#A89 INTEGERS 20 (2020)

DISTINCT COVERING SYSTEMS IN NUMBER FIELDS

Daniel Baczkowski
Department of Mathematics, The University of Findlay, Findlay, Ohio
baczkowski@findlay.edu

Aaron Blodgett
Department of Mathematics, The University of Findlay, Findlay, Ohio
blodgetti@findlay.edu

Received: 1/9/20, Accepted: 10/14/20, Published: 10/19/20

Abstract

Beginning in the late 1960s to study the minimum modulus and odd covering problems of Erdős, Jordan and others investigated analogous problems in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$. It is known that distinct coverings exist for $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ and that the latter has a distinct covering with all moduli having odd norm. We prove similar results hold more generally in any ring of integers with certain properties. As an application of our general constructions, we prove that an analogous problem to that of the unresolved problem of Erdős, the odd covering problem, holds affirmatively in infinitely many quadratic integer rings; more precisely, there exist infinitely many quadratic integer rings possessing a covering system with distinct ideal moduli that have odd norms greater than or equal to 3. All our coverings are explicitly constructed.

1. Introduction

A *covering system of congruences* (or more often simply called a *covering*) for the rational integers is a finite collection of congruences with the property that every integer satisfies at least one congruence in the system. More precisely, a *covering* for the integers is a finite set $\{(r_1, m_1), (r_2, m_2), \ldots, (r_t, m_t)\}$ for which each integer n satisfies $n \equiv r_i \pmod{m_i}$ for some $1 \leq i \leq t$.

The notion of coverings has been applied to many problems in number theory. First introduced by Erdős, who later applied the idea to disprove a century-old conjecture of de Polignac, Erdős showed there are infinitely many odd integers that are not of the form $2^k + p$ where p is a prime [8]. This led to related investigations on sequences of numbers of the form $k - 2^n$, $k \cdot 2^n \pm 1$ (so-called Sierpiński [25] and Riesel [24] numbers), and many more similarly related numbers (cf. [5, 6, 7]). Related problems involving Fibonacci numbers [20, 21, 22], the Lucas numbers [3], and polygonal numbers [1, 2] appear in the literature, too.

A covering system for the integers is called *distinct* (or *incongruent*) if all the moduli m_i are distinct and ≥ 1. An example of a distinct covering for the integers is the set of congruences $\{(0,2),(0,3),(1,4),(5,6),(7,12)\}$. Erdős asked whether for any arbitrarily large N there exists a distinct covering system with the minimum of the moduli $\geq N$. Hough [13] solved the problem by answering negatively; that is, Hough proved there is an (effective) upper bound for the smallest moduli in a distinct covering.

Erdős offered \$25 for a proof of the nonexistence of a distinct covering system having all odd moduli, while Selfridge offered \$900 for an explicit example of such a covering [12]. It is known that if such a covering system exists, then the least common multiple of the moduli must have at least 22 distinct prime divisors [11].

Work has been done in the more general setting of the ring of the integers in a number field rather than the rational integers. Analogous problems to many of those mentioned above can be studied within this setting, and more rigorous details will be provided in the next section. Jordan proved that there exists a covering for the Gaussian integers $\mathbb{Z}[i]$ with the moduli being neither units nor associates of another modulus [17]. Jordan also proved there exists a covering for $\mathbb{Z}[\sqrt{-2}]$ with the moduli being neither units nor associates of another modulus and the norm of all moduli are odd [16]. Within the setting of $\mathbb{Z}[\sqrt{-2}]$, this answered an analogous unsolved problem of Erdős on whether or not there exists a covering of the rational integers having all odd distinct moduli.

Also in $\mathbb{Z}[\sqrt{-2}]$, an investigation into a problem similar to the minimum modulus problem of Erdős for rational integers was studied and results were proven showing for this ring that there exists certain types of coverings where norms of the moduli are all > 2, > 3 and > 5 [18]. Moreover, the authors offered monetary rewards for a proof of existence (and proof of nonexistence) of a certain type of covering for $\mathbb{Z}[\sqrt{-2}]$ such that the minimum modulus can (or cannot) have arbitrarily large norm [18]. There is also a monetary award for the analogous problem in $\mathbb{Z}[i]$ [18].

A positive, odd integer k is called a Sierpiński number if $k2^n + 1$ is composite for all positive integers n. In 1962, John Selfridge conjectured that $k = 78557$ is the smallest Sierpiński number. This conjecture is still unresolved today. The analogous problem of Selfridge in all rings of integers $\mathbb{Q}(\sqrt{d})$ with $d < 0$ and having unique factorization was answered by Jones and White [15].

Within this work, we extend some of the aforementioned results of Jordan et al. We construct various coverings for rings of integers of number fields (with ideals for moduli). We discuss both the case with general ideals and with principal ideals for moduli. As an application of our work, we prove that the unresolved odd covering problem of Erdős holds affirmatively in infinitely many quadratic integer rings; more precisely, there exist infinitely many quadratic integer rings possessing a covering system with distinct ideal moduli that have odd norms ≥ 3.

2. Terminology

For positive integers m, let $\zeta_m = e^{2\pi i/m}$. Since ζ_m is a root of the polynomial $x^m - 1$, one deduces that ζ_m is an algebraic integer. Also, $\zeta_m, \zeta_m^2, \zeta_m^3, \ldots, \zeta_m^m$ are the roots of $x^m - 1$ and referred to as *roots of unity*. One refers to ζ_m^k with $1 \leq k \leq m$ and $\gcd(k, m) = 1$ (of which there are $\phi(m)$ choices) as *primitive roots of unity* since each is not a root of $x^\ell - 1$ for any $\ell < m$. It is well known that $\mathbb{Z}[\zeta_m]$ is the ring of integers of $\mathbb{Q}(\zeta_m)$.

More generally, suppose K is a finite algebraic extension of $\mathbb{Q}$. It is known that $K = \mathbb{Q}(\alpha)$ for some algebraic number α; that is, K is an *algebraic number field* (or simply *number field*). Let $\beta \in K$, and suppose that $\beta, \beta_2, \beta_3, \ldots, \beta_n$ (not necessarily distinct) are the field conjugates of β. The *norm* of β, denoted by $N(\beta)$, is often defined as $N(\beta) = \beta\beta_2\beta_3 \cdots \beta_n$. Moreover, if $f(x) = \sum_{0 \leq j \leq m} a_j x^j$ is the minimal polynomial for β, then

$$N(\beta) = (-1)^n a_0^{n/m}. \tag{1}$$

The norm satisfies the property for any $\beta, \gamma \in K = \mathbb{Q}(\alpha)$ that $N(\beta\gamma) = N(\beta)N(\gamma)$.

