Giuga Ideals

Duncan Gichimu and Kerrek Stinson

Abstract

In 1950, Giussipe Giuga conjectured that an integer n satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$ if and only if n is prime. Sixty-five years later and this problem is yet to be solved. The complexity of working in the integers has indeed proven challenging. To explore this problem further, we consider the Generalized Giuga Conjecture for ideals in number rings. We introduce the idea of correspondence between weak Giuga numbers and weak Giuga ideals. These concepts are further developed in the quadratic extensions.

1 Introduction

We begin by stating Giuga's conjecture.

Giuga's Conjecture. *[4] n is prime if and only if*

$$s_n = \sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$$

The forward direction holds by Fermat's Little Theorem. Giuga was unable to prove the converse, but he determined the conditions necessary for a counterexample. This is presented in the following theorem.

Theorem 1.1. *[2] A composite number n satisfies $s_n \equiv -1 \pmod{n}$ if and only if for all prime divisors p of n,*

$$\textbf{1)} \quad p \mid \frac{n}{p} - 1 \qquad\qquad \textbf{2)} \quad p - 1 \mid \frac{n}{p} - 1$$

From Theorem 1.1, we have the following definition.

Definition 1.1. *A weak Giuga number is a composite number that satisfies condition* **1** *of Theorem 1.1.*

It follows from the definition that a weak Giuga number is squarefree. Furthermore, squarefree numbers satisfying the second condition were studied extensively by Robert Carmichael in 1910 and are thus termed Carmichael numbers. Formally, a Carmichael number is a composite number n that satisfies $a^n \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$. By Korselt's criterion, this is equivalent to n being square free and $p-1$ dividing $n/p-1$ for all prime divisors p of n. Therefore, a counterexample to Giuga's conjecture is a number which is both weak Giuga and Carmichael. We characterize this condition in the following definition.

Definition 1.2. *A strong Giuga number is a number that is both weak Giuga and Carmichael.*

There are also equivalent characterizations of weak Giuga numbers.

Theorem 1.2. *A composite squarefree number n is a weak Giuga number if and only if it satisfies*

$$\sum_{i=1}^{n} i^{\phi(n)} \equiv -1 \pmod{n},$$

where ϕ is Euler's totient function.

Theorem 1.3. *[4] A composite number $n = p_1 \cdots p_k$, p_i prime, is weak Giuga if and only if*

$$\sum_{i=1}^{k} \frac{1}{p_i} - \prod_{i=1}^{k} \frac{1}{p_i} \in \mathbb{N}.$$

Only a handful of weak Giuga numbers have been discovered. Whether infinitely many exist is unknown, but it is known that there are infinitely many Carmichael numbers. On the other hand, strong Giuga numbers have not been found. If one exists, it has been shown that it would have at least 13,800 prime factors! To overcome this computational nightmare, we move to number rings and explore Giuga's conjecture in a broader context.

2 Generalized Giuga Conjecture

Let K be a number field. Its ring of integers O_K is a Dedekind domain, so every non-zero ideal in O_K may be uniquely factored into a product of prime ideals, up to reordering.
The following notation is used throughout the paper. For composite ideal $\mathcal{N} \subset O_K$, $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$, where $\mathscr{P}_i \subset O_K$ is a prime ideal for all i. We let $Q_i = \prod_{j \neq i} \mathscr{P}_j$. We similarly define q_i for $n \in \mathbb{Z}, n = p_1 \cdots p_k$.
As given by [3], an appropriate generalization of the conjecture is:

Generalized Giuga Conjecture. *Let K be a number field, $\mathcal{N}$ an ideal in O_K and define $I_{\mathcal{N}}$ to be a complete set of non-zero residues of $O_K/\mathcal{N}$, then $\mathcal{N}$ is a prime ideal if and only if*

$$s_{\mathcal{N}} = \sum_{j \in I_{\mathcal{N}}} j^{N(\mathcal{N})-1} \equiv -1 \pmod{\mathcal{N}} \tag{1}$$

It is clear that in the case that $O_K = \mathbb{Z}$, this reduces to the original conjecture. As with Giuga numbers, the generalized conjecture fails if there exists a composite ideal satisfying (1). Such an ideal is characterized by the following theorem, which provides the generalization of Theorem 1.1.

