suffices to compute $\Phi(\mathfrak{p}^n)$ where \mathfrak{p} is a prime ideal in \mathcal{O} and $n \in \mathbb{N}$. This has been done ([3]) as has a form reminiscent of its classical counterpart:

$$\Phi(\mathfrak{p}^n) = (\mathfrak{N}(\mathfrak{p}))^n - (\mathfrak{N}(\mathfrak{p}))^{n-1}.$$

Although it will not be crucial to the work that follows, but we can now give a full set of equivalence classes for $(\mathcal{O}/\mathfrak{p}^n)^*$ whenever \mathfrak{p} is not ramified (again generalizing a result of Cross [1]).

Theorem 9. *Equivalence classes of units.*

- (1) *Suppose that \mathfrak{p} lies above a split rational prime p . Then, $a \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if $\gcd(a, p) = 1$.*
- (2) *Suppose that p is inert (so that $\mathfrak{p} = \langle p \rangle$). Then, $x + y\omega \in (\mathcal{O}/\mathfrak{p}^n)^*$ if and only if at least one of x and y is relatively prime to p .*

Proof. (1) Note that $a \in \mathcal{O}/\mathfrak{p}^n$ is a unit if and only if $ab = 1$ for some $b \in \mathcal{O}/\mathfrak{p}^n$. This is true if and only if $1 \in \langle a \rangle + \mathfrak{p}^n$. This is equivalent to saying that $\gcd(\langle a \rangle, \mathfrak{p}^n) = \langle 1 \rangle$ or more simply $\gcd(\langle a \rangle, \mathfrak{p}) = \langle 1 \rangle$. Finally, this is equivalent in the split case to saying $\gcd(a, p) = 1$.

(2) As in (1), $x + y\omega \in \mathcal{O}/\mathfrak{p}^n$ is a unit if and only if $\gcd(\langle x + y\omega \rangle, \mathfrak{p}^n) = \langle 1 \rangle$. Hence, $x + y\omega \in \mathcal{O}/\mathfrak{p}^n$ is a unit if and only if $\mathfrak{p}^n \nmid \langle x + y\omega \rangle$. This is equivalent to saying that $\mathfrak{p} \nmid \langle x + y\omega \rangle$, or alternately $p \nmid x$ or $p \nmid y$. □

Mimicking results again for \mathbb{Z} , the following notational shorthand will prove useful.

Definition 11. Suppose that $\alpha, \beta \in \mathcal{O}$ and fix an ideal \mathfrak{a} in \mathcal{O} . We say that α **is congruent to β modulo \mathfrak{a}** , written $\alpha \equiv \beta \pmod{\mathfrak{a}}$, iff $(\alpha - \beta) \in \mathfrak{a}$.

From this definition, we see that $\alpha \equiv \beta \pmod{\mathfrak{a}}$ iff α and β belong to the same equivalence class in \mathcal{O}/\mathfrak{a} .

The following proposition ([8]) is a variant of Hensel's lifting lemma in \mathbb{Z} that will prove useful in the work that follows. This allows us to 'lift' a solution to a polynomial congruence from one power of a prime ideal to the next power.

Proposition 1. Suppose that $f(x) \in \mathcal{O}[x]$ and \mathfrak{p} is a prime ideal in \mathcal{O} . If $x = \alpha \in \mathcal{O}$ is a solution to $f(x) \equiv 0 \pmod{\mathfrak{p}^{n-1}}$ for some $n \geq 2$ and $f'(\alpha) \in \gcd(\langle f'(\alpha) \rangle, \mathfrak{p}^n)$, then $f(x) \equiv 0 \pmod{\mathfrak{p}^n}$ has a solution in \mathcal{O} .

Proof. We first establish the following claim: For any $\alpha, \beta \in \mathcal{O}$,

$$f(\alpha + \beta) = f(\alpha) + \beta f'(\alpha) + \beta^2 \gamma \text{ for some } \gamma \in \mathcal{O}.$$

To show this, note that for any $k \in \mathbb{Z}_{\geq 0}$, the Binomial Theorem yields

$$(\alpha + \beta)^k = \alpha^k + k\alpha^{k-1}\beta + \beta^2 \delta_k \text{ for some } \delta_k \in \mathcal{O}.$$

Writing $f(x) = \sum_{k=0}^n \rho_k x^k$ for some $\rho_k \in \mathcal{O}$ and $n \in \mathbb{N}$, we have

$$\begin{aligned}
f(\alpha + \beta) &= \sum_{k=0}^n \rho_k (\alpha + \beta)^k \\
&= \left[\sum_{k=2}^n \rho_k (\alpha^k + k\alpha^{k-1}\beta + \beta^2\delta_k) \right] + \rho_1(\alpha + \beta) + \rho_0 \\
&= \sum_{k=0}^n \rho_k \alpha^k + \beta \cdot \sum_{k=1}^n k\rho_k \alpha^{k-1} + \beta^2 \cdot \sum_{k=0}^n \rho_k \delta_k \\
&= f(\alpha) + \beta f'(\alpha) + \beta^2 \gamma, \text{ where } \gamma = \sum_{k=0}^n \rho_k \delta_k.
\end{aligned}$$

Now, we are ready to prove this proposition. Suppose that $f(\alpha) \equiv 0 \pmod{\mathfrak{p}^{n-1}}$. We want to solve $f(x) \equiv 0 \pmod{\mathfrak{p}^n}$ using α . To do this, we write $x = \alpha + \beta$ for some $\beta \in \mathfrak{p}^{n-1}$.

Substituting this into $f(\alpha) \equiv 0 \pmod{\mathfrak{p}^n}$ and using the claim yields (for some $\gamma \in \mathcal{O}$)

$$f(\alpha + \beta) = f(\alpha) + \beta f'(\alpha) + \beta^2 \gamma \equiv 0 \pmod{\mathfrak{p}^n}.$$

Since $\beta^2 \in \mathfrak{p}^{2n-2}$ and $2n - 2 \geq n$, the previous relation reduces to

$$f(\alpha) + \beta f'(\alpha) \equiv 0 \pmod{\mathfrak{p}^n}.$$

This has a solution if and only if $f(\alpha) \in \gcd(\langle f'(\alpha) \rangle, \mathfrak{p}^n)$.

□

Remark: This version of Hensel lifting is sufficient for our purposes, because either $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{p}}$ or n will be sufficiently large so that $f(\alpha) \in \mathfrak{p}^n$.

3. UNIT GROUP STRUCTURE THEOREMS

3.1. Splitting Case. In this section, we suppose that p splits in \mathcal{O} ; that is, $\langle p \rangle = \mathfrak{p}\bar{\mathfrak{p}}$ for some distinct prime ideals $\mathfrak{p}, \bar{\mathfrak{p}}$ in \mathcal{O} . Then, with little effort, we derive the following group structure theorem, which asserts that $(\mathcal{O}/\mathfrak{p}^n)^*$ is a cyclic group.

Theorem 10. *Suppose that \mathfrak{p} lies above the split rational prime p . Then,*

$$(\mathcal{O}/\mathfrak{p}^n)^* = \langle g \rangle \cong \mathbb{Z}_{p^n - p^{n-1}},$$

where g is a primitive root modulo p^n .

Proof. In Theorem 9, the set of elements $a \in (\mathcal{O}/\mathfrak{p}^n)^*$ is formally the same as $(\mathbb{Z}_{p^n})^*$. This leads us to consider the well-defined homomorphism $\psi : (\mathcal{O}/\mathfrak{p}^n)^* \rightarrow (\mathbb{Z}_{p^n})^*$ defined by $\psi(a) = a$ (the fact that ψ is well-defined follows immediately from $\mathfrak{p} \mid \langle p \rangle$). Moreover ψ is a bijection by construction; thus ψ is an isomorphism. Since $(\mathbb{Z}_{p^n})^* \cong \mathbb{Z}_{p^n - p^{n-1}}$, we conclude that $(\mathcal{O}/\mathfrak{p}^n)^* \cong \mathbb{Z}_{p^n - p^{n-1}}$. □

3.2. Inert Case. In this section, we assume that p is inert in \mathcal{O} so that we can simply write $\mathfrak{p} = \langle p \rangle$. Before stating the group structure theorem, we record a few lemmas.

Lemma 1. *Let $k \in \mathbb{N}$.*

(a) *If p is an odd rational prime, then $(1 + p\omega)^{p^k} = 1 + p^{k+1}\omega + p^{k+2}\gamma$ for some $\gamma \in \mathcal{O}$.*

(b) *$(1 + 2\omega)^{2^k} = 1 + 2^{k+1} + 2^{k+2}\gamma$ for some $\gamma \in \mathcal{O}$.*

Proof. To establish this lemma, we use the following claim.

Claim: Let $\beta \in \mathcal{O}$ and r be a prime in \mathbb{Z} . Then,

$$(1 + \beta r)^{r^k} = 1 + \beta r^{k+1} + \frac{1}{2}\beta^2(r^k - 1)r^{k+2} + \delta r^{k+2}$$

for some $\delta \in \mathcal{O}$.

We prove this claim by induction on k . For $k = 1$, the Binomial Theorem yields

$$(1 + \beta r)^r = 1 + \beta r^2 + \frac{1}{2}\beta^2 r^3(r - 1) + \left[\sum_{j=3}^r \binom{r}{j} \beta^j r^{j-3} \right] \cdot r^3.$$

Since $\binom{r}{j} \in \mathbb{N}$ and $j \geq 3$, it follows immediately that $\delta = \sum_{j=3}^r \binom{r}{j} \beta^j r^{j-3} \in \mathcal{O}$, thereby establishing the base case.

Now, assuming that the claim is true for k , we show that it is true for $k + 1$. By the Inductive Hypothesis,

$$(1 + \beta r)^{r^{k+1}} = [(1 + \beta r)^{r^k}]^r = \left[1 + \left(\beta r^{k+1} + \frac{1}{2} \beta^2 (r^k - 1) r^{k+2} + \delta r^{k+2} \right) \right]^r.$$

Applying the Binomial Theorem to the right side of the equation yields

$$1 + \beta r^{k+2} + \frac{1}{2} \beta^2 (r^k - 1) r^{k+3} + \delta r^{k+3} + \sum_{j=2}^r \binom{r}{j} \left(\beta + \frac{1}{2} \beta^2 (r^k - 1) r + \delta r \right)^j r^{j(k+1)}.$$

Since $j(k + 1) \geq k + 3$ for all integers $j \geq 2$ and $k \in \mathbb{N}$, we have:

$$(1 + \beta r)^{r^{k+1}} = 1 + \beta r^{k+2} + \frac{1}{2} \beta^2 (r^k - 1) r^{k+3} + \hat{\delta} r^{k+3}.$$

for some $\hat{\delta} \in \mathcal{O}$.