Let $\mathcal{O}_K$ denote the ring of integers for K, and let $\mathfrak{a}$ denote a nonzero ideal of $\mathcal{O}_K$. The *norm of* $\mathfrak{a}$ is $N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|$. If $\mathfrak{a} = \langle a \rangle$ is a principal ideal, then $N(\mathfrak{a}) = |N(a)|$.

We consider the analogous notion of a covering for $\mathcal{O}_K$; namely, a covering system of congruences for $\mathcal{O}_K$ is a set $C = \{(\alpha_1, \mathfrak{a}_1), (\alpha_2, \mathfrak{a}_2), \ldots, (\alpha_t, \mathfrak{a}_t)\}$ for which every element x in $\mathcal{O}_K$ satisfies $x \equiv \alpha_i \pmod{\mathfrak{a}_i}$ for some $1 \leq i \leq t$. Similarly, we call a covering system *distinct* in $\mathcal{O}_K$ if the moduli are all different ideals. In the case where the ideals are principal, this agrees with the definition used by Jordan et al. that no two of the ideal generators are associates. If the norm for each of the moduli in C is distinct, that is $N(\mathfrak{a}_i) \neq N(\mathfrak{a}_j)$ for all $i \neq j$, then we say C is a *distinct-norm covering* for $\mathcal{O}_K$. Note that the latter is a stronger property, since it implies no two of the moduli from C are the same.

Another fundamental tool for our proofs is the well-known Chinese remainder theorem (cf. [19]). We state this, along with notation used within this work.

Lemma 1 (Chinese remainder theorem). *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals of a commutative ring with unity R such that $\mathfrak{a}_i + \mathfrak{a}_j = R$ for all $i \neq j$. Given elements $x_1, x_2, \ldots, x_n \in R$, there exists $x \in R$ such that $x \equiv x_i \pmod{\mathfrak{a}_i}$ for all i.*

Within this work to help simplify our notation, we denote the congruence class $(x, \prod_{1 \leq i \leq n} \mathfrak{a}_i)$ existing via the Chinese remainder theorem by

$$\big[(x_1, \mathfrak{a}_1), (x_2, \mathfrak{a}_2), \ldots, (x_n, \mathfrak{a}_n)\big] = \Big(x, \prod_{1 \leq i \leq n} \mathfrak{a}_i\Big).$$

Lastly, we state a rudimentary idea that we will use several times, which allows one to use some of our constructions to produce covering systems with principal ideals.

Proposition 1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals in a commutative ring with unity, then $\mathfrak{ab}$ is a principal ideal.*

3. Main Results

We are now ready for the results and proofs of the paper. Throughout, we assume in general that K is a finite algebraic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. The following result is intended to familiarize the reader with the notions used within this work and provide a connection between coverings in $\mathbb{Z}$ to those in $\mathcal{O}_K$.

Theorem 1. *If $\mathcal{O}_K$ has a prime ideal $\mathfrak{p}$ of norm 2, then it has a distinct-norm covering system. Moreover, if the ideal $\mathfrak{p}$ is principal, then all ideals in the covering are principal.*

Proof. Let $\mathfrak{c}$ be any nonzero ideal that is relatively prime to $\mathfrak{p}$ having residue classes represented by $\gamma_1, \gamma_2, \ldots, \gamma_n$. The two residue classes modulo $\mathfrak{p}$ can be represented by 0 and $\beta_1 := 1$. Recursively for $k \geq 2$, define β_k and β_k' to be representatives for the two residue classes modulo $\mathfrak{p}^k$ that lie inside β_{k-1} modulo $\mathfrak{p}^{k-1}$. The set of congruences

$$(0, \mathfrak{p}), (\beta_2', \mathfrak{p}^2), \ldots, (\beta_{n-1}', \mathfrak{p}^{n-1})$$

is only missing $(\beta_{n-1}, \mathfrak{p}^{n-1})$, which can be covered by

$$(\gamma_1, \mathfrak{c}), \big[(\gamma_2, \mathfrak{c}), (\beta_1, \mathfrak{p})\big], \ldots, \big[(\gamma_n, \mathfrak{c}), (\beta_{n-1}, \mathfrak{p}^{n-1})\big].$$

Putting together all of these congruences forms a covering. Lastly, it is easily seen to be a distinct-norm covering upon considering the norms of the ideals. The latter part of the theorem follows from Proposition 1 with $\mathfrak{p}$ and $\mathfrak{c} = \langle 3 \rangle$. □

Using Theorem 1, one can deduce immediate results for some cyclotomic fields.

Corollary 1. *For any integer $n \geq 1$, there exists a distinct-norm covering having all principal ideals for $\mathbb{Z}[\zeta_{2^n}]$.*

Proof. For $n = 1$, one easily discovers that $\mathbb{Z}[\zeta_2] = \mathbb{Z}$, which has a distinct covering as mentioned in the introduction. Now, we deal with $n \geq 2$. Let $\zeta = \zeta_{2^n}$, $\beta = 1 + \zeta$, and $k = 2^{n-1}$. It is well known that the minimal polynomial for ζ_{2^n} is $x^k + 1$. By the fact that $f(x)$ is irreducible if and only if $f(x-1)$ is irreducible, one deduces that $g(x) := (x-1)^k + 1$ is irreducible and has the root β. Therefore, $g(x)$ is the minimal polynomial for β. By (1), we deduce $N(\langle \beta \rangle) = N(\beta) = 2$. By Theorem 1, there exists a distinct-norm covering for $\mathbb{Z}[\zeta]$. By Theorem 1 with $\mathfrak{p} = \langle \beta \rangle$, one finds that all ideal moduli are principal. □

The next theorem pertains to distinct-norm coverings with the norm of each modulus being ≥ 4.