Theorem 2.1. *[3] Let $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$ be an ideal of O_K. $\mathcal{N}$ satisfies (1), if and only if for all $\mathscr{P}_i$,*

$$\textbf{1)} \quad N(Q_i) \equiv 1 \pmod{\mathscr{P}_i} \qquad \textbf{2)} \quad N(\mathscr{P}_i) - 1 \mid N(\mathcal{N}) - 1$$

From the above theorem, the general definitions of weak Giuga ideals and Carmichael ideals become apparent.

Definition 2.1. *A weak Giuga ideal is a composite ideal $\mathcal{N} \subset O_K$, satisfying condition* **1** *of Theorem 2.1.*

Similar to weak Giuga numbers, weak Giuga ideals are squarefree in a more general sense; the norms of all prime factors are relatively prime.

Proposition 2.2. *For any prime factors of a weak Giuga ideal, $\mathscr{P}_1$ and $\mathscr{P}_2$, we have* $\gcd(N(\mathscr{P}_1), N(\mathscr{P}_2)) = 1$.

Proof. Let us suppose that $\gcd(N(\mathscr{P}_1), N(\mathscr{P}_2)) \neq 1$. Let p be the prime under $\mathscr{P}_1$ and $\mathscr{P}_2$. Thus as $N(\mathscr{P}_2)|N(Q_1)$, $p|N(Q_1)$ and $p|N(Q_1)-1$. This directly implies $p|1$, but this cannot be. Thus, we must have $\gcd(N(\mathscr{P}_1), N(\mathscr{P}_2) = 1$. □

Definition 2.2. *A Carmichael ideal is a squarefree composite ideal $\mathcal{N} \subset O_K$ satisfying condition* **2** *of Theorem 2.1.*

Once again, we characterize the counterexamples to the conjecture with a definition.

Definition 2.3. *A strong Giuga ideal is both weak Giuga and Carmichael.*

A strong Giuga number must be odd. The following theorem presents the general result, which says that the norm of a strong Giuga ideal must be odd, as the norm of all its prime factors are odd.

Proposition 2.3. *If $\mathcal{N}$ is a strong Giuga ideal in O_K, then for all prime ideals $\mathscr{P}$, such that $\mathscr{P} \mid \mathcal{N}$, $N(\mathscr{P})$ is odd.*

Proof. We write $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$. The Carmichael condition states that $N(\mathscr{P}_i) - 1|N(Q_i) - 1$ for all i. Assume to the contrary that $N(\mathscr{P}_j) = 2^f$ for some prime ideal factor and $f \in \mathbb{N}$. By Proposition 2.2, $\mathscr{P}_j$ must be the only factor with even norm. Considering prime factor $\mathscr{P}_m$, $m \neq j$, we have $N(\mathscr{P}_m) - 1|N(Q_m) - 1$. But this is impossible, as $N(\mathscr{P}_m) - 1$ is even and $N(Q_m) - 1$ is odd. □

We form the following analogous characterizations of weak Giuga ideals. Extending Theorem 1.2, we have:

Theorem 2.4. *[3] A composite square-free ideal $\mathcal{N}$ is a weak Giuga ideal if and only if*

$$\sum_{j \in I_{\mathcal{N}}} j^{\phi(\mathcal{N})} \equiv -1 \pmod{\mathcal{N}}$$

where $\phi(n)$ is the Euler-Totient function for ideals.

Similarly, we generalize Theorem 1.3.

Theorem 2.5. *Let $\mathcal{N} \subset O_K$ be an ideal. $\mathcal{N}$ is a weak Giuga ideal if and only if*