To write this in the form to resemble the claim for $k + 1$, we rewrite this by strategically adding zero:

$$(1 + \beta r)^{r^{k+1}} = 1 + \beta r^{k+2} + \frac{1}{2} \beta^2 (r^{k+1} - 1) r^{k+3} + \frac{1}{2} \beta^2 r^k r^{k+3} - \frac{1}{2} \beta^2 r^{k+1} r^{k+3} + \hat{\delta} r^{k+3}.$$

Letting $\tilde{\delta} = \hat{\delta} - \frac{1}{2} \beta^2 r^k (r - 1) \in \mathcal{O}$ allows us to establish the claim for $k + 1$ as required:

$$(1 + \beta r)^{r^{k+1}} = 1 + \beta r^{k+2} + \frac{1}{2} \beta^2 (r^{k+1} - 1) r^{k+3} + \tilde{\delta} r^{k+3}.$$

Part (a) of the lemma follows now directly from this claim by letting $r = p$ for some odd prime p , $\beta = \omega$, and collecting like terms.

As for part (b), we let $r = 2$ and $\beta = \omega$:

$$(1 + 2\omega)^{2^k} = 1 + 2^{k+1}(\omega + (2^k - 1)\omega^2) + 2^{k+2}\delta$$

for some $\delta \in \mathcal{O}$.

Rearranging terms, we have

$$(1 + 2\omega)^{2^k} = 1 + 2^{k+1}(\omega + \omega^2) + 2^{k+2}\epsilon$$

for some $\epsilon \in \mathcal{O}$.

We can simplify this further. Since $\langle 2 \rangle$ being inert is equivalent to $d \equiv 5 \pmod{8}$, we have $\omega = \frac{1+\sqrt{d}}{2}$. In particular, $\omega^2 + \omega = \frac{d-1}{4} \equiv 1 \pmod{2}$.

Therefore,

$$(1 + 2\omega)^{2^k} = 1 + 2^{k+1} + 2^{k+2}\gamma \text{ for some } \gamma \in \mathcal{O}.$$

□

The previous lemma now allows us to find the order of $1 + p\omega$ in $(\mathcal{O}/\mathfrak{p}^n)^*$.

Lemma 2. *Let $m \in \mathbb{N}_{>2}$ and $m, n \in \mathbb{N}_{>1}$ and suppose that p is inert in \mathcal{O} .*

(a) *The order of $1 + p\omega$ in $(\mathcal{O}/\mathfrak{p}^n)^*$ equals p^{n-1} .*

(b) *The order of $1 + 2\omega$ in $(\mathcal{O}/\langle 2^n \rangle)^*$ equals 2^{n-1} .*

Proof. (a) Letting $k = n - 1$ in part a of Lemma 1 yields

$$(1 + p\omega)^{p^{n-1}} = 1 + p^n\omega + p^{n+1}\gamma \text{ for some } \gamma \in \mathcal{O}.$$

Reducing modulo p^n then gives $(1 + p\omega)^{p^{n-1}} \equiv 1 \pmod{p^n}$. Thus, by Lagrange's Theorem, the order of $1 + p\omega$ divides p^{n-1} .

Similarly, letting $k = n - 2$ in part (a) of Lemma 1 and reducing modulo p^n yields $(1 + p\omega)^{p^{n-1}} \not\equiv 1 \pmod{p^n}$. Therefore, the order of $1 + p\omega$ in $(\mathcal{O}/\mathfrak{p}^n)^*$ equals p^{n-1} .

(b) Letting $k = n - 1$ in part b of Lemma 1 yields

$$(1 + 2\omega)^{2^{n-1}} = 1 + 2^n + 2^{n+1}\gamma \text{ for some } \gamma \in \mathcal{O}.$$

Reducing modulo 2^n then gives $(1 + 2\omega)^{2^{n-1}} \equiv 1 \pmod{2^n}$. Thus, by Lagrange's Theorem, the order of $1 + 2\omega$ divides 2^{n-1} .

Similarly, letting $k = n - 2$ in part (b) of Lemma 1 and reducing modulo 2^n yields $(1 + 2\omega)^{2^{n-1}} \not\equiv 1 \pmod{2^n}$. Therefore, the order of $1 + 2\omega$ in $(\mathcal{O}/\langle 2^n \rangle)^*$ equals 2^{n-1} .

□

This next lemma shows that two special cyclic subgroups of $(\mathcal{O}/\mathfrak{p}^n)^*$ have trivial intersection.

Lemma 3. *Suppose that \mathfrak{p} is inert in \mathcal{O} . Then, if $a \in \mathbb{Z}$ has order p^k for some positive integer k in $(\mathcal{O}/\mathfrak{p}^n)^*$, then we have $\langle 1 + p\omega \rangle \cap \langle a \rangle = \{1\}$ in $(\mathcal{O}/\mathfrak{p}^n)^*$.*

Proof. Note that both cyclic groups are of power of the same prime p .

Then, $\langle 1+p\omega \rangle \cap \langle a \rangle$ is also cyclic of order p^k for some $k = \{0, 1, 2, \dots, n-1\}$.

We want to show that $k = 0$.

If $k \geq 1$, then $\langle 1+p\omega \rangle \cap \langle a \rangle$ contains a cyclic subgroup of order p .

Since $1+p\omega$ has order p^{n-1} in $(\mathcal{O}/\mathfrak{p}^n)^*$ is p^{n-1} by Lemma 2, it follows that $(1+p\omega)^{p^{n-2}} = 1+p^{n-1}\omega$ is an element in $\langle 1+p\omega \rangle$ that has order p ; hence all others elements of order p in $\langle 1+p\omega \rangle$ have the form $1+p^{n-1}k\omega$, where $k = \{1, 2, 3, \dots, p-1\}$. Since none of these are in $\langle a \rangle$, we conclude that the intersection is trivial. \square

Now, we can state the group structure theorems for $(\mathcal{O}/\mathfrak{p}^n)^*$ in the case that p is inert. We start with the case when p is odd.

Theorem 11. *Suppose that $\langle p \rangle = \mathfrak{p}$ with p being an odd rational prime.*

Then, there exists $a \in \mathbb{Z}$ and $\beta \in \mathcal{O}$ such that

$$(\mathcal{O}/\mathfrak{p}^n)^* = \langle 1+p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Proof. We have already examined $\langle 1+p\omega \rangle$ in Lemma 2.

Now, we construct a . Consider the homomorphism $\psi : (\mathbb{Z}_{p^n})^* \rightarrow (\mathcal{O}/\mathfrak{p}^n)^*$ defined by $\psi(b) = b$. Since $(\mathbb{Z}_{p^n})^*$ is cyclic of order $\phi(p^n) = p^{n-1}(p-1)$, there exists $a \in (\mathbb{Z}_{p^n})^*$ having order p^{n-1} . In fact, if g is a primitive root

mod p^n , then let $a = g^{p-1}$. Consider the cyclic group $\langle a \rangle$. By Lemma 3, $\langle 1 + p\omega \rangle \cap \langle a \rangle = \{1\}$.

Finally, we construct β . Since p is prime in \mathcal{O} , and prime ideals in a Dedekind Domain (such as \mathcal{O}) are maximal, \mathcal{O}/\mathfrak{p} is a field with $\mathfrak{N}(\mathfrak{p}) = p^2$ elements. Thus, $(\mathcal{O}/\mathfrak{p})^*$ is a cyclic group of order $p^2 - 1$; let β be a generator. Since $\beta^{p^2-1} \equiv 1 \pmod{p}$, we have $\beta^{p^2-1} = 1 + \gamma p$ for some $\gamma \in \mathcal{O}$. Using the techniques of Lemma 2, $(\beta^{p^2} - 1)^{p^{n-1}} = (1 + \gamma p)^{p^{n-1}} = 1 + \delta p^n \in \mathcal{O}$ for some $\delta \in \mathcal{O}$. Therefore, $(\beta^{p^2-1})^{p^{n-1}} \equiv 1 \pmod{p^n}$, or equivalently $(\beta^{p^{n-1}})^{p^2-1} \equiv 1 \pmod{p^n}$. Thus, $\beta^{p^{n-1}}$ has order t dividing $p^2 - 1$. Then, $\beta^{tp^{n-1}} \equiv 1 \pmod{p}$ implies that $(p^2 - 1) \mid tp^{n-1}$, and thus $(p^2 - 1) \mid t$. Therefore, $t = p^2 - 1$.

Now, consider $\langle \beta^{p^{n-1}} \rangle$. Since all elements of $\langle 1 + p\omega \rangle \times \langle a \rangle$ have orders being powers of p , and $\langle \beta^{p^{n-1}} \rangle$ has order $p^2 - 1$, which is relatively prime to p , we can conclude that $(\langle 1 + p\omega \rangle \times \langle a \rangle) \cap \langle \beta^{p^{n-1}} \rangle = \{1\}$. Hence, we can construct the direct product $\langle 1 + p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle$.

Using the Φ -function, we know that the order of $(\mathcal{O}/\mathfrak{p}^n)^*$ is $p^{2n} - p^{2n-2} = p^{2n-2}(p^2 - 1)$. Moreover, $\langle 1 + p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle = p^{2n-2}(p^2 - 1)$. Since $\langle 1 + p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle$ is a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^*$ having the same order as $(\mathcal{O}/\mathfrak{p}^n)^*$, we conclude that $(\mathcal{O}/\mathfrak{p}^n)^* = \langle 1 + p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle$. \square

To complete our discussion of the inert prime case, we now address the case when $p = 2$.

Theorem 12. *The group structure of $(\mathcal{O}/\langle 2^n \rangle)^*$ when 2 is inert.*

(1) $(\mathcal{O}/\langle 2 \rangle)^* = \langle \omega \rangle \cong \mathbb{Z}_3.$

(2) $(\mathcal{O}/\langle 2^2 \rangle)^* = \langle 1 + 2\omega \rangle \times \langle -1 \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ for some $\alpha \in \mathcal{O}.$

(3) For $n \geq 3$ and for some $\alpha \in \mathcal{O},$

$$(\mathcal{O}/\langle 2^n \rangle)^* = \langle 1 + 2\omega \rangle \times \langle 1 + 4\omega \rangle \times \langle -1 \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Proof. (1) Since $\mathcal{O}/\langle 2 \rangle$ is a field with 2^2 elements, $(\mathcal{O}/\langle 2 \rangle)^*$ is a cyclic group of order $2^2 - 1 = 3$. Since $\omega \neq 1$ in $\mathcal{O}/\langle 2 \rangle$, we conclude that ω is a generator for $(\mathcal{O}/\langle 2 \rangle)^*.$

(2) Plainly, -1 is an element of order 2 in $(\mathcal{O}/\langle 2^2 \rangle)^*.$ Moreover, $1 + 2\omega$ has order 2 in $(\mathcal{O}/\langle 2^2 \rangle)^* ,$ since $(1 + 2\omega)^2 = 1 + 4\omega + 4\omega^2 \equiv 1 \pmod{4},$ since $\omega^2 + \omega + \frac{1-d}{4} = 0$ and $d \equiv 5 \pmod{8}.$

Next, we construct an element α having order 3 in $(\mathcal{O}/\langle 2^2 \rangle)^* .$ To this end, recall that $\omega^3 \equiv 1 \pmod{2}.$ We lift ω to a solution to $x^3 \equiv 1 \pmod{4}.$ To do this, write $\alpha = \omega + 2\beta$ for some $\beta \in \mathcal{O}.$

Thus, we need to solve $(\omega + 2\beta)^3 \equiv 1 \pmod{4}.$ This reduces to $\omega^3 + 2\omega^2\beta \equiv 1 \pmod{4}.$ Hence, $\omega^2\beta \equiv \frac{1-\omega^3}{2} \pmod{2}$ (remember that $\frac{1-\omega^3}{2} \in \mathcal{O},$ because $\omega^3 \equiv 1 \pmod{2}.$) Now, multiplying both sides by ω yields $\beta \equiv \frac{\omega(1-\omega^3)}{2} \pmod{2}.$ Since $\alpha = \omega + 2\beta,$ we obtain $\alpha \equiv 2\omega - \omega^4 \pmod{4}.$ (Alternately, we can apply Hensel lifting for the existence of this generator.)