Theorem 2. *If $\mathcal{O}_K$ has ideals $\mathfrak{p}$ and $\mathfrak{b}$ with $N(\mathfrak{p}) = 2$ and $N(\mathfrak{b}) = 3$, then it has a distinct-norm covering with the norm of each modulus being ≥ 4. Moreover, if $\mathfrak{p}$ and $\mathfrak{b}$ are principal ideals, then all ideals in the covering are principal.*

Proof. Let $\mathfrak{c}$ be an ideal that is relatively prime to $\mathfrak{p}$ and $\mathfrak{b}$ having residue classes represented by $\gamma_1, \gamma_2, \ldots, \gamma_n$. The two residue classes modulo $\mathfrak{p}$ can be represented by $\alpha_1 := 0$ and $\beta_1 := 1$. Recursively, define α_k and α_k' to be representatives for the two residue classes modulo $\mathfrak{p}^k$ that lie inside α_{k-1} modulo $\mathfrak{p}^{k-1}$. Recursively, define β_k and β_k' to be representatives for the two residue classes modulo $\mathfrak{p}^k$ that lie inside β_{k-1} modulo $\mathfrak{p}^{k-1}$. Let S denote the covering within the proof of Theorem 1, namely

$$(0, \mathfrak{p}),\ (\beta_2', \mathfrak{p}^2), \ldots, (\beta_{n-1}', \mathfrak{p}^{n-1})$$

and

$$(\gamma_1, \mathfrak{c}),\ \big[(\gamma_2, \mathfrak{c}), (\beta_1, \mathfrak{p})\big], \ldots, \big[(\gamma_n, \mathfrak{c}), (\beta_{n-1}, \mathfrak{p}^{n-1})\big].$$

Let $S_1 = S \setminus \{(0, \mathfrak{p})\}$, and take note that S_1 covers $(1, \mathfrak{p})$.

Let S' denote the similar covering containing the set of congruences:

$$(1, \mathfrak{p}),\ (\alpha_2', \mathfrak{p}^2), \ldots, (\alpha_{n-1}', \mathfrak{p}^{n-1})$$

and

$$(\gamma_1, \mathfrak{c}),\ \big[(\gamma_2, \mathfrak{c}), (\alpha_1, \mathfrak{p})\big], \ldots, \big[(\gamma_n, \mathfrak{c}), (\alpha_{n-1}, \mathfrak{p}^{n-1})\big].$$

Let $S_0 = S' \setminus \{(1, \mathfrak{p})\}$, and take note that S_0 covers $(0, \mathfrak{p})$.

Again, we construct a covering C for $\mathcal{O}_K$. Start by including S_1 in C. It suffices to cover $(0, \mathfrak{p})$ to finish the covering. The residue classes modulo $\mathfrak{b}$ can be represented by 0, 1, and 2. In addition, $(0, \mathfrak{p})$ is equivalent to $c_1 = [(0, \mathfrak{p}), (0, \mathfrak{b})]$, $[(0, \mathfrak{p}), (1, \mathfrak{b})]$, $[(0, \mathfrak{p}), (2, \mathfrak{b})]$. We include c_1 in C. We also include $S_2 = \bigcup_{c \in S_0} [c, (1, \mathfrak{b})]$, which covers the second of these. It remains to cover $c' = [(0, \mathfrak{p}), (2, \mathfrak{b})]$. Observe that $(2, \mathfrak{b})$ is equivalent to $(\delta_1, \mathfrak{b}^2)$, $(\delta_2, \mathfrak{b}^2)$, and $(\delta_3, \mathfrak{b}^2)$ for some $\delta_1, \delta_2, \delta_3$; therefore, c' is equivalent to the union of classes

$$c_2 = \big[(0, \mathfrak{p}), (\delta_1, \mathfrak{b}^2)\big],\ \big[(0, \mathfrak{p}), (\delta_2, \mathfrak{b}^2)\big], \text{ and } \big[(0, \mathfrak{p}), (\delta_3, \mathfrak{b}^2)\big].$$

We include c_2 in C, and the second is contained in $c_3 = (\delta_2, \mathfrak{b}^2)$, which we also include. The third is contained in $S_3 = \bigcup_{c \in S_0} [c, (\delta_3, \mathfrak{b}^2)]$. All together, C consists of the congruences c_1, c_2, c_3 and the sets of congruences S_1, S_2, S_3.

The norms of the ideals in the first three classes are $2 \cdot 3$, $2 \cdot 3^2$, and 3^2, respectively. For $k \in \{1, 2, 3\}$, the norms of the ideals in S_k are $2^i 3^{k-1}$ with $2 \leq i \leq n - 1$ and $2^j 3^{k-1} n$ with $0 \leq j \leq n - 1$. The integer n is relatively prime to 2 and 3 by choice of $\mathfrak{c}$; thus, all ideals have distinct norms. For the latter part of the theorem, one need only pick $\mathfrak{c}$ to be principal at the beginning of the proof and use Proposition 1. $\square$

Our upcoming results for quadratic integer rings utilize the following lemma. Within certain quadratic integer rings, the lemma provides necessary conditions for an element and its conjugate to not be associates.

Lemma 2. *Let* $n \neq \pm 1$ *be an odd squarefree integer. Also, let* $d \equiv 2, 3 \pmod 4$ *be squarefree with* $\gcd(d, n) = 1$. *If there exists* $\gamma := a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ *having norm* n*, then* $\langle \gamma^i \rangle + \langle \bar{\gamma}^j \rangle = \mathbb{Z}[\sqrt{d}]$ *and* γ^i *and* $\bar{\gamma}^j$ *are not associates for any* $i, j \geq 1$. *Moreover, both* $\langle \gamma^i \rangle + \langle 2^j \rangle$ *and* $\langle \bar{\gamma}^i \rangle + \langle 2^j \rangle$ *equal* $\mathbb{Z}[\sqrt{d}]$ *for any* $i, j \geq 1$.

Proof. Suppose $\gamma := a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $N(\gamma) = a^2 - b^2 d = n$. Since n is squarefree, notice that $\gcd(a, b) = 1$. Since $\gcd(d, n) = 1$, one deduces that $\gcd(a, n) = \gcd(b, n) = 1$, too. Let I denote $\langle \gamma \rangle + \langle \bar{\gamma} \rangle$. Note that $\sqrt{d}(\gamma - \bar{\gamma}) = 2bd$ and n are in I. Since $\gcd(2bd, n) = 1$; we deduce that $I = \mathbb{Z}[\sqrt{d}]$, from which it follows that $\gcd(\gamma, \bar{\gamma}) = 1$ in $\mathbb{Z}[\sqrt{d}]$. Thus, for $\alpha := \gamma^i$ and $\beta := \bar{\gamma}^j$ with $i, j \geq 1$, one has that $\gcd(\alpha, \beta) = 1$ in $\mathbb{Z}[\sqrt{d}]$ and there exists $x, y \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha x + \beta y = 1$. If α and β were associates, then there exists a unit $u \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha = \beta u$. Thus, $\alpha(ux + y) = \alpha ux + \beta uy = u$ implying α must be a unit. But, $N(\alpha) \neq \pm 1$; therefore, it follows that α and β are not associates. Lastly, since each of $\langle \gamma^i \rangle$ and $\langle \bar{\gamma}^i \rangle$ contain $N(\gamma^i) = n^i$ and $\langle 2^j \rangle$ contains 2^j, one easily deduces for any positive integers i and j that $\langle \gamma^i \rangle + \langle 2^j \rangle$ and $\langle \bar{\gamma}^i \rangle + \langle 2^j \rangle$ equal $\mathbb{Z}[\sqrt{d}]$. □

In 1931, using the Möbius inversion formula, Estermann [9] calculated an asymptotic density for the number of squarefree integers of the form $n^2 + D$ with D fixed. Just two years later, the result of Estermann was generalized to general quadratic polynomials by Ricci [23]. More recently, further results were obtained uniformly in D as well [10]. We state a specific result that follows from Ricci's work.