$$\sum_{i=1}^{k} N(Q_i) - 1 \in \mathcal{N}. \tag{2}$$

Proof. **Weak Giuga $\implies$ (2)**
By assumption $\mathcal{N}$ is a weak Giuga ideal. Thus $N(Q_i)-1 \in \mathscr{P}_i,\ \forall i = 1, \ldots, k$. As seen from the prime factorization of $\mathcal{N}$, $\prod_{i=1}^{k}(N(Q_i) - 1) \in \mathcal{N}$. We expand this product, dropping all terms which have a $N(\mathcal{N})$ as a factor, as $N(\mathcal{N}) \in \mathcal{N}$; this includes any term containing $N(Q_m)N(Q_l),\ m \neq l$. We conclude $(-1)^{k-1}\sum_{i=1}^{k} N(Q_i) + (-1)^k \in \mathcal{N}$, which directly implies $\sum_{i=1}^{k} N(Q_i) - 1 \in \mathcal{N}$.
(2) $\implies$ Weak Giuga
$\sum_{i=1}^{k} N(Q_i) - 1 \in \mathcal{N} \implies \sum_{i=1}^{k} N(Q_i) - 1 \in \mathscr{P}_j,\ \forall j = 1, \ldots, k$. For any $j = 1, \ldots, k$, as $N(\mathscr{P}_j) \in \mathscr{P}_j$, $N(Q_i) \in \mathscr{P}_j, \forall i \neq j$. From this, we conclude that $\sum_{i=1}^{k} N(Q_i) - 1 - (\sum_{i\neq j} N(Q_i)) = N(Q_j) - 1 \in \mathscr{P}_j$ as desired. □

It is not known if strong Giuga ideals exist; however, infinitely many Carmichael ideals exist in any normal extension [5]. For two number rings, we have computationally found weak Giuga ideals, thus showing their existence in infinitely many extensions by Corollary 4.4, but it is not known if there is a weak Giuga ideal in every extension or are infinitely many in a single extension. Our paper predominantly explores weak Giuga ideals as this is the first step to expanding to the more specific case of strong Giuga ideals.

In the following examples we present some weak Giuga ideals as their prime factorization in the Gaussian integers and $\mathbb{Z}(\sqrt{-5})$.

Example 1. *Gaussian integers, $\mathbb{Z}[i]$*

1. $(1+i)(3)(4+i)$
2. $(71)(107)(211)$
3. $(1+i)(79)(631)(1087)$
4. $(47)(71)(139)$
5. $(1+i)(47)(631)$
6. $(79)(131)(199)$
7. $(7)(11)(4+i)(17+2i)$
8. $(1231)(1511)(47+10i)$

Example 2. $\mathbb{Z}(\sqrt{-5})$

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

It is worth noting that if a prime factor of a Giuga ideal has the same norm as some other ideal in O_K, then that other ideal can substituted into the prime factorization and the result will still be weak Giuga. For instance, from example 1.1, $(1+i)(3)(4-i)$ is also a weak Giuga ideal.

3 Correspondence

One of the primary motivations for working in the general framework of number rings is to gain insight into the behavior of weak Giuga numbers. Thus, we develop the idea of correspondence which relates ideals and numbers. We begin by defining the corresponding ideal:

Definition 3.1. *Given $n = p_1 \cdots p_k \in \mathbb{N}$, p_i prime, and a ring of integers O_K, we define a corresponding ideal to be $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$, where $\mathscr{P}_i \subset O_K$ is a prime ideal and $\mathscr{P}_i \,|(p_i)$. We say that n corresponds to $\mathcal{N}$.*

We note that there may be many corresponding ideals in O_K for a given $n \in \mathbb{N}$. Similarly, we define the corresponding number of the ideal $\mathcal{N}$, $n \in \mathbb{N}$.

Definition 3.2. *Given ideal $\mathcal{N} \subset O_K$, we define the corresponding number of $\mathcal{N}$ to be the unique $n \in \mathbb{N}$ such that $\mathcal{N} \cap \mathbb{Z} = (n)$.*

We say that $\mathcal{N}$ is above n or n is below $\mathcal{N}$.

Example 3. *Take the Gaussian integers, $30 = 2 \cdot 3 \cdot 5$ corresponds to $(1+i)(3)(2+i) \subset \mathbb{Z}[i]$ because $(2) = (1+i)^2$, $(3) = (3)$ and $(5) = (2+i)(2-i)$.*

Definition 3.3. *$\mathcal{N} \subset O_K$ and $\mathcal{N}' \subset O_{K'}$ are associated ideals if they lie above the same $n \in \mathbb{N}$. More formally described, $\mathcal{N}$ and $\mathcal{N}'$ are associated if $\mathcal{N} \cap \mathbb{Z} = \mathcal{N}' \cap \mathbb{Z}$. We denote this association $\mathcal{N} \sim \mathcal{N}'$.*

We note that $\mathcal{N} \cap \mathbb{Z} = (p_1 \cdots p_k)$ where p_i is such that $(p_i) = \mathscr{P}_i \cap \mathbb{Z}$; this directly implies that if $\mathcal{N} \sim \mathcal{N}'$, then each ideal has the same number of prime factors.
The following theorem provides criteria for when an associated ideal of a weak Giuga ideal is itself weak Giuga.