Plainly, these three subgroups have pairwise trivial intersections, and the product of their orders equals $\Phi(2^2) = 2^4 - 2^2 = 12$ as required.

(3) Since $1 + 2\omega$ has order 2^{n-1} from Lemma 2 part 2, we have $\langle 1 + 2\omega \rangle \cong \mathbb{Z}_{2^{n-1}}$. Since -1 has order 2, we can take $\langle -1 \rangle \cong \mathbb{Z}_2$. By Hensel lifting, we can inductively find an element α such that $\alpha^3 \equiv 1 \pmod{2^n}$. (This is valid, because if we let $f(x) = x^3 - 1$, $f'(\alpha) = 3\alpha^2 \notin \mathfrak{p}$.) Hence, $\langle \alpha \rangle \cong \mathbb{Z}_3$.

For the fourth cyclic subgroup, we claim that $\langle 1 + 4\omega \rangle \cong \mathbb{Z}_{2^{n-2}}$. This follows from the fact that $(1 + 4\omega)^{2^{n-3}} \equiv 1 + 2^{n-1}\omega \pmod{2^n}$, which is easy to prove by induction.

We next observe that the four cyclic subgroups are pairwise disjoint. The only tricky case is showing that $\langle 1 + 4\omega \rangle \cap \langle 1 + 2\omega \rangle = \{1\}$. To this end, note that since $\langle 1 + 4\omega \rangle$ is cyclic of order 2^{n-2} and $\langle 1 + 2\omega \rangle$ is cyclic of order 2^{n-1} , if their intersection has a nontrivial element, then they both would share an element of order 2. This is impossible, since the two cyclic subgroups' elements of order 2 are distinct, namely $1 + 2^{n-1}\omega$ and $1 + 2^{n-1}$, respectively.

Finally, the product of the orders of the cyclic subgroups equals $\Phi(2^n) = 2^{2n} - 2^{2n-2} = 2^{2n-2} \cdot 3$ as required.

□

3.3. Ramifying Case. In this section, suppose that p ramifies in \mathcal{O} ; that is, $\langle p \rangle = \mathfrak{p}^2$ for some prime ideal \mathfrak{p} in \mathcal{O} .

First, we describe the generators of \mathfrak{p} , which we will use in our work that follows.

Lemma 4. *Suppose p ramifies in \mathcal{O} .*

- (1) *If p is odd, then $\mathfrak{p} = \langle p, \sqrt{d} \rangle$.*
- (2) *If $p = 2$, then $\mathfrak{p} = \begin{cases} \langle 2, \sqrt{d} \rangle & \text{if } d \equiv 2 \pmod{4} \\ \langle 2, \sqrt{d} - 1 \rangle & \text{if } d \equiv 3 \pmod{4}. \end{cases}$*

Proof. Now, we assume that p is odd. Note that

$$\langle p, \sqrt{d} \rangle^2 = \langle p^2, p\sqrt{d}, d \rangle.$$

Since $p \mid d$ and $p \nmid d^2$, we know that $d = ap$ for some integer a not divisible by p . Hence, there exist integers x and y such that $ax + py = 1$. So,

$$\langle p, \sqrt{d} \rangle^2 = \langle p^2, p\sqrt{d}, d, dx + p^2y \rangle.$$

However, $dx + p^2y = p(ax + py) = p$. Therefore, since $p \mid d$, we conclude that $\langle p, \sqrt{d} \rangle^2 = \langle p \rangle$.

Next, assume that $p = 2$. If $d \equiv 2 \pmod{4}$, then $2 \mid d$ and the arguments in the previous paragraph go through verbatim. Now, we assume that $d \equiv 3 \pmod{4}$. In this case, we apply Dedekind's Theorem [9]. The minimal

polynomial for \sqrt{d} over \mathbb{Q} is $x^2 - d$ which factors as $(x - 1)^2 \pmod{2}$. Hence, Dedekind's Theorem gives us $\langle 2 \rangle = \langle 2, \sqrt{d} - 1 \rangle^2$.

□

We first address the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ for small powers of \mathfrak{p} .

Theorem 13. *Suppose that \mathfrak{p} lies above the ramifying rational prime p .*

(1) $(\mathcal{O}/\mathfrak{p})^* = \langle g \rangle \cong \mathbb{Z}_{p-1}$, where g is a primitive root modulo p .

$$(2) (\mathcal{O}/\mathfrak{p}^2)^* = \begin{cases} \langle 1 + \sqrt{d} \rangle \times \langle g \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_{p-1} & \text{if } p \text{ is odd} \\ \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_2 & \text{if } p = 2. \end{cases}$$

Here, g is a primitive root modulo p .

$$(3) (\mathcal{O}/\mathfrak{p}^3)^* = \begin{cases} \langle 1 + \sqrt{d} \rangle \times \langle g \rangle \cong \mathbb{Z}_p \times (\mathbb{Z}_{p-1} \times \mathbb{Z}_p) & \text{if } p \text{ is odd} \\ \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_4 & \text{if } p = 2 \text{ and } d \equiv 2 \pmod{4} \\ \langle \sqrt{d} \rangle \cong \mathbb{Z}_4 & \text{if } p = 2 \text{ and } d \equiv 3 \pmod{4}. \end{cases}$$

Proof. (1) Since \mathfrak{p} is prime and thus maximal, \mathcal{O}/\mathfrak{p} is a field with $\mathfrak{N}(\mathfrak{p}) = p$ elements. Hence, $(\mathcal{O}/\mathfrak{p})^*$ is a cyclic group with $p - 1$ elements. Incidentally, since $(\mathcal{O}/\mathfrak{p})^* = \{1, 2, \dots, p - 1\}$, we can generate this group by using a primitive root g modulo p .

(2) We break this down into two cases.

Assume that p is odd.

Since $\psi : (\mathbb{Z}_p)^* \rightarrow (\mathcal{O}/\mathfrak{p}^2)^*$ defined by $\psi(a) = a$ is an injective group homomorphism, we see that if we set $(\mathbb{Z}_p)^* = \langle g \rangle$, then $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^2)^*$ having order $|(\mathbb{Z}_p)^*| = p - 1$.

Next, we show that $1 + \sqrt{d}$ has order p in $(\mathcal{O}/\mathfrak{p}^2)^*$. To do this, we first prove that $(1 + \sqrt{d})^k \equiv 1 + k\sqrt{d} \pmod{\mathfrak{p}^2}$ by induction. This claim is trivially true for $k = 1$. Assuming that the claim is true for k , we have by the inductive hypothesis

$$(1 + \sqrt{d})^{k+1} \equiv (1 + \sqrt{d})^k(1 + \sqrt{d}) \equiv (1 + k\sqrt{d})(1 + \sqrt{d}) \pmod{\mathfrak{p}^2}.$$

This simplifies to $(1 + \sqrt{d})^{k+1} \equiv 1 + (k + 1)\sqrt{d} \pmod{\mathfrak{p}^2}$, because $p \mid kd$ due to $p \mid d$ and $\mathfrak{p}^2 = \langle p \rangle$.

From this claim, it is immediate that $(1 + \sqrt{d})^p \equiv 1 \pmod{\mathfrak{p}^2}$, but $(1 + \sqrt{d})^{p-1} \equiv 1 + (p - 1)\sqrt{d} \not\equiv 1 \pmod{\mathfrak{p}^2}$. Therefore, the order of $1 + \sqrt{d}$ is equal to p in $(\mathcal{O}/\mathfrak{p}^2)^*$.

Finally, we check that these two generators are sufficient. The order of the direct product of $\langle g \rangle$ and $\langle 1 + \sqrt{d} \rangle$ equals $p(p - 1)$. This matches the order of $(\mathcal{O}/\mathfrak{p}^2)^*$, since it equals $\Phi(\mathfrak{p}^2) = \mathfrak{N}(\mathfrak{p}^2) - \mathfrak{N}(\mathfrak{p}) = p^2 - p = p(p - 1)$.

Next, we examine the remaining case $p = 2$. Since $\Phi(\mathfrak{p}^2) = \mathfrak{N}(\mathfrak{p}^2) - \mathfrak{N}(\mathfrak{p}) = 2^2 - 2 = 2$ (which is a prime number), we deduce that $(\mathcal{O}/\mathfrak{p}^2)^*$ is a cyclic group with 2 elements. One such generator is $1 + \sqrt{d}$, because

$1 + \sqrt{d} \neq 1$ and $(1 + \sqrt{d})^2 \equiv 1 + 2\sqrt{d} + d^2 \equiv 1 \pmod{\mathfrak{p}^2}$. The last congruence follows from $2 \mid d$ and $\mathfrak{p}^2 = \langle 2 \rangle$.

(3) First, suppose that p is odd.

Since $\psi : (\mathbb{Z}_{p^2})^* \rightarrow (\mathcal{O}/\mathfrak{p}^3)^*$ defined by $\psi(a) = a$ is an injective group homomorphism, we see that if we set $(\mathbb{Z}_{p^2})^* = \langle g \rangle$, then $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^3)^*$ having order $|(\mathbb{Z}_{p^2})^*| = p(p-1)$. (Thus, $\langle g \rangle \cong \mathbb{Z}_{p(p-1)} \cong \mathbb{Z}_p \times \mathbb{Z}_{p-1}$.)

Next, we construct a second cyclic subgroup of order p . By the Binomial Theorem,

$$(1 + \sqrt{d})^p = 1 + p\sqrt{d} + \frac{1}{2}p(p-1)\sqrt{d} + \dots + (\sqrt{d})^p.$$

Reducing modulo \mathfrak{p}^3 and noting that $\mathfrak{p} = \langle p, \sqrt{d} \rangle$, we find that $(1 + \sqrt{d})^p \equiv 1 \pmod{\mathfrak{p}^3}$. Hence, $1 + \sqrt{d}$ has order p in $(\mathcal{O}/\mathfrak{p}^3)^*$.