Lemma 3. *Let* a*,* D*, and* b *be integers with* a *and* D *nonzero. If* $f(n) = (an+b)^2 + D$ *is irreducible and has no fixed square divisor, then the number of positive integers* $n \leq N$ *such that* $f(n)$ *is squarefree is asymptotic to* cN *where* c *is a positive constant depending on* a *and* b.

In what follows, we will use the previous lemmas along with our results applying to a general ring of integers $\mathcal{O}_K$ to deduce consequences for quadratic extensions. We are now ready for the first such result. We show how Lemma 3 together with Theorem 1 provides us with the following consequence.

Corollary 2. *For infinitely many squarefree* d*, the ring of integers in* $\mathbb{Q}(\sqrt{d})$ *possesses a distinct-norm covering having all principal ideals.*

Proof. By Lemma 3 there exists infinitely many squarefree $d \equiv 2, 3 \pmod 4$ such that $d = n^2 - 2$ for some positive integer n. Recall for such d that $N(a + b\sqrt{d}) = a^2 - db^2$; therefore, the element $n + \sqrt{d}$ has norm 2 for such d. By Theorem 1 with $\mathfrak{p} = \langle n + \sqrt{d} \rangle$, one finds that all ideal moduli are principal. □

In other words, Corollary 2 follows from the fact that there exists infinitely many rings of integers $\mathbb{Z}[\sqrt{d}]$ (with $d \equiv 2, 3 \pmod 4$) possessing an element of norm 2. Theorem 1 can be used to produce coverings whenever the ring of integers $\mathbb{Z}[\sqrt{d}]$ has an ideal with norm 2. The rest of this work focuses on the existence of various types of coverings with the norm of each modulus being ≥ 3.

The next theorem should be compared to Jordan and Schneider's [18]. To show that $\mathbb{Z}[\sqrt{-2}]$ has a distinct covering with each moduli having norm ≥ 3, they use that $\mathbb{Z}[\sqrt{-2}]$ possesses an ideal having norm 2 and two distinct ideals having norm 3. It is easy to generalize their result. Indeed, suppose $\mathfrak{b}$, $\mathfrak{p}$, $\bar{\mathfrak{p}}$ are ideals in $\mathcal{O}_K$ such that $N(\mathfrak{b}) = 2$, $N(\mathfrak{p}) = N(\bar{\mathfrak{p}}) = 3$, and $\mathfrak{p} + \bar{\mathfrak{p}} = \mathcal{O}_K$. Also, suppose that 0 and β are coset representatives for $\mathcal{O}_K$ modulo $\mathfrak{b}^2$ that lie inside $(0, \mathfrak{b})$. Then, the following forms a covering for $\mathcal{O}_K$:

$$(0,\mathfrak{p}),\ (0,\bar{\mathfrak{p}}),\ \big[(1,\mathfrak{p}),(1,\bar{\mathfrak{p}})\big],\ \big[(1,\mathfrak{b})\,(2,\mathfrak{p})\big],\ \big[(0,\mathfrak{b}),(2,\bar{\mathfrak{p}})\big],\ (0,\mathfrak{b}^2),\ \big[(\beta,\mathfrak{b}^2),(2,\mathfrak{p})\big],\\ \big[(1,\mathfrak{b}),(1,\mathfrak{p}),(2,\bar{\mathfrak{p}})\big]$$

The next result replaces the assumption that $\mathcal{O}_K$ has an ideal with norm 2.

Theorem 3. *If $\mathcal{O}_K$ has ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of norm 3 such that $\mathfrak{p} + \bar{\mathfrak{p}} = \mathcal{O}_K$ and an ideal $\mathfrak{q}$ of norm 4, then it has a distinct covering with the norm of each modulus being ≥ 3. Moreover, if $\mathfrak{p}$, $\bar{\mathfrak{p}}$, and $\mathfrak{q}$ are principal ideals, then all ideals in the covering are principal.*

Proof. The goal will be to construct a distinct covering for the ring of integers $\mathcal{O}_K$, which we label $C = \cup_{1\leq i\leq 18} c_i$ where each c_i is a particular congruence class in $\mathcal{O}_K$. Since $\mathfrak{p}+\bar{\mathfrak{p}} = \mathcal{O}_K$, one has that $\mathfrak{p}^i+\bar{\mathfrak{p}}^j = \mathcal{O}_K$ for all $i, j \geq 1$. In addition, $\mathfrak{p}^i+\mathfrak{q}^j$ and $\bar{\mathfrak{p}}^i + \mathfrak{q}^j$ equal $\mathcal{O}_K$ for all $i, j \geq 1$. Therefore, take note for all our congruence classes in C of the form $[(a, \mathfrak{a}), (b, \mathfrak{b})]$ and of the form $[(a, \mathfrak{a}), (b, \mathfrak{b}), (c, \mathfrak{c})]$ found below, we remark that one may apply the Chinese remainder theorem to deduce that the moduli are $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}\mathfrak{c}$, respectively.

The construction of the covering C begins by using the fact that both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ have three cosets that may be represented by 0, 1, and 2. First, include $c_1 = (2, \mathfrak{p})$ in C, which leaves $(0, \mathfrak{p})$ and $(1, \mathfrak{p})$ to be covered. The congruence class $(1, \mathfrak{p})$ is equivalent to the union of $[(1, \mathfrak{p}), (0, \bar{\mathfrak{p}})]$, $[(1, \mathfrak{p}), (1, \bar{\mathfrak{p}})]$, and $[(1, \mathfrak{p}), (2, \bar{\mathfrak{p}})]$. By including in C the second of these $c_2 = [(1, \mathfrak{p}), (1, \bar{\mathfrak{p}})]$ and $c_3 = (2, \bar{\mathfrak{p}})$, which contains the latter of these, it remains to cover $(0, \mathfrak{p})$ and $[(1, \mathfrak{p}), (0, \bar{\mathfrak{p}})]$.

