#A10 INTEGERS 12A (2012): John Selfridge Memorial Issue

SIERPIŃSKI NUMBERS IN IMAGINARY QUADRATIC FIELDS

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania
lkjone@ship.edu

Daniel White
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania

Received: 5/30/11, Revised: 4/18/12, Accepted: 6/30/12, Published:

Abstract

In 1960, Sierpiński proved that there exist infinitely many odd positive rational integers k such that $k \cdot 2^n + 1$ is composite in $\mathbb{Z}$ for all $n \geq 1$. Any such integer k is now known as a Sierpiński number, and the smallest value of k produced by Sierpiński's proof is $k = 15511380746462593381$. In 1962, John Selfridge showed that $k = 78557$ is also a Sierpiński number, and he conjectured that this value of k is the smallest Sierpiński number. This conjecture, however, is still unresolved today.

In this article, we investigate the analogous problem in the ring of integers $\mathcal{O}_d$ of each imaginary field $\mathbb{Q}(\sqrt{d})$ having class number one. More precisely, for each $\mathcal{O}_d$, with $d < 0$, that has unique factorization, we determine all $\alpha \in \mathcal{O}_d$, with minimal odd norm larger than 1, such that $\alpha \cdot 2^n + 1$ is composite in $\mathcal{O}_d$ for all $n \geq 1$. We call these numbers *Selfridge numbers* in honor of John Selfridge.

1. Introduction

In 1960, using a covering of the integers (a concept originally due to Erdős [1]; see Definition 17), Sierpiński [6] proved that there exist infinitely many odd positive rational integers k such that $k \cdot 2^n + 1$ is composite for all $n \geq 1$. Such values of k are the classical Sierpiński numbers. The smallest value of k produced by the covering argument in Sierpiński's proof is $k = 15511380746462593381$. This value of k, however, is not the smallest Sierpiński number. In 1962, John Selfridge used a different covering to show that $k = 78557$ is also a Sierpiński number. It is still unknown whether $k = 78557$ is the smallest Sierpiński number, although currently only six smaller numbers remain as viable candidates for the smallest (see Section 6.2). There is an additional problem, known as the *prime Sierpiński problem*, of trying to establish that 271129 is the smallest rational prime p such that $p \cdot 2^n + 1$ is composite in $\mathbb{Z}$ for all integers $n \geq 1$. There are currently eleven candidates below 271129. The interested reader should visit www.seventeenorbust.com [2].

In this article, we investigate the analogous problems of determining the "smallest" Sierpiński number and Sierpiński prime in imaginary quadratic field extensions of the rational numbers with class number one. To make this idea precise, we give the following definitions. For a square-free integer d, we let $\mathcal{O}_d$ denote the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{d})$. It is well-known that $\mathbb{Q}(\sqrt{d})$, $d < 0$, has class number one precisely when $d \in \mathcal{D} = \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$, and $\mathcal{O}_d$ has unique factorization exactly for these negative values of d. Throughout this article, we assume that $d \in \mathcal{D}$. Recall that the *norm* of an element $\alpha \in \mathcal{O}_d$ is $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ is the algebraic conjugate of α in $\mathcal{O}_d$.

Definition 1. We call $\alpha \in \mathcal{O}_d$ a *Sierpiński number* if $N(\alpha) > 1$ is odd, and $\alpha \cdot 2^n + 1$ is composite in $\mathcal{O}_d$ for all $n \geq 1$. A Sierpiński number $\sigma \in \mathcal{O}_d$ is called a *Selfridge number* if

$$N(\sigma) = \min \left\{ N(\alpha) \,\middle|\, \alpha \text{ is a Sierpiński number in } \mathcal{O}_d \right\}.$$

A Sierpiński number $\pi \in \mathcal{O}_d$ is called a *Selfridge prime* if

$$N(\pi) = \min \left\{ N(\alpha) \,\middle|\, \alpha \text{ is a prime Sierpiński number in } \mathcal{O}_d \right\}.$$

Remarks 2. (i) The condition that $N(\alpha)$ be odd in Definition 1 is analogous to the requirement that k be odd in Sierpiński's original theorem. (ii) It is immediate from Definition 1 that α is a Sierpiński number in $\mathcal{O}_d$ if and only if $\overline{\alpha}$ is a Sierpiński number in $\mathcal{O}_d$.