Theorem 3.1. *Let O_K and $O_{K'}$ be number rings. $\mathcal{N} \subset O_K$ and $\mathcal{N}' \subset O_{K'}$ with $\mathcal{N} \sim \mathcal{N}'$. If $N(\mathcal{N}) = N(\mathcal{N}')$, then $\mathcal{N}$ is weak Giuga if and only if $\mathcal{N}'$ is weak Giuga.*

Proof. Assume that $\mathcal{N}$ is a weak Giuga ideal. By the preceding comments, both $\mathcal{N}$ and $\mathcal{N}'$ have k prime factors. By Proposition 2.2, each prime factor $\mathscr{P}_i$ of $\mathcal{N}$ is above a different prime $p_i \in \mathbb{N}$. For a given prime factor of $\mathcal{N}$, we know that $N(\mathscr{P}_i) = p_i^f$, where p_i is the prime beneath $\mathscr{P}_i$ and $f \in \mathbb{N}$. As $N(\mathscr{P}_i) | N(\mathcal{N}) = N(\mathcal{N}')$, there exists a prime factor $\mathscr{P}'_i$ of $\mathcal{N}'$ above p_i. As $\mathcal{N}$ and $\mathcal{N}$ have the same number of prime factors, we obtain a bijection from the prime factors of $\mathcal{N}$ to the prime factors of $\mathcal{N}'$ with $N(\mathscr{P}_i) = N(\mathscr{P}'_i)$.

As $N(\mathscr{P}_i) = N(\mathscr{P}'_i)$, $\mathscr{P}_i \sim \mathscr{P}'_i$. By the association, we have $\mathscr{P}_i \cap \mathbb{Z} = (p_i) = \mathscr{P}'_i \cap \mathbb{Z}$. This implies that $p_i | N(Q_i) - 1 = N(Q'_i) - 1$, and consequently that $N(Q'_i) - 1 \in \mathscr{P}'_i$ for all i. □

An equivalent hypothesis for the above theorem is that $\mathcal{N}$ and $\mathcal{N}'$ have the same number of prime factors, and for each prime factor, the norm is equal, i.e. $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k \subset O_K$ and $\mathcal{N}' = \mathscr{P}'_1 \cdots \mathscr{P}'_k \subset O_{K'}$ and for each i, $N(\mathscr{P}_i) = N(\mathscr{P}'_i)$.

It is natural at this point to ask when a number has a corresponding weak Giuga ideal. We find that every squarefree composite number corresponds to a weak Giuga ideal in a cyclotomic extension. By Proposition 2.2, this is the largest set of numbers possible.

The result shows that looking at corresponding numbers generally is unrestrictive, and we are encouraged to focus on specific extensions. Section 4 on quadratic extensions does precisely this.

Let ζ_m be a primitive mth root of unity.

Theorem 3.2. *[1, pg.260] Given $m \in \mathbb{N}$, let $K = \mathbb{Q}(\zeta_m)$ and $p \in \mathbb{N}$ be a prime with $m = p^r m_1$, where $r \in \mathbb{N} \cup \{0\}$, $m_1 \in \mathbb{N}$, and $p \nmid m_1$. Let h be*

the least positive integer such that $p^h \equiv 1 \pmod{m_1}$. *Then for a prime ideal* $\mathscr{P} \subset O_K$ *such that* $\mathscr{P} \,|(p)$, $N(\mathscr{P}) = p^h$.