Since $(1, \mathfrak{p})$ is equivalent to the union of classes $(\alpha_1, \mathfrak{p}^2)$, $(\alpha_2, \mathfrak{p}^2)$, and $(\alpha_3, \mathfrak{p}^2)$ for some $\alpha_1, \alpha_2, \alpha_3$, observe $[(1, \mathfrak{p}), (0, \bar{\mathfrak{p}})]$ is equivalent to the union of classes

$$[(\alpha_1, \mathfrak{p}^2), (0, \bar{\mathfrak{p}})],\ [(\alpha_2, \mathfrak{p}^2), (0, \bar{\mathfrak{p}})],\ \text{and}\ [(\alpha_3, \mathfrak{p}^2), (0, \bar{\mathfrak{p}})].$$

Again by including in C the second of these $c_4 = [(\alpha_2, \mathfrak{p}^2), (0, \bar{\mathfrak{p}})]$ and $c_5 = [(\alpha_3, \mathfrak{p}^2)]$, which contains the latter of these, it remains to cover $(0, \mathfrak{p})$ and $c' = [(\alpha_1, \mathfrak{p}^2), (0, \bar{\mathfrak{p}})]$.

Now, note that $\mathcal{O}_K$ modulo $\mathfrak{q}$ has four congruence classes represented by some $\beta_1, \beta_2, \beta_3, \beta_4$ in $\mathcal{O}_K$. The class c' is equivalent to the union of classes

$$c_6 = [c', (\beta_1, \mathfrak{q})],\ [c', (\beta_2, \mathfrak{q})],\ [c', (\beta_3, \mathfrak{q})], \text{ and } [c', (\beta_4, \mathfrak{q})].$$

The second of these is contained in $c_7 = [(\alpha_1, \mathfrak{p}^2), (\beta_2, \mathfrak{q})]$, the third is contained in $c_8 = [(0, \bar{\mathfrak{p}}), (\beta_3, \mathfrak{q})]$, and the latter of these is contained in $c_9 = (\beta_4, \mathfrak{q})$. By including c_6, c_7, c_8, and c_9 in C, it remains to cover $(0, \mathfrak{p})$.

Similarly, the congruence class $(0, \mathfrak{p})$ is equivalent to the union of classes

$$[(0, \mathfrak{p}), (\beta_1, \mathfrak{q})],\ c_{10} = [(0, \mathfrak{p}), (\beta_2, \mathfrak{q})],\ [(0, \mathfrak{p}), (\beta_3, \mathfrak{q})], \text{ and } [(0, \mathfrak{p}), (\beta_4, \mathfrak{q})].$$

The class $(\beta_4, \mathfrak{q})$ is already in the covering C, and covers the last class in the list. Let $c_{11} = [(0, \mathfrak{p}), (1, \bar{\mathfrak{p}}), (\beta_3, \mathfrak{q})]$ in C. This class c_{11} together with $(2, \bar{\mathfrak{p}})$ and $[(0, \bar{\mathfrak{p}}), (\beta_3, \mathfrak{q})]$, which are already in C, cover the third class in the list $[(0, \mathfrak{p}), (\beta_3, \mathfrak{q})]$.

It remains to cover $c'' = [(0, \mathfrak{p}), (\beta_1, \mathfrak{q})]$, which is equivalent to the union of $[c'', (0, \bar{\mathfrak{p}})]$, $[c'', (1, \bar{\mathfrak{p}})]$, and $[c'', (2, \bar{\mathfrak{p}})]$. The class $(2, \bar{\mathfrak{p}})$ is already in C and covers the third class in that list. Note that $(1, \bar{\mathfrak{p}})$ is equivalent to the union of $(\gamma_1, \bar{\mathfrak{p}}^2)$, $(\gamma_2, \bar{\mathfrak{p}}^2)$, and $(\gamma_3, \bar{\mathfrak{p}}^2)$ for some $\gamma_1, \gamma_2, \gamma_3$. Thus, the second class $[c'', (1, \bar{\mathfrak{p}})]$ is contained in the union of $c_{12} = [(0, \mathfrak{p}), (\gamma_1, \bar{\mathfrak{p}}^2)]$, $c_{13} = [(\beta_1, \mathfrak{q}), (\gamma_2, \bar{\mathfrak{p}}^2)]$, and $c_{14} = (\gamma_3, \bar{\mathfrak{p}}^2)$. It remains to cover the first class $c''' = [c'', (0, \bar{\mathfrak{p}})] = [(0, \mathfrak{p}), (0, \bar{\mathfrak{p}}), (\beta_1, \mathfrak{q})]$. Note that $(\beta_1, \mathfrak{q})$ is equivalent to the union of $(\delta_1, \mathfrak{q}^2)$, $(\delta_2, \mathfrak{q}^2)$, $(\delta_3, \mathfrak{q}^2)$, and $(\delta_4, \mathfrak{q}^2)$ for some $\delta_1, \delta_2, \delta_3, \delta_4$ in $\mathcal{O}_K$. Thus, c''' is contained in the union of $c_{15} = [(0, \mathfrak{p}), (\delta_1, \mathfrak{q}^2)]$, $c_{16} = (\delta_2, \mathfrak{q}^2)$, $c_{17} = [(0, \bar{\mathfrak{p}}), (\delta_3, \mathfrak{q}^2)]$, and $c_{18} = [(0, \mathfrak{p}), (0, \bar{\mathfrak{p}}), (\delta_4, \mathfrak{q}^2)]$. All together, the union of congruences C forms a covering for $\mathcal{O}_K$.

Among the 18 moduli, it is easy to see that the moduli are all distinct and the norm of each modulus is ≥ 3. By Proposition 1, if $\mathfrak{p}$, $\bar{\mathfrak{p}}$, and $\mathfrak{q}$ are principal ideals in $\mathcal{O}_K$, then the latter part of the theorem holds, since all ideals are generated by the pairwise relatively prime ideals $\mathfrak{p}$, $\bar{\mathfrak{p}}$, and $\mathfrak{q}$. □

For any integer A that is odd, let $d := A^2 - 3 \equiv 2 \pmod 4$. Thus, the ring of integers $\mathbb{Z}[\sqrt{d}]$ has an element $A + \sqrt{d}$ that has norm 3. If in addition A is not divisible by 3, then d will not be divisible by 3. In other words, if $A \equiv 1, 5 \pmod 6$, then the ring of integers $\mathbb{Z}[\sqrt{d}]$ has the elements $A + \sqrt{d}$ and $A - \sqrt{d}$, which have norm 3. By Lemma 3 with $a = 6$, $b \in \{1, 5\}$, and $D = -3$, (where $A = an + b$) there are infinitely many such d that are squarefree. By Lemma 2, $A + \sqrt{d}$ and its conjugate are not associates, and the ideals generated by each are relatively prime. Therefore, there are infinitely many squarefree d such that $\mathbb{Z}[\sqrt{d}]$ possesses two distinct principal ideals with norm 3. The ideal generated by 2, namely $\langle 2 \rangle$, has norm 4 in $\mathbb{Z}[\sqrt{d}]$. Hence, the next corollary follows from Theorem 3.

