

# A group-theoretic approach to covering systems

Lenny Jones and Daniel White

Communicated by L. A. Kurdachenko

ABSTRACT. In this article, we show how group actions can be used to examine the set of all covering systems of the integers with a fixed set of distinct moduli.

## 1. Introduction

A (*finite*) *covering system*  $C$ , or simply a *covering*, of the integers is a system of  $t$  congruences  $x \equiv r_i \pmod{m_i}$ , with  $m_i > 1$  for all  $1 \leq i \leq t$ , such that every integer  $n$  satisfies at least one of these congruences. The concept of a covering was introduced by Paul Erdős in a paper in 1950 [8], where he used a covering to find an arithmetic progression of counterexamples to Polignac’s conjecture that every positive integer can be written in the form  $2^k + p$ , where  $p$  is a prime. Since then, numerous authors have used covering systems to investigate and solve various problems [1–4, 4–7, 9–16, 18–21, 23–30, 32–35, 37–41, 43–49].

Under the restriction that all moduli in a covering are distinct, Erdős made the following statement in [8]:

*“It seems likely that for every  $c$  there exists such a system all the moduli of which are  $> c$ .”*

This conjecture, known as the *minimum modulus problem*, remained unresolved until recently when Bob Hough [20] showed that it is false. Since the minimum modulus in a covering is now known to be bounded

---

**2010 MSC:** Primary 11B25; Secondary 05E18, 11A07.

**Key words and phrases:** covering system, group action, congruence.

above, one can naively speculate as to whether a categorization of all covering systems with a fixed minimum modulus might be possible in some way. Admittedly, such a notion seems intractable, if not impossible. But perhaps, a less ambitious task is possible. For example, could an enumeration be given of all coverings with a fixed set of moduli or a fixed least common multiple of the moduli? Recently [31], we have accomplished this goal for a very specific situation involving primitive covering numbers—a notion introduced by Zhi-Wei Sun [47] in 2007. While the methods in [31] are purely combinatorial, we show in this article how certain group actions can be used to examine the set of all covering systems of the integers with a fixed set of distinct moduli.

## 2. Preliminaries

It will be convenient on occasion to write any covering  $C = \{(r_i, m_i)\}$ , where  $x \equiv r_i \pmod{m_i}$  is a congruence in the covering, simply as  $C = [r_1, r_2, \dots, r_t]$ , when the moduli are written as a list  $[m_1, m_2, \dots, m_t]$ . We write  $\text{lcm}(M)$  to denote the least common multiple of the elements in a set or list of moduli  $M$ . We let  $\Gamma_M$ , or simply  $\Gamma$ , if there is no ambiguity, denote the set of all coverings having moduli  $M$ . We define a covering  $C$  to be *minimal* if no proper subset of  $C$  is a covering. We also define a set, or list, of distinct moduli  $M$  to be *minimal* if every possible covering using all the elements of  $M$  is minimal. A positive integer  $L$  is called a *covering number* if there exists a covering of the integers where the moduli are distinct divisors of  $L$  greater than 1. A covering number  $L$  is called a *primitive covering number* if no proper divisor of  $L$  is a covering number. The following two theorems concerning covering numbers, which we state without proof, are due to Zhi-Wei Sun [47].

**Theorem 2.1.** *Let  $p_1, p_2, \dots, p_r$  be distinct primes, and let  $a_1, a_2, \dots, a_r$  be positive integers. Suppose that*

$$\prod_{0 < t < s} (a_t + 1) \geq p_s - 1 + \delta_{r,s}, \quad \text{for all } s = 1, 2, \dots, r, \quad (1)$$

where  $\delta_{r,s}$  is Kronecker's delta, and the empty product  $\prod_{0 < t < 1} (a_t + 1)$  is defined to be 1. Then  $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$  is a covering number.

Infinitely many primitive covering numbers can be constructed using Theorem 2.1. We let  $\lfloor x \rfloor$  denote the greatest integer less than or equal to  $x$ .

**Theorem 2.2.** *Let  $r > 1$  and let  $2 = p_1 < p_2 < \dots < p_r$  be primes. Suppose further that  $p_{t+1} \equiv 1 \pmod{p_t - 1}$  for all  $0 < t < r - 1$ , and  $p_r \geq (p_{r-1} - 2)(p_{r-1} - 3)$ . Then*

$$p_1^{\frac{p_2-1}{p_1-1}-1} \cdots p_{r-2}^{\frac{p_{r-1}-1}{p_{r-2}-1}-1} \left\lfloor \frac{p_r-1}{p_{r-1}-1} \right\rfloor p_r$$

*is a primitive covering number.*

It is straightforward to see that Theorem 2.2 produces an infinite set  $\mathcal{L}$  of primitive covering numbers, and that every element of  $\mathcal{L}$  satisfies (1). In [47], Sun conjectured that every primitive covering number  $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ , where  $p_1, \dots, p_r$  are distinct primes, satisfies (1). However, this conjecture is now known to be false [31].