We check that these generators is sufficient. The order of the direct product of $\langle g \rangle$ and $\langle 1 + \sqrt{d} \rangle$ equals $p^2(p-1)$. This matches the order of $(\mathcal{O}/\mathfrak{p}^3)^*$, since it equals $\Phi(\mathfrak{p}^3) = \mathfrak{N}(\mathfrak{p}^3) - \mathfrak{N}(\mathfrak{p}^2) = p^3 - p^2 = p^2(p-1)$.

Finally, we examine the remaining case $p = 2$. Since $\Phi(\mathfrak{p}^3) = \mathfrak{N}(\mathfrak{p}^3) - \mathfrak{N}(\mathfrak{p}^2) = 2^3 - 2^2 = 4$, we deduce that $(\mathcal{O}/\mathfrak{p}^2)^*$ has order 4. In fact, it is a cyclic group.

If $d \equiv 3 \pmod{4}$, then \sqrt{d} is a generator, because $(\sqrt{d})^2 = d \not\equiv 1 \pmod{\mathfrak{p}^3}$, but $(\sqrt{d})^4 \equiv 1 \pmod{4}$ and thus $(\sqrt{d})^4 \equiv 1 \pmod{\mathfrak{p}^3}$, since $\mathfrak{p}^3 \mid \langle 4 \rangle$.

If $d \equiv 2 \pmod{4}$, then $1 + \sqrt{d}$ is a generator, because $(1 + \sqrt{d})^2 = (1 + d) + 2\sqrt{d} \not\equiv 1 \pmod{\mathfrak{p}^3}$, but $(1 + \sqrt{d})^4 = 1 + 4\sqrt{d} + 6d + 4d\sqrt{d} + d^2 \equiv 1 \pmod{4}$ and thus $(1 + \sqrt{d})^4 \equiv 1 \pmod{\mathfrak{p}^3}$.

□

We next investigate higher powers of \mathfrak{p} . This has to be handled in three cases, depending on which rational prime \mathfrak{p} lies above: 2, 3, or any $p \geq 5$. We first consider the third case, as this is the easiest case to address. (The theorems addressing the other two cases are proved in collaboration with Brian Sittinger.)

Theorem 14. *Suppose that \mathfrak{p} lies above a ramifying rational prime $p \geq 5$.*

Then for any $m \geq 2$,

$$(1) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{m-1}}) \times \mathbb{Z}_{p^m},$$

where g is a primitive root modulo p^m .

$$(2) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^m}) \times \mathbb{Z}_{p^m},$$

where g is a primitive root modulo p^{m+1} .

Proof. Since $\psi_1 : (\mathbb{Z}_{p^m})^* \rightarrow (\mathcal{O}/\mathfrak{p}^{2m})^*$ defined by $\psi_1(a) = a$ is an injective group homomorphism, we see that if we set $(\mathbb{Z}_{p^m})^* = \langle g \rangle$, then $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^{2m})^*$ having order $|(\mathbb{Z}_{p^m})^*| = p^{m-1}(p-1)$. (Thus, $\langle g \rangle \cong \mathbb{Z}_{p^{m-1}(p-1)} \cong \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p-1}$.)

Similarly, $\psi_2 : (\mathbb{Z}_{p^{m+1}})^* \rightarrow (\mathcal{O}/\mathfrak{p}^{2m+1})^*$ defined by $\psi_2(a) = a$ shows that $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ having order $p^m(p-1)$.

Using the same techniques from Lemma 1-3 (from the section about the inert case), one can check that the order of $1 + p\omega$ in either $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ equals p^{m-1} , and that $\langle 1 + p\omega \rangle \cap \langle g \rangle = \{1\}$. Hence, we are justified to consider the direct product $\langle g \rangle \times \langle 1 + \sqrt{d} \rangle$.

In the case of $(\mathcal{O}/\mathfrak{p}^{2m})^*$, note that

$$\Phi(\mathfrak{p}^{2m}) = \mathfrak{N}(\mathfrak{p}^{2m}) - \mathfrak{N}(\mathfrak{p}^{2m-1}) = p^{2m} - p^{2m-1} = p^{2m-1}(p-1).$$

This matches the order of $\langle g \rangle \times \langle 1 + \sqrt{d} \rangle$, and we can conclude that $(\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle$.

Similarly, we have $(\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle$.

□

Next, we address the case where \mathfrak{p} lies above $\langle 3 \rangle$. Observe that $3|d$, but $3^2 \nmid d$. So, $\frac{d}{3}$ is an integer congruent to 1 or 2 mod 3. It turns out that the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ depends on d in the aforementioned manner.

Theorem 15. *Suppose that \mathfrak{p} lies above the ramifying rational prime 3.*

Then for any $m \geq 2$:

(1) *If $\frac{d}{3} \equiv 1 \pmod{3}$, then*

$$(a) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^{m-1}}) \times \mathbb{Z}_{3^m},$$

where g is a primitive root modulo 3^m .

$$(b) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g \rangle \times \langle 1 + \sqrt{d} \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^m}) \times \mathbb{Z}_{3^m},$$

where g is a primitive root modulo 3^{m+1} .

(2) If $\frac{d}{3} \equiv 2 \pmod{3}$, then for some $\alpha \in \mathcal{O}$:

$$(a) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle g \rangle \times \langle 1 + 3\sqrt{d} \rangle \times \langle \alpha \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^{m-1}}) \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3,$$

where g is a primitive root modulo 3^m .

$$(b) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle g \rangle \times \langle 1 + 3\sqrt{d} \rangle \times \langle \alpha \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_{3^m}) \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3,$$

where g is a primitive root modulo 3^{m+1} .

Proof. Since $\psi_1 : (\mathbb{Z}_{3^m})^* \rightarrow (\mathcal{O}/\mathfrak{p}^{2m})^*$ defined by $\psi_1(a) = a$ is an injective group homomorphism, we see that if we set $(\mathbb{Z}_{3^m})^* = \langle g \rangle$, then $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^{2m})^*$ having order $|(\mathbb{Z}_{3^m})^*| = 2 \cdot 3^{m-1}$. (Thus, $\langle g \rangle \cong \mathbb{Z}_{2 \cdot 3^{m-1}} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^{m-1}}$.)

Similarly, $\psi_2 : (\mathbb{Z}_{3^{m+1}})^* \rightarrow (\mathcal{O}/\mathfrak{p}^{2m+1})^*$ defined by $\psi_2(a) = a$ shows that $\langle g \rangle$ is a cyclic subgroup of $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ having order $2 \cdot 3^m$. (Thus, $\langle g \rangle \cong \mathbb{Z}_{2 \cdot 3^m} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^m}$.)

Now, it remains to address the remaining cyclic subgroups.

(1) First of all, suppose that $\frac{d}{3} \equiv 1 \pmod{3}$. We claim that $1 + \sqrt{d}$ has order 3^m in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$.

By the Binomial Theorem, for any positive integer k ,

$$(1 + \sqrt{d})^{3^k} = 1 + \sum_{j=1}^{3^k} \binom{3^k}{j} (\sqrt{d})^j.$$

Letting $k = m$, we find that $(1 + \sqrt{d})^{3^m} \equiv 1 \pmod{\mathfrak{p}^{2m+1}}$ since $\sqrt{d} \in \mathfrak{p}$ and $3^m \in \mathfrak{p}^{2m}$. Moreover, this implies that $(1 + \sqrt{d})^{3^m} \equiv 1 \pmod{\mathfrak{p}^{2m}}$. Therefore, the order of $(1 + \sqrt{d})$ divides 3^m in both cases.

Next, we let $k = m - 1$ and rearrange terms to find that

$$(1 + \sqrt{d})^{3^{m-1}} = \left[1 + \binom{3^{m-1}}{2} d\right] + \left[3^{m-1} + \binom{3^{m-1}}{3} d\right] \sqrt{d} + \sum_{j=4}^{3^{m-1}} \binom{3^{m-1}}{j} (\sqrt{d})^j.$$

Now, we analyze each term. First of all, since $\frac{d}{3} \equiv 1 \pmod{3}$, we have $d = 3(1 + 3j)$ for some $j \in \mathbb{N}$. In particular, $d \in \mathfrak{p}^2 \setminus \mathfrak{p}^3$.

Moreover, since $\sqrt{d} \in \mathfrak{p}$ and $3 \in \mathfrak{p}^2$, we have the following:

- $1 + \binom{3^{m-1}}{2} d = \frac{1}{2} \cdot 3^m (3^{m-1} - 1)(1 + 3j) \in \mathfrak{p}^{2m} \setminus \mathfrak{p}^{2m+1}$.
- $\left[3^{m-1} + \binom{3^{m-1}}{3} d\right] \sqrt{d} \in \mathfrak{p}^{2m-1} \setminus \mathfrak{p}^{2m}$, since this quantity equals $3^{m-1} [1 + \frac{1}{2}(3^{m-1} - 1)(3^{m-1} - 2)(1 + 3j)] \sqrt{d}$, and $x := 1 + \frac{1}{2}(3^{m-1} - 1)(3^{m-1} - 2)(1 + 3j)$ is not divisible by 3, because $x \equiv 2 \pmod{3}$.
- $\sum_{j=4}^{3^{m-1}} \binom{3^{m-1}}{j} (\sqrt{d})^j \in \mathfrak{p}^{2m+2}$.

Hence, it follows that $(1 + \sqrt{d})^{3^{m-1}} \equiv 1 + \alpha + \beta \pmod{\mathfrak{p}^{2m+2}}$ for some nonzero $\alpha \in \mathfrak{p}^{2m-1} \setminus \mathfrak{p}^{2m}$ and $\beta \in \mathfrak{p}^{2m} \setminus \mathfrak{p}^{2m+1}$.

Thus, $(1 + \sqrt{d})^{3^{m-1}} \not\equiv 1 \pmod{\mathfrak{p}^{2m}}$ and therefore $(1 + \sqrt{d})^{3^{m-1}} \not\equiv 1 \pmod{\mathfrak{p}^{2m+1}}$ as well. So, we can conclude that the order of $1 + \sqrt{d}$ in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ equals 3^m .

(2) Now, suppose that $\frac{d}{3} \equiv 2 \pmod{3}$.

