Rose-Hulman Undergraduate Mathematics Journal

Volume 18
Issue 1

Article 5

Giuga's Primality Conjecture for Number Fields

Jamaris Burns
Johnson C. Smith University

Katherine Casey
Cornell University

Duncan Gichimu
Towson University

Kerrek Stinson
Colorado School of Mines

Rose-Hulman Undergraduate Mathematics Journal

Giuga's Primality Conjecture for Number Fields

Jamaris Burns[a] Katherine Casey[b]
Duncan Gichimu[c] Kerrek Stinson[d]

Volume 18, No. 1, Spring 2017

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
mathjournal@rose-hulman.edu
scholar.rose-hulman.edu/rhumj

[a]Johnson C. Smith University
[b]Cornell University
[c]Towson University
[d]Colorado School of Mines

Rose-Hulman Undergraduate Mathematics Journal
Volume 18, No. 1, Spring 2017

Giuga's Primality Conjecture for Number Fields

Jamaris Burns Katherine Casey Duncan Gichimu Kerrek Stinson

Abstract. Giuseppe Giuga conjectured in 1950 that a natural number n is prime if and only if it satisfies the congruence $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$. Progress in validating or disproving the conjecture has been minimal, with the most significant advance being the knowledge that a counter-example would need at least 19,907 digits. To gain new insights into Giuga's conjecture, we explore it in the broader context of number fields. We present a generalized version of the conjecture and prove generalizations of many of the major results related to the conjecture. We introduce the concept of a Giuga ideal and perform computational searches for partial counter-examples to the generalized conjecture. We investigate the relationship between the existence of a counter-example in one number field with the existence of counter-examples in others, with a particular focus on quadratic extensions. This paper lays the preliminary foundation for answering the question: When does the existence of a counter-example in a number field imply the existence of a counter-example in the integers?

Acknowledgements: We wish to thank our advisor Prof. Gregory Johnson for patiently guiding us through this research with such contagious enthusiasm and strong encouragement. This research was conducted during the Summer Undergraduate Applied Mathematics Institute (SUAMI) at Carnegie Mellon University. We are grateful to Prof. Deborah Brandon, the director of SUAMI, for all of her efforts. Funding for SUAMI was provided by the NSA as well as Carnegie Mellon University and its Department of Mathematical Sciences.

1 Introduction

Giuseppe Giuga proposed in 1950:

Conjecture 1.1 (**Giuga's Primality Conjecture** [9])**.** *For all positive integers n, n is prime if and only if*

$$s_n = \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n} \tag{1.1}$$

That n is prime implies the congruence $s_n \equiv -1 \pmod{n}$ follows immediately from Fermat's Little Theorem. However, neither Giuga nor anyone since has been able to prove the converse [3]. Thus, whether (1.1) may provide an alternate definition for a prime number is still unknown. Computational work has determined that no counter-examples with less than 19,907 digits exist [4].

That the conjecture remains open suggests we take another approach for verifying it. Since Euler's day, studying questions about the integers in the more general setting of number fields has been a standard and often helpful approach [19]. Generalizing the conjecture, that is, taking it out of the specific setting of the integers and into a broader context, may ultimately result in greater insights into the conjecture. For example, it is possible that a counter-example could be obtained for the generalized conjecture and then be brought back down to the specific case of the integers. It is with this hope that we proceed.

We generalize the conjecture in terms of ideals of number rings. Following Giuga's approach for the conjecture in the integers, we group the conditions required for an ideal to be a counter-example into two parts: (1) to be a Carmichael ideal and (2) to be a "weak Giuga ideal". Carmichael ideals have been previously studied [18], therefore, a key contribution of this paper is the set of results regarding weak Giuga ideals: their properties, how plentiful they are, where they exist, and when existence in one number field implies existence in another or infinitely many others. We also prove results relating integers and ideals, helping to lay the groundwork for how one could use these generalizations to establish the validity of the original conjecture.

First, to better understand the conjecture, we present some of Giuga's major theorems as well as a useful framework for understanding the nature of counter-examples. While Giuga was unable to prove his conjecture in full, he did prove the following theorem which characterizes positive integers satisfying (1.1).

Theorem 1.2 (Giuga [9])**.** *Let n be a positive integer. Then $s_n \equiv -1 \pmod{n}$ if and only if the following two properties hold:*

(C) $p - 1 \mid \frac{n}{p} - 1$ *for all* $p \mid n$,

(WG) $p \mid \frac{n}{p} - 1$ *for all* $p \mid n$.

Note that an integer satisfying condition **(WG)** must be square-free. A counter-example to the conjecture would therefore minimally need to be both square-free and composite. A number with these properties that additionally satisfies condition **(C)** is a *Carmichael number*, according to Korselt's Criterion [13].

Remark. Sometimes **(C)** is written as $p-1 \mid n-1$ for all $p \mid n$. To see that these conditions are equivalent, suppose $n = pk$. Then we may express $n-1$ as follows:

$$n - 1 = pk - 1 = (p-1)k + k - 1$$

This means that if $p-1 \mid n-1$, $p-1$ must divide $k-1$. Noting that by definition $k = n/p$, we may conclude that $p-1 \mid n-1 \implies p-1 \mid n/p-1$. It is easy to show that $p-1 \mid n/p-1 \implies p-1 \mid n-1$, therefore $p-1 \mid n-1 \iff p-1 \mid n/p-1$.

All Carmichael numbers are odd, and it is known that infinitely many Carmichael numbers exist [2]. The three smallest Carmichael numbers are 561, 1105, and 1729.

We introduce the following definition to characterize composite numbers satisfying condition **(WG)**.

Definition 1.3. We say that a positive composite integer n is a *weak Giuga number* to mean that n satisfies $p \mid \frac{n}{p} - 1$ for all prime $p \mid n$.

The three smallest weak Giuga numbers are 30, 858, and 1722 [5]. It is not known whether there are infinitely many weak Giuga numbers or any odd weak Giuga numbers. With a view toward finding counter-examples, we may now restate Giuga's conjecture:

Corollary 1.4 (**Counter-Example Conjecture**, [3])**.** *A composite integer n satisfies $s_n \equiv -1 \pmod{n}$ if and only if n is both a Carmichael number and a weak Giuga number.*

In light of Theorem 1.2, we characterize a counter-example with the following definition:

Definition 1.5. We say that n is a *strong Giuga number* to mean that the following condition holds:

(SG) The integer n is composite and satisfies conditions **(C)** and **(WG)**, that is, n is both a Carmichael number and a weak Giuga number.

Consequently, strong Giuga numbers are precisely the counter-examples to Giuga's conjecture.

Since much is known about Carmichael numbers [2, 7, 10, 12, 14, 15, 17], the investigation into the existence of strong Giuga numbers centers around understanding weak Giuga numbers better. Notably, if it could be shown that there are no odd weak Giuga numbers, then Giuga's conjecture would hold.

In Section 3, we will generalize all of the above results.

The following theorem presents two useful characterizations of weak Giuga numbers proved by Giuga himself. Theorems 4.1 and 4.2 will generalize these characterizations in the number field setting.

Theorem 1.6 (**Weak Giuga Equivalences**, [9])**.** *Let n be a square-free positive integer with prime decomposition $n = p_1 p_2 \cdots p_k$, and let $\varphi(n)$ be the Euler phi function. Then the following are equivalent:*

1. n is a weak Giuga number
2. $\displaystyle\sum_{i=1}^{n} i^{\varphi(n)} \equiv -1 \pmod{n}$
3. $\displaystyle\sum_{i=1}^{k} \frac{1}{p_i} - \prod_{i=1}^{k} \frac{1}{p_i} \in \mathbb{N}$

The remainder of this paper is outlined as follows: In Section 2, we will introduce the essential mathematical background for the rest of the paper, in case the reader may be unfamiliar with algebraic number theory. In Section 3, we generalize the conjecture and establish properties for partial and full counter-examples to the generalized conjecture. Section 4 focuses on equivalences and examples of partial counter-examples to the conjecture. We continue in Section 5 with the development of a correspondence between partial counter-examples in the number field setting and partial counter-examples in the integers. We also define an association between partial counter-examples so that the existence of one counter-example may be used to help find more counter-examples. Section 6 focuses on partial and full counter-examples in the context of quadratic extensions. Finally, Section 7 provides some possible routes for future research. Appendix A contains the essential parts of the code used to generate partial counter-examples, and Appendix B provides complete lists of the partial counter-examples found.

2 Mathematical Background

This section introduces notation and basic results from algebraic number theory used throughout the paper. Those readers already familiar with algebraic number theory may wish to skip this section and only refer back to the appropriate subsections as needed.

We will be presenting the bare minimum of algebraic number theory concepts required to follow our results. The enthusiastic reader wishing to obtain a deeper understanding of algebraic number theory is referred to the text by Alaca and Williams [1] and additionally to

the "Preliminary Reading" and "Lecture Notes" sections of the University of Oxford Mathematical Institute's Algebraic Number Theory course materials [20]. For a good reference in algebra, see the text by Dummit and Foote [6].

To generalize from the integers $\mathbb{Z}$, we must determine of which mathematical structure the integers are a specific instance. Formally, $\mathbb{Z}$ is the *number ring* (also called *ring of (algebraic) integers*) for the *number field* $\mathbb{Q}$, the rationals.

Definition 2.1. A *number field* (or *algebraic number field*) K is a field containing $\mathbb{Q}$ such that when viewing K as a vector space over $\mathbb{Q}$, the dimension is finite.

Example 2.2. Examples of number fields include $\mathbb{Q}(i)$, $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$, and $\mathbb{Q}\Big(\sqrt[3]{1+\sqrt{2}}+\sqrt[3]{1-\sqrt{2}},\sqrt{53}+\sqrt[3]{5}\Big)$.

Definition 2.3. If R is a ring, then $R[x]$ represents the set of polynomials in the variable x with coefficients in R. We say that $\alpha \in K$ is an *algebraic integer* to mean that there exists a monic polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$.

Definition 2.4. A *number ring* $\mathcal{O}_K$ is the set of all algebraic integers in a number field K.

Example 2.5. Examples of number rings include: $\mathbb{Z}(i)$, $\mathbb{Z}\big(\sqrt{3}\big)$, and $\mathbb{Z}\Big(\frac{-1+\sqrt{-3}}{2}\Big)$.

For simplicity, we will let the symbol $\mathfrak{o}$ represent $\mathcal{O}_K$. In the case that we are considering two (potentially distinct) number fields, K and K', we will let $\mathfrak{o}' = \mathcal{O}_{K'}$.

One might think that the number rings of various number fields form the natural setting for our generalization. However, the integers have special properties not always found in number rings. If, for example, we were to use the number ring $\mathbb{Z}(\sqrt{-5})$, we would encounter the unexpected fact that unique factorization does not exist there:

Example 2.6. In $\mathbb{Z}(\sqrt{-5})$, we can factor 6 into two distinct products of irreducible elements: $6 = 2(3)$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Thus we need unique factorization to be a characteristic of whatever setting we choose for generalizing. Environments with unique factorization as a feature are called *Unique Factorization Domains* (UFDs). While number rings are not always UFDs, they are *Dedekind domains*.

Proposition 2.7. *Let $\mathfrak{o}$ be a Dedekind Domain. Then the following hold:*

1. *Every proper nonzero ideal $\mathfrak{a} \subset \mathfrak{o}$ factors uniquely into a product of prime ideals.*
2. *Every prime ideal $\mathfrak{p} \subset \mathfrak{o}$ is maximal, and the residue field $\mathfrak{o}/\mathfrak{p}$ is* finite of characteristic *p where $\mathfrak{p} \cap \mathfrak{o} = p\mathbb{Z}$. (To be* finite of characteristic *p means that for all $a \in \mathfrak{o}/\mathfrak{p}$, $pa = 0$.)*

Since every Dedekind domain has the property that *ideals* have unique factorization, the natural generalization of Giuga's conjecture is in terms of ideals. To help develop a better understanding of ideals, we list some definitions and examples below:

Definition 2.8. (Ideal) An *ideal* $\mathfrak{n}$ of an integral domain (Dedekind domains are integral domains with special properties) D is a nonempty subset of D having the following two properties:

1. $\alpha \in \mathfrak{n}, \beta \in \mathfrak{n} \implies \alpha + \beta \in \mathfrak{n}$,

2. $\alpha \in \mathfrak{n}, \delta \in D \implies \delta\alpha \in \mathfrak{n}$

Example 2.9. If $\{a_1, \ldots, a_n\}$ is a set of elements of the integral domain D, then the set of all finite linear combinations of $a_1, \ldots, a_n$

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in D \right\}$$

is an ideal of D, which we denote by $\langle a_1, \ldots, a_n \rangle$.

Definition 2.10. (Principal Ideal) An ideal $\mathfrak{n}$ of an integral domain D is called a *principal ideal* if there exists an element $a \in \mathfrak{n}$ such that $\mathfrak{n} = \langle a \rangle$. The element a is called a generator of the ideal $\mathfrak{n}$.

Example 2.11. The ideal $8\mathbb{Z}$, also written $\langle 8 \rangle$, consists of all multiples of 8 in the integers.

Definition 2.12. An ideal $\mathfrak{n}$ of an integral domain D is called a *proper ideal* of D if $\mathfrak{n} \neq \langle 0 \rangle$, $\langle 1 \rangle$.