Theorem 3.3. *For every squarefree composite* $n = p_1 \cdots p_k \in \mathbb{N}$, *there exists* O_K *such that a corresponding ideal* $\mathcal{N} \subset O_K$ *of* n *is a weak Giuga ideal.*

Proof. Let $K = \mathbb{Q}(\zeta_n)$. Let $\mathcal{N} \subset O_K$ be a corresponding ideal of n. By the preceding theorem, we know that for $\mathscr{P}_j \,|(p_j)$, $\mathscr{P}_j$ a prime factor of $\mathcal{N}$, $N(\mathscr{P}_j) \equiv 1 \pmod{n/p_j} \implies N(\mathscr{P}_j) \equiv 1 \pmod{p_i}$ for all $i \neq j$. Thus $N(Q_i) = \prod_{j \neq i} N(\mathscr{P}_j) \equiv 1 \pmod{p_i}$ for all i as desired. □

4 Quadratic Extensions

We further our exploration of Giuga's conjecture in quadratic extensions. These extensions are very tractable as the norms of prime ideals are simple to calculate. We consider correspondences between Giuga numbers and Giuga ideals in quadratic extensions.

Theorem 4.1. *Let* $n \in \mathbb{N}$, $n = p_1 \cdots p_k$, p_i *prime for all* i. *Let* O_K *be a quadratic extension.*

1. *If all* p_i *split or ramify in* O_K, *then* n *is a weak Giuga number if and only if the corresponding ideal* $\mathcal{N}$ *is a weak Giuga ideal.*

2. *If all* p_i *are inert in* O_K *and* n *is a weak Giuga number, a corresponding ideal* $\mathcal{N} \subset O_K$ *is a weak Giuga ideal.*

Proof. **1.** In this case, $(p_i) = \mathscr{P}_{i,1}\,\mathscr{P}_{i,2}$, where $\mathscr{P}_{i,j}$ is a nontrivial prime ideal. We define the corresponding ideal $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$, where $\mathscr{P}_i = \mathscr{P}_{i,1}$ or $\mathscr{P}_i = \mathscr{P}_{i,2}$. From the Ramification and Inertial Degree identity ($\sum e_i f_i = n$, where $n = 2$ for quadratic extensions), we have that $N(\mathscr{P}_i) = p_i$ for all i. By Theorem 3.1, we see that n is a weak Giuga number if and only if $\mathcal{N}$ is a weak Giuga ideal.

2. In the inert case, we have $(p_i) = \mathscr{P}_i$ a prime ideal. We define $\mathcal{N} = \mathscr{P}_1 \cdots \mathscr{P}_k$. By the Ramification and Inertial Degree identity, we have that $N(\mathscr{P}_i) = p_i^2$ for all i. For $\mathcal{N}$ to be weak Giuga, we must have $N(Q_i) - 1 \in \mathscr{P}_i$ for all i. $N(Q_i) - 1 = q_i^2 - 1 = (q_i - 1)(q_i + 1)$. By hypothesis, $p_i | q_i - 1$, which implies $p_i | N(Q_i) - 1$; equivalently, it is implied $N(Q_i) - 1 \in \mathscr{P}_i$ for all i. Thus, $\mathcal{N}$ is a weak Giuga ideal. □

Example 4. *In Example 2.6,* $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(\sqrt{-5})$ *corresponds to the weak Giuga number* 30*. The rational primes underneath the ideals are 2,3 and 5 respectively. Also note that 2,3 and 5 either split or ramify.* $2O_K = (2, 1+\sqrt{-5})^2$, $3O_K = (3, 2+\sqrt{-5})(3, 1+\sqrt{-5})$ *and* $5O_K = (\sqrt{-5})^2$

From comments following Theorem 3.1, we know that we may construct Giuga ideals from other Giuga ideals when norms are preserved for the prime factors of the ideals. The following theorem provides the tools to do exactly this in quadratic number rings.

Theorem 4.2. *Given distinct positive rational primes* $p_1, \ldots, p_k$*, and a tripartition of* $\{1, \ldots, k\}$*,* U_r, U_s*, and* U_n*, we may construct infinitely many distinct quadratric number rings* O_K *such that* U_r, U_s*, and* U_n *contain indices for ramified, split, and inert primes respectively.*

Proof. We assume $p_i \neq 2$ for i. For the case when $p_i = 2$ for some i, an additional equation as given by [6, p.74] is included in the system of equations (3) below. Otherwise, the argument is the same.