For one generator, we claim that the order of $1 + 3\sqrt{d}$ equals 3^{m-1} . By the Binomial Theorem, $(1 + 3\sqrt{d})^{3^{m-1}} \equiv 1 + 3^m \sqrt{d} \pmod{\mathfrak{p}^{2m+1}}$, since all other terms are contained in \mathfrak{p}^{2m+1} . Moreover, since $\sqrt{d} \in \mathfrak{p}$ and $3 \in \mathfrak{p}^2$, it follows that $3^m \sqrt{d} \in \mathfrak{p}^{2m+1}$. Thus, $(1 + 3\sqrt{d})^{3^{m-1}} \equiv 1 \pmod{\mathfrak{p}^{2m+1}}$, and the order of $1 + 3\sqrt{d}$ in $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ (and thus $(\mathcal{O}/\mathfrak{p}^{2m})^*$) divides 3^{m-1} .

A similar calculation shows $(1 + 3\sqrt{d})^{3^{m-2}} \equiv 1 + 3^{m-1} \sqrt{d} \pmod{\mathfrak{p}^{2m}}$. However, $3^m \sqrt{d} \in \mathfrak{p}^{2m-1}$. Therefore, $(1 + 3\sqrt{d})^{3^{m-2}} \not\equiv 1 \pmod{\mathfrak{p}^{2m}}$ (and also modulo \mathfrak{p}^{2m+1}). So, the order of $1 + 3\sqrt{d}$ in both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$ equals 3^{m-1} .

Note that $\langle 1 + 3\sqrt{d} \rangle \cap \langle g \rangle = \{1\}$, since as in previous cases any positive power of $1 + 3\sqrt{d}$ less than 3^{m-1} has a nontrivial \sqrt{d} coefficient.

For the other generator, given any integer $k \geq 4$, we need to find $\alpha \in \mathcal{O}_{\neq 1}$ such that $\alpha^3 \equiv 1 \pmod{\mathfrak{p}^k}$. By direct calculation, when $k = 4$, we can let $\alpha = 1 + \sqrt{d}$. For $k > 4$, we inductively invoke Hensel lifting. Suppose we have found $\alpha \in \mathcal{O}_{\neq 1}$ such that $\alpha^3 \equiv 1 \pmod{\mathfrak{p}^k}$. Letting $f(x) = x^3 - 1$, note that $f'(x) = 3x^2$. Although $f'(\alpha) \in \mathfrak{p}$, $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2 \setminus \mathfrak{p}^3$ (since

α is a unit modulo \mathfrak{p}^k . Thus, indeed $f(\alpha) \in \gcd(f'(\alpha), \mathfrak{p}^k) = \mathfrak{p}^{k-2}$ and we can lift α to a solution to $x^3 \equiv 1 \pmod{\mathfrak{p}^{k+1}}$.

It remains to show $\langle \alpha \rangle \cap (\langle 1 + 3\sqrt{d} \rangle \cap \langle g \rangle) = \{1\}$. Again, we prove this inductively on $k \geq 4$. This is true for $k = 4$, since $1 + \sqrt{d}$ and $(1 + \sqrt{d})^2 \equiv 1 + 2\sqrt{d} \pmod{\mathfrak{p}^4}$ are not in $\langle 1 + 3\sqrt{d} \rangle \cap \langle g \rangle$ (due to having coefficients \sqrt{d} not divisible by 3). Assume that the claim is true for \mathfrak{p}^k : There exist $x, y \in \mathbb{Z}$ such that $(x + y\sqrt{d})^3 \equiv 1 \pmod{\mathfrak{p}^k}$ with $3 \nmid y$. Then, $x + y\sqrt{d}$ lifts to a solution modulo \mathfrak{p}^{k+1} of the form $(x + y\sqrt{d}) + (r + s\sqrt{d})$ where $(r + s\sqrt{d}) \in \mathfrak{p}^k$. Then, $3 \mid s$ and thus $3 \nmid (y + s)$, thereby establishing the inductive step.

□

Finally, we address the case where \mathfrak{p} lies above the ramifying rational prime 2. Not so surprisingly, this is the most involved case. Recall that $\langle 2 \rangle$ ramifies iff $d \equiv 2, 3 \pmod{4}$. This gives some indication how the group structure of $(\mathcal{O}/\mathfrak{p}^n)^*$ behaves. However, when $d \equiv 3 \pmod{4}$, it turns out that we have to investigate modulo 8, in which case $d \equiv 3$ or $7 \pmod{8}$.

Theorem 16. *Suppose that \mathfrak{p} lies above the ramifying rational prime 2.*

$$(\mathcal{O}/\mathfrak{p}^4)^* = \begin{cases} \langle 1 + 2\sqrt{d} \rangle \times \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{if } d \equiv 2 \pmod{4}, \\ \langle 1 + 2\sqrt{d} \rangle \times \langle \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

$$(\mathcal{O}/\mathfrak{p}^5)^* = \begin{cases} \langle -1 \rangle \times \langle 1 + 2\sqrt{d} \rangle \times \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{if } d \equiv 2 \pmod{4}, \\ \langle -1 \rangle \times \langle 1 + 2\sqrt{d} \rangle \times \langle \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Moreover, for any $m \geq 3$, we have the following:

(1) If $d \equiv 2 \pmod{4}$, then

$$(a) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle -1 \rangle \times \langle 5 \rangle \times \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^m}.$$

$$(b) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle -1 \rangle \times \langle 5 \rangle \times \langle 1 + \sqrt{d} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^m}.$$

(2) If $d \equiv 7 \pmod{8}$, then for some $\alpha \in \mathcal{O}$

$$(a) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle \alpha \rangle \times \langle 5 \rangle \times \langle 1 + 2\sqrt{d} \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^{m-1}}.$$

$$(b) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle \alpha \rangle \times \langle 5 \rangle \times \langle 1 + 2\sqrt{d} \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}}.$$

(3) If $d \equiv 3 \pmod{8}$, then for some $\alpha \in \mathcal{O}$

$$(a) (\mathcal{O}/\mathfrak{p}^{2m})^* = \langle -1 \rangle \times \langle 1 + 2\sqrt{d} \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}}.$$

$$(b) (\mathcal{O}/\mathfrak{p}^{2m+1})^* = \langle -1 \rangle \times \langle 1 + 2\sqrt{d} \rangle \times \langle \alpha \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^m}.$$

Proof. We first consider $(\mathcal{O}/\mathfrak{p}^4)^*$. Since $\mathfrak{p}^4 = \langle 4 \rangle$, it follows that $(1 + 2\sqrt{d})^2 \equiv 1 \pmod{\mathfrak{p}^4}$. Thus, $1 + 2\sqrt{d}$ has order 2 in $(\mathcal{O}/\mathfrak{p}^4)^*$. Next, if $d \equiv 2 \pmod{4}$, we have $(1 + \sqrt{d})^2 = (1 + d) + 2\sqrt{d} \not\equiv 1 \pmod{\mathfrak{p}^4}$, but $(1 + \sqrt{d})^4 \equiv 1 \pmod{\mathfrak{p}^4}$; so $1 + \sqrt{d}$ has order 4 in $(\mathcal{O}/\mathfrak{p}^4)^*$. If $d \equiv 3 \pmod{4}$, we have $(\sqrt{d})^2 = d \not\equiv 1 \pmod{\mathfrak{p}^4}$, but $(\sqrt{d})^4 \equiv 1 \pmod{\mathfrak{p}^4}$; so \sqrt{d} has order 4 in $(\mathcal{O}/\mathfrak{p}^4)^*$. For both cases of d , both $(\sqrt{d})^2$ and $(1 + \sqrt{d})^2$ are not equal

to $1 + 2\sqrt{d}$ in $(\mathcal{O}/\mathfrak{p}^4)^*$. This, combined with $\mathfrak{N}(\mathfrak{p}^4) = 8$ gives the desired group structure for $(\mathcal{O}/\mathfrak{p}^4)^*$.

Next, we consider $(\mathcal{O}/\mathfrak{p}^5)^*$. Plainly -1 is an element of order 2 for both $d \equiv 2, 3 \pmod{4}$. Moreover, $1 + 2\sqrt{d}$ has order 2, because when $d \equiv 2 \pmod{4}$, $(1 + 2\sqrt{d})^2 = 1 + 4\sqrt{d} + 4d \equiv 1 \pmod{\mathfrak{p}^5}$ (since $\sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$), and when $d \equiv 3 \pmod{4}$, $(1 + 2\sqrt{d})^2 = 1 + 4\sqrt{d}(1 - \sqrt{d}) \equiv 1 \pmod{\mathfrak{p}^5}$ (since $1 - \sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$).

Now, we find a generator having order 4. When $d \equiv 2 \pmod{4}$, we use $1 + \sqrt{d}$, because $(1 + \sqrt{d})^2 = (1 + d) + 2\sqrt{d} \not\equiv 1 \pmod{\mathfrak{p}^5}$, but $(1 + \sqrt{d})^4 \equiv 1 + (6d + d^2) + 4\sqrt{d}(1 + d) \equiv 1 \pmod{\mathfrak{p}^5}$ (since $8 \mid (6d + d^2)$). When $d \equiv 3 \pmod{4}$, we use \sqrt{d} , because $(\sqrt{d})^2 = d \not\equiv 1 \pmod{\mathfrak{p}^5}$, but $(\sqrt{d})^4 \equiv 1 \pmod{\mathfrak{p}^5}$. In both cases, the cyclic subgroups generated by this element of order 4 has trivial intersections with those generated by -1 and $1 + 2\sqrt{d}$.

Finally, since the order of the direct product of these three cyclic groups equals $\mathfrak{N}(\mathfrak{p}^5) = 16$ for both cases of d , we have the desired group structure for $(\mathcal{O}/\mathfrak{p}^5)^*$.

Now, we consider $(\mathcal{O}/\mathfrak{p}^n)^*$ for $n \geq 6$.

(1) Suppose that $d \equiv 2 \pmod{4}$.

Since $(\mathbb{Z}_{2^m})^* \subset (\mathcal{O}/\mathfrak{p}^{2^m})^*$ (as before), and $(\mathbb{Z}_{2^m})^* = \langle -1 \rangle \times \langle 5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$, we have our generators for $\mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$. Similarly, since $(\mathbb{Z}_{2^{m+1}})^* \subset (\mathcal{O}/\mathfrak{p}^{2^{m+1}})^*$, -1 and 5 , respectively, are the generators for $\mathbb{Z}_2 \times \mathbb{Z}_{2^{m-1}}$.

It remains to find an element of order 2^m for both $(\mathcal{O}/\mathfrak{p}^{2^m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2^{m+1}})^*$.

We claim that one such element is $1 + \sqrt{d}$. We prove this by induction on $m \geq 3$ by showing

$$(A) \quad (1 + \sqrt{d})^{2^m} \equiv 1 \pmod{\mathfrak{p}^{2^{m+1}}}, \text{ and}$$

$$(B) \quad (1 + \sqrt{d})^{2^{m-1}} \equiv 1 + \gamma \not\equiv 1 \pmod{\mathfrak{p}^{2^m}} \text{ for some } \gamma \in \mathfrak{p}^{2^{m-1}} \setminus \mathfrak{p}^{2^m}.$$

(Note how these readily imply that $(1 + \sqrt{d})^{2^m} \equiv 1 \pmod{\mathfrak{p}^{2^m}}$, and

$(1 + \sqrt{d})^{2^{m-1}} \not\equiv 1 \pmod{\mathfrak{p}^{2^{m+1}}}$ as well.)