Definition 2.13. A proper ideal $\mathfrak{m}$ of an integral domain D is called a *maximal ideal* if whenever $\mathfrak{n}$ is an ideal of D such that $\mathfrak{m} \subseteq \mathfrak{n} \subseteq D$ then $\mathfrak{n} = \mathfrak{m}$ or $\mathfrak{n} = D$.

Definition 2.14. The ideal $\mathfrak{p}$ is a *prime ideal* if given $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Example 2.15. In $\mathbb{Z}$, an ideal generated by a prime number is a prime ideal.

Definition 2.16. (Product of Ideals) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathfrak{o}$. The *product* of $\mathfrak{a}$ and $\mathfrak{b}$, denoted by $\mathfrak{ab}$, is the set of all finite sums of elements of the form ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

Definition 2.17. (Divisibility of Ideals) Let D be a Dedekind domain. Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals of D. We say that $\mathfrak{a}$ *divides* $\mathfrak{b}$, written $\mathfrak{a} \mid \mathfrak{b}$, if there exists an ideal $\mathfrak{c}$ of D such that $\mathfrak{b} = \mathfrak{ac}$.

2.1 Arithmetic Modulo Ideals

Since our generalization is in terms of ideals, and the original conjecture involved arithmetic modulo integers, it is natural that arithmetic modulo ideals should play a significant role in this paper.

Definition 2.18. Given a ring $\mathfrak{o}$, an ideal $\mathfrak{n} \subset \mathfrak{o}$, and a, $b \in \mathfrak{o}$, we write $a \equiv b \pmod{\mathfrak{n}}$ to mean that $a - b \in \mathfrak{n}$.

Definition 2.19. The *quotient ring* $\mathfrak{o}/\mathfrak{n}$ for a ring $\mathfrak{o}$ is a ring of equivalence classes modulo $\mathfrak{n}$. For example when $\mathfrak{n} = 2\mathbb{Z}$ (the even integers), the quotient ring $\mathbb{Z}/2\mathbb{Z}$ consists of the integers 0 and 1, with even numbers getting mapped to 0 and odd numbers getting mapped to 1.

Definition 2.20. We say that a subset $R_\mathfrak{n} \subseteq \mathfrak{o}$ is a *complete set of residues modulo* $\mathfrak{n}$ if the natural map $R_\mathfrak{n} \to \mathfrak{o}/\mathfrak{n}$ is a bijection. (By *natural map*, sometimes *canonical map*, we refer to the map that is both easy to define and apparent given the domain and codomain.)

2.2 Norms of Ideals

Working with norms of ideals allows us to obtain an integer value associated with an ideal—this property proves to be essential in generalizing the conjecture and characterizing its counter-examples.

Definition 2.21. The *norm of an ideal*, $N(\mathfrak{n}) = |\mathfrak{o}/\mathfrak{n}|$ is the order of (number of elements in) the quotient ring $\mathfrak{o}/\mathfrak{n}$. It can be shown that $N(\mathfrak{n}) \in \mathfrak{n}$.

Let $I_\mathfrak{a}$ be a complete set of *nonzero* residues of $\mathfrak{o}/\mathfrak{a}$. If $\mathfrak{a}$ is prime, this set forms a multiplicative group with order $N(\mathfrak{a}) - 1$. Note that as with any group, when an element of the group is raised to the order of the group, the result is equal to the identity element of the group, in our case, 1. This fact will be used several times in the proofs in this paper.

Definition 2.22. For a prime ideal $\mathfrak{p} \subset \mathfrak{o}$, we call the unique prime $p \in \mathbb{Z}$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ the *prime (lying) below* $\mathfrak{p}$.

Note that for a prime ideal $\mathfrak{p}$, $N(\mathfrak{p})$ is necessarily a power of p since $\mathfrak{o}/\mathfrak{p}$ has characteristic p. The characteristic of $\mathfrak{o}/\mathfrak{p}$ also tells us that $p \in \mathfrak{p}$.

Theorem 2.23. (See pages 229-231 of the text by Alaca and Williams [1] for a proof.) *Let* $\mathfrak{n}$ *and* $\mathfrak{m}$ *be nonzero ideals in* $\mathfrak{o}$*, then:*

$$N(\mathfrak{nm}) = N(\mathfrak{n})N(\mathfrak{m})$$

2.3 Chinese Remainder Theorem

Later in this paper we will use the standard Chinese Remainder Theorem to find a solution to a system of congruences modulo integers. We will also use a generalized version of the Chinese Remainder Theorem to find a solution to a system of congruences modulo ideals.

Theorem 2.24. *Let $m_1, m_2, \ldots, m_r$ be positive integers that are relatively prime in pairs, that is, $gcd(m_i, m_j) = 1$ if $i \neq j$. Then for any integers $a_1, a_2, \ldots, a_r$, the r congruences*

$$x \equiv a_i \pmod{m_i} \qquad (i = 1, 2, \ldots, r)$$

have a common solution, and any two solutions are congruent modulo the product $m_1 m_2 \cdots m_r$.

Theorem 2.25 (**Chinese Remainder Theorem for Ideals**, [1, p. 213])**.** *Let D be a Dedekind domain. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ be pairwise relatively prime ideals of D. Let $\alpha_1, \ldots, \alpha_k$ be elements of D. Then there exists $\alpha \in D$ such that*

$$\alpha \equiv \alpha_i \pmod{\mathfrak{a}_i}, \qquad i = 1, 2, \ldots, k.$$

3 Generalized Conjecture and Characterization

We begin to implement our strategy for discovering more about this conjecture, and ultimately about the nature of prime numbers, by generalizing most of the results from Section 1 (results 1.1-1.5). We also introduce the definitions of weak and strong Giuga ideals and prove results about their properties.

Conjecture 3.1 (**Generalized Conjecture**)**.** *For any ideal $\mathfrak{n}$ of $\mathfrak{o}$, define $I_\mathfrak{n}$ to be a complete set of* nonzero *residues of $\mathfrak{o}/\mathfrak{n}$ (including zero in the residues does not affect the validity of the conjecture, but it would make subsequent proofs less straightforward). Then $\mathfrak{n}$ is a prime ideal if and only if*

$$\sigma_\mathfrak{n} = \sum_{x \in I_\mathfrak{n}} x^{N(\mathfrak{n})-1} \equiv -1 \pmod{\mathfrak{n}}$$

It can be shown that when $\mathfrak{o} = \mathbb{Z}$, this generalized conjecture reduces to the original conjecture. As with the original conjecture, that $\mathfrak{n}$ is a prime ideal implies the congruence $\sigma_\mathfrak{n} \equiv -1 \pmod{\mathfrak{n}}$ follows trivially. We focus on answering the question: Can there exist composite ideals $\mathfrak{n}$ such that $\sigma_\mathfrak{n} \equiv -1 \pmod{\mathfrak{n}}$?

Before generalizing Theorem 1.2, we need to prove two lemmas. The analog in the elementary setting of the first lemma was crucial to proving Theorem 1 in the paper by Borwein and Wong [5].

Lemma 3.2. *Let $I_\mathfrak{p}$ be a complete set of nonzero residues of $\mathfrak{o}/\mathfrak{p}$. For all ideals $\mathfrak{n} \subset \mathfrak{o}$ and prime ideals $\mathfrak{p} \mid \mathfrak{n}$,*

$$\sigma_\mathfrak{n}^\mathfrak{p} \coloneqq \sum_{x \in I_\mathfrak{p}} x^{N(\mathfrak{n})-1} \equiv \begin{cases} -1 \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1 \\ 0 \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p})-1 \nmid N(\mathfrak{n})-1 \end{cases}$$

Proof. First, observe that if $N(\mathfrak{n})-1 = k(N(\mathfrak{p})-1)$ for some $k \in \mathbb{Z}$, then substituting this into the summation $\sum_{x \in I_\mathfrak{p}} x^{N(\mathfrak{n})-1}$, we obtain

$$\sum_{x \in I_\mathfrak{p}} x^{k(N(\mathfrak{p})-1)} \tag{3.1}$$

Because $I_\mathfrak{p}$ is a multiplicative group, any element raised to the order of this group, $N(\mathfrak{p})-1$, is equal to 1:

$$(3.1) \equiv \sum_{x \in I_\mathfrak{p}} 1^k \equiv \sum_{x \in I_\mathfrak{p}} 1 \equiv N(\mathfrak{p}) - 1 \equiv -1 \pmod{\mathfrak{p}}$$

Conversely, if $N(\mathfrak{p})-1 \nmid N(\mathfrak{n})-1$ then $N(\mathfrak{n})-1 = k(N(\mathfrak{p})-1)+\ell$ for some $k, \ell \in \mathbb{Z}$ with $0 < \ell < N(\mathfrak{p})-1$. Since $\mathfrak{p}$ is prime, and hence by (2) in Proposition 2.7 is a maximal ideal of $\mathfrak{o}$, $\mathfrak{o}/\mathfrak{p}$ is a *finite field* (that is, $\mathfrak{o}/\mathfrak{p}$ is a field that contains only a finite number of elements). Being a finite field implies that $\mathfrak{o}/\mathfrak{p}$ has a primitive root, that is, an element, which we will call g, such that:

$$\{g^i \pmod{\mathfrak{p}} : 0 \le i < N(\mathfrak{p})-1\} = \{\text{the set of nonzero elements of } \mathfrak{o}/\mathfrak{p}\}$$

Using g, we can rewrite our summation $\sum_{x \in I_\mathfrak{p}} x^{N(\mathfrak{n})-1}$ as:

$$\sum_{i=0}^{N(\mathfrak{p})-2} (g^i)^{N(\mathfrak{n})-1} \tag{3.2}$$

Substituting in our expression for $N(\mathfrak{n})-1$:

$$(3.2) \equiv \sum_{i=0}^{N(\mathfrak{p})-2} (g^i)^{k(N(\mathfrak{p})-1)+\ell} \equiv \sum_{i=0}^{N(\mathfrak{p})-2} (g^i)^{k(N(\mathfrak{p})-1)} (g^i)^\ell \pmod{\mathfrak{p}} \tag{3.3}$$

Again, since $I_\mathfrak{p}$ is a group:

$$\begin{aligned} (3.3) &\equiv \sum_{i=0}^{N(\mathfrak{p})-2} 1^k (g^i)^\ell \pmod{\mathfrak{p}} \\ &\equiv 1 + g^\ell + g^{2\ell} + \cdots + g^{(N(\mathfrak{p})-2)\ell} \pmod{\mathfrak{p}} \end{aligned} \tag{3.4}$$

Now, because $|I_{\mathfrak{p}}| = N(\mathfrak{p}) - 1$ and $g^{\ell} \not\equiv 0 \pmod{\mathfrak{p}}$, we have:

$$g^{(N(\mathfrak{p})-1)\ell} - 1 \equiv 0 \pmod{\mathfrak{p}}. \tag{3.5}$$

We note that (3.5) can be expressed as a product of $(g^{\ell} - 1)$ and (3.4):

$$g^{(N(\mathfrak{p})-1)\ell} - 1 = (1 + g^{\ell} + g^{2\ell} + \cdots + g^{(N(\mathfrak{p})-2)\ell})(g^{\ell} - 1)$$

thus

$$(1 + g^{\ell} + g^{2\ell} + \cdots + g^{(N(\mathfrak{p})-2)\ell})(g^{\ell} - 1) \equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathfrak{o}/\mathfrak{p}$ is an integral domain and therefore has no zero divisors, either $(1 + g^{\ell} + g^{2\ell} + \cdots + g^{(N(\mathfrak{p})-2)\ell})$ or $(g^{\ell} - 1)$ must be congruent to $0 \pmod{\mathfrak{p}}$.

Because g is a primitive root and $0 < \ell < N(\mathfrak{p}) - 1$, we have: $g^{\ell} - 1 \not\equiv 0 \pmod{\mathfrak{p}}$. We may thus conclude that

$$1 + g^{\ell} + g^{2\ell} + \cdots + g^{(N(\mathfrak{p})-2)\ell} \equiv 0 \pmod{\mathfrak{p}}$$

and therefore that $\sigma_{\mathfrak{n}}^{\mathfrak{p}} \equiv 0 \pmod{\mathfrak{p}}$.

□

Before stating our second lemma, we first introduce some notation. For an ideal $\mathfrak{n} \subset \mathfrak{o}$, given $\mathfrak{p}$ a prime ideal and $\mathfrak{p} \mid \mathfrak{n}$, we define $\mathfrak{n}_{\mathfrak{p}} \coloneqq \mathfrak{n}\mathfrak{p}^{-1}$, that is, $\mathfrak{n} = \mathfrak{p}\mathfrak{n}_{\mathfrak{p}}$. Similarly, we define $n_p \coloneqq np^{-1}$ for $n \in \mathbb{Z}$, where p is a prime divisor of n.