We find a set H of infinite cardinality such that for $c \in H$ and $K = \mathbb{Q}(\sqrt{c})$, O_K has the desired splitting properties. By [6, p.74], if c is such that

$$\begin{aligned} c &\equiv a_i \pmod{p_i}, \forall\ i \in U_s \\ c &\equiv b_i \pmod{p_i}, \forall\ i \in U_n, \end{aligned} \tag{3}$$

where a_i is a nonzero quadratic residue of p_i and b_i is a quadratic nonresidue of p_i, then O_K will have the desired splitting properties for p_i, $i \in U_s \cup U_n$. As $p_i \geq 3$ for all $i \in \{1, \ldots, k\}$, the desired a_i and b_i exist. As $\gcd(p_i, p_j) = 1$ for $i \neq j$, we apply the Chinese Remainder Theorem to find a residue class $\bar{c}$ of $\mathbb{Z}/S\mathbb{Z}$, $S = \prod_{i \in U_s \cup U_n} p_i$, such that for $c \in \bar{c}$, the system of equations (3) is satisfied. We note that $\bar{c} = \{t + Sx : \ x \in \mathbb{Z}\}$, for some t, $0 < t < S$, with $\gcd(t, S) = 1$; this follows from our choice of nonzero quadratic residues.

Let us now consider U_r. For O_K to have the desired properties, we must have $p_i | c$, for all $i \in U_r$ [6, p.74]. Thus $c \in \bar{W} = \{Wy : y \in \mathbb{Z}\}$, $W = \prod_{i \in U_r} p_i$. Thus our desired $H = \{c \in \bar{W} \cap \bar{c} : c \text{ is squarefree}\}$. Let us show that this set is nonempty and of infinite cardinality. Consider $c \in \bar{W} \cap \bar{c}$. $c = Wy = t + Sx$ for some $x, y \in \mathbb{Z}$. We show that such x and y exist. We rewrite our equation as $Wy + (-S)x = t$. By Bezout's Identity, there exist $x_0, y_0 \in \mathbb{Z}$ such

that $Wy_0 + (-S)x_0 = \gcd(W, -S) = 1$. Multiplying by t, we construct a general solution to our original equation: $x = tx_0 + rW$ and $y = ty_0 + rS$, $r \in \mathbb{Z}$. Thus for $c \in \bar{W} \cap \bar{c}$, we may write $c = W(ty_0 + rS)$, $r \in \mathbb{Z}$. We now show that there are infinitely many nonsquares of this form. Clearly, this condition will be satisfied if there are infinitely many primes of the form $ty_0 + rS$. By Dirichlet's Theorem on arithmetic progressions, this is true if $\gcd(ty_0, S) = 1$. If $\gcd(ty_0, S) \neq 1$, then $\gcd(y_0, S) \neq 1$ as t and S are relatively prime. However, by construction of y_0, this would imply there exists $p \geq 2$ such that $p|1$. This of course cannot be the case, and we conclude $\gcd(ty_0, S) = 1$. From previous remarks, we conclude that H is of infinite cardinality, as desired. □

Note that this proof holds so long as $U_r, U_s,$ or U_n is nonempty.

Corollary 4.3. *There are infinitely many quadratic extensions O_K such that $n = p_1 \cdots p_k \in \mathbb{N}$, a weak Giuga number, corresponds to a weak Giuga ideal $\mathcal{N}$. There also exists infinitely many O_K such that (n) is a weak Giuga. Furthermore, if n is a strong Giuga number, there are infinitely many O_K with a corresponding strong Giuga ideal, $\mathcal{N}$.*

Proof. By Theorem 4.1, we have that $\mathcal{N}$ is a weak Giuga ideal if $p_1, \ldots, p_k$ are ramified or inert for all i. Theorem 4.2 shows that we may construct infinitely many O_K such that this is true. In the inert case, (n) is the corresponding Giuga ideal. If n is a strong Giuga number, $\mathcal{N}$ is a strong Giuga ideal in the ramified case as $N(\mathscr{P}_i) = p_i$ for all i. □

Corollary 4.3 shows that a weak Giuga number corresponds to infinitely many weak Giuga ideals in quadratic extensions under weaker conditions than those of Theorem 3.1. This motivates us to ask whether a weak Giuga number can correspond to a weak Giuga ideal in all quadratic extensions. Theorem 4.5, although of interest in its own right, is used to show that this cannot be the case.