For $m = 3$, since $\sqrt{d} \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$, we have modulo \mathfrak{p}^7

$$\begin{aligned} (1 + \sqrt{d})^{2^3} &\equiv 1 + 8\sqrt{d} + 28(\sqrt{d})^2 + 56(\sqrt{d})^3 + 70(\sqrt{d})^4 + 0 \\ &\equiv 1 + 28(\sqrt{d})^2 + 70(\sqrt{d})^4 \\ &\equiv 1 + 7 \cdot 2(\sqrt{d})^2(2 + 5d) \\ &\equiv 1 + 7 \cdot 2(\sqrt{d})^2(2 + 5(2 + 4k)) \text{ since } d = 2 + 4k \text{ for some integer } k \\ &\equiv 1 + 7 \cdot 2^3(\sqrt{d})^2(3 + 5k) \\ &\equiv 1 \pmod{\mathfrak{p}^7}. \end{aligned}$$

This establishes (A). For (B), working modulo \mathfrak{p}^6 yields

$$\begin{aligned}
(1 + \sqrt{d})^{2^2} &\equiv 1 + 4\sqrt{d} + 6(\sqrt{d})^2 + 4(\sqrt{d})^3 + (\sqrt{d})^4 \\
&\equiv 1 + 4\sqrt{d} + 6(\sqrt{d})^2 + (\sqrt{d})^4 \\
&\equiv 1 + 4\sqrt{d} \text{ since } d \equiv 2 \pmod{4} \\
&\not\equiv 1 \pmod{\mathfrak{p}^6}.
\end{aligned}$$

Moreover, $4\sqrt{d} \in \mathfrak{p}^5 \setminus \mathfrak{p}^6$, thereby finishing the inductive step.

Now we assume the claim is true for m and show it is true for $m + 1$:

To show (A), by the inductive hypothesis, $(1 + \sqrt{d})^{2^m} \equiv 1 \pmod{\mathfrak{p}^{2m+1}}$.

Thus, we can write $(1 + \sqrt{d})^{2^m} = 1 + \alpha$ for some $\alpha \in \mathfrak{p}^{2m+1}$.

Then, $(1 + \sqrt{d})^{2^{m+1}} = (1 + \alpha)^2 = 1 + 2\alpha + \alpha^2$. Reducing modulo \mathfrak{p}^{2m+3} immediately yields $(1 + \sqrt{d})^{2^{m+1}} \equiv 1 \pmod{\mathfrak{p}^{2m+3}}$.

To establish (B), by the inductive hypothesis, $(1 + \sqrt{d})^{2^{m-1}} \equiv 1 + \gamma \pmod{\mathfrak{p}^{2m}}$ for some $\gamma \in \mathfrak{p}^{2m-1} \setminus \mathfrak{p}^{2m}$. So, we have $(1 + \sqrt{d})^{2^{m-1}} = 1 + \gamma + \delta$ for some $\delta \in \mathfrak{p}^{2m}$. Then, $(1 + \sqrt{d})^{2^m} = (1 + \gamma + \delta)^2 \equiv 1 + 2\gamma \not\equiv 1 \pmod{\mathfrak{p}^{2m+2}}$, because $2\gamma \in \mathfrak{p}^{2m+1} \setminus \mathfrak{p}^{2m+2}$, as required. This concludes the induction.

Since no nontrivial power of $1 + \sqrt{d}$ is an integer, we conclude that $\langle 1 + \sqrt{d} \rangle \cap (\langle -1 \rangle \times \langle 5 \rangle) = \{1\}$. Finally, since the order of $\langle -1 \rangle \times \langle 5 \rangle \times \langle 1 + \sqrt{d} \rangle$ equals $\mathfrak{N}(\mathfrak{p}^n)$ with $n \geq 6$, we have the desired unit group structure result.

(2) Now, suppose that $d \equiv 7 \pmod{8}$.

As in the proof of (1), we know that 5 has order 2^{m-2} (as one of the generators of $(Z_{2^m})^*$).

It remains to find an element of order 2^{m-1} for both $(\mathcal{O}/\mathfrak{p}^{2m})^*$ and $(\mathcal{O}/\mathfrak{p}^{2m+1})^*$. We claim that one such element is $1 + 2\sqrt{d}$. We prove this by induction on $m \geq 3$ by showing

$$(A) \quad (1 + 2\sqrt{d})^{2^{m-1}} \equiv 1 \pmod{\mathfrak{p}^{2m+1}}, \text{ and}$$

$$(B) \quad (1 + \sqrt{d})^{2^{m-2}} \equiv 1 + \gamma \not\equiv 1 \pmod{\mathfrak{p}^{2m}} \text{ for some } \gamma \in \mathfrak{p}^{2m-1} \setminus \mathfrak{p}^{2m}.$$

For $m = 3$, since $(\sqrt{d} - 1) \in \mathfrak{p}$ and $2 \in \mathfrak{p}^2$, we have modulo \mathfrak{p}^7

$$\begin{aligned} (1 + \sqrt{d})^{2^{3-1}} &\equiv 1 + 4(2\sqrt{d}) + 6(2\sqrt{d})^2 + 4(2\sqrt{d})^3 + (2\sqrt{d})^4 \\ &\equiv 1 + 16d + 8(\sqrt{d} - 1) \\ &\equiv 1 \pmod{\mathfrak{p}^7}. \end{aligned}$$

This establishes (A). For (B), working modulo $\mathfrak{p}^6 = \langle 8 \rangle$ yields

$$\begin{aligned} (1 + \sqrt{d})^{2^{3-2}} &\equiv 1 + 2(2\sqrt{d}) + (2\sqrt{d})^2 \\ &\equiv 1 + 4\sqrt{d}(\sqrt{d} - 1) \\ &\not\equiv 1 \pmod{\mathfrak{p}^6}. \end{aligned}$$

Moreover, $4\sqrt{d}(\sqrt{d} - 1) \in \mathfrak{p}^5 \setminus \mathfrak{p}^6$, thereby finishing the inductive step.

Now we assume the claim is true for m and show it is true for $m + 1$:

To show (A), by the inductive hypothesis, $(1 + 2\sqrt{d})^{2^{m-1}} \equiv 1 \pmod{\mathfrak{p}^{2m+1}}$.

Thus, we can write $(1 + 2\sqrt{d})^{2^{m-1}} = 1 + \alpha$ for some $\alpha \in \mathfrak{p}^{2m+1}$.

Then, $(1 + 2\sqrt{d})^{2^m} = (1 + \alpha)^2 = 1 + 2\alpha + \alpha^2$. Reducing modulo \mathfrak{p}^{2m+3} immediately yields $(1 + 2\sqrt{d})^{2^{m+1}} \equiv 1 \pmod{\mathfrak{p}^{2m+3}}$.

To establish (B), by the inductive hypothesis, $(1 + 2\sqrt{d})^{2^{m-2}} \equiv 1 + \gamma \pmod{\mathfrak{p}^{2m}}$ for some $\gamma \in \mathfrak{p}^{2m-1} \setminus \mathfrak{p}^{2m}$. So, we have $(1 + 2\sqrt{d})^{2^{m-1}} = 1 + \gamma + \delta$ for some $\delta \in \mathfrak{p}^{2m}$. Then, $(1 + 2\sqrt{d})^{2^m} = (1 + \gamma + \delta)^2 \equiv 1 + 2\gamma \not\equiv 1 \pmod{\mathfrak{p}^{2m+2}}$, because $2\gamma \in \mathfrak{p}^{2m+1} \setminus \mathfrak{p}^{2m+2}$, as required. This concludes the induction.

For the third generator, we find an element of order 4. To make sure the cyclic subgroup generated by this element has trivial intersection with those generated by 5 and $1 + 2\sqrt{d}$, we make sure that its square equals -1 . Hence, it suffices to solve $\alpha^2 \equiv -1 \pmod{\mathfrak{p}^k}$ for $k \geq 6$. We actually begin with $k = 4$, because we can let $\alpha = \sqrt{d}$. For $k > 4$, we inductively invoke Hensel lifting. Suppose we have found $\alpha \in \mathcal{O}$ such that $\alpha^2 \equiv -1 \pmod{\mathfrak{p}^k}$. Letting $f(x) = x^2 - 1$, note that $f'(x) = 2x$. Then, $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2 \setminus \mathfrak{p}^3$ (since α is a unit modulo \mathfrak{p}^k). Thus, indeed $f(\alpha) \in \gcd(\langle f'(\alpha) \rangle, \mathfrak{p}^k) = \mathfrak{p}^{k-2}$ and we can lift α to a solution to $x^2 \equiv -1 \pmod{\mathfrak{p}^{k+1}}$.

Now, it is routine to show that the order of $\langle \alpha \rangle \times \langle 5 \rangle \times \langle 1 + 2\sqrt{d} \rangle$ equals $\mathfrak{N}(\mathfrak{p}^n)$ for $n \geq 6$.

(3) Suppose that $d \equiv 3 \pmod{8}$.

Clearly, -1 has order 2 and $1 + 2\sqrt{d}$ has order 2^{m-1} (using the same proof as in (2)).

It remains to find a generator for $\mathbb{Z}_{2^{m-1}}$ and \mathbb{Z}_{2^m} , depending on m being even or odd, respectively. Since ± 5 has order 2^{m-2} and 2^{m-1} (as m is even or odd), a generator α can be constructed to satisfy $\alpha^2 \equiv -5 \pmod{\mathfrak{p}^n}$ with $n \geq 6$. (Note that this cyclic subgroup generated by α will necessarily have trivial intersection with those generated by -1 and $1 + 2\sqrt{d}$.)

Hence, it suffices to solve $\alpha^2 \equiv -1 \pmod{\mathfrak{p}^k}$ for $k \geq 6$. We begin with $k = 6$, because we can let $\alpha = 4 + \sqrt{d}$, because $(4 + \sqrt{d})^2 = 16 + 8\sqrt{d} + d \equiv -5 \pmod{8}$. For $k > 6$, we inductively invoke Hensel lifting. Suppose we have found $\alpha \in \mathcal{O}$ such that $\alpha^2 \equiv -5 \pmod{\mathfrak{p}^k}$. Letting $f(x) = x^2 - 1$, note that $f'(x) = 2x$. Then, $f(\alpha) \in \mathfrak{p}^k$ and $f'(\alpha) \in \mathfrak{p}^2 \setminus \mathfrak{p}^3$ (since α is a unit modulo \mathfrak{p}^k). Thus, indeed $f(\alpha) \in \gcd(\langle f'(\alpha) \rangle, \mathfrak{p}^k) = \mathfrak{p}^{k-2}$ and we can lift α to a solution to $x^2 \equiv -5 \pmod{\mathfrak{p}^{k+1}}$.