Lemma 3.3. *Let $\mathfrak{n}$ be an ideal of $\mathfrak{o}$. Let $\mathfrak{p}$ be a prime ideal which divides $\mathfrak{n}$, and let μ be a non-negative integer. Then:*

$$\sum_{x \in I_{\mathfrak{n}}} x^{\mu} \equiv N(\mathfrak{n}_{\mathfrak{p}}) \sum_{x \in I_{\mathfrak{p}}} x^{\mu} \pmod{\mathfrak{p}} \tag{3.6}$$

Proof. For simplicity, we will first prove the following congruence:

$$\sum_{x \in \mathfrak{o}/\mathfrak{n}} x^{\mu} \equiv N(\mathfrak{n}_{\mathfrak{p}}) \sum_{x \in \mathfrak{o}/\mathfrak{p}} x^{\mu} \pmod{\mathfrak{p}} \tag{3.7}$$

Consider the natural map $\pi : \mathfrak{o}/\mathfrak{n} \to \mathfrak{o}/\mathfrak{p}$. This map sends an element $a \pmod{\mathfrak{n}}$ to the element $a \pmod{\mathfrak{p}}$. By the *First Isomorphism Theorem* (for more background and a proof of this theorem, see Theorem 7 on page 243 of the text by Dummit and Foote [6]), we have the relationship $(\mathfrak{o}/\mathfrak{n})/\ker \pi \simeq \mathfrak{o}/\mathfrak{p}$. From this, we know that there will be $N(\mathfrak{p})$ cosets of $\ker \pi$ since $N(\mathfrak{p})$ is the order of $\mathfrak{o}/\mathfrak{p}$ and the cosets of $\ker \pi$ are the fibers of π. We may therefore decompose the left-hand sum of (3.7) according to cosets of $\ker \pi$, which we will denote $c_1, \ldots, c_{N(\mathfrak{p})}$, as follows:

$$\sum_{x \in \mathfrak{o}/\mathfrak{n}} x^{\mu} = \sum_{x \in c_1} x^{\mu} + \cdots + \sum_{x \in c_{N(\mathfrak{p})}} x^{\mu} \tag{3.8}$$

To determine how many elements are in each of the coset sums, recall that $\mathfrak{n} = \mathfrak{p}\mathfrak{n}_\mathfrak{p}$. Since the original sum (the left-hand side of (3.8)) has $N(\mathfrak{n})$ elements, and there are $N(\mathfrak{p})$ cosets, there are

$$\frac{N(\mathfrak{n})}{N(\mathfrak{p})} \tag{3.9}$$

elements in each coset. Since $\mathfrak{n} = \mathfrak{p}\mathfrak{n}_\mathfrak{p}$, we can apply Theorem 2.23 to $N(\mathfrak{n})$ to obtain:

$$N(\mathfrak{n}) = N(\mathfrak{p})N(\mathfrak{n}_\mathfrak{p})$$

and therefore rewrite (3.9):

$$\frac{N(\mathfrak{n})}{N(\mathfrak{p})} = \frac{N(\mathfrak{p})N(\mathfrak{n}_\mathfrak{p})}{N(\mathfrak{p})} = N(\mathfrak{n}_\mathfrak{p})$$

Thus every sum on the right-hand side of (3.8) will have $N(\mathfrak{n}_\mathfrak{p})$ elements.

We will now walk through the action of π on the right-hand side of (3.8):

$$\sum_{x\in c_1} x^\mu + \cdots + \sum_{x\in c_{N(\mathfrak{p})}} x^\mu \equiv \pi\left(\sum_{x\in c_1} x^\mu + \cdots + \sum_{x\in c_{N(\mathfrak{p})}} x^\mu\right) \pmod{\mathfrak{p}} \tag{3.10}$$

Since π is a ring homomorphism:

$$(3.10) \equiv \ \pi\left(\sum_{x\in c_1} x^\mu\right) + \cdots + \pi\left(\sum_{x\in c_{N(\mathfrak{p})}} x^\mu\right) \pmod{\mathfrak{p}} \tag{3.11}$$

For each term in the coset sums, by the ring homomorphism, provided that μ is a non-negative integer, we also have:

$$\pi(x^\mu) = \pi(x)^\mu \equiv x^\mu \pmod{\mathfrak{p}}$$

Therefore we have the equivalence:

$$(3.11) \equiv \sum_{x\in c_1} x^\mu + \cdots + \sum_{x\in c_{N(\mathfrak{p})}} x^\mu \pmod{\mathfrak{p}} \tag{3.12}$$

Since every sum on the right-hand side of (3.12) has $N(\mathfrak{n}_\mathfrak{p})$ elements:

$$\sum_{x\in c_1} x^\mu + \cdots + \sum_{x\in c_{N(\mathfrak{p})}} x^\mu \pmod{\mathfrak{p}} \equiv \ N(\mathfrak{n}_\mathfrak{p})\left(x_{c_1}^\mu + \cdots + x_{c_{N(\mathfrak{p})}}^\mu\right) \pmod{\mathfrak{p}} \tag{3.13}$$

where x_{c_i} is an element from the coset c_i.

Since $\mathfrak{o}/\mathfrak{p}$ is a complete set of representatives from each coset of $\ker \pi$, we have:

$$(3.13) \equiv \quad N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in \mathfrak{o}/\mathfrak{p}} x^\mu \pmod{\mathfrak{p}} \tag{3.14}$$

And thus, since

$$\sum_{x \in \mathfrak{o}/\mathfrak{n}} x^\mu \equiv (3.10) \equiv (3.11) \equiv (3.12) \equiv (3.13) \equiv (3.14)$$

we can conclude:

$$\sum_{x \in \mathfrak{o}/\mathfrak{n}} x^\mu \equiv N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in \mathfrak{o}/\mathfrak{p}} x^\mu \pmod{\mathfrak{p}} \tag{3.15}$$

Finally, we note that the difference between $\mathfrak{o}/\mathfrak{n}$ and $I_\mathfrak{n}$ is that $\mathfrak{o}/\mathfrak{n}$ contains a zero term, but since this has no effect on the sum, we can replace the sum $\sum_{x \in \mathfrak{o}/\mathfrak{n}} x^\mu$ in (3.15) with the sum $\sum_{x \in I_\mathfrak{n}} x^\mu$. Similarly, since the $N(\mathfrak{n}_\mathfrak{p})$ instances of the zero term in $\mathfrak{o}/\mathfrak{p}$ will not affect the overall sum, we can replace the sum $\sum_{x \in \mathfrak{o}/\mathfrak{p}} x^\mu$ with the sum $\sum_{x \in I_\mathfrak{p}} x^\mu$, and so obtain:

$$\sum_{x \in I_\mathfrak{n}} x^\mu \equiv N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in I_\mathfrak{p}} x^\mu \pmod{\mathfrak{p}}$$

as desired. □

We can now proceed to prove the generalization of Theorem 1.2.

Theorem 3.4 (**Generalized Characterization**). *Let* $\mathfrak{n}$ *be an ideal of* $\mathfrak{o}$. *Then* $\sigma_\mathfrak{n} \equiv -1 \pmod{\mathfrak{n}}$ *if and only if the following two properties hold:*

(CI) $N(\mathfrak{p}) - 1 \mid N(\mathfrak{n}_\mathfrak{p}) - 1$ *for all* $\mathfrak{p} \mid \mathfrak{n}$,

(WGI) $N(\mathfrak{n}_\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$ *for all* $\mathfrak{p} \mid \mathfrak{n}$.

Proof. We will first employ our lemmas to establish a useful setup. From Lemma 3.2, we have for any prime ideal $\mathfrak{p} \mid \mathfrak{n}$:

$$\sum_{x \in I_\mathfrak{p}} x^{N(\mathfrak{n})-1} \equiv \begin{cases} -1 \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p}) - 1 \mid N(\mathfrak{n}) - 1 \\ 0 \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p}) - 1 \nmid N(\mathfrak{n}) - 1 \end{cases}$$

Multiplying through by $N(\mathfrak{n}_\mathfrak{p})$ and applying Lemma 3.3, we obtain:

$$N(\mathfrak{n}_\mathfrak{p})\sigma_\mathfrak{n}^\mathfrak{p} = N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in I_\mathfrak{p}} x^{N(\mathfrak{n})-1} \equiv \begin{cases} (-1)N(\mathfrak{n}_\mathfrak{p}) \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p}) - 1 \mid N(\mathfrak{n}) - 1 \\ (0)N(\mathfrak{n}_\mathfrak{p}) \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p}) - 1 \nmid N(\mathfrak{n}) - 1 \end{cases}$$

Simplifying:

$$\sigma_{\mathfrak{n}} = \sum_{x \in I_{\mathfrak{n}}} x^{N(\mathfrak{n})-1} \equiv \begin{cases} -N(\mathfrak{n}_{\mathfrak{p}}) \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1 \\ 0 \pmod{\mathfrak{p}} & \text{if } N(\mathfrak{p})-1 \nmid N(\mathfrak{n})-1 \end{cases} \tag{3.16}$$

Now, suppose $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{n}}$. Then $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p} \mid \mathfrak{n}$. Using (3.16), we conclude that for all $\mathfrak{p} \mid \mathfrak{n}$, $N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1$ and

$$\sigma_{\mathfrak{n}} \equiv -N(\mathfrak{n}_{\mathfrak{p}}) \pmod{\mathfrak{p}}.$$

From our initial assumption, it follows that $1 \equiv N(\mathfrak{n}_{\mathfrak{p}}) \pmod{\mathfrak{p}}$. Hence **(WGI)** is satisfied.

To see that condition **(CI)** is satisfied, note that since by Theorem 2.23, $N(\mathfrak{n}) = N(\mathfrak{p})N(\mathfrak{n}_{\mathfrak{p}})$, we can write:

$$N(\mathfrak{n}) - 1 = N(\mathfrak{n}_{\mathfrak{p}})(N(\mathfrak{p})-1) + N(\mathfrak{n}_{\mathfrak{p}}) - 1 \tag{3.17}$$

Since we already know that $N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1$, it follows that $N(\mathfrak{p})-1 \mid N(\mathfrak{n}_{\mathfrak{p}})-1$, as desired.

Conversely, suppose $\mathfrak{n}$ is an ideal of $\mathfrak{o}$ satisfying conditions **(CI)** and **(WGI)**. Since $N(\mathfrak{p})-1 \mid N(\mathfrak{n}_{\mathfrak{p}})-1$, it can be easily shown from equation (3.17) that $N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1$. Hence $\sigma_{\mathfrak{n}} \equiv -N(\mathfrak{n}_{\mathfrak{p}}) \pmod{\mathfrak{p}}$. Since $N(\mathfrak{n}_{\mathfrak{p}}) \equiv 1 \pmod{\mathfrak{p}}$, $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{p}}$.

If we can show that $\mathfrak{n}$ is square-free, then we can conclude that $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{n}}$ as desired, by the Chinese Remainder Theorem for Ideals (Theorem 2.25). This is because by being square-free, $\mathfrak{n}$ will be a product of distinct prime ideals $\mathfrak{p}$, and $-1 \pmod{\mathfrak{n}}$ will be a solution to every congruence $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{p}}$ due to the natural map π mentioned in the proof of Lemma 3.3 which maps $a \pmod{\mathfrak{n}}$ to $a \pmod{\mathfrak{p}}$.

Assume for the sake of contradiction that $\mathfrak{n}$ is not square-free. Then for some $\mathfrak{p} \mid \mathfrak{n}$ we have $\mathfrak{n} = \mathfrak{p}\mathfrak{n}_{\mathfrak{p}}$ with $\mathfrak{p} \mid \mathfrak{n}_{\mathfrak{p}}$. This then implies that $N(\mathfrak{p}) \mid N(\mathfrak{n}_{\mathfrak{p}})$. But since $N(\mathfrak{p}) \in \mathfrak{p}$, we have $N(\mathfrak{n}_{\mathfrak{p}}) \in \mathfrak{p}$ as well, contradicting the assumption that $N(\mathfrak{n}_{\mathfrak{p}}) - 1 \in \mathfrak{p}$. Thus $\mathfrak{n}$ must be square-free. □

As in the elementary case, we note that any square-free, composite ideal satisfying condition **(CI)** is known as a *Carmichael ideal* [18] (by a similar argument to the one for the Carmichael number condition equivalence, it can be shown that **(CI)** is equivalent to $N(\mathfrak{p})-1 \mid N(\mathfrak{n})-1$). Furthermore, we generalize the notion of a weak Giuga number by calling an ideal satisfying condition **(WGI)** a weak Giuga ideal.

We have the following corollary, generalizing Corollary 1.4:

Corollary 3.5. *A composite ideal $\mathfrak{n} \subset \mathfrak{o}$ satisfies $\sigma_{\mathfrak{n}} \equiv -1 \pmod{\mathfrak{n}}$ if and only if $\mathfrak{n}$ is both a Carmichael ideal and a weak Giuga ideal.*

3.1 Weak Giuga Ideals

We provide the definition of a weak Giuga ideal, for reference:

Definition 3.6 (**Weak Giuga Ideal**)**.** We say that a composite ideal $\mathfrak{n} \subset \mathfrak{o}$ is a *weak Giuga ideal* to mean that $\mathfrak{n}$ satisfies $N(\mathfrak{n}_\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p} \mid \mathfrak{n}$.