Corollary 3. *For infinitely many squarefree d, the ring of integers in $\mathbb{Q}(\sqrt{d})$ has a distinct covering such that each modulus is a principal ideal with norm ≥ 3.*

A longstanding open problem of Erdős is whether or not a distinct covering for the rational integers exists with all odd moduli. The main motivation of the next theorem is to study this within the setting of $\mathcal{O}_K$. As a consequence of the next theorem, we prove for infinitely many squarefree d that the ring of integers in $\mathbb{Q}(\sqrt{d})$ has such a covering. The proof for the following theorem will be similar to that of Theorem 3 in many ways, and the notable difference from Theorem 3 is that it is possible to form a distinct covering for $\mathcal{O}_K$ *also with* all moduli having odd norms.

Theorem 4. *If $\mathcal{O}_K$ has ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of norm 3 such that $\mathfrak{p} + \bar{\mathfrak{p}} = \mathcal{O}_K$ and has ideals $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ of norm 5 such that $\mathfrak{q} + \bar{\mathfrak{q}} = \mathcal{O}_K$, then it has a distinct covering with the norm of each modulus being ≥ 3 and odd. Moreover, if $\mathfrak{p}$, $\bar{\mathfrak{p}}$, $\mathfrak{q}$, and $\bar{\mathfrak{q}}$ are principal ideals, then all ideals in the covering are principal.*

Proof. We label $C = \cup_{1 \leq i \leq 23} c_i$ where each c_i is a particular congruence class in $\mathcal{O}_K$ to be described below. Under the given assumptions, notice that $\mathfrak{i}^k + \mathfrak{j}^\ell = \mathcal{O}_K$ for all $k, \ell \geq 1$ and $\mathfrak{i}, \mathfrak{j} \in \{\mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{q}, \bar{\mathfrak{q}}\}$ with $\mathfrak{i} \neq \mathfrak{j}$. Hence, for all our congruence classes in C of the form $[(a, \mathfrak{a}), (b, \mathfrak{b})]$ and of the form $[(a, \mathfrak{a}), (b, \mathfrak{b}), (c, \mathfrak{c})]$ found below, we remark that one may apply the Chinese remainder theorem to deduce that the moduli are $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}\mathfrak{c}$, respectively.

The construction of the covering C begins by using the fact that both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ have three congruence classes that may be represented by 0, 1, and 2. Likewise, congruence classes of both $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ may be represented by 0, 1, 2, 3, and 4.

First, include $c_1 = (2, \mathfrak{p})$ in C. The congruence class $(1, \mathfrak{p})$ is equivalent to the union of $[(1, \mathfrak{p}), (0, \bar{\mathfrak{p}})]$, $[(1, \mathfrak{p}), (1, \bar{\mathfrak{p}})]$, and $[(1, \mathfrak{p}), (2, \bar{\mathfrak{p}})]$. By including in C the last of these $c_2 = [(1, \mathfrak{p}), (2, \bar{\mathfrak{p}})]$ and $c_3 = (0, \bar{\mathfrak{p}})$, which contains the first of these, it remains to cover $(0, \mathfrak{p})$ and $[(1, \mathfrak{p}), (1, \bar{\mathfrak{p}})]$.

Since $(1, \mathfrak{p})$ is equivalent to the union of classes $(\alpha_1, \mathfrak{p}^2)$, $(\alpha_2, \mathfrak{p}^2)$, and $(\alpha_3, \mathfrak{p}^2)$ for some $\alpha_1, \alpha_2, \alpha_3$ in $\mathcal{O}_K$, observe $[(1, \mathfrak{p}), (1, \bar{\mathfrak{p}})]$ is equivalent to the union of classes

$$[(\alpha_1, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})],\ [(\alpha_2, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})],\ \text{and}\ [(\alpha_3, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})].$$

Again, by including in C the first of these, $c_4 = [(\alpha_1, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})]$, and $c_5 = [(\alpha_2, \mathfrak{p}^2)]$, which contains the second of these, it remains to cover $(0, \mathfrak{p})$ and $[(\alpha_3, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})]$.

Now, note that $c' = [(\alpha_3, \mathfrak{p}^2), (1, \bar{\mathfrak{p}})]$ is contained in the union of classes

$$[c', (0, \mathfrak{q})], [c', (1, \mathfrak{q})],\ [c', (2, \mathfrak{q})],\ [c', (3, \mathfrak{q})],\ \text{and}\ [c', (4, \mathfrak{q})].$$

Since $(\alpha_3, \mathfrak{p}^2)$ is contained in $(1, \mathfrak{p})$, the second in the list of congruences is contained in $[(1, \mathfrak{p}), (1, \mathfrak{q})]$. The latter list of five congruences are all covered, respectively, by

$$c_6 = (0, \mathfrak{q}),\ c_7 = [(1, \mathfrak{p}), (1, \mathfrak{q})],\ c_8 = [(\alpha_3, \mathfrak{p}^2), (2, \mathfrak{q})],$$
$$c_9 = [(1, \bar{\mathfrak{p}}), (3, \mathfrak{q})],\ \text{and}\ c_{10} = [(\alpha_3, \mathfrak{p}^2), (1, \bar{\mathfrak{p}}), (4, \mathfrak{q})].$$

It remains to cover $(0,\mathfrak{p})$, which is equivalent to the union of $[(0,\mathfrak{p}),(0,\bar{\mathfrak{p}})]$, $[(0,\mathfrak{p}),(1,\bar{\mathfrak{p}})]$, and $[(0,\mathfrak{p}),(2,\bar{\mathfrak{p}})]$. The first of these is included in the congruence class c_3, so we need only consider the other two to finish the covering C.