As before, the order of $\langle -1 \rangle \times \langle 1 + 2\sqrt{d} \rangle \times \langle \alpha \rangle$ equals $\mathfrak{N}(\mathfrak{p}^n)$ for $n \geq 6$.

□

4. PRIMITIVE ROOTS IN QUADRATIC NUMBER RINGS

As an application of our work, we give a quadratic number ring generalization of primitive roots modulo m from \mathbb{Z} in this section.

Definition 12. Fix an algebraic number ring \mathcal{O} and an ideal \mathfrak{a} in \mathcal{O} . Then we say that $\alpha \in \mathcal{O}$ is a **primitive root** modulo \mathfrak{a} iff $\gcd(\langle \alpha \rangle, \mathfrak{a}) = \langle 1 \rangle$ and α has order $\Phi(\mathfrak{a})$ in $(\mathcal{O}/\mathfrak{a})^*$.

Plainly, a **primitive root** modulo \mathfrak{a} exists if and only if $(\mathcal{O}/\mathfrak{a})^*$ is a cyclic group. The following theorem catalogs when primitive roots exist.

Theorem 17. Suppose that \mathcal{O} is a quadratic number ring. Then, primitive roots exist modulo:

- (1) \mathfrak{p}^n for any prime ideal \mathfrak{p} lying above a split odd rational prime with $n \in \mathbb{N}$, or lying above the split rational prime 2 with $n = 1, 2$.
- (2) $\langle p \rangle$ for any inert rational prime p .
- (3) \mathfrak{p}^n for any prime ideal \mathfrak{p} lying above a ramifying odd rational prime with $n = 1, 2$, or lying above the ramifying rational prime 2 with $n = 1, 2, 3$.
- (4) If 2 splits in \mathcal{O} with \mathfrak{p} lying above 2:
 - (a) $\mathfrak{p}\langle q \rangle$, where q is an inert odd rational prime.

- (b) $\mathfrak{p}\mathfrak{q}^n$, where \mathfrak{q} lies over a ramifying odd rational prime and $n = 1, 2$.
 - (c) $\mathfrak{p}\mathfrak{q}^n$, where \mathfrak{q} lies over a split odd rational prime and $n \in \mathbb{N}$.
- (5) If 2 is inert:
- (a) $\langle 2 \rangle \mathfrak{p}^n$, where \mathfrak{p} lies over a split odd rational prime $\neq 3$ and $n \in \mathbb{N}$.
 - (b) $\langle 2 \rangle \mathfrak{p}^n$, where \mathfrak{p} lies over a ramifying odd rational prime $\neq 3$ and $n = 1, 2$.
 - (c) $\langle 6 \rangle$ where 3 is also inert.
- (6) If 2 ramifies in \mathcal{O} with \mathfrak{p} lying above 2:
- (a) $\mathfrak{p}\mathfrak{q}^n$, where \mathfrak{q} lies over a split odd rational prime and $n \in \mathbb{N}$.
 - (b) $\mathfrak{p}\langle q \rangle$, where q is an inert odd rational prime.
 - (c) $\mathfrak{p}\mathfrak{q}^n$, where \mathfrak{q} lies over a ramifying odd rational prime and $n = 1, 2$.

Proof. Facts (1)-(3) follows immediately from our unit group structure theorems, while facts (4)-(6) follow from these same theorems, along with the fact that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$. \square

We give two corollaries of this theorem. The first of these gives the existence of primitive roots modulo γ in the Gaussian integers (also given in Cross [1]).

Corollary 1. *In $\mathbb{Z}[i]$, a primitive root modulo $\langle \gamma \rangle$ exists if and only if $\gamma = \pi^n, (1+i)\pi^n, q, (1+i)q$, or $(1+i)^k$, where π is a factor of an rational prime $p \equiv 1 \pmod{4}$, $q \equiv 3 \pmod{4}$ is a rational prime, $n \in \mathbb{N}$, and $k = 1, 2$.*

Proof. This follows immediately from the previous theorem, along with the characterization of primes in $\mathbb{Z}[i]$: A rational prime p is inert in $\mathbb{Z}[i]$ if $p \equiv 3 \pmod{4}$, split in $\mathbb{Z}[i]$ if $p \equiv 1 \pmod{4}$, and ramifies if $p = 2$. \square

The second corollary gives a companion result to the case of the Eisenstein integers $\mathbb{Z}[\omega]$.

Corollary 2. *In $\mathbb{Z}[\omega]$, a primitive root modulo $\langle \gamma \rangle$ exists if and only if $\gamma = \pi^n, 2\pi^n, q$, or $(1-\omega)^k$, where π is a factor of an rational prime $p \equiv 1 \pmod{3}$, $q \equiv 2 \pmod{3}$ is a rational prime, $n \in \mathbb{N}$, and $k = 1, 2$.*

Proof. This follows immediately from the previous theorem, along with the characterization of primes in $\mathbb{Z}[\omega]$: A rational prime p is inert in $\mathbb{Z}[\omega]$ if $p \equiv 2 \pmod{3}$, split in $\mathbb{Z}[\omega]$ if $p \equiv 1 \pmod{3}$, and ramifies if $p = 3$. \square

5. APPENDIX: EISENSTEIN INTEGERS

Remark: The results in this section can be found in more detail in a self-contained manner in Kutin's masters thesis [5]. We leave this as an appendix, because this case provided (along with the results for the Gaussian integers) motivation on how to choose the generators in the general quadratic number ring case. Any proofs that are written out in this section are left for contrast with their generalizations.

In this section, we consider the set of **Eisenstein integers** $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$. Note that $\mathbb{Z}[\omega]$ too has similar arithmetic properties reminiscent of \mathbb{Z} and $\mathbb{Z}[i]$, such as divisibility, primes, and being a PID (and UFD).

We now identify the prime numbers in $\mathbb{Z}[\omega]$.

Proposition 2. *Primes in $\mathbb{Z}[\omega]$.*

- (1) *If $p \equiv 1 \pmod{3}$, then $p = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[\omega]$, and π and $\bar{\pi}$ are distinct primes in $\mathbb{Z}[\omega]$.*
- (2) *If $p \equiv 2 \pmod{3}$, then p remains prime in $\mathbb{Z}[\omega]$.*
- (3) *$3 = -\omega^2(1 - \omega)^2$, and $1 - \omega$ is prime in $\mathbb{Z}[\omega]$.*

Proof. This follows directly from Theorem 6, noting that by quadratic reciprocity $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ equals 1 iff $p \equiv 1 \pmod{3}$ and equals -1 iff $p \equiv 2 \pmod{3}$. Alternately, a proof without using Theorem 10 may be found in [6]. \square

Much like in $\mathbb{Z}[i]$, we can do modular arithmetic in $\mathbb{Z}[\omega]$. Since $\mathbb{Z}[\omega]$ is a PID, any ideal in $\mathbb{Z}[\omega]$ can be written in the form $\langle \gamma \rangle$ for some $\gamma \in \mathbb{Z}[\omega]$. Then, for fixed nonzero $\gamma \in \mathbb{Z}[\omega]$ we consider the quotient ring $\mathbb{Z}[\omega]/\langle \gamma \rangle$.

As in the cases for \mathbb{Z} and $\mathbb{Z}[i]$, we want to determine the unit structure of the quotients rings modulo an Eisenstein integer. Since $\mathbb{Z}[\omega]$ is a UFD, it suffices by the Chinese Remainder Theorem to find the unit structure of $\mathbb{Z}[\omega]/\langle \pi^n \rangle$ for some prime $\pi \in \mathbb{Z}[\omega]$.

We first give the equivalence classes of $\mathbb{Z}[\omega]/\langle \pi^n \rangle$.

Proposition 3. *The equivalence classes of $\mathbb{Z}[\omega]$ modulo a power of a prime are given as follows:*

(1) *If π is a factor of a rational prime $p \equiv 1 \pmod{3}$, then*

$$\mathbb{Z}[\omega]/\langle \pi^n \rangle = \{0, 1, 2, \dots, p^n - 1\}.$$

(2) *If π is a rational prime $p \equiv 2 \pmod{3}$, then*

$$\mathbb{Z}[\omega]/\langle p^n \rangle = \{a + b\omega \mid a, b = 0, 1, 2, \dots, p^n - 1\}.$$

(3) $\mathbb{Z}[\omega]/\langle (1 - \omega)^{2m} \rangle = \{a + b\omega \mid a, b = 0, 1, 2, \dots, 3^m - 1\}$.

(4) $\mathbb{Z}[\omega]/\langle (1 - \omega)^{2m+1} \rangle = \{a + b\omega \mid a = 0, 1, \dots, 3^{m+1} - 1, b = 0, 1, \dots, 3^m - 1\}$.

Proof. (1) Suppose that π is a factor of a rational prime $p \equiv 1 \pmod{3}$.

We first show that any $x + y\omega \in \mathbb{Z}[\omega]$ is equal to one of $0, 1, \dots, p^n - 1$ in

$\mathbb{Z}[\omega]/\langle\pi^n\rangle$. To do this, we show that ω is equal to one of $0, 1, \dots, p^n - 1$ in $\mathbb{Z}[\omega]/\langle\pi^n\rangle$.

First of all, $\pi^n = a - b\omega$ for some $a, b \in \mathbb{Z}$. So, $a \equiv b\omega \pmod{\pi^n}$. We claim that $\gcd(p, b) = 1$. If this were not the case, then $p \mid b$. Since $p = \pi\bar{\pi}$, it follows that $\pi \mid b$. Hence, $\pi \mid a$ and thus $\bar{\pi} \mid \bar{a} = a$. Since $\gcd(\pi, \bar{\pi}) = 1$ it follows that $p \mid a$. Therefore, $p \mid (a - b\omega) = \pi^n$. This yields a contradiction, because $\bar{\pi} \nmid \pi$.

Since $\gcd(p, b) = 1$, there exists $z \in \mathbb{Z}$ such that $bz \equiv 1 \pmod{p^n}$. Then, $az \equiv (b\omega)z \equiv \omega \pmod{p^n}$ (and thus we have reduced ω to an integer in $\mathbb{Z}[\omega]/\langle\pi^n\rangle$). Finally, $x + y\omega \equiv x + y \cdot az \pmod{\pi^n}$ which can be equivalent to one of $0, 1, \dots, p^n - 1$ by reducing modulo p^n and noting that $\pi \mid p$.

Now we show that these equivalence classes are distinct. Suppose that $a = b$ in $\mathbb{Z}[\omega]/\langle\pi^n\rangle$ for some $a, b \in \{0, 1, \dots, p^n - 1\}$. Then, $\pi^n \mid (a - b)$ and by conjugation $\bar{\pi}^n \mid (a - b)$. Since $\gcd(\pi, \bar{\pi}) = 1$, it follows that $(\pi\bar{\pi})^n = p^n \mid (a - b)$. Hence, $a = b$, since $a, b \in \{0, 1, \dots, p^n - 1\}$.