We will now prove a number of important results about the nature of weak Giuga ideals. Note that as in the elementary setting, weak Giuga ideals are also square-free:

Theorem 3.7. *If $\mathfrak{n} \subset \mathfrak{o}$ is a weak Giuga ideal, then for any prime factors $\mathfrak{p}, \mathfrak{q}$ of $\mathfrak{n}$, $\mathfrak{p} \neq \mathfrak{q}$.*

Proof. Assume for the sake of contradiction that $\mathfrak{n} \subset \mathfrak{o}$ is a product of distinct primes, save one prime, $\mathfrak{q}$, which is squared. For $\mathfrak{n}$ to be a weak Giuga ideal, we need $N(\mathfrak{n}_\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p} \mid \mathfrak{n}$. Because there are two copies of $\mathfrak{q}$ in $\mathfrak{n}$, $\mathfrak{n}_\mathfrak{q}$ will have $\mathfrak{q}$ as a factor, and so $N(\mathfrak{n}_\mathfrak{q})$ will have $N(\mathfrak{q})$ as a factor. Since the norm of an ideal is an element of the ideal, $N(\mathfrak{q}) \in \mathfrak{q}$, and thus $N(\mathfrak{n}_\mathfrak{q}) \equiv 0 \pmod{\mathfrak{q}}$. Therefore, $\mathfrak{n}$ cannot be a weak Giuga ideal. We may thus conclude that a weak Giuga ideal must be square-free. □

As we shall see below, the norm of a weak Giuga ideal is also square-free.

Theorem 3.8. *If $\mathfrak{n} \subset \mathfrak{o}$ is a weak Giuga ideal, then $N(\mathfrak{p}) \neq N(\mathfrak{q})$ for any prime factors $\mathfrak{p}, \mathfrak{q}$ of $\mathfrak{n}$.*

Proof. We will prove by contradiction. Let $\mathfrak{n} \subset \mathfrak{o}$ be composed of distinct prime factors, including $\mathfrak{p}$ and $\mathfrak{q}$, where $N(\mathfrak{p}) = N(\mathfrak{q})$. Since $N(\mathfrak{p}) \in \mathfrak{p}$, $N(\mathfrak{q}) \in \mathfrak{p}$ as well. Thus $N(\mathfrak{n}_\mathfrak{p})$ will still contain an element of $\mathfrak{p}$, so $N(\mathfrak{n}_\mathfrak{p}) \equiv 0 \pmod{\mathfrak{p}}$. Therefore $\mathfrak{n}$ will not be a weak Giuga ideal. So, to be a weak Giuga ideal, each prime factor must have a distinct norm. □

The following corollary will be needed to prove Theorem 5.5.

Corollary 3.9. *If $\mathfrak{n} \subset \mathfrak{o}$ is a weak Giuga ideal, then $\mathfrak{n}$ is a product of non-conjugate primes of $\mathfrak{o}$.*

Proof. Suppose we let $\mathfrak{n} \subset \mathfrak{o}$ be an ideal with $\mathfrak{p}$ a prime factor and $\mathfrak{p}$'s conjugate, $\bar{\mathfrak{p}}$, a prime factor of $\mathfrak{n}$ as well. The distinct prime ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ will have the same norm value, that is, $N(\mathfrak{p}) = N(\bar{\mathfrak{p}})$. Therefore, by Theorem 3.8, $\mathfrak{n}$ cannot be a weak Giuga ideal. Thus a weak Giuga ideal must be a product of non-conjugate primes. □

We conclude this subsection with one more property about the norms of the factors of weak Giuga ideals.

Proposition 3.10. *Let $\mathfrak{n} \subset \mathfrak{o}$ be a weak Giuga ideal. For any distinct prime factors $\mathfrak{p}$ and $\mathfrak{q}$, we have:* $\gcd(N(\mathfrak{p}), N(\mathfrak{q})) = 1$.

Proof. Let $\mathfrak{n} \subset \mathfrak{o}$ be a weak Giuga ideal. Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime divisors of $\mathfrak{n}$. Let d be a positive integer dividing both $N(\mathfrak{p})$ and $N(\mathfrak{q})$. Then $d = p^a q^b$ for some non-negative integers a, b where p and q are the primes below $\mathfrak{p}$ and $\mathfrak{q}$, respectively (refer to Section 2.2). Since $\mathfrak{n}$ is assumed to be weak Giuga, we have that

$$N(\mathfrak{n}_\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}} \quad \text{and} \quad N(\mathfrak{n}_\mathfrak{q}) \equiv 1 \pmod{\mathfrak{q}}.$$

We further note that

$$d \mid N(\mathfrak{p}) \Rightarrow d \mid N(\mathfrak{n}_\mathfrak{q}) \quad \text{and} \quad d \mid N(\mathfrak{q}) \Rightarrow d \mid N(\mathfrak{n}_\mathfrak{p}).$$

It follows that d is a *unit* mod $\mathfrak{p}$ and mod $\mathfrak{q}$ (an element a of $\mathfrak{o}$ is called a *unit* if $a \mid 1$). Unpacking definitions, $d \mid 1 \pmod{\mathfrak{p}}$ implies that for some $\alpha \in \mathfrak{o}$, $\alpha d \equiv 1 \pmod{\mathfrak{p}} \Rightarrow \alpha d - 1 \in \mathfrak{p}$. We also know that $\alpha = N(\mathfrak{n}_\mathfrak{p})/d$, so $\alpha \in \mathbb{Z}$. Since $\alpha d - 1 \in \mathbb{Z}$, and $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$, $\alpha d - 1$ must be a multiple of p. This implies that $\alpha d \equiv 1 \pmod{p}$. Since $d \mid \alpha d$, d must be a unit mod p. By a similar argument, it can be shown that d is also a unit mod q.

Since $d = p^a q^b$, it follows that $a = b = 0$, that is, $d = 1$. Hence, $\gcd(N(\mathfrak{p}), N(\mathfrak{q})) = 1$. □

3.2 Strong Giuga Ideals

As in the elementary setting, given Theorem 3.4, we characterize a counter-example to the generalized conjecture with the following definition:

Definition 3.11 (**Strong Giuga Ideal**)**.** We say that an ideal $\mathfrak{n}$ of $\mathfrak{o}$ is a *strong Giuga ideal* to mean that the following condition holds:

(SGI) The ideal $\mathfrak{n}$ is composite and satisfies conditions **(CI)** and **(WGI)**, that is, $\mathfrak{n}$ is both a Carmichael ideal and a weak Giuga ideal.

Recall that strong Giuga numbers must be odd. We have a similar property for strong Giuga ideals.

Proposition 3.12. *Let $\mathfrak{n} \subset \mathfrak{o}$ be a strong Giuga ideal. Then for all prime ideals $\mathfrak{p} \mid \mathfrak{n}$, $N(\mathfrak{p})$ is odd, and hence $N(\mathfrak{n})$ is odd.*

Proof. Recall from Section 2.2 that norms of prime ideals are prime powers. Let $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. Assume for the sake of contradiction that for some index i we have $N(\mathfrak{p}_i) = 2^f$ for some $f \in \mathbb{Z}$. By Proposition 3.10, $\mathfrak{p}_i$ must be the only factor with an even norm. Consider a prime factor $\mathfrak{p}_j$ for $j \neq i$. Since $\mathfrak{n}$ is a strong Giuga ideal, we have $N(\mathfrak{p}_j) - 1 \mid N(\mathfrak{n}_{\mathfrak{p}_j}) - 1$. But this is impossible, as $N(\mathfrak{p}_j) - 1$ is even and $N(\mathfrak{n}_{\mathfrak{p}_j}) - 1$ is odd.

Thus $N(\mathfrak{p})$ is odd for all $\mathfrak{p} \mid \mathfrak{n}$, and since by Theorem 2.23 the norm is multiplicative, $N(\mathfrak{n})$ must be odd. □

4 Weak Giuga Ideals: Equivalences and Examples

Developing a stronger understanding of weak Giuga ideals is essential to determining whether or where strong Giuga ideals exist, as Carmichael ideals are understood far better. In this section, we extend Theorem 1.6 to number rings and demonstrate a third weak Giuga equivalence as well. We provide examples of weak Giuga ideals found in our computational searches and use the findings to compare abundance of weak Giuga ideals in specific number rings.

Theorem 4.1. *Let* $\Phi(\mathfrak{n})$ *be the* Euler phi function for ideals*, which is equal to the number of units (elements with inverses) in* $\mathfrak{o}/\mathfrak{n}$*, and defined as*

$$\Phi(\mathfrak{n}) \coloneqq N(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{n}} (1 - N(\mathfrak{p})^{-1})$$

A composite ideal $\mathfrak{n}$ *is a weak Giuga ideal if and only if*

$$\sum_{x \in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv -1 \pmod{\mathfrak{n}}$$

Proof. First, assume $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ is a weak Giuga ideal. That is, $\mathfrak{n}$ is square-free and $N(\mathfrak{n}_\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$ for all primes $\mathfrak{p} \mid \mathfrak{n}$. By Lemma 3.3 we have:

$$\sum_{x \in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in I_\mathfrak{p}} x^{\Phi(\mathfrak{n})} \pmod{\mathfrak{p}} \tag{4.1}$$

The definition of the Euler phi function for ideals can be rewritten using the fact that norms of ideals are multiplicative (Theorem 2.23):

$$\begin{aligned}
\Phi(\mathfrak{n}) &\coloneqq N(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{n}} (1 - N(\mathfrak{p})^{-1}) \\
&= N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_k)[(1 - N(\mathfrak{p}_1)^{-1}) \cdots (1 - N(\mathfrak{p}_k)^{-1})] \\
&= (N(\mathfrak{p}_1) - 1) \cdots (N(\mathfrak{p}_k) - 1) \\
&= \prod_{\mathfrak{p}|\mathfrak{n}} (N(\mathfrak{p}) - 1)
\end{aligned}$$

Substituting the definition of $\Phi(\mathfrak{n})$ into the right-hand side of (4.1):

$$N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in I_\mathfrak{p}} x^{\prod_{\mathfrak{p}|\mathfrak{n}} (N(\mathfrak{p})-1)} \equiv N(\mathfrak{n}_\mathfrak{p}) \sum_{x \in I_\mathfrak{p}} 1 \pmod{\mathfrak{p}} \tag{4.2}$$

Since there are $N(\mathfrak{p}) - 1$ elements in $I_\mathfrak{p}$:

$$(4.2) \equiv N(\mathfrak{n}_\mathfrak{p})(N(\mathfrak{p}) - 1) \equiv -N(\mathfrak{n}_\mathfrak{p}) \pmod{\mathfrak{p}} \equiv -1 \pmod{\mathfrak{p}}$$

Hence $\sum_{x\in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv -1 \pmod{\mathfrak{n}}$ by the Chinese Remainder Theorem for Ideals (Theorem 2.25).

Conversely, assume

$$\sum_{x\in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv -1 \pmod{\mathfrak{n}}$$

Let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{n}$. Note that

$$N(\mathfrak{p}) - 1 \mid \Phi(\mathfrak{n})$$

It then follows that

$$\sum_{x\in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \overset{\text{(Lemma 3.3)}}{\equiv} N(\mathfrak{n}_{\mathfrak{p}}) \sum_{x\in I_{\mathfrak{p}}} x^{\Phi(\mathfrak{n})} \equiv N(\mathfrak{n}_{\mathfrak{p}}) \sum_{x\in I_{\mathfrak{p}}} 1 \equiv -N(\mathfrak{n}_{\mathfrak{p}}) \pmod{\mathfrak{p}}$$

Furthermore, by assumption we have $\sum_{x\in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv -1 \pmod{\mathfrak{n}}$ and hence $\sum_{x\in I_{\mathfrak{n}}} x^{\Phi(\mathfrak{n})} \equiv -1 \pmod{\mathfrak{p}}$. Thus $N(\mathfrak{n}_{\mathfrak{p}}) \equiv 1 \pmod{\mathfrak{p}}$, as desired. □

Theorem 4.1 generalized the equivalence of (1) and (2) from Theorem 1.6 to the number field setting. Similarly, the following theorem generalizes the equivalence of (1) and (3) in Theorem 1.6 to the number field setting:

Theorem 4.2. *The composite ideal $\mathfrak{n} \subset \mathfrak{o}$ is a weak Giuga ideal if and only if $1 - \sum_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{n}_{\mathfrak{p}}) \in \mathfrak{n}$.*

Proof. Let $\mathfrak{n}$ have prime decomposition $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. Note that $1 - \sum_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{n}_{\mathfrak{p}}) = 1 - \sum_{i=1}^{k} N(\mathfrak{n}_{\mathfrak{p}_i})$. Assuming $\mathfrak{n}$ is a weak Giuga ideal, $N(\mathfrak{n}_{\mathfrak{p}_i}) - 1 \in \mathfrak{p}_i$ for all i, and therefore $1 - N(\mathfrak{n}_{\mathfrak{p}_i}) \in \mathfrak{p}_i$ for all i by Definition 2.8 with $\delta = -1$. From the prime factorization of $\mathfrak{n}$ and Definition 2.16, it follows that $\prod_{i=1}^{k}(1 - N(\mathfrak{n}_{\mathfrak{p}_i})) \in \mathfrak{n}$. Since $N(\mathfrak{n}) \in \mathfrak{n}$ (see Definition 2.21), expanding this product and ignoring all terms with $N(\mathfrak{n})$ in their expression, we have

$$1 - \sum_{i=1}^{k} N(\mathfrak{n}_{\mathfrak{p}_i}) \in \mathfrak{n}$$

which directly implies $1 - \sum_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{n}_{\mathfrak{p}}) \in \mathfrak{n}$.