We prove the following theorems in this article:

Theorem 3. *For each $d \in \mathcal{D}$, all Selfridge numbers $\sigma \in \mathcal{O}_d$ are given in Table 7.*

Theorem 4. *For each $d \in \{-1, -2, -3, -7, -11, -19\}$, all Selfridge primes in $\mathcal{O}_d$ are given in Table 7.*

Theorem 5. *Let $\mathcal{S}$ be the set of all odd positive rational integers k such that, for all $n \geq 1$, the integers $k \cdot 2^n + 1$ are simultaneously composite in $\mathcal{O}_d$ for all $d \in \mathcal{D}$. Then $\mathcal{S}$ properly contains the set of classical Sierpiński numbers.*

We provide the reader with an overview of the approach used in this paper. The proofs of Theorem 3 and Theorem 4 rely on Theorem 15, Corollary 16 and quadratic reciprocity. Theorem 15 is well-known and gives a description of the primes in the ring of integers of a quadratic field in which unique factorization holds. Corollary 16, which follows from Theorem 15, gives criteria to determine whether certain elements of $\mathcal{O}_d$ are prime in $\mathcal{O}_d$. To find candidates $\alpha \in \mathcal{O}_d$ that might be Sierpiński numbers, we first use a computer search to eliminate values of α with small norm. Theorem 15 and Corollary 16 provide us with the necessary tools

to decide if a candidate $\alpha \in \mathcal{O}_d$ is a Sierpiński number by calculating either the norm $N(\alpha \cdot 2^n + 1)$ or the Legendre symbol $\left(\frac{d}{\alpha \cdot 2^n + 1}\right)$. Additionally, Theorem 15 and Corollary 16 allow us to determine if a Sierpiński number α is in fact a prime in $\mathcal{O}_d$ by checking the primality of the norm $N(\alpha)$ or computing the Legendre symbol $\left(\frac{d}{\alpha}\right)$. For the values of α not eliminated by the initial norm search, it is often useful to use a covering system (see Definition 17) to verify that α is indeed a Sierpiński number. All of these ideas are described in greater detail in Section 2. Computer calculations were done using MAPLE$^{\text{TM}}$ and PARI/GP.

2. Preliminaries

In this section we provide the necessary background material needed to establish Theorem 15 and Corollary 16, the main tools in the proofs of Theorem 3 and Theorem 4. We begin by reminding the reader of some basic ideas concerning quadratic reciprocity and quadratic field extensions of the rational numbers [5]. We let $\left(\frac{*}{*}\right)$ denote the Legendre symbol.

Theorem 6. *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Theorem 7. *(Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Corollary 8. *Let p be an odd prime. Then $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1$ or $11 \pmod{12}$.*

Although all of the following ideas apply to positive values of d as well, our focus here is on values of $d < 0$.

Proposition 9. *The ring of integers in $\mathbb{Q}(\sqrt{d})$ is given by*

$$\mathcal{O}_d = \begin{cases} \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\} & \text{if } d \equiv 2, 3 \pmod 4 \\ \left\{ \frac{a + b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z}, \quad a \equiv b \pmod 2 \right\} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Definition 10. The *discriminant* δ_d of $\mathbb{Q}(\sqrt{d})$ is defined as

$$\delta_d = \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Definition 11. An element $u \in \mathcal{O}_d$ is called a *unit* in $\mathcal{O}_d$ if $N(u) = \pm 1$. Two elements α and β in $\mathcal{O}_d$ are called *associates* if $\alpha = u\beta$, for some unit $u \in \mathcal{O}_d$.

Proposition 12. *Let U be the set of units in $\mathbb{Q}(\sqrt{d})$. Then*

$$U = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & \text{if } d = -1 \\ \left\{\pm 1, \dfrac{\pm 1 \pm \sqrt{-3}}{2}\right\} & \text{if } d = -3 \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

Proposition 13. *Let $\alpha \in \mathcal{O}_d$. If $N(\alpha) = \pm p$, where p is a rational prime, then α is prime in $\mathcal{O}_d$.*

Remark 14. Note that in our situation we have $d < 0$ so that $N(\alpha) \geq 0$ for all $\alpha \in \mathcal{O}_d$.