Note that $(1,\bar{\mathfrak{p}})$ is equivalent to the union of classes $(\bar{\alpha}_1,\bar{\mathfrak{p}}^2)$, $(\bar{\alpha}_2,\bar{\mathfrak{p}}^2)$, and $(\bar{\alpha}_3,\bar{\mathfrak{p}}^2)$ for some $\bar{\alpha}_1,\bar{\alpha}_2,\bar{\alpha}_3$. Observe the class $[(0,\mathfrak{p}),(1,\bar{\mathfrak{p}})]$ is equivalent to the union of classes $[(0,\mathfrak{p}),(\bar{\alpha}_1,\bar{\mathfrak{p}}^2)]$, $[(0,\mathfrak{p}),(\bar{\alpha}_2,\bar{\mathfrak{p}}^2)]$, and $[(0,\mathfrak{p}),(\bar{\alpha}_3,\bar{\mathfrak{p}}^2)]$. The first and second are contained in $c_{11}=(\bar{\alpha}_1,\bar{\mathfrak{p}}^2)$ and $c_{12}=[(0,\mathfrak{p}),(\bar{\alpha}_2,\bar{\mathfrak{p}}^2)]$, respectively. The third, $c''=[(0,\mathfrak{p}),(\bar{\alpha}_3,\bar{\mathfrak{p}}^2)]$, can be written as the union of classes

$$[c'',(0,\mathfrak{q})],\ [c'',(1,\mathfrak{q})],\ [c'',(2,\mathfrak{q})],\ [c'',(3,\mathfrak{q})],\text{ and }[c'',(4,\mathfrak{q})].$$

The first is a subset of c_6. The second and third classes are subsets of $c_{13}=[(0,\mathfrak{p}),(1,\bar{\mathfrak{p}}),(1,\mathfrak{q})]$ and $c_{14}=[(\bar{\alpha}_3,\bar{\mathfrak{p}}^2),(2,\mathfrak{q})]$, respectively. The fourth is a subset of c_9. The fifth, $c_{15}=[c'',(4,\mathfrak{q})]$, is included in C.

It remains to cover $c'''=[(0,\mathfrak{p}),(2,\bar{\mathfrak{p}})]$, which is the union of classes

$$[c''',(0,\bar{\mathfrak{q}})],\ [c''',(1,\bar{\mathfrak{q}})],\ [c''',(2,\bar{\mathfrak{q}})],\ [c''',(3,\bar{\mathfrak{q}})],\text{ and }[c''',(4,\bar{\mathfrak{q}})].$$

The first four of those classes are contained in $c_{16}=(0,\bar{\mathfrak{q}})$, $c_{17}=[(0,\mathfrak{p}),(1,\bar{\mathfrak{q}})]$, $c_{18}=[(2,\bar{\mathfrak{p}}),(2,\bar{\mathfrak{q}})]$, and $c_{19}=[c''',(3,\bar{\mathfrak{q}})]$, respectively. The last of these classes, $c^{(4)}=[(0,\mathfrak{p}),(2,\bar{\mathfrak{p}}),(4,\bar{\mathfrak{q}})]$, is equivalent to

$$[c^{(4)},(0,\mathfrak{q})],\ [c^{(4)},(1,\mathfrak{q})],\ [c^{(4)},(2,\mathfrak{q})],\ [c^{(4)},(3,\mathfrak{q})],\text{ and }c_{20}=[c^{(4)},(4,\mathfrak{q})].$$

The first is contained in c_6. The next three are contained in $c_{21}=[(4,\bar{\mathfrak{q}}),(1,\mathfrak{q})]$, $c_{22}=[(0,\mathfrak{p}),(4,\bar{\mathfrak{q}}),(2,\mathfrak{q})]$, and $c_{23}=[(2,\bar{\mathfrak{p}}),(4,\bar{\mathfrak{q}}),(3,\mathfrak{q})]$, respectively. The last is included in C. All together, this completes the covering of $\mathcal{O}_K$. Table 1 consists of these moduli and their corresponding norms. Among the moduli in C, it is easy to see that they are all distinct and have odd norm ≥ 3. By Proposition 1, if $\mathfrak{p}$, $\bar{\mathfrak{p}}$, $\mathfrak{q}$, and $\bar{\mathfrak{q}}$ are principal ideals in $\mathcal{O}_K$, then the latter part of the theorem holds. □

$N(\mathfrak{a})$	c_i in C	modulus in c_i, respectively
3	$c_1,\ c_3$	$\mathfrak{p},\ \bar{\mathfrak{p}}$
5	$c_6,\ c_{16}$	$\mathfrak{q},\ \bar{\mathfrak{q}}$
9	$c_2,\ c_5,\ c_{11}$	$\mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p}^2,\ \bar{\mathfrak{p}}^2$
15	$c_7,\ c_9,\ c_{17},\ c_{18}$	$\mathfrak{p}\mathfrak{q},\ \bar{\mathfrak{p}}\mathfrak{q},\ \mathfrak{p}\bar{\mathfrak{q}},\ \bar{\mathfrak{p}}\bar{\mathfrak{q}}$
25	c_{21}	$\mathfrak{q}\bar{\mathfrak{q}}$
27	$c_4,\ c_{12}$	$\mathfrak{p}^2\bar{\mathfrak{p}},\ \mathfrak{p}\bar{\mathfrak{p}}^2$
45	$c_8,\ c_{13},\ c_{14},\ c_{19}$	$\mathfrak{p}^2\mathfrak{q},\ \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q},\ \bar{\mathfrak{p}}^2\mathfrak{q},\ \mathfrak{p}\bar{\mathfrak{p}}\bar{\mathfrak{q}}$
75	$c_{22},\ c_{23}$	$\mathfrak{p}\mathfrak{q}\bar{\mathfrak{q}},\ \bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$
135	$c_{10},\ c_{15}$	$\mathfrak{p}^2\bar{\mathfrak{p}}\mathfrak{q},\ \mathfrak{p}\bar{\mathfrak{p}}^2\mathfrak{q}$
225	c_{20}	$\mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$