Conversely, assume $\nu = 1 - \sum_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{n}_{\mathfrak{p}}) \in \mathfrak{n}$. Written in the language of ideals, we have $\mathfrak{n} \mid \nu\mathfrak{o}$. Let $\mathfrak{q} \mid \mathfrak{n}$ where $\mathfrak{p} \neq \mathfrak{q}$. Then $\mathfrak{q} \mid \nu\mathfrak{o}$, that is, $\nu \in \mathfrak{q}$. So we have

$$\nu = \overbrace{1 - N(\mathfrak{n}_{\mathfrak{q}})}^{:=\xi} - \overbrace{\sum_{\substack{\mathfrak{p}|\mathfrak{n} \\ \mathfrak{p}\neq\mathfrak{q}}} N(\mathfrak{n}_{\mathfrak{p}})}^{:=\xi'} \in \mathfrak{q}$$

Because $N(\mathfrak{n}_\mathfrak{q})$ is excluded from ξ', we know that every element in the sum of ξ' will have a factor of $N(\mathfrak{q})$. From Definition 2.21, we know that $N(\mathfrak{q}) \in \mathfrak{q}$, and thus $\xi' \in \mathfrak{q}$. Since $\xi' \in \mathfrak{q}$, it must be that $\xi \in \mathfrak{q}$ as well. This further implies that $N(\mathfrak{n}_\mathfrak{q}) - 1 \in \mathfrak{q}$. Since $\mathfrak{q}$ was arbitrary, it follows that $\mathfrak{n}$ is a weak Giuga ideal, as desired. □

We provide one more weak Giuga ideal equivalence which will be used in Section 6.

Lemma 4.3. *An ideal $\mathfrak{n} \subset \mathfrak{o}$ is a weak Giuga ideal if and only if for all primes p such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ where $\mathfrak{p}$ is prime and $\mathfrak{p} \mid \mathfrak{n}$ we have:*

$$p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$$

Proof. First, assume that $\mathfrak{n}$ is a weak Giuga ideal, that is, $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{n}$. Since $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then any integer in $\mathfrak{p}$ is also in $p\mathbb{Z}$. That is, for an integer $a \in \mathfrak{p}$, $a = pb$, for some $b \in \mathbb{Z}$. Therefore, since $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p}$, $N(\mathfrak{n}_\mathfrak{p}) - 1 = pb$, and thus $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$.

Next, assume that $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$. Then $N(\mathfrak{n}_\mathfrak{p}) - 1$ is a multiple of p, that is, $N(\mathfrak{n}_\mathfrak{p}) - 1 \in p\mathbb{Z}$. Furthermore, this means that $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p} \cap \mathbb{Z}$, which implies that $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{n}$. Thus, $\mathfrak{n}$ is a weak Giuga ideal. □

Like weak Giuga numbers, there is much that is unknown about the existence of weak Giuga ideals. It still remains open whether or not there exist weak Giuga ideals in every number ring, as well as whether there are infinitely many weak Giuga ideals in any one number ring.

Our definition of a weak Giuga ideal is equivalent to the definition of a weak Giuga number when the number ring in question is $\mathbb{Z}$ and the norm of each integer is taken to be the absolute value.

A computational search for weak Giuga ideals in the rings $\mathbb{Z}(i)$ and $\mathbb{Z}(\sqrt{-5})$ found them to be more plentiful than in $\mathbb{Z}$. We chose to compare abundance of weak Giuga ideals by looking at how many ideals with a certain number of prime factors existed in one ring versus another. The main part of the code used to generate these examples is provided in Appendix A. For a list of known weak Giuga numbers, see pages 12 and 13 of the paper by Borwein and Wong [5].

In their paper [5], Borwein and Wong determined through an exhaustive search that there is only one weak Giuga number which has 3 factors, whereas in $\mathbb{Z}(i)$ with a *non-exhaustive* search, we were able to find 58 distinct weak Giuga ideals with 3 factors—an increase of an order of magnitude.

Whereas in their exhaustive search, Borwein and Wong could only obtain a total of 4 weak Giuga numbers with 3, 4 and 5 factors, in $\mathbb{Z}(\sqrt{-5})$ in a *non-exhaustive* search, we found 53 distinct weak Giuga ideals with 3, 4, and 5 factors—again an increase of an order of magnitude.

We provide the complete set of search results from our computations in Appendix B. Below, we give a sampling of the search results for each ring.

Example 4.4. Weak Giuga ideals in the Gaussian integers, $\mathbb{Z}(i)$:

1. $(1+i)(3)(4+i)$
2. $(71)(107)(211)$
3. $(2i+1)(11)(151)$
4. $(47)(71)(139)$
5. $(1+i)(47)(631)$
6. $(79)(131)(199)$
7. $(7)(11)(19)$
8. $(71)(83)(491)$
9. $(127)(139)(1471)$
10. $(199)(379)(419)$
11. $(127)(131)(4159)$
12. $(127)(191)(379)$

Example 4.5. Weak Giuga ideals in $\mathbb{Z}(\sqrt{-5})$:

1. $(11)(13)(71)$
2. $(79)(131)(199)$
3. $(191)(197)(6271)$
4. $(199)(331)(499)$
5. $(239)(251)(4999)$
6. $(2,1+\sqrt{-5})(3,1+\sqrt{-5})(\sqrt{-5})$
7. $(2,1+\sqrt{-5})(3,2+\sqrt{-5})(\sqrt{-5})$
8. $(\sqrt{-5})(2,3+\sqrt{-5})(3,2+5\sqrt{-5})$
9. $(2,1+\sqrt{-5})(3,1+\sqrt{-5})(\sqrt{-5})(13)(137)$
10. $(2,1+\sqrt{-5})(3,2+\sqrt{-5})(\sqrt{-5})(13)(137)$
11. $(2,1+\sqrt{-5})(3,1+\sqrt{-5})(6+\sqrt{-5})(7,4+\sqrt{-5})$
12. $(2,1+\sqrt{-5})(3,2+\sqrt{-5})(6+\sqrt{-5})(7,4+\sqrt{-5})$

We look at the weak Giuga ideal in example 4.4.6, and show how to check that an ideal is weak Giuga. In the process of this, we must show

$$N((79)(131)) \equiv 1 \pmod{(199)},$$

and likewise for other permutations of the prime factors in the above expression. Note that this is equivalent to showing $N((79)(131)) - 1 \in (199)$. From Theorem 2.23, we know that $N((79)(131))-1 = N((79))N((131))-1 = 79^2131^2-1 = 107101800$, which is in fact divisible by 199, and therefore $N((79)(131)) - 1 \in (199)$.

5 Correspondences and Associations

One of the primary motivations for working in the general framework of number rings is to gain insight into the properties of weak Giuga numbers. Thus, we develop a correspondence which relates weak Giuga ideals and numbers. We also define when weak Giuga ideals are associated; this enables us to use the existence of a weak Giuga ideal in one number field to find another weak Giuga ideal in the same, or even a different, number field.

We begin by defining a *corresponding ideal*. We note that there may be many corresponding ideals in $\mathfrak{o}$ for any given $n \in \mathbb{N}$.

Definition 5.1. Given $n = p_1 \cdots p_k \in \mathbb{N}$, p_i prime, and a number ring $\mathfrak{o}$, we say that an ideal $\mathfrak{n} \subset \mathfrak{o}$ is a *corresponding ideal* to n to mean that $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ where each $\mathfrak{p}_i$ is prime and $\mathfrak{p}_i \mid p_i\mathfrak{o}$.

Similarly, we define the *corresponding number* $n \in \mathbb{N}$ for an ideal $\mathfrak{n} \subset \mathfrak{o}$.

Definition 5.2. Given an ideal $\mathfrak{n} \subset \mathfrak{o}$, we define the *corresponding number* of $\mathfrak{n}$ to be the unique positive integer n such that $\mathfrak{n} \cap \mathbb{Z} = n\mathbb{Z}$.

We say that $\mathfrak{n}$ is *above* n, or n is *below* $\mathfrak{n}$, to indicate correspondence.

Example 5.3. Consider the ideal $\mathfrak{n} = (1+i)(3)(2+i) \subset \mathbb{Z}(i)$. Then $n = 30$ corresponds to $\mathfrak{n}$ since $30 = 2 \cdot 3 \cdot 5$ and $(2) = (1+i)^2$, $(3) = (3)$, $(5) = (2+i)(2-i)$.

Building off this correspondence, we define an association between ideals in potentially distinct number rings.

Definition 5.4. We say that $\mathfrak{n} \subset \mathfrak{o}$ and $\mathfrak{n}' \subset \mathfrak{o}'$ are *associated ideals* to mean that they lie above the same positive integer n. Equivalently, $\mathfrak{n}$ and $\mathfrak{n}'$ are associated means that $\mathfrak{n} \cap \mathbb{Z} = \mathfrak{n}' \cap \mathbb{Z}$. We indicate that two ideals $\mathfrak{n}$ and $\mathfrak{n}'$ are associated as follows: $\mathfrak{n} \sim \mathfrak{n}'$.

We note that $\mathfrak{n} \cap \mathbb{Z} = (p_1 \cdots p_k)$ where p_i is such that $p_i\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$.

The following theorem provides criteria for when an associated ideal of a weak Giuga ideal is itself weak Giuga.

Theorem 5.5. *Let $\mathfrak{n} \subset \mathfrak{o}$ and $\mathfrak{n}' \subset \mathfrak{o}'$ be ideals such that $\mathfrak{n} \sim \mathfrak{n}'$ and $N(\mathfrak{n}) = N(\mathfrak{n}')$. If $\mathfrak{n}$ is a weak Giuga ideal, then so is $\mathfrak{n}'$.*

Proof. (The reader may wish to refer to the primer on norms of ideals in Section 2.2.) Suppose $\mathfrak{n}$ is a weak Giuga ideal of $\mathfrak{o}$ and $\mathfrak{n}'$ is an associated ideal of $\mathfrak{n}$ in some number ring $\mathfrak{o}'$, not necessarily different from $\mathfrak{o}$, that satisfies $N(\mathfrak{n}) = N(\mathfrak{n}')$. Since $\mathfrak{n}$ is a weak Giuga ideal, it follows by Theorem 3.7 and Corollary 3.9 that $\mathfrak{n}$ must be a product of distinct non-conjugate primes of $\mathfrak{o}$. Let the prime ideal $\mathfrak{p}'$ divide $\mathfrak{n}'$. Then $N(\mathfrak{p}') \mid (N(\mathfrak{n}') = N(\mathfrak{n}))$. Let p' be the prime below $\mathfrak{p}'$ and let $\mathfrak{p}$ be the prime of $\mathfrak{o}$ above p' that divides $\mathfrak{n}$. Since $\mathfrak{n}$ is assumed to be a weak Giuga ideal, by Lemma 4.3, it follows that $p' \mid (N(\mathfrak{n}_\mathfrak{p}) - 1 = N(\mathfrak{n}'_{\mathfrak{p}'}) - 1)$. Since $\mathfrak{p}'$ was an arbitrary divisor of $\mathfrak{n}'$, by Lemma 4.3, it follows that $\mathfrak{n}'$ is a weak Giuga ideal as claimed. □

The following theorem is very similar to the preceding theorem but has a different though equivalent hypothesis.

Theorem 5.6. *Let $\mathfrak{n} \subset \mathfrak{o}$ and $\mathfrak{n}' \subset \mathfrak{o}'$ be ideals such that $\mathfrak{n}$ and $\mathfrak{n}'$ have the same number of prime factors and there exists a correspondence between the prime factors such that $N(\mathfrak{p}) = N(\mathfrak{p}')$ for all $\mathfrak{p} \mid \mathfrak{n}$. If $\mathfrak{n}$ is a weak Giuga ideal, then so is $\mathfrak{n}'$.*

Proof. The proof is similar in nature to that of Theorem 5.5. □

It is natural at this point to ask when a number has a corresponding weak Giuga ideal. We find that every square-free composite integer corresponds to a weak Giuga ideal in a cyclotomic extension (Theorem 5.8). By Proposition 3.10, we know that this is the largest possible subset of integers that could have corresponding weak Giuga ideals. To prove Theorem 5.8, we will need the following result (Theorem 5.7) about cyclotomic extensions. We let ζ_m denote the primitive m^{th} root of unity. This is the element which generates the cyclic group (under multiplication) of m^{th} roots of unity. For example, $\zeta_4 = i$. A cyclotomic extension $\mathbb{Q}(\zeta_m)$ is made by adjoining an m^{th} root of unity to $\mathbb{Q}$. Thus in previous examples when we considered $\mathbb{Z}(i)$, we were in fact considering the number ring of the cyclotomic extension $\mathbb{Q}(\zeta_4)$.