Theorem 15. *Suppose that $\mathbb{Q}(\sqrt{d})$ has class number one. Then*

1. *Any rational prime p is either a prime π in $\mathcal{O}_d$, or a product $\pi_1\pi_2$ of two primes π_1 and π_2, not necessarily distinct, in $\mathcal{O}_d$.*
2. *The totality of primes π, π_1, π_2 obtained by applying Part 1. to all rational primes, together with their associates, constitutes the set of all primes in $\mathcal{O}_d$.*
3. *The behavior of the rational prime 2 in $\mathcal{O}_d$ is given below.*
   (a) *If $\delta_d \equiv 1 \pmod 2$ and $d \equiv 1 \pmod 8$, then $2 = \pi_1\pi_2$, where $\pi_1 \neq \pi_2$ are primes in $\mathcal{O}_d$.*
   (b) *If $\delta_d \equiv 1 \pmod 2$ and $d \equiv 5 \pmod 8$, then 2 remains prime in $\mathcal{O}_d$.*
   (c) *If $\delta_d \equiv 0 \pmod 2$, then $2 = u\pi^2$, where $\pi \in \mathcal{O}_d$ is prime, and $u \in \mathcal{O}_d$ is a unit.*
4. *The behavior of an odd rational prime p in $\mathcal{O}_d$ is given below.*
   (a) *If $\delta_d \not\equiv 0 \pmod p$ and $\left(\dfrac{d}{p}\right) = 1$, then $p = \pi_1\pi_2$, where $\pi_1 \neq \pi_2$ are primes in $\mathcal{O}_d$. Furthermore, π_1 and π_2 are not associates, but π_1 and $\overline{\pi}_2$ are, and π_2 and $\overline{\pi}_1$ are.*
   (b) *If $\delta_d \not\equiv 0 \pmod p$ and $\left(\dfrac{d}{p}\right) = -1$, then p remains prime in $\mathcal{O}_d$.*
   (c) *If $\delta_d \equiv 0 \pmod p$, then $p = u\pi^2$, where $\pi \in \mathcal{O}_d$ is prime, and $u \in \mathcal{O}_d$ is a unit.*

A main tool used in the proofs of Theorem 3 and Theorem 4 is the following partial converse of Proposition 13. Recall Remark 14.

Corollary 16. *Let $\alpha \in \mathcal{O}_d$. Suppose that α is not a rational integer and $N(\alpha)$ is not prime in $\mathbb{Z}$.*

1. *If $d \notin \{-1, -3\}$, then α is not prime in $\mathcal{O}_d$.*
2. *If $d = -1$ or $d = -3$, then either (i) α is not prime in $\mathcal{O}_d$, or (ii) $\alpha = pu$, where p is a rational prime with $\left(\frac{d}{p}\right) = -1$, and u is a unit in $\mathcal{O}_d$.*

Proof. Assume that α is prime in $\mathcal{O}_d$. By Theorem 15 (Part *2.)*, we have that there exists a rational prime p such that either $p = v\alpha\beta$ or $p = v\alpha$, where v is a unit and $\beta \in \mathcal{O}_d$ is prime. If $p = v\alpha\beta$, then $p^2 = N(\alpha) \cdot N(\beta)$. Since $N(\alpha)$ is not prime and α is not a unit, we have that $N(\alpha) = p^2$. But then $N(\beta) = 1$, which contradicts the fact that β is prime in $\mathcal{O}_d$. Therefore, $p = v\alpha$ or equivalently, $\alpha = pu$, where $u = v^{-1}$ is a unit. Since α is not a rational integer, it must be that u is not a rational integer as well. But this is impossible if $d \notin \{-1, -3\}$, which proves Part *1.* To finish the proof of Part *2.*, if $\left(\frac{d}{p}\right) \neq -1$, then $p = \pi_1\pi_2$, where π_1 and π_2 are (not necessarily distinct) primes in $\mathcal{O}_d$. But this contradicts the assumption that α is prime in $\mathcal{O}_d$. □

The following concept is originally due to Erdős [1].

Definition 17. A (finite) *covering system*, or simply a *covering*, of the rational integers is a system of congruences $n \equiv r_i \pmod{m_i}$, with $1 \leq i \leq t$, such that every integer n satisfies at least one of the congruences.

Using Definition 17, we can describe a covering (or a partial covering) $\mathcal{C}$ as a set of ordered pairs (r, m), where the congruence $n \equiv r \pmod{m}$ is a congruence in the covering. In this article, however, we describe $\mathcal{C}$ as a set of ordered triples (r, m, p), where the congruence $n \equiv r \pmod{m}$ is a congruence in the covering, and p is a rational prime "associated" to the particular congruence. This association typically means that p is a prime divisor of $2^m - 1$, and this will be the case throughout the paper, unless stated otherwise.