Corollary 4.4. *Let O_K be a quadratic number ring. Given a weak (strong) Giuga ideal $\mathcal{N} \subset O_K$ we may find infinitely many other quadratic number rings with a weak (strong) Giuga ideal.*

Proof. We know from Theorem 3.1 that if we find $K' = \mathbb{Q}(\sqrt{c})$ such that each corresponding prime p_i has the same splitting properties in $O_{K'}$ as O_K, then there exists a weak Giuga ideal in $O_{K'}$. By Theorem 4.2, a set F of infinite

cardinality such that $c \in F$ constructs a desired ring of integers exists. This proof holds for strong Giuga ideals as preservation of splitting properties implies preservation of norms for associated prime ideals. □

From our examples in Section 2, we may now conclude infinitely many quadratic extensions have weak Giuga ideals. Although Corollary 4.4 is somewhat limited in scope, 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.

Theorem 4.5. *Let O_K be a quadratic extension. If n is a weak Giuga number that has a corresponding weak Giuga ideal $\mathcal{N}$ in O_K, and n has at least one prime factor which splits or ramifies and at least one which is inert, then n is a nonunit multiple of another weak Giuga number.*

Proof. Partition $\{1, \ldots, k\}$ into U_s and U_n, such that for $i \in U_s$, p_i splits or ramifies in O_K, and for $i \in U_n$, p_i is inert in O_K. For $i \in U_s$, $N(\mathscr{P}_i) = p_i$, and for $i \in U_n$, $N(\mathscr{P}_i) = p_i^2$. As $\mathcal{N}$ is a weak Giuga ideal, we have $p_i | N(Q_i) - 1$ for all i. Let $m_i = \prod_{j \in U_n - \{i\}} p_j$. We have $N(Q_i) - 1 = q_i(m_i - 1) + (q_i - 1)$. By hypothesis, $p_i | q_i - 1$ for all i; thus, $p_i | m_i - 1$ for all i, as it clearly cannot divide q_i. Narrowing this statement, we have $p_i | m_i - 1$ for all $i \in U_n$. Consequently, $\prod_{i \in U_n} p_i$ is a weak Giuga number. By hypothesis, $U_s \neq \emptyset$, and we have our conclusion. □

If n is an even weak Giuga number which satisfies the hypothesis of Theorem 4.5 and 2 ramifies or splits in the given extension, then we have the existence of an odd weak Giuga number. As a strong Giuga number must be odd, further study of this relation may be of value.

Corollary 4.6. *Given weak Giuga number n, there are infinitely many quadratic number rings O_K for which the corresponding ideals are not weak Giuga ideals.*

Proof. Partition $\{1, \ldots, k\}$ into U_s and U_n such that $|U_n| = 2$. By Theorem 4.2, there exist infinitely many O_K such that for $i \in U_s$, p_i splits or ramifies, and for $i \in U_n$, p_i is inert. By Theorem 4.5, $m = \prod_{i \in U_n}$ is a weak Giuga number. But this is a contradiction, as there exist no weak Giuga numbers with exactly two prime factors. Thus in each such O_K, $\mathcal{N}$ is not a weak Giuga ideal. □

for $i \in U_s$, p_i splits or ramifies

5 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. Such findings suggest that the following questions may be more tractable in the context of number rings, and 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?

References

[1] Ş. Alaca, K. Williams, *Introductory Algebraic Number Theory*. Cambridge University Press, New York, NY, 2004.

[2] D. Borwein, J. M. Borwein, P. B. Borwein,and R. Girgensohn, *Giuga's Conjecture on Primality*. 1991.

[3] J. Burns, K. Casey, and G. Johnson, *Generalizations of the Giuga Number and Some of Its Properties to Number Fields*. Unpublished paper, 2014.

[4] G. Giuga *Su una presumible proprieta caratteristica dei numeri primi* Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. 14(83) (1950), 511–528.

[5] K. Kim, *Generalization of Carmichael Ideals in a field Extension*. Unpublished paper, 2015.

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