Theorem 5.7. ([1, p. 260]) *Given $m \in \mathbb{N}$, let $K = \mathbb{Q}(\zeta_m)$, and let $p \in \mathbb{N}$ be a prime with $m = p^r m_1$ for $r \in \mathbb{N} \cup \{0\}$, $m_1 \in \mathbb{N}$, and $p \nmid m_1$. Further, let h be the least positive integer such that $p^h \equiv 1 \pmod{m_1}$. Then for any prime ideal $\mathfrak{p} \subset \mathfrak{o}$ such that $\mathfrak{p} \mid p\mathfrak{o}$, $N(\mathfrak{p}) = p^h$.*

Theorem 5.8. *For every square-free composite $n \in \mathbb{Z}$ there exists a number ring $\mathfrak{o}$ in $K = \mathbb{Q}(\zeta_n)$ such that $\mathfrak{n}$, a corresponding ideal of n, is a weak Giuga ideal.*

Proof. Let $\mathfrak{n} \subset \mathfrak{o}$ be an ideal corresponding to n. By Theorem 5.7 with $m = n = qn_q$ for all primes $q \mid n$ satisfying $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$ where $\mathfrak{q}$ is prime and $\mathfrak{q} \mid \mathfrak{n}$, we have that $N(\mathfrak{q}) \equiv 1 \pmod{n_q}$. Thus $N(\mathfrak{q}) \equiv 1 \pmod{p}$ for $p \neq q$. So, for $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ satisfying $\mathfrak{p} \mid \mathfrak{n}$, we have:

$$N(\mathfrak{n}_\mathfrak{p}) = \prod_{\substack{q \mid n \\ q \neq p}} N(\mathfrak{q}) \equiv 1 \pmod{p}$$

which implies that $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$ for all primes $p \mid n$, so by Lemma 4.3, $\mathfrak{n}$ is a weak Giuga ideal, as desired. □

Cyclotomic extensions are not the only fields in which we can find weak Giuga ideals. In the next section, we will exploit characteristics of quadratic extensions to gain significant insight into the existence of weak Giuga ideals in that setting.

6 Giuga Ideals in Quadratic Extensions

We further our exploration of Giuga's conjecture by considering correspondences between Giuga numbers and Giuga ideals in quadratic extensions. A quadratic extension K of a field F is a field containing F where $K = F(\sqrt{d})$, with d being a square-free element in F. Our field F will be $\mathbb{Q}$. Quadratic extensions are very tractable as the norms of prime ideals are

simple to calculate as we shall see below. Throughout this section, the rings $\mathfrak{o}$ and $\mathfrak{o}'$ will be assumed to be quadratic number rings.

We now introduce the terms *split*, *ramify*, and *inert*, which describe the three possibilities for how a prime ideal $p\mathfrak{o}$ can be factorized:

Definition 6.1. If a prime number p *splits* in $\mathfrak{o}$, then the ideal $p\mathfrak{o}$ is the product of two distinct prime ideals: $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$.

Definition 6.2. If a prime number p is *ramified* in $\mathfrak{o}$, then $p\mathfrak{o}$ is the square of a prime ideal: $p\mathfrak{o} = \mathfrak{p}^2$.

Definition 6.3. If a prime number p is *inert* in $\mathfrak{o}$, then $p\mathfrak{o}$ is a prime ideal: $p\mathfrak{o} = \mathfrak{p}$.

For quadratic extensions, if $\mathfrak{p}$ is a prime ideal dividing $p\mathfrak{o}$, $N(\mathfrak{p}) = p^2$ if p is inert, and $N(\mathfrak{p}) = p$ otherwise.

We will now use these definitions to better understand the relationship between weak Giuga numbers and their corresponding ideals.

Theorem 6.4. *Let $n \in \mathbb{Z}$, and let $\mathfrak{o}$ be the number ring of a quadratic extension.*

1. *If all $p \mid n$ split or ramify in $\mathfrak{o}$, then n is a weak Giuga number if and only if all of its corresponding ideals $\mathfrak{n} \subset \mathfrak{o}$ are weak Giuga ideals.*
2. *If all $p \mid n$ are inert in $\mathfrak{o}$ and n is a weak Giuga number, then all of its corresponding ideals $\mathfrak{n} \subset \mathfrak{o}$ are weak Giuga ideals.*

Proof.

1. Since each $p \mid n$ splits or ramifies in $\mathfrak{o}$, we have $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_i$ is a nontrivial prime ideal and where $\mathfrak{p}_1 = \mathfrak{p}_2$ in the ramified case. From our facts about norms in quadratic extensions, we know that $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$. Thus whether we choose $\mathfrak{p}_1$ or $\mathfrak{p}_2$ to be a factor of a corresponding ideal of n, the norm will be the same. By definition, any corresponding ideal $\mathfrak{n}$ of n will be associated to another corresponding ideal $\mathfrak{n}'$ of n.

   Since $\mathfrak{n}$ and $\mathfrak{n}'$ will not only be associated but will also have the same norm, we may apply Theorem 5.5 to conclude that if $\mathfrak{n}$ is a weak Giuga ideal, then so is $\mathfrak{n}'$. As a result, our proof now reduces to showing that n is a weak Giuga number if and only if one of its corresponding ideals $\mathfrak{n}$ is a weak Giuga ideal.

   Since $N(\mathfrak{p}) = p$, a corresponding ideal $\mathfrak{n}$ of n will have a norm equal to n, as we now show:

$$N(\mathfrak{n}) = N(\mathfrak{p}_1 \cdots \mathfrak{p}_k) \tag{6.1}$$

   and from Theorem 2.23, we know that:

$$(6.1) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_k) \tag{6.2}$$

then since the primes split or ramify:

$$(6.2) = p_1 \cdots p_k = n \tag{6.3}$$

Thus $N(\mathfrak{n}) = n$. From this, we may conclude that $N(\mathfrak{n}_\mathfrak{p}) = n_p$.

We first assume that n is a weak Giuga number and show that one of its corresponding ideals $\mathfrak{n}$ is a weak Giuga ideal. Since n is a weak Giuga number, $p \mid n_p - 1$ for all $p \mid n$. Since $N(\mathfrak{n}_\mathfrak{p}) = n_p$, we also have that $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$. Therefore, by Lemma 4.3, $\mathfrak{n}$ is a weak Giuga ideal.

We now assume that $\mathfrak{n}$ is a weak Giuga ideal and show that its corresponding number n is a weak Giuga number. Since $\mathfrak{n}$ is a weak Giuga ideal, $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{n}$. By Lemma 4.3, the corresponding number p for every $\mathfrak{p} \mid \mathfrak{n}$ satisfies:

$$p \mid N(\mathfrak{n}_\mathfrak{p}) - 1 \tag{6.4}$$

Since $N(\mathfrak{n}_\mathfrak{p}) = n_p$, (6.4) is equivalent to:

$$p \mid n_p - 1$$

for all $p \mid n$. Therefore, n is a weak Giuga number.

2. Since each $p \mid n$ is inert in $\mathfrak{o}$, we have $p\mathfrak{o} = \mathfrak{p}$ is a prime ideal. Thus $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ is the only ideal in $\mathfrak{o}$ corresponding to n. Furthermore, we know that $N(\mathfrak{p}) = p^2$. By Theorem 2.23, $N(\mathfrak{n}_\mathfrak{p})$ is a product of norms of prime ideals, so we have $N(\mathfrak{n}_\mathfrak{p}) - 1 = n_p^2 - 1 = (n_p - 1)(n_p + 1)$. By assumption, n is weak Giuga, so $p \mid n_p - 1$ for all $p \mid n$. Thus $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$ for all $p \mid n$. Equivalently, $N(\mathfrak{n}_\mathfrak{p}) - 1 \in \mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{n}$. Hence $\mathfrak{n}$ is a weak Giuga ideal.

□

Example 6.5. Recall that $30 = 2 \cdot 3 \cdot 5$ is the smallest weak Giuga number. In $\mathbb{Z}(\sqrt{-5})$, it is the case that 2, 3, and 5 either split or ramify:

$$\begin{aligned}(2) &= (2, 1 + \sqrt{-5})^2 \\ (3) &= (3, 2 + \sqrt{-5})(3, 1 + \sqrt{-5}) \\ (5) &= (\sqrt{-5})^2\end{aligned}$$

Thus by Theorem 6.4, case (1), any ideal in $\mathbb{Z}(\sqrt{-5})$ corresponding to 30 is a weak Giuga ideal. For instance, $\mathfrak{n} = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(\sqrt{-5})$ is a weak Giuga ideal which we also saw in Example 4.5.6.

By Theorem 5.6, we know that we may construct weak Giuga ideals from other weak Giuga ideals when norms are preserved for the prime factors of the ideals. Theorem 6.13 below provides the tools to create quadratic number rings where these norms are preserved. To prove this, we will need the following result about splitting, ramification, and inertness of primes in quadratic extensions. Henceforth, we will refer to these properties of primes as *splitting properties*.

Theorem 6.6. [16, p. 74] *Let $m \in \mathbb{Z}$ be square-free and $K = \mathbb{Q}(\sqrt{m})$. For $p \in \mathbb{Z}$ prime, $p\mathfrak{o}$ decomposes in the following ways:*

- *If $p \mid m$, then $p\mathfrak{o} = (p, \sqrt{m})^2$*
- *If m is odd, then*

$$2\mathfrak{o} = \begin{cases} (2, 1+\sqrt{m})^2 & \text{if } m \equiv 3 \pmod 4 \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & \text{if } m \equiv 1 \pmod 8 \\ 2\mathfrak{o} & \text{if } m \equiv 5 \pmod 8 \end{cases}$$

- *If p is odd, $p \nmid m$, then*

$$p\mathfrak{o} = \begin{cases} (p, n+\sqrt{m})(p, n-\sqrt{m}) & \text{if } m \equiv n^2 \pmod p \\ p\mathfrak{o} & \text{if } m \text{ is not a square mod } p \end{cases}$$

Example 6.7. Examples 4.4.6 and 4.5.2 are associated ideals because by Theorem 6.6, the prime numbers below the ideals in their factorizations are inert in both number rings ($\mathbb{Z}(i)$ and $\mathbb{Z}(\sqrt{-5})$), making 4.4.6 and 4.5.2 corresponding ideals of $n = 79 \cdot 131 \cdot 199$.

To make the proof of Theorem 6.13 read more smoothly, we remind the reader of some results and definitions from elementary number theory:

Definition 6.8. *Rational primes* are the primes in $\mathbb{Q}$, as opposed to the primes in $\mathbb{Q}(\sqrt{d})$. The primes in $\mathbb{Q}$ are just the standard prime numbers from $\mathbb{Z}$.

Definition 6.9. Let p be an odd prime with $\gcd(m, p) = 1$, for $m \in \mathbb{Z}$. If the congruence $x^2 \equiv m \pmod p$ is solvable, then m is called a *quadratic residue* mod p. Otherwise, m is called a *quadratic non-residue* mod p.

Theorem 6.10. [11, p. 87] *For any odd prime p, there are $\frac{1}{2}(p-1)$ quadratic residues and $\frac{1}{2}(p-1)$ quadratic non-residues.*

Identity 6.11 (**Bézout's Identity (also Bézout's Lemma)**). *Given $d = \gcd(a, b)$, then for some $r, s \in \mathbb{Z}$, $d = ar + bs$.*

Theorem 6.12 (**Dirichlet's Theorem**). *For $a, d, k \in \mathbb{Z}$, if $\gcd(a, d) = 1, d \neq 0$, then for infinitely many k, $a + dk$ is prime.*

We are now ready to present the theorem:

Theorem 6.13. *Let P be a finite set of distinct, positive, odd rational primes, and fix a tripartition of P:*

$$P = U_r \cup U_s \cup U_i$$

Then there exist infinitely many quadratic extensions of $\mathbb{Q}$, denoted K, whose respective number rings are represented by $\mathfrak{o}$, such that the following simultaneously hold:

(i) if $p \in U_r$, then p is ramified in $\mathfrak{o}$

(ii) if $p \in U_s$, then p is split in $\mathfrak{o}$

(iii) if $p \in U_i$, then p is inert in $\mathfrak{o}$

Proof. We will show that there exists a set H of infinite cardinality such that for $m \in H$ and $K = \mathbb{Q}(\sqrt{m})$, $\mathfrak{o}$ has the desired splitting properties.

From Theorem 6.6, we know that if m is square-free, and m is such that

$$m \equiv a_p \pmod{p} \ \ \forall\ p \in U_s$$
$$m \equiv b_p \pmod{p} \ \ \forall\ p \in U_i$$

where a_p is a quadratic residue mod p, b_p is a quadratic non-residue mod p, and $p \nmid m$ for all $p \in U_s \cup U_i$, then $\mathfrak{o}$ will satisfy (ii) and (iii). As $p \geq 3$ for all $p \in P$, by Theorem 6.10, the desired a_p and b_p exist.

Since $\gcd(p, q) = 1$ for distinct p and q in P, if we let $\pi_{s,i} = \prod_{p \in U_s \cup U_i} p$, then the Chinese Remainder Theorem (Theorem 2.24) implies that there exists a residue class $t \in \mathbb{Z}/\pi_{s,i}\mathbb{Z}$ satisfying the above system of equivalences. We note that for any representative element of t, also written as t, that $\gcd(t, \pi_{s,i}) = 1$. This is because as $p \nmid m$, it will never be true that $m \equiv 0 \pmod{p}$, and since $m \in t$, it follows that t must not include any element from $U_s \cup U_i$.

For $\mathfrak{o}$ to additionally satisfy (i), we must have $p \mid m$ for all $p \in U_r$. Thus letting $\pi_r = \prod_{p \in U_r} p$, the proof will be complete if we can show that the set

$$H = \{m \in t : m \text{ is square-free and } \pi_r \mid m\}$$

is of infinite cardinality.