(2) Suppose that $p \equiv 2 \pmod{3}$. Given $x + y\omega \in \mathbb{Z}[\omega]$, reducing x and y modulo p^n yields an element in one of the desired equivalence classes. Now, suppose that $a + b\omega = c + d\omega \in \mathbb{Z}[\omega]/\langle p^n \rangle$ for some $a, b, c, d \in \{0, 1, \dots, p^n - 1\}$. Then, both $p^n \mid (a - c)$ and $p^n \mid (b - d)$, and thus $a = c$ and $b = d$, due to $a, b, c, d \in \{0, 1, \dots, p^n - 1\}$.

(3) This is proved in the same manner as (2).

(4) Given $x+y\omega \in \mathbb{Z}[\omega]$, reducing x and y modulo 3^{m+1} yields $x+y\omega \equiv c+d\omega \pmod{3^{m+1}}$, where $c, d \in \{0, 1, \dots, 3^{m+1} - 1\}$.

We want to reduce d further; by the Division Algorithm, $d = q \cdot 3^m + k$, for some $q \in \mathbb{Z}_{\geq 0}$ and $k \in \{0, 1, \dots, 3^m - 1\}$. Then, this yields $c + d\omega \equiv (c + d - k) + k\omega \pmod{\alpha^{2m+1}}$. By reducing $c + d - k$ modulo 3^{m+1} as needed, we can write $x + y\omega$ in the required form.

Now, suppose $a+b\omega = c+d\omega$ in $\mathbb{Z}[\omega]/\langle\alpha^{2m+1}\rangle$ for some $a, c \in \{0, 1, \dots, 3^{m+1} - 1\}$ and $b, d \in \{0, 1, \dots, 3^m - 1\}$. Then, $3^m|(b - d)$ and since $b, d < 3^m$, we have $b = d$. Thus, we obtain $a = c$ in $\mathbb{Z}[\omega]/\langle\alpha^{2m+1}\rangle$, which is equivalent to $3^m(1 - \omega)|(a - c)$. Then, we have $a - c = 3^m \cdot k$ for some $k \in \mathbb{Z}$. This gives us $(1 - \omega)|k$ and thus $(1 - \bar{\omega})|k$. Therefore, $3|k^2$, and so $3|k$. Hence, $3^{m+1}|(a - c)$, which immediately yields $a = c$. \square

Now, we can identify the equivalence classes that are units in their respective quotient rings.

Proposition 4. *Using the equivalence classes in the previous theorem:*

(1) *If π is a factor of a rational prime $p \equiv 1 \pmod{3}$, then $a \in (\mathbb{Z}[\omega]/\langle\pi^n\rangle)^*$ if and only if $\gcd(a, p) = 1$*

(2) *If π is a rational prime $p \equiv 2 \pmod{3}$, then $a + b\omega \in (\mathbb{Z}[\omega]/\langle p^n\rangle)^*$ if and only if at least one of a and b is relatively prime to p .*

(3) $a + b\omega \in (\mathbb{Z}[\omega]/\langle(1 - \omega)^n\rangle)^*$ if and only if $a \not\equiv -b \pmod{3}$.

Proof. Fix $\beta, \gamma \in \mathbb{Z}[\omega]$. We claim that β is a unit in $\mathbb{Z}[\omega]/\langle\gamma\rangle$ if and only if $\gcd(\beta, \gamma) = 1$.

To show this, note that β is a unit in $\mathbb{Z}[\omega]/\langle\gamma\rangle$ if and only if $\beta\delta \equiv 1 \pmod{\gamma}$ for some δ in $\mathbb{Z}[\omega]$. This is true if and only if $\beta\delta + \eta\gamma = 1$ for some $\eta \in \mathbb{Z}[\omega]$. This is equivalent to saying that $\gcd(\beta, \gamma) = 1$ since $\mathbb{Z}[\omega]$ is a UFD.

Now, we can quickly prove this theorem.

(1) By the claim, $a \in \mathbb{Z}[\omega]/\langle\pi^n\rangle$ is a unit if and only if $\gcd(a, \pi^n) = 1$.

However, $\gcd(a, \pi^n) = 1$ is equivalent to $\gcd(a, \pi) = 1$ and thus $\gcd(a, p) = 1$ since $p = \pi\bar{\pi}$ and $\gcd(\pi, \bar{\pi}) = 1$.

(2) By the claim, $a + b\omega \in \mathbb{Z}[\omega]/\langle p^n\rangle$ is a unit if and only if $\gcd(a + b\omega, p^n) = 1$.

However, $p \nmid (a + b\omega)$ if and only if $p \nmid a$ or $p \nmid b$.

(3) By the claim, $a + b\omega \in \mathbb{Z}[\omega]/\langle(1 - \omega)^n\rangle$ is a unit if and only if $(1 - \omega) \nmid (a + b\omega)$.

However, $\frac{a+b\omega}{1-\omega} = \frac{1}{3}((2a - b) + (a + b\omega))$ is in $\mathbb{Z}[\omega]$ if and only if $a \equiv -b \pmod{3}$. Thus, we need $a \not\equiv -b \pmod{3}$.

□

This theorem gives us the following corollary which we will use in proving the group structure theorems below.

Corollary 3. *Using the notation as in the previous theorem:*

(1) If π is a factor of a rational prime $p \equiv 1 \pmod{3}$, then

$$|(\mathbb{Z}[\omega]/\langle \pi^n \rangle)^*| = p^n - p^{n-1}.$$

(2) If π is a rational prime $p \equiv 2 \pmod{3}$, then

$$|(\mathbb{Z}[\omega]/\langle p^n \rangle)^*| = p^{2n} - p^{2n-2}.$$

(3) $|\mathbb{Z}[\omega]/\langle (1 - \omega)^n \rangle|^* = 3^n - 3^{n-1}$.

Remark: Note that this corollary agrees with the results that the Φ -function would have given us in the case of the Eisenstein integers.

Now, we are ready to state and prove the unit group structure theorems.

We start with the case that p splits.

Theorem 18. *Suppose that π is an Eisenstein prime such that $\pi\bar{\pi} = p$ for some rational prime $p \equiv 1 \pmod{3}$. Then,*

$$(\mathbb{Z}[\omega]/\langle \pi^n \rangle)^* = \langle g \rangle \cong \mathbb{Z}_{p^n - p^{n-1}},$$

where g is a generator for $(\mathbb{Z}_{p^n})^*$.

Proof. This follows immediately from Theorem 10. □

Now, we consider the case where p is inert.

Theorem 19. *Suppose that $p \equiv 2 \pmod{3}$ is an odd rational prime. Then, there exists $a \in \mathbb{Z}$ and $\beta \in \mathbb{Z}[\omega]$ such that*

$$(\mathbb{Z}[\omega]/\langle p^n \rangle)^* = \langle 1 + p\omega \rangle \times \langle a \rangle \times \langle \beta^{p^{n-1}} \rangle \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Proof. This is proved in exactly the same manner as Theorem 11. □

Since 2 is also inert in $\mathbb{Z}[\omega]$, we state its own structure theorem.

Theorem 20. *Group structure for $(\mathbb{Z}[\omega]/\langle 2^n \rangle)^*$.*

$$(1) (\mathbb{Z}[\omega]/\langle 2 \rangle)^* = \langle \omega \rangle \cong \mathbb{Z}_3.$$

$$(2) (\mathbb{Z}[\omega]/\langle 2^2 \rangle)^* = \langle 1 + 2\omega \rangle \times \langle -\omega \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_6.$$

$$(3) \text{ For } n \geq 4, (\mathbb{Z}[\omega]/\langle 2^n \rangle)^* = \langle 1 + 2\omega \rangle \times \langle 1 + 4\omega \rangle \times \langle -\omega \rangle \\ \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_6.$$

Proof. This is proved as we proved Theorem 12. The main difference is that ω is an element of order 3 for any of the unit groups $(\mathbb{Z}[\omega]/\langle 2^n \rangle)^*$ (so no Hensel lifting is needed). □

Finally, we consider the ramifying case; this occurs for $\langle 3 \rangle = \langle 1 - \omega \rangle^2$.

Theorem 21. *Group structure of $(\mathbb{Z}[\omega]/\langle (1 - \omega)^n \rangle)^*$.*

$$(1) (\mathbb{Z}[\omega]/\langle (1 - \omega) \rangle)^* = \langle -1 \rangle \cong \mathbb{Z}_2.$$

$$(2) (\mathbb{Z}[\omega]/\langle (1 - \omega)^2 \rangle)^* = \langle -\omega \rangle \cong \mathbb{Z}_6.$$

$$(3) (\mathbb{Z}[\omega]/\langle (1 - \omega)^3 \rangle)^* = \langle 1 + 3\omega \rangle \times \langle -\omega \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_6.$$

$$(4) (\mathbb{Z}[\omega]/\langle(1-\omega)^{2m}\rangle)^* = \langle 1+3\omega \rangle \times \langle g \rangle \times \langle -\omega \rangle \cong \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_{2 \cdot 3^{m-1}} \times \mathbb{Z}_3,$$

where g is a generator for $(\mathbb{Z}_{3^m})^*$.

$$(5) (\mathbb{Z}[\omega]/\langle(1-\omega)^{2m+1}\rangle)^* = \langle 1+3\omega \rangle \times \langle g \rangle \times \langle -\omega \rangle \cong \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_{2 \cdot 3^m} \times \mathbb{Z}_3,$$

where g is a generator for $(\mathbb{Z}_{3^{m+1}})^*$.

Proof. This follows immediately from Theorem 15 part 1 (since $d = -3$ and thus $\frac{d}{3} \equiv 2 \pmod{3}$). □

REFERENCES

- [1] J. Cross, The Euler ϕ Function in the Gaussian Integers, *The American Mathematical Monthly*, **90** (1983) 518-528.
- [2] D. Dummit and R. Foote, Abstract Algebra, third ed., John Wiley and Sons, 2003.
- [3] I. Kiming, The Φ Function, 2004, available at http://www.math.ku.dk/~kiming/lecture_notes/2003-2004-algebraic_number_theory_koch/phi.pdf.
- [4] G. Kohler, Eta Products and Theta Series Identities, Springer-Verlag, 2011.
- [5] B. Kutin, Masters Thesis California State University Channel Islands.
- [6] D.A. Marcus, Number Fields, second ed., Springer-Verlag, 1995.
- [7] I. Niven, An Introduction to the Theory of Numbers, John Wiley and Sons, 1991.
- [8] B. Sittinger, Unpublished notes.
- [9] I. Stewart and D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd ed., AK Peters/CRC Press, 2001.
- [10] X. Wang, G. Xu, M. Wang, and X. Meng, Mathematical Foundations of Public Key Cryptography, CRC Press, 2015.