3. The Proof of Theorem 3

The general strategy here is to first use a computer to search for candidate Sierpiński numbers α in $\mathcal{O}_d$. For any fixed positive rational integer M, there are only finitely many elements $\alpha \in \mathcal{O}_d$ such that $N(\alpha) = M$, and they are straightforward to

calculate. So, we set upper limits for n and M, and find all $\alpha \in \mathcal{O}_d$ with $N(\alpha)$ odd and $1 < N(\alpha) \leq M$. Then we check that $\alpha \cdot 2^n + 1$ is composite in $\mathcal{O}_d$ using Theorem 15 and Corollary 16. Once a nonempty set T of candidates is found, then each $\alpha \in T$ is examined in detail, starting with elements of smallest norm, to determine if α can be proven to be a Sierpiński number in $\mathcal{O}_d$, or whether a value of n can be found such that $\alpha \cdot 2^n + 1$ is prime in $\mathcal{O}_d$. If no element of T is found to be a Sierpiński number in $\mathcal{O}_d$, then a new computer search is conducted increasing the limits of M in the search.

Since many of the proofs are similar, we give details only for certain values of d. When proving that a particular $\sigma \in \mathcal{O}_d$ from Table 7 is a Selfridge number, or whether a particular $\pi \in \mathcal{O}_d$ from Table 7 is a Selfridge prime, it will be convenient to write s_n for $\sigma \cdot 2^n + 1$ or $\pi \cdot 2^n + 1$, respectively.

3.1. $d = -1$

For the purpose of readability, we let $i = \sqrt{-1}$ in this section. In a personal communication with E. Weisstein at MathWorld, Ed Pegg Jr. noted that $10 + 3i$, $25 + 3i$, and $40 + 3i$ are all Sierpiński numbers in $\mathcal{O}_d$ [7]. This fact is easy to see. For example, if $\alpha = 10 + 3i$, we have that

$$N(\alpha \cdot 2^n + 1) = 109 \cdot 2^{2n} + 20 \cdot 2^n + 1 \equiv \begin{cases} 0 \pmod 3 & \text{if } n \equiv 1 \pmod 2 \\ 0 \pmod 5 & \text{if } n \equiv 0 \pmod 2. \end{cases}$$

Since $N(\alpha \cdot 2^n + 1) > 25$ for all $n \geq 1$, it is clear that $\alpha \cdot 2^n + 1 \neq pu$, for some rational prime p and some unit u. Thus, we can conclude from Corollary 16 that $\alpha \cdot 2^n + 1$ is composite in $\mathcal{O}_d$ for all $n \geq 1$. We show, however, that $10 + 3i$ is not a Selfridge number in $\mathcal{O}_d$. With a computer we are able to eliminate as candidates for Sierpiński numbers in $\mathcal{O}_d$ all α with odd norm smaller than 25. We show that $\sigma = -4 + 3i$ is a Sierpiński number in $\mathcal{O}_d$, and hence a Selfridge number in $\mathcal{O}_d$, since $N(\sigma) = 25$. There appears to be no simple pattern to the prime divisors of $N(s_n)$ as in the case of $N((10 + 3i) \cdot 2^n + 1)$, and so we use a different method to establish that is a Sierpiński number. For even n, we have

$$s_n = (-4 + 3i) \cdot 2^n + 1 \equiv -2^n + 1 \equiv 0 \pmod 3.$$

For odd n, we have

$$\begin{aligned} s_n &= (-4 + 3i) \cdot 2^n + 1 \\ &= -i \cdot (1 - 2i)^2 \cdot \left(-i \cdot (1 + i)^2\right)^n + 1 \\ &= \begin{cases} \left(i \cdot (1 - 2i)(1 + i)^n\right)^2 + 1 & \text{if } n \equiv 1 \pmod 4 \\ \left((1 - 2i)(1 + i)^n\right)^2 + 1 & \text{if } n \equiv 3 \pmod 4 \end{cases} \\ &= \begin{cases} -\left((1 - 2i)(1 + i)^n + 1\right) \cdot \left((1 - 2i)(1 + i)^n - 1\right) & \text{if } n \equiv 1 \pmod 4 \\ \left((1 - 2i)(1 + i)^n + i\right) \cdot \left((1 - 2i)(1 + i)^n - i\right) & \text{if } n \equiv 3 \pmod 4, \end{cases} \end{aligned}$$

so that s_n factors nontrivially in $\mathcal{O}_d$.

3.2. $d = -2$ and $d = -11$

Since the approach is the same in each of these cases, we give details only for $d = -2$. It is easy to check by computer that no element of $\mathcal{O}_d$ with odd norm smaller than 11 is a Sierpiński number in $\mathcal{O}_d$. Let $\sigma = 3 + \sqrt{-2}$. Then, since $N(s_n) = 11 \cdot 2^{2n} + 6 \cdot 2^n + 1 \equiv 0 \pmod 3$, it follows from Corollary 16 that σ is a Selfridge number in $\mathcal{O}_d$. The proof is identical for the other values of σ in Table 7 when $d = -2$.