We will start by showing that a less restrictive set, $H' = \{m \in t : \pi_r \mid m\}$ is nonempty. Any $m \in t$ satisfying $\pi_r \mid m$ is such that $m = \pi_r y = t + \pi_{s,i} x$ for some $x, y \in \mathbb{Z}$. We claim that such an x and y exist. To see this, rewrite the equation as $\pi_r y + (-\pi_{s,i})x = t$. Note that $\gcd(\pi_r, -\pi_{s,i}) = 1$ since π_r and $-\pi_{s,i}$ are both products of distinct primes and U_r, U_i, and U_s are mutually disjoint sets. By Bézout's Identity (Identity 6.11), there exist $x_0, y_0 \in \mathbb{Z}$ such that $\pi_r y_0 + (-\pi_{s,i})x_0 = \gcd(\pi_r, -\pi_{s,i}) = 1$. Multiplying by t, we construct a general solution

to our original equation: $x = tx_0 + k\pi_r$ and $y = ty_0 + k\pi_{s,i}$, $k \in \mathbb{Z}$. Thus for $m \in t$ satisfying $\pi_r \mid m$, we may write $m = \pi_r(ty_0 + k\pi_{s,i})$, $k \in \mathbb{Z}$.

It remains to show that there are infinitely many square-free numbers of the form $\pi_r(ty_0 + k\pi_{s,i})$, $k \in \mathbb{Z}$. This condition will be satisfied if there are infinitely many primes of the form $ty_0 + k\pi_{s,i}$, and we will prove this below. The fact that π_r is a product of primes will not prevent the construction of square-free m values since π_r is a product of a *finite* number of primes as P is finite and $U_r \subset P$. Even if some of the primes of the form $ty_0 + k\pi_{s,i}$ are in U_r, there will still be infinitely many other primes available.

By Dirichlet's Theorem (Theorem 6.12), there are infinitely many primes of the form $ty_0 + k\pi_{s,i}$ as long as $\gcd(ty_0, \pi_{s,i}) = 1$. Note that $\gcd(ty_0, \pi_{s,i}) = \gcd(y_0, \pi_{s,i})$ since t and $\pi_{s,i}$ are relatively prime. Recall from earlier that

$$\pi_r y_0 - \pi_{s,i} x_0 = 1.$$

If an integer d divides both y_0 and $\pi_{s,i}$, then $d \mid 1$. Hence $\gcd(ty_0, \pi_{s,i}) = 1$ and this completes the proof of the theorem. □

The following two lemmas will give us more flexibility in applying Theorem 6.13.

Lemma 6.14. Theorem 6.13 *also holds when* $2 \in P$.

Proof. We assumed $2 \notin P$. If we want to include 2 in P, then when m is odd, an additional congruence (depending on whether 2 will split, ramify or be inert in $\mathfrak{o}$) from the second bullet point of Theorem 6.6 needs to be included in the system of congruences used in the Chinese Remainder Theorem to find t. Otherwise, the argument is the same. If m is even, then by Theorem 6.6, 2 will ramify in $\mathfrak{o}$, so no changes will be needed in the proof. □

Lemma 6.15. *If at least one of* U_r, U_s *or* U_i *is nonempty, then* Theorem 6.13 *holds.*

Proof. Each case can be shown through minor alterations to Theorem 6.13's proof. □

Corollaries 6.16 and 6.17 of Theorem 6.13 will allow us to conclude that infinitely many quadratic extensions have weak Giuga ideals.

Corollary 6.16. *If* $n \in \mathbb{Z}$ *is a weak Giuga number, then there exist infinitely many quadratic number rings* $\mathfrak{o}$ *such that* $\mathfrak{n}$*, a corresponding ideal of* n*, is a weak Giuga ideal.*

Proof. We know that $n \in \mathbb{Z}$ is a weak Giuga number. By Theorem 6.4, we have that $\mathfrak{n}$ is a weak Giuga ideal if either (1) all the prime factors of n split or ramify in $\mathfrak{o}$ or (2) all the prime factors of n are inert in $\mathfrak{o}$. Let P be the set of prime divisors of n. We will apply Theorem 6.13 to two different cases, using P as the required set of primes (which by Lemma 6.14 may include 2). In the first case, so that we have the right conditions for n to satisfy (1),

we will let U_i, the partition of P with inert primes, be empty (Theorem 6.13 is still valid in this case by Lemma 6.15). In this way, all the primes dividing n necessarily split or ramify, making $\mathfrak{n}$ a weak Giuga ideal by Theorem 6.4, and from Theorem 6.13, we know that there will be infinitely many quadratic number rings $\mathfrak{o}$ for which case (1) will hold. Analogously, in the second case, we will let $U_s \cup U_r = \emptyset$ so that n's factors are inert. Thus $\mathfrak{n}$ is a weak Giuga ideal by Theorem 6.4, and from Lemma 6.15, we know that we can apply Theorem 6.13 to show that there are infinitely many $\mathfrak{o}$'s for which this is true. □

Corollary 6.17. *If $n \in \mathbb{Z}$ is a weak Giuga number, then there exist infinitely many quadratic number rings $\mathfrak{o}$ such that $n\mathfrak{o}$ itself is a weak Giuga ideal.*

Proof. Let n be a weak Giuga number such that $n = p_1 \cdots p_k$. When all of the factors $p \mid n$ are inert in $\mathfrak{o}$, then by Theorem 6.4, a corresponding ideal $\mathfrak{n}$ is a weak Giuga ideal. Recall that because the prime factors p of n are inert, $\mathfrak{p} = p\mathfrak{o}$ is a prime ideal, making the corresponding ideal $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ unique. We may rewrite $\mathfrak{n}$ as follows:

$$\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_k = p_1\mathfrak{o} \cdots p_k\mathfrak{o} \tag{6.5}$$

Since in quadratic fields the product of principal ideals is also principal, we have:

$$(6.5) = (p_1 \cdots p_k)\mathfrak{o} = n\mathfrak{o}$$

Therefore $\mathfrak{n} = n\mathfrak{o}$, so $n\mathfrak{o}$ is a weak Giuga ideal. By Theorem 6.13, there exist infinitely many $\mathfrak{o}$ for which this is true. As in the proof of Corollary 6.16, the set of primes P needed for Theorem 6.13 will be the set of prime factors of n (where again, by Lemma 6.14, n may have a factor of 2), and as in the second case of that corollary's proof, $U_s \cup U_r = \emptyset$ (which is again allowed by Lemma 6.15). □

Corollaries 6.18 and 6.19 of Theorem 6.13 will allow us to conclude that if we have a strong Giuga ideal, then there are infinitely many quadratic extensions with strong Giuga ideals.

Corollary 6.18. *If n is a strong Giuga number, then there are infinitely many quadratic number rings $\mathfrak{o}$ with a corresponding strong Giuga ideal, $\mathfrak{n}$.*

Proof. Since n is a strong Giuga number, the prime 2 will not be one of its factors. Let all the prime factors of n split or ramify in $\mathfrak{o}$. To be a strong Giuga number, n must also be a weak Giuga number, so we may apply case (1) of Theorem 6.4 to show that $\mathfrak{n}$ is a weak Giuga ideal. Because all of n's prime factors split/ramify, $N(\mathfrak{p}) = p$ for all $p \mid n$, with $\mathfrak{p}$ being a corresponding ideal of p. As a consequence, $N(\mathfrak{n}_\mathfrak{p}) = n_p$. To show that $\mathfrak{n}$ is a strong Giuga ideal, we need to show that condition **(CI)** is satisfied, that is, $N(\mathfrak{p}) - 1 \mid N(\mathfrak{n}_\mathfrak{p}) - 1$ for all $\mathfrak{p} \mid \mathfrak{n}$. This condition can be simplified in our split/ramify case to: $p - 1 \mid n_p - 1$ for all $p \mid n$. Since n satisfies this condition by virtue of being a strong Giuga number, $\mathfrak{n}$ is a strong Giuga ideal. We can show that infinitely many $\mathfrak{o}$ exist such that this is true by letting P be the set of prime factors of n, letting $U_i = \emptyset$, and applying Theorem 6.13 (where U_i is allowed to be empty by Lemma 6.15). □

Corollary 6.19. *Let $\mathfrak{o}$ be a quadratic number ring. Given a weak (strong) Giuga ideal $\mathfrak{n} \subset \mathfrak{o}$, we may find infinitely many other quadratic number rings $\mathfrak{o}'$ with a weak (strong) Giuga ideal.*

Proof. We will first prove the statement for the weak Giuga case. Let n be the corresponding number of $\mathfrak{n}$. Let $\mathfrak{n}'$ be a corresponding ideal of n in the quadratic number ring $\mathfrak{o}'$, which has the property that every prime $p \mid n$ has the same splitting properties in $\mathfrak{o}'$ as it does in $\mathfrak{o}$ (for example, if p ramifies in $\mathfrak{o}$, then it will ramify in $\mathfrak{o}'$). Since they lie above the same positive integer n, $\mathfrak{n} \sim \mathfrak{n}'$, and since the prime factors of n have the same splitting properties in both rings, $N(\mathfrak{n}) = N(\mathfrak{n}')$. Therefore, by Theorem 5.5 we may conclude that $\mathfrak{n}'$ is also a weak Giuga ideal. By Theorem 6.13, if we let P be equal to the set of prime factors of n (which may include 2 by Lemma 6.14) and partition P so that the same terms which are inert/split/ramify in $\mathfrak{o}$ are placed into the respective partitions U_i, U_s, U_r (where as many as two of the partitions may be empty by Lemma 6.15), then there will exist infinitely many $\mathfrak{o}'$ such that $\mathfrak{n}'$ is a weak Giuga ideal.

When $\mathfrak{n}$ is a strong Giuga ideal, it is a weak Giuga ideal which additionally satisfies: $N(\mathfrak{p})-1 \mid N(\mathfrak{n}_\mathfrak{p}) - 1$ for all $\mathfrak{p} \mid \mathfrak{n}$. From earlier in the proof, we know that since the prime factors of n have the same splitting properties in $\mathfrak{o}$ and $\mathfrak{o}'$ that $N(\mathfrak{p}) = N(\mathfrak{p}')$ for every $\mathfrak{p}' \mid \mathfrak{n}'$. Therefore, $N(\mathfrak{p}') - 1 \mid N(\mathfrak{n}_{\mathfrak{p}'}) - 1$ for all $\mathfrak{p}' \mid \mathfrak{n}'$; that is, $\mathfrak{n}'$ satisfies the Carmichael condition. Thus, since we know that if $\mathfrak{n}$ is a weak Giuga ideal, then $\mathfrak{n}'$ is also a weak Giuga ideal, $\mathfrak{n}'$ satisfies both necessary conditions, and is therefore a strong Giuga ideal. By the same argument as above, by Theorem 6.13 (without the addition of Lemma 6.14 since by Proposition 3.12, to be a strong Giuga ideal, $N(\mathfrak{n}) = N(\mathfrak{n}')$ must be odd) there will exist infinitely many $\mathfrak{o}'$ for which this is true. □

Although Corollary 6.19 is somewhat limited in scope, since we needed to *already have* a weak Giuga ideal to find other number rings which have a weak Giuga ideal, it is of hope that similar results may be used to reduce the complexity of showing that *all* quadratic extensions contain a weak Giuga ideal.

We will now learn about a case when one weak Giuga number is a multiple of another weak Giuga number.

Theorem 6.20. *Let $\mathfrak{o}$ be a quadratic number ring. If n is a weak Giuga number that has a corresponding weak Giuga ideal $\mathfrak{n} \subset \mathfrak{o}$, and n has at least one prime factor which splits or ramifies in $\mathfrak{o}$, as well as at least three prime factors which are inert in $\mathfrak{o}$, then n is a* non-unit multiple *of another weak Giuga number (that is, if w is the other weak Giuga number, then $n = aw$, where $a \in \mathbb{Z}$ and $a \nmid 1$).*

Proof. Let n be a weak Giuga number and let $n = a \cdot b$ where a is the product of all those prime factors of n that are inert in $\mathfrak{o}$. By assumption, we have that a is composite. Let $\mathfrak{n} = \mathfrak{a} \cdot \mathfrak{b}$ where $\mathfrak{a}$ consists precisely of those prime ideals lying above the prime numbers dividing a. Let the prime $p \mid a$ and let $\mathfrak{p}$ be the prime of $\mathfrak{o}$ lying over p that divides $\mathfrak{a}$. Then

$n_p = a_p b$ so that we have:

$$\begin{aligned} N(\mathfrak{n}_\mathfrak{p}) - 1 &= N(\mathfrak{a}_\mathfrak{p})N(\mathfrak{b}) - 1 \\ &= a_p^2 \cdot b - 1 \\ &= n_p(a_p - 1) + (n_p - 1) \end{aligned} \tag{6.6}$$

Since n is a weak Giuga number, it follows that $p \mid n_p - 1$. Since $\mathfrak{n}$ is a weak Giuga ideal, by Lemma 4.3, it follows that $p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$. Since $\gcd(n_p, p) = 1$ (recall that n must be square-free), the above equality (6.6) gives us that $p \mid a_p - 1$. Since p was an arbitrary divisor of a, it follows that a is a weak Giuga number. And so $n = a \cdot b$ is a multiple of another weak Giuga number, as claimed. □

Example 6.21. If n is an even weak Giuga number which satisfies the hypothesis of Theorem 6.20, and 2 ramifies or splits in the given extension, then by Theorem 6.20, we know that there exists an odd weak Giuga number n' of which n is a multiple.