Unless stated otherwise, we assume throughout this article that the moduli in all coverings are distinct, and that all sets of moduli are minimal.

### 3. Counting the number of coverings without group theory

While it is the main goal of this paper to use group-theoretic techniques to impose some structure on, and examine, the set of all coverings with a fixed list of distinct moduli, there are certain situations when some information can be obtained without the use of group theory. In particular, using a combinatorial approach, a formula was given in [31] for  $|\Gamma_M|$ , when  $L \in \mathcal{L}$  and  $M$  is minimal with  $\text{lcm}(M) = L$ . The following theorem illustrates another situation when  $|\Gamma_M|$  can be determined without the use of group theory.

**Theorem 3.1.** *For  $k \geq 2$ , let*

$$M_k = [2, 2^2, \dots, 2^k, 3, 2^{k-1} \cdot 3, 2^k \cdot 3].$$

*For brevity of notation, let  $\Gamma_k$  denote the set of all coverings using the moduli  $M_k$ . Then*

$$|\Gamma_k| = 2^{k+1} \cdot 3.$$

*Proof.* The proof is by induction on  $k$ . First let  $k = 2$ . The set  $\Gamma_2$  of all possible coverings using the moduli  $M_2 = [2, 4, 3, 6, 12]$  is easy to generate

using a computer. We get that

$$\begin{aligned} \Gamma_2 = \{ & [0, 1, 0, 1, 11], [0, 1, 0, 5, 7], [0, 1, 1, 3, 11], [0, 1, 1, 5, 3], \\ & [0, 1, 2, 1, 3], [0, 1, 2, 3, 7], [1, 2, 0, 2, 4], [1, 0, 0, 2, 10], \\ & [1, 0, 0, 4, 2], [1, 0, 1, 0, 2], [1, 2, 0, 4, 8], [1, 0, 1, 2, 6], \\ & [1, 0, 2, 0, 10], [1, 2, 1, 0, 8], [1, 0, 2, 4, 6], [1, 2, 1, 2, 0], \\ & [1, 2, 2, 0, 4], [1, 2, 2, 4, 0], [0, 3, 0, 1, 5], [0, 3, 0, 5, 1], \\ & [0, 3, 1, 3, 5], [0, 3, 1, 5, 9], [0, 3, 2, 1, 9], [0, 3, 2, 3, 1] \}. \end{aligned} \tag{2}$$

Observe that  $|\Gamma_2| = 24$ , so that the base case is verified. Let  $L_k = 2^k \cdot 3$ . Assume, by induction, that  $|\Gamma_k| = 2^{k+1} \cdot 3$ . Let  $\widehat{M}_k = \{2, 2^2, \dots, 2^k, 3, 2^k \cdot 3\}$ . Let  $\widehat{R}_k$  be a list of residues in a covering in  $\Gamma_k$  corresponding to the moduli  $\widehat{M}_k$ . There is just one hole modulo  $L_k$  left to fill to complete a covering in  $\Gamma_k$ , and this can be done in exactly one way using a residue  $r \pmod{2^{k-1} \cdot 3}$ . Thus, there are exactly two holes modulo  $L_{k+1}$  that need to be filled to complete a covering in  $\Gamma_k$ . These two holes can be filled in exactly two ways using the two moduli  $2^{k+1}$  and  $2^{k+1} \cdot 3$  in the following way. We can use either

$$r \pmod{2^{k+1}} \quad \text{and} \quad r + 2^k \cdot 3 \pmod{2^{k+1} \cdot 3},$$

or

$$r + 2^k \cdot 3 \pmod{2^{k+1}} \quad \text{and} \quad r \pmod{2^{k+1} \cdot 3}.$$

Thus, we have shown that  $|\Gamma_{k+1}| = 2|\Gamma_k| = 2^{k+2} \cdot 3$ , and the proof is complete.  $\square$

**Remark 3.2.** Note that when  $k = 2$  in Theorem 3.1, we have  $L = 12 \in \mathcal{L}$ , and so this is a special case addressed in [31].