3.3. $d = -3$ and $d = -7$

Since the techniques used are similar for each value of d, we give details only for $d = -7$. Let $\sigma = 7$. First note that s_n is composite when $n = 1$. Then, if s_n is prime for some $n \geq 2$, we have by Theorem 7 that

$$\left(\frac{d}{s_n}\right) = \left(\frac{s_n}{7}\right) = \left(\frac{1}{7}\right) = 1,$$

which establishes that σ is a Sierpiński number in $\mathcal{O}_d$ by Theorem 15 (Part *4.*). To prove that σ is a Selfridge number, we examine the set T of all elements in $\mathcal{O}_d$ other than σ having odd norm N with $3 < N \leq 49 = N(\sigma)$:

$T = \{-7, \pm 5, \pm 3, \sqrt{-7}, \pm 1 + 2\sqrt{-7}, \pm 3 + 2\sqrt{-7}, \pm 2 + \sqrt{-7}, \pm 4 + \sqrt{-7}, \pm 6 + \sqrt{-7}\}$.

Fortunately, it is easy to show that no element of T is a Sierpiński number in $\mathcal{O}_d$. For example, if $\alpha = 5$, then

$$\left(\frac{d}{\alpha \cdot 2^3 + 1}\right) = \left(\frac{-7}{41}\right) = -1,$$

and so $\alpha = 5$ is not a Sierpiński number in $\mathcal{O}_d$ by Theorem 15 (Part *4.*). As another example, let $\alpha = 1 + 2\sqrt{-7}$. Then $N(\alpha \cdot 2^3 + 1) = 29 \cdot 2^6 + 2^4 + 1 = 1873$, and since 1873 is prime in $\mathbb{Z}$, we have that $\alpha \cdot 2^3 + 1$ is prime in $\mathcal{O}_d$ by Proposition 13. Hence, $\alpha = 1 + 2\sqrt{-7}$ is not a Sierpiński number in $\mathcal{O}_d$.

3.4. $d = -19$

Let $\sigma = \dfrac{5 + 3\sqrt{-19}}{2}$. We use techniques similar to those used for $d = -7$ to verify that there are no Sierpiński numbers in $\mathcal{O}_d$ with odd norm smaller than $N(\sigma) = 49$. Then we observe that

$$N(s_n) = 49 \cdot 2^{2n} + 5 \cdot 2^n + 1 \equiv \begin{cases} 0 \pmod 3 & \text{if } n \equiv 1 \pmod 2 \\ 0 \pmod 5 & \text{if } n \equiv 0 \pmod 2, \end{cases}$$

which implies, by Corollary 16, that σ is a Selfridge number in $\mathcal{O}_d$. The result is identical for the other value of σ in Table 7.

3.5. $d = -43$, $d = -67$ and $d = -163$

The techniques for these cases are similar so we present the details only for $d = -43$. To verify that there are no Sierpiński numbers in $\mathcal{O}_d$ with odd norm smaller than 169, we use PARI/GP to obtain certificates of primality in certain cases. For example, let $\alpha = \dfrac{11 + 3\sqrt{-43}}{2}$. Then $N(\alpha) = 127$. To show that α is not a Sierpiński number in $\mathcal{O}_d$, we examine $N(\alpha \cdot 2^n + 1) = 127 \cdot 2^{2n} + 11 \cdot 2^n + 1$, which is easily seen to be composite for all $n \leq 39$. We then use PARI/GP to prove that $N(\alpha \cdot 2^{40} + 1)$ is prime, and conclude by Proposition 13 that α is not a Sierpiński number in $\mathcal{O}_d$. Now, let $\sigma = \dfrac{17 + 3\sqrt{-43}}{2}$. Observe that if $n \equiv 1 \pmod 2$, then

$$N(s_n) = 169 \cdot 2^{2n} + 17 \cdot 2^n + 1 \equiv 0 \pmod 3.$$

For $n \equiv 0 \pmod 2$, we can write

$$\begin{aligned} N(s_n) &= (13 \cdot 2^n + 1)^2 - (3 \cdot 2^{n/2})^2 \\ &= \left(13 \cdot 2^n + 1 - 3 \cdot 2^{n/2}\right)\left(13 \cdot 2^n + 1 + 3 \cdot 2^{n/2}\right). \end{aligned}$$

Thus, by Corollary 16, σ is a Selfridge number in $\mathcal{O}_d$. The proof for the other value of σ is identical.