As a strong Giuga number must be odd, further study of this relation may be of value.

Corollary 6.16 showed that a weak Giuga number corresponds to a weak Giuga ideal in infinitely many quadratic extensions. This motivates us to ask whether a weak Giuga number can correspond to a weak Giuga ideal in all quadratic extensions. Theorem 6.23, although of interest in its own right, is used to show that this cannot be the case.

Before proceeding to Theorem 6.23, we need to prove the following lemma about weak Giuga numbers.

Lemma 6.22. *There exists no weak Giuga number with exactly two prime factors.*

Proof. Suppose for the sake of contradiction that we have a square-free integer $n = p_1 p_2$, where p_1, p_2 are two distinct prime numbers such that $p_1 < p_2$. We need to show that $p_1 \mid p_2 - 1$ and $p_2 \mid p_1 - 1$ for n to be weak Giuga. Since $p_2 > p_1$, it will be impossible for p_2 to divide $p_1 - 1$, as the only integer multiple of p_2 which will give a non-negative product smaller than p_2 is 0, and $p_1 - 1 \neq 0$, as $p_1 \geq 2$. Therefore, since not all of the weak Giuga requirements can be satisfied, n is not a weak Giuga number. □

Theorem 6.23. *Let n be an odd weak Giuga number. Then there are infinitely many quadratic number rings $\mathfrak{o}$ for which $\mathfrak{n}$, a corresponding ideal of n, is not a weak Giuga ideal.*

Proof. Let P denote the set of prime divisors of n, and let L be the set of indices labelling the primes in P. Partition L into U_s and U_i such that $|U_i| = 2$. By Theorem 6.13, there exist infinitely many $\mathfrak{o}$ such that for $j \in U_s$, p_j splits or ramifies, and for $j \in U_i$, p_j is inert.

By Lemma 4.3, $\mathfrak{n}$ is a weak Giuga ideal if and only if for all $p \in P$ such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ where $\mathfrak{p} \mid \mathfrak{n}$ we have:

$$p \mid N(\mathfrak{n}_\mathfrak{p}) - 1$$

We will show that for the $\mathfrak{o}$ we have just constructed, $p \nmid N(\mathfrak{n}_\mathfrak{p}) - 1$ for at least one $p \mid n$. This will then show that $\mathfrak{n}$ is not a weak Giuga ideal.

Let p_k be a prime whose index is in U_i, and let $a = \prod_{m \in U_i} p_m$. From the proof of Theorem 6.20, we know that:

$$N(\mathfrak{n}_{\mathfrak{p}_k}) - 1 = n_{p_k}(a_{p_k} - 1) + (n_{p_k} - 1)$$

Because n is a weak Giuga number, we know that $p_k \mid n_{p_k} - 1$. Therefore, for $\mathfrak{n}$ not to be a weak Giuga ideal, we need to show that $p_k \nmid n_{p_k}(a_{p_k} - 1)$ for at least one $p_k \mid n$. We already know that $p_k \nmid n_{p_k}$ since $p_k \mid n_{p_k} - 1$. So we only need to show that $p_k \nmid a_{p_k} - 1$.

By Lemma 6.22, in the $\mathfrak{o}$ we have constructed, a cannot be a weak Giuga number because it only has two prime factors. Therefore, $p_k \nmid a_{p_k} - 1$ for at least one of the primes p_k whose index is in U_i, and so $\mathfrak{n}$ is not a weak Giuga ideal in infinitely many quadratic number rings $\mathfrak{o}$, as desired. □

7 Open Questions

This exploration of Giuga ideals has just scratched the surface. Through computational examples, we have found an abundance of weak Giuga ideals in basic number rings. In light of our findings, the following questions are of immediate interest:

1. Which number rings have infinitely many weak Giuga ideals?
2. Do weak Giuga ideals exist in every number ring?
3. Does Giuga's conjecture fail in any number ring?

Appendix A: SageMath Code

Here we provide the main SageMath [S+09] code which was used in our searches for weak Giuga ideals. The parameter "R" stands for the number ring. The parameter "r" stands for the root for the number ring; for example, $r = \sqrt{-1}$ for $\mathbb{Z}(i)$. Lists of primes in $\mathbb{Z}(i)$ and $\mathbb{Z}(\sqrt{-5})$ were made, and depending on the particular test, all combinations of m factors (where $m = 3$ or 4 or 5) were then tested for being weak Giuga. For further information on the coding aspect of the paper, please contact K. Casey at: kac323@cornell.edu.

```
K.<i> = QuadraticField(-1)
OK = K.ring_of_integers()
L.<j> = QuadraticField(-5)
OL = L.ring_of_integers()

def wg_condition_check(candidate_ready, p, R):
    candidate = candidate_ready-1
    idP = R.ideal(p)
    return idP.divides(candidate)

def make_np(primes_of_n, p, R):
    np = 1
    avoid = primes_of_n.index(p)
    bound = len(primes_of_n)
    for i in range(0, bound):
        if i == avoid:
            np = np*1
        else:
            np = np*R.ideal(primes_of_n[i]).absolute_norm()
    return np

def is_weak_giuga_ideal(factors, R):
    primes_list = factors
    listLength = len(factors)
    listCounter = listLength
    location = 0
    bool = True
    while listCounter > 0 and location < len(primes_list):
        p = primes_list[location]
        np = make_np(factors, p, R)
        if wg_condition_check(np, p, R) == False:
            bool = False
            break
```

```
            listCounter = listCounter -1
            location = location + 1
        return bool

    def weak_giuga_testing(R, l):
        i = 0
        outcomes = []
        while i < len(l):
            if is_weak_giuga_ideal(l[i], R) == True:
                outcomes.append(l[i])
            i = i + 1
        return outcomes
```

Appendix B: Weak Giuga Ideal Examples

Weak Giuga ideals found in the ring $\mathbb{Z}(i)$:

1. $(1+i)(3)(4+i)$
2. $(7)(11)(19)$
3. $(2i+1)(11)(151)$
4. $(47)(71)(139)$
5. $(1+i)(47)(631)$
6. $(71)(83)(491)$
7. $(71)(107)(211)$
8. $(79)(131)(199)$
9. $(127)(131)(4159)$
10. $(127)(139)(1471)$
11. $(127)(191)(379)$
12. $(127)(239)(271)$
13. $(151)(251)(379)$
14. $(167)(251)(499)$
15. $(191)(199)(4751)$
16. $(191)(271)(647)$
17. $(199)(211)(3499)$
18. $(199)(331)(499)$
19. $(199)(379)(419)$
20. $(223)(239)(3331)$
21. $(223)(251)(1999)$
22. $(223)(271)(1259)$
23. $(239)(251)(4999)$
24. $(239)(379)(647)$
25. $(271)(307)(2311)$
26. $(311)(331)(5147)$
27. $(311)(571)(683)$
28. $(431)(467)(5591)$
29. $(431)(491)(3527)$
30. $(431)(503)(3011)$
31. $(431)(647)(1291)$
32. $(599)(859)(1979)$
33. $(631)(811)(2843)$
34. $(631)(1051)(1579)$
35. $(727)(1091)(2179)$
36. $(911)(1223)(3571)$
37. $(911)(1367)(2731)$
38. $(919)(1123)(5059)$
39. $(991)(1487)(2971)$
40. $(1087)(1811)(2719)$
41. $(1151)(1511)(4831)$
42. $(1151)(2111)(2531)$
43. $(1231)(1559)(5851)$
44. $(1231)(1847)(3691)$
45. $(1279)(1847)(4159)$
46. $(1423)(2371)(3559)$
47. $(1471)(2143)(4691)$
48. $(1559)(2699)(3691)$
49. $(1567)(3079)(3191)$
50. $(1847)(2699)(5851)$
51. $(1871)(3191)(4523)$
52. $(1951)(2927)(5851)$
53. $(1951)(3511)(4391)$
54. $(1999)(3331)(4999)$
55. $(1999)(3499)(4663)$
56. $(2143)(4019)(4591)$
57. $(2311)(3851)(5779)$
58. $(2551)(4523)(5851)$

Weak Giuga ideals found in the ring $\mathbb{Z}(\sqrt{-5})$:

1. $(11)(13)(71)$
2. $(11)(17)(31)$
3. $(31)(37)(191)$
4. $(59)(79)(233)$
5. $(71)(73)(2591)$
6. $(71)(113)(191)$
7. $(79)(131)(199)$
8. $(151)(251)(379)$
9. $(191)(197)(6271)$
10. $(191)(199)(4751)$
11. $(199)(211)(3499)$
12. $(199)(331)(499)$
13. $(199)(379)(419)$
14. $(5273)(1319)(1759)$
15. $(5471)(911)(1093)$
16. $(211)(271)(953)$
17. $(211)(317)(631)$
18. $(239)(251)(4999)$
19. $(271)(373)(991)$
20. $(311)(373)(1871)$
21. $(311)(431)(1117)$
22. $(359)(479)(1433)$
23. $(419)(457)(5039)$
24. $(491)(631)(2213)$
25. $(599)(859)(1979)$
26. $(631)(911)(2053)$
27. $(631)(1051)(1579)$
28. $(811)(1231)(2377)$
29. $(2897)(4831)(1811)$
30. $(2897)(1931)(5791)$
31. $(2953)(1231)(2111)$
32. $(3037)(991)(1471)$
33. $(3271)(1091)(1637)$
34. $(859)(1117)(3719)$
35. $(911)(1471)(2393)$
36. $(971)(1553)(2591)$
37. $(1091)(1871)(2617)$
38. $(1151)(4831)(1511)$
39. $(1151)(2111)(2531)$
40. $(1231)(1559)(5851)$
41. $(4591)(1531)(2297)$
42. $(4817)(1979)(3359)$
43. $(4999)(1999)(3331)$
44. $(1559)(2699)(3691)$
45. $(1951)(3511)(4391)$
46. $(2311)(3851)(5779)$
47. $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(\sqrt{-5})$
48. $(2, 1+\sqrt{-5})(3, 2+\sqrt{-5})(\sqrt{-5})$
49. $(\sqrt{-5})(2, 3+\sqrt{-5})(3, 2+5\sqrt{-5})$
50. $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(\sqrt{-5})(13)(137)$
51. $(2, 1+\sqrt{-5})(3, 2+\sqrt{-5})(\sqrt{-5})(13)(137)$
52. $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(6+\sqrt{-5})(7, 4+\sqrt{-5})$
53. $(2, 1+\sqrt{-5})(3, 2+\sqrt{-5})(6+\sqrt{-5})(7, 4+\sqrt{-5})$

References

[1] Şaban Alaca and Kenneth S. Williams, Introductory Algebraic Number Theory, *Cambridge University Press*, New York, NY, 2004.

[2] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* (2) **139**:3 1994 703-722.

[3] D. Borwein, J.M. Borwein, P.B. Borwein, and R. Girgensohn, Giuga's Conjecture on Primality, *The American Mathematical Monthly* **103** 1996 40-50.

[4] J. Borwein, M. Skerritt and C. Maitland, Computation of a lower bound to Giuga's primality conjecture, *Integers* 13 2013.

[5] J. M. Borwein and E. Wong, A survey of results relating to Giuga's conjecture on primality, 1995.

[6] David S. Dummit and Richard M. Foote, Abstract Algebra, *John Wiley and Sons, Inc.*, Hoboken, NJ, 2004.

[7] P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** 1956 201-206.

[8] Graham Everest and Thomas Ward, An Introduction to Number Theory, *Springer-Verlag London Limited*, 2005.

[9] G. Giuga, Su Una Presumibile Proprietà Caratteristica Dei Numeri Primi, *Ist. Lombardo Sci. Lett. Rend. A* **83** 1950 511-528.

[10] D. Guillaume and F. Morain, Building Carmichael numbers with a large number of prime factors, Technical Report LIX/RR/92/01, École Polytechnique, Laboratoire d'Informatique, Palaiseau, France, February 1992.

[11] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th ed., *Oxford University Press Inc.*, New York, 2008.

[12] G. Harman, On the number of Carmichael numbers up to x, *Bull. London Math. Soc.* **37**:5 2005 641-650.

[13] A. Korselt, Problème Chinois, *L'intermédiare des Mathématiciens* **6** 1899 142-143.

[14] G. Löh, On Carmichael numbers whose Carmichael function is squarefree, *Abstracts Amer. Math. Soc.* **14** 1993 390, Abstract 93T-11-61.

[15] G. Löh and W. Niebuhr, Carmichael numbers with a large number of prime factors, II. *Abstracts Amer. Math. Soc.* **10** 1989 305, Abstract 89T-11-131.

[16] D. Marcus, Number Fields, *Springer*, New York, NY, 1977.

[17] R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** 1993 381-391.

[18] G. Ander Steele, Carmichael numbers in number rings, *Journal of Number Theory* **128** 2008 910-917.

[S+09] W. A. Stein et al., *Sage Mathematics Software (Version 7.2)*, The Sage Development Team, 2016, `http://www.sagemath.org`.

[19] Peter Stevenhagen, The arithmetic of number rings, *Algorithmic Number Theory, MSRI Publications*, **44** 2008 209-266.

[20] University of Oxford Mathematical Institute: Course Material for B3.4: Algebraic Number Theory, https://www0.maths.ox.ac.uk/courses/course/28742/material, accessed 17 May 2016.