Table 1: Moduli for congruences in C

Before proceeding, we quickly recall some algebraic number theory facts (cf. [4]). Fix a squarefree integer d. Let $D = d$ if $d \equiv 1 \pmod 4$ and $D = 4d$ otherwise. Define the function $\chi = \chi_d$ on integers m such that $\gcd(m, D) = 1$ by

$$\chi(m) = \begin{cases} \left(\frac{m}{|d|}\right) & \text{for } d \equiv 1 \pmod 4 \\ (-1)^{(m-1)/2}\left(\frac{m}{|d|}\right) & \text{for } d \equiv 3 \pmod 4 \\ (-1)^{[(m^2-1)/8]+[(m-1)/2]\cdot[(d'-1)/2]}\left(\frac{m}{|d'|}\right) & \text{for } d = 2d' \end{cases}$$

where $(\frac{a}{b})$ denotes the Jacobi symbol. The function χ is a completely multiplicative map (that is, $\chi(mn) = \chi(m)\chi(n)$ whenever $\gcd(m, D) = \gcd(n, D) = 1$). Let $K = \mathbb{Q}(\sqrt{d})$. If p is a rational prime, then it is known how $\langle p \rangle$ factors into prime ideals in $\mathcal{O}_K$, in particular

$$\text{if } \chi(p) = 1 \text{ then } \langle p \rangle = \mathfrak{i}\,\mathfrak{i}',\ \mathfrak{i} \neq \mathfrak{i}',\ N(\mathfrak{i}) = N(\mathfrak{i}') = p.$$

There are infinitely many squarefree d such that $\mathcal{O}_K$ possesses distinct ideals $\mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{q}$, and $\bar{\mathfrak{q}}$ with $N(\mathfrak{p}) = N(\bar{\mathfrak{p}}) = 3$ and $N(\mathfrak{q}) = N(\bar{\mathfrak{q}}) = 5$. For example, consider primes $d \equiv 1, 31 \pmod{60}$. For each such d, $\chi(3) = \chi(5) = 1$. Applying Theorem 4 to such rings of integers, we deduce the following result.

Corollary 4. *For infinitely many squarefree d, the ring of integers in $\mathbb{Q}(\sqrt{d})$ has a distinct covering with the norm of each modulus being ≥ 3 and odd.*

Similarly, for primes d with $d \equiv 1 \pmod{24}$, $D = d$ and $\chi(2) = \chi(3) = 1$. Then, one can apply Theorem 2 to deduce the following result.

Corollary 5. *For infinitely many squarefree d, the ring of integers in $\mathbb{Q}(\sqrt{d})$ has a distinct-norm covering with the norm of each modulus being ≥ 4.*

4. Conclusion and Conjectures

According to the Cohen-Lenstra heuristic, it is expected that infinitely many of the primes p (> 0.75 of the primes) satisfy the condition that $\mathbb{Q}(\sqrt{p})$ has ring of integers with class number one [14], or equivalently, the ring of integers of $\mathbb{Q}(\sqrt{p})$ is a principal ideal domain for infinitely many primes p. Thus, we conclude with the following two conjectures having the same implications as Corollary 4 and Corollary 5 along with the additional implication that the ideal moduli are all principal.

Conjecture 1. For infinitely many squarefree d, the ring of integers in $\mathbb{Q}(\sqrt{d})$ has a distinct covering with each modulus a principal ideal having odd norm ≥ 3.

Conjecture 2. For infinitely many squarefree d, the ring of integers in $\mathbb{Q}(\sqrt{d})$ has a distinct-norm covering with each modulus a principal ideal having norm ≥ 4.

References

[1] D. Baczkowski and J. Eitner, Polygonal-Sierpiński-Riesel sequences with terms having at least two distinct prime divisors, *Integers* **16** (2016), Paper No. A40, 17 pp.

[2] D. Baczkowski, J. Eitner, C. Finch, M. Kozek, B. Suminski, Polygonal, Sierpiński, and Riesel numbers, *J. Integer Seq.*, **18** (2015), no. 8, Article 15.8.1, 12 pp.

[3] D. Baczkowski, O. Fasoranti and C. E. Finch, Lucas-Sierpiński and Lucas-Riesel numbers, *Fibonacci Quart.* **49** (2011), no. 4, 334–339.

[4] A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York, 1966.

[5] Y.-G. Chen, On integers of the form $k2^n + 1$, *Proc. Amer. Math. Soc.* **129** (2001), no. 2, 355–361.

[6] Y.-G. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory* **98** (2003), no. 2, 310–319.

[7] Y.-G. Chen, On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$, *J. Number Theory* **125** (2007) 14–25.

[8] P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.

[9] T. Estermann, Einige Sätze über quadratfreie Zahlen, *Math. Ann.* **105** (1931), no. 1, 653–662.

[10] J. B. Friedlander and H. Iwaniec, Square-free values of quadratic polynomials, *Proc. Edinb. Math. Soc.* (2) **53** (2010), no. 2, 385–392.

[11] Song Guo; Zhi-Wei Sun, On odd covering systems with distinct moduli, *Adv. in Appl. Math.* **35** (2005), no. 2, 182–187.

[12] R. K. Guy, *Unsolved problems in number theory*, third edition, Problem Books in Mathematics, Springer-Verlag, New York, 2004 (Sections F13 and F14).

[13] B. Hough, Solution of the minimum modulus problem for covering systems, *Ann. of Math.* (2) **181** (2015), no. 1, 361–382.

[14] H. te Riele and H. Williams, New computations concerning the Cohen-Lenstra heuristics, *Experiment. Math.* **12** (2003), no. 1, 99–113.

[15] L. Jones and D. White, Sierpiński numbers in imaginary quadratic fields, *Integers* **12** (2012), no. 6, 1265–1278.

[16] J. H. Jordan, A covering class of residues with odd moduli, *Acta Arith.* **13** (1967/1968), 335–338.

[17] J. H. Jordan, Covering classes of residues, *Canad. J. Math.* **19** (1967), 514–519.

[18] J. H. Jordan and D. G. Schneider, Covering classes of residues in $Z(\sqrt{-2})$, *Math. Mag.* **44** (1971), 257–261.

[19] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.

[20] F. Luca and V. J. Mejía Huguet, Fibonacci-Riesel and Fibonacci-Sierpiński numbers, *Fibonacci Quart.* **46/47** (2008/09), no. 3, 216–219.

[21] F. Luca and P. Stanica, Fibonacci numbers of the form $p^a \pm p^b$, Proceedings of the Eleventh International Conference on Fibonacci Numbers and their Applications. *Congr. Numer.* **194** (2009), 177–183.

[22] F. Luca and P. Stanica, Fibonacci numbers that are not sums of two prime powers, *Proceedings of Amer. Math. Soc.*, **133** (2005), 1887–1890.

[23] G. Ricci, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo* **57** (1933), 433–475.

[24] H. Riesel, Några stora primtal, *Elementa* **39** (1956), 258–260.

[25] W. Sierpiński, Sur un problème concernant les nombres $k2^n + 1$, *Elem. Math.* **15** (1960), 73–74.