4. The Proof of Theorem 4

The strategy here is the same as the strategy employed in the proof of Theorem 3 with an additional step. The additional step required here is that our Sierpiński candidates α must be prime in $\mathcal{O}_d$. Primality of α in $\mathcal{O}_d$ can be verified by simply checking that $N(\alpha)$ is prime in $\mathbb{Z}$ when $\alpha \notin \mathbb{Z}$ (Proposition 13), or that $\left(\dfrac{d}{\alpha}\right) = -1$ when α is a prime in $\mathbb{Z}$ (Theorem 15 (Part *4.*)).

Since many of the proofs are similar for various values of d, we give details only in selected cases. For convenience, we define $s_n := \pi \cdot 2^n + 1$, where π is a Selfridge prime from Table 7.

4.1. $d = -1$ and $d = -2$

Using the techniques used to prove Theorem 3, it is straightforward to establish that the Selfridge primes for $d = -2$ are $\pi = \pm 3 \pm \sqrt{-2}$, and that the only Selfridge prime for $d = -1$ is $\pi = 7$.

4.2. $d = -7$

Using a computer to check up to $n = 400$ and norm 2209, the only candidate for a Selfridge prime is $\pi = 47$. To verify that $\pi = 47$ is indeed a Selfridge prime, we must show that s_n is composite in $\mathcal{O}_d$ for all $n \geq 1$. To accomplish this task, we use the partial covering $\mathcal{C} = \{(0, 2, 3), (1, 4, 5), (3, 12, 13), (11, 12, 7)\}$. It is then straightforward to show that $47 \cdot 2^n + 1 \equiv 0 \pmod{p}$, when $n \equiv r \pmod{m}$ for each $(r, m, p) \in \mathcal{C}$. The only "hole" in our partial covering $\mathcal{C}$ is $n \equiv 7 \pmod{12}$. But for these values of n we have that $47 \cdot 2^n + 1 \equiv 4 \pmod{7}$. Hence, if $p = 47 \cdot 2^n + 1$ is prime in $\mathbb{Z}$, it follows that $\left(\frac{-7}{p}\right) = 1$, so that p is composite in $\mathcal{O}_d$. Therefore, we have established that 47 is the Selfridge prime in $\mathcal{O}_d$ by Theorem 15 (Part *4.*).

4.3. $d = -11$

In this case, each Selfridge number $\frac{\pm 3 \pm \sqrt{-11}}{2}$ has norm 5, and therefore each Selfridge number is also a Selfridge prime by Proposition 13.

4.4. $d = -19$

Let $\pi = \frac{-25 - 3\sqrt{-19}}{2}$. Note that

$$N(s_n) = 199 \cdot 2^{2n} - 25 \cdot 2^n + 1 \equiv \begin{cases} 0 \pmod 3 & \text{if } n \equiv 1 \pmod 2 \\ 0 \pmod 5 & \text{if } n \equiv 0 \pmod 2, \end{cases}$$

which proves, by Corollary 16, that π is a Sierpiński number in $\mathcal{O}_d$. Since $N(\pi) = 199$ is prime, we have by Proposition 13 that π is prime in $\mathcal{O}_d$. Using a computer, it is straightforward to show that π is a Sierpiński number in $\mathcal{O}_d$ with smallest odd prime norm, which implies that π is a Selfridge prime. The proof that $\frac{-25 + 3\sqrt{-19}}{2}$ is a Selfridge prime is identical.

5. Proof of Theorem 5

Recall that $\mathcal{D} = \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$, and that $\mathcal{S}$ is the set of all odd positive rational integers k such that, for all $n \geq 1$, the integers $k \cdot 2^n + 1$ are simultaneously composite in $\mathcal{O}_d$ for all $d \in \mathcal{D}$. Clearly, all classical Sierpiński numbers are contained in $\mathcal{S}$. To see that this containment is proper, let $z \equiv 111 \pmod{130}$ be a positive integer, and let $k = 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163 \cdot z$. Then $k \cdot 2 + 1$ and $k \cdot 2^2 + 1$ are both composite in $\mathbb{Z}$ since

$$k \cdot 2 + 1 \equiv 0 \pmod 5 \quad \text{and} \quad k \cdot 2^2 + 1 \equiv 0 \pmod{13}.$$

Let $d \in \mathcal{D}$, assume that $n \geq 3$, and suppose that $p = k \cdot 2^n + 1$ is prime in $\mathbb{Z}$. Then, $p \equiv 1 \pmod 8$ and, by Theorem 6 and Theorem 7, we have that $\left(\frac{d}{p}\right) = 1$. Hence, $k \in \mathcal{S}$. The smallest value of k produced by this process is $k = 228780719937$, and we note that this value of k is not a classical Sierpiński number since $228780719937 \cdot 2^3 + 1 = 1830245759497$ is prime in $\mathbb{Z}$.

6. Comments, Conjectures and Conclusions

6.1. Extending Theorem 4

While we were not able to find the Selfridge primes for $d \in \{-43, -67, -163\}$, we give in Table 7 a list of conjectured Selfridge primes for $d = -43$ and $d = -67$, and some justification below for these conjectured values.

6.1.1. $d = -43$

Since $\pi = \dfrac{289 - 45\sqrt{-43}}{2}$ has norm 42649, which is prime, we know by Proposition 13 that π is prime in $\mathcal{O}_d$. Now consider the covering $\mathcal{C} = \{(0, 2, 3), (1, 4, 5), (3, 4, 17)\}$. Note that here the prime 17 associated to the third congruence in $\mathcal{C}$ is not a prime divisor of $2^4 - 1$. However, 17 does divide $N(s_n)$ for values of $n \equiv 3 \pmod 4$. Apply $\mathcal{C}$ to the exponent n in $N(s_n) = N(\pi \cdot 2^n + 1)$ to get that

$$N(s_n) = 42649 \cdot 2^{2n} + 289 \cdot 2^n + 1 \equiv \begin{cases} 0 \pmod 3 & \text{if } n \equiv 0 \pmod 2 \\ 0 \pmod 5 & \text{if } n \equiv 1 \pmod 4, \\ 0 \pmod{17} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Hence, π is a Sierpiński number in $\mathcal{O}_d$. To prove that π is a Selfridge prime, we must rule out all primes in $\mathcal{O}_d$ with norm less than 42649. Unfortunately, there are several candidates which we have been unable to eliminate. For example, for the prime $\alpha = \dfrac{-67 + 15\sqrt{-43}}{2}$, with norm 3541, the number $c_n = \alpha \cdot 2^n + 1$ is composite for all $n \leq 50000$. Because there appears to be no "nice" pattern to the prime divisors of $N(c_n)$, we believe that there exists $m > 50000$ such that $N(c_m)$ is prime. Thus, c_m would be prime in $\mathcal{O}_d$, and α would not be a Selfridge prime.

6.1.2. $d = -67$

The covering $\mathcal{C} = \{(0, 2, 3), (1, 4, 5), (3, 4, 17)\}$ used in 6.1.1 can be used in this case to verify that the prime $\pi = -238 + 15\sqrt{-67}$ in $\mathcal{O}_d$ is a Sierpiński number. But we are faced with the same difficulties as in the case of $d = -43$ in showing that π is a Selfridge prime.

6.1.3. $d = -163$

We tested, up to $n = 5000$, all elements $\alpha \in \mathcal{O}_d$ such that $N(\alpha)$ is prime and $N(\alpha)$ is less than the 50000th prime, and we found no Selfridge prime candidates.

6.2. Comments on Theorem 5

Of course the classical Sierpiński number $k = 78557$ found by Selfridge is contained in $\mathcal{S}$, but is it the smallest element of $\mathcal{S}$? It can be shown, with little effort, that $|d|$ is the smallest rational integer that is a Sierpiński number in $\mathcal{O}_d$ for each $d \in \{-3, -7, -11, -19, -43, -67, -163\}$, although to rule out smaller rational integers requires checking up to some large exponents. For example, to show that 47 is not a Sierpiński number in the case of $d = -67$, we have to check up to $n = 6115$ since this is the smallest value of n for which $47 \cdot 2^n + 1$ is prime in $\mathcal{O}_d$. It is also straightforward to show that the smallest rational Sierpiński numbers in $\mathcal{O}_d$ for $d = -1$ and $d = -2$ are 7 and 5, respectively. For example, to show that 5 is the smallest rational Sierpiński number in $\mathcal{O}_d$ when $d = -2$, we first observe that $3 \cdot 2 + 1 = 7$ is prime in $\mathcal{O}_d$. This rules out 3 as a Sierpiński number in $\mathcal{O}_d$. Next, we see that while $5 \cdot 2^n + 1$ is prime in $\mathbb{Z}$ for $n = 1$ and $n = 3$, these primes (11 and 41) are both composite in $\mathcal{O}_d$. Also, $5 \cdot 2^2 + 1 = 21$ is obviously composite. Then, for $n \geq 3$, if $p = 5 \cdot 2^n + 1$ is prime in $\mathbb{Z}$, we have that $p \equiv 1 \pmod 8$ and so $\left(\frac{-2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = 1$, which proves that 5 is a Sierpiński number in $\mathcal{O}_d$, by Theorem 15 (Part *4.*). "Piecing" together this information is what is done in the proof of Theorem 5 to get a value of k that is a Sierpiński number in $\mathcal{O}_d$ for all $d \in \mathcal{D}$. However, the smallest value of k produced by these methods is much larger than the Sierpiński number $k = 78557$ found by Selfridge. Computer calculations show that all of the values of $k < 78557$ for which a value of n is known such that $k \cdot 2^n + 1$ is prime in the rational integers, also fail to be Sierpiński in $\mathcal{O}_d$ for at least one $d \in \mathcal{D}$. The remaining six rational Sierpiński candidates [2] are the elements of $\mathcal{B} = \{10223, 21181, 22699, 24737, 55459, 67607\}$. If $p = k \cdot 2^n + 1$ is a rational prime for any $k \in \mathcal{B}$, then $p \equiv 5 \pmod{12}$ and thus $\left(\frac{-3}{p}\right) = -1$, so that p remains prime for $d = -3$, by Theorem 15 (Part *4.*). In other words, if $k \in \mathcal{B}$ is not a rational Sierpiński number, then $k \notin \mathcal{S}$. Thus we have the following:

Theorem 18. *The smallest element of $\mathcal{S}$ is either $k = 78557$ or the smallest Sierpiński number in $\mathcal{B}$.*

6.3. Two Avenues for Future Investigation

For $d \in \{-1, -3, -7\}$, the rational prime 2 does not remain prime in $\mathcal{O}_d$. So one could conduct an investigation similar to the topics in this paper to find $\alpha \in \mathcal{O}_d$

such that $\alpha \cdot \pi^n + 1$ is composite in $\mathcal{O}_d$ for all $n \geq 1$, where $\pi \in \mathcal{O}_d$ is a prime divisor of 2.

A possible second area of investigation would be to focus on real quadratic fields. This situation might be complicated by the fact that there could be infinitely many solutions to the equation $x^2 - dy^2 = N$, for a nonzero integer N, and finding these solutions can be somewhat involved [5, 3, 4]. In addition, another complicating factor is that it is conjectured that there are infinitely many such fields with class number one.

7. Tables

d	σ	$N(\sigma)$
-1	$-4 \pm 3\sqrt{-1}$	25
-2	$\pm 3 \pm \sqrt{-2}$	11
-3	3	9
-7	7	49
-11	$\frac{\pm 3 \pm \sqrt{-11}}{2}$	5
-19	$\frac{5 \pm 3\sqrt{-19}}{2}$	49
-43	$\frac{17 \pm 3\sqrt{-43}}{2}$	169
-67	$\frac{29 \pm 3\sqrt{-67}}{2}$	361
-163	$\frac{77 \pm 3\sqrt{-163}}{2}$	1849

Table 1: Selfridge Numbers σ in $\mathcal{O}_d$

d	π	$N(\pi)$
-1	7	49
-2	$\pm 3 \pm \sqrt{-2}$	11
-3	-5	25
-7	47	2209
-11	$\frac{\pm 3 \pm \sqrt{-11}}{2}$	5
-19	$\frac{-25 \pm 3\sqrt{-19}}{2}$	199

Table 2: Selfridge Primes π in $\mathcal{O}_d$

d	π	$N(\pi)$
-43	$\frac{289-45\sqrt{-43}}{2}$	42649
-67	$-238+15\sqrt{-67}$	71719
-163	?	?

Table 3: Conjectured Selfridge Primes π in $\mathcal{O}_d$

Acknowledgements The authors thank the referee for the many valuable suggestions.

References

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

[2] L.Helm, D. Norris et al., Seventeen or Bust: A Distributed Attack on the Sierpiński Problem, available online at `http://www.seventeenorbust.com/`.

[3] K. Matthews, The Diophantine equation $x^2 - Dy^2 = N,\ D > 0$. *Expo. Math.* **18** (2000), 323-?331.

[4] K. Matthews, Thue's theorem and the diophantine equation $x^2 - Dy^2 = \pm N$, *Math. Comp.* **71** (2002), 1281–1286.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley, New York, 1991.

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

[7] E. Weisstein, Sierpiński Number of the Second Kind, from MathWorld — A Wolfram Web Resource, `http://mathworld.wolfram.com/SierpinskiNumberoftheSecondKind.html`.