### 4. Group theory and covering systems

In this section, we develop a group-theoretic approach to describe a relationship among the elements in  $\Gamma$ , and to help determine  $|\Gamma|$ . In particular, we investigate when there exist finite groups that act on  $\Gamma$  and we exploit this action to enumerate and categorize the elements of  $\Gamma$ . We let  $\text{orb}_G(C)$  and  $\text{stab}_G(C)$  denote, respectively, the orbit and stabilizer of  $C \in \Gamma$  under the action of some group  $G$ . We begin by providing a brief analysis, without general proofs, in the situation when  $L \in \mathcal{L}$  and  $M$  is minimal.

**4.1. A group action in Sun’s primitive covering number situation**

A formula was given in [31] for  $|\Gamma_M|$  when  $L \in \mathcal{L}$  and  $M$  is minimal with  $\text{lcm}(M) = L$ . From this formula, a finite group  $G$  can be constructed that acts transitively on  $\Gamma_M$ . This formula, and consequently the group  $G$ , are quite complicated in general. However, in special situations,  $G$  can be described fairly easily. Let

$$L = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{r-1}^{\alpha_{r-1}} p_r \in \mathcal{L}.$$

Under certain restrictions, the formula in [31] for  $|\Gamma_M|$  reduces to

$$|\Gamma_M| = \prod_{i=1}^r (p_i!)^{\alpha_i}. \tag{3}$$

**Remark 4.1.** Formula 3 also holds for values of  $L \notin \mathcal{L}$ . See Table 1.

A consequence of (3) is the existence of a finite group

$$G \simeq (S_{p_1})^{\alpha_1} \times \cdots \times (S_{p_r})^{\alpha_r}, \tag{4}$$

where

$$(S_{p_i})^{\alpha_i} = \underbrace{S_{p_i} \times \cdots \times S_{p_i}}_{\alpha_i\text{-factors}}$$

and  $S_{p_i}$  is the symmetric group on  $p_i$  letters, that acts transitively on  $\Gamma$  by appropriately permuting the residues. The following example illustrates this process.

**An example:  $L = 12$  with  $M = [m_1, m_2, m_3, m_4, m_5] = [2, 4, 3, 6, 12]$**

We see easily that  $L = 12$  is a primitive covering number satisfying (1).

- $p_1 = 2$   
 We seek a group  $H_1 \simeq S_2 \times S_2$ . We start with the element  $h = (12)(34)$ . To construct the other three nontrivial elements of  $H_1$ , we conjugate  $h$  by the elements (24) and (23) to get

$$H_1 = \{(1), (12)(34), (14)(23), (13)(24)\}$$

- $p_2 = 3$   
 We seek a group  $H_2 \simeq S_3$ . Let

$$H_2 = \{(1), (12), (23), (13), (123), (132)\}.$$

Therefore,  $G = H_1 \times H_2$ . We write a covering  $C$  as  $[r_1, r_2, r_3, r_4, r_5]$ , where  $r_i \pmod{m_i}$  is a congruence in  $C$ . We illustrate the action on the set  $\Gamma$  of all 24 coverings given in (2). As an example, let  $C = [1, 2, 1, 0, 8]$ . We use the Chinese remainder theorem to decompose the residues on the composite moduli into prime power moduli, and we substitute  $p_i^k \pmod{p_i^k}$  for  $0 \pmod{p_i^k}$ . We also place subscripts on the residues in these decompositions to remind us of the prime power moduli. Thus,

$$C = [1, 2, 1, [2_2, 3_3], [4_4, 2_3]].$$

Let  $g = ((14)(23), (123))$ . Then

$$g.C = [4, 3, 2, [3_2, 1_3], [1_4, 3_3]] = [0, 3, 2, 1, 9] \in \Gamma,$$

and it is easy to verify that  $\text{orb}_G(C) = \Gamma$ .

If it is the desire to navigate explicitly among the coverings  $C \in \Gamma$  via this action of  $G$ , we see from the previous example that the process is somewhat cumbersome. We show in the next section that, for any value of  $L$ , there is a more easily-described group that acts on the set of all coverings. The disadvantage is that the action is not always transitive.

### 4.2. A group action in the general situation

In this section, we lift the restriction that  $L$  must satisfy (1). Let  $\mathbb{Z}_L$  be the additive group of integers modulo  $L$ . We define the *holomorph* of  $\mathbb{Z}_L$  to be

$$\text{Hol}(\mathbb{Z}_L) = \text{Aut}(\mathbb{Z}_L) \rtimes \mathbb{Z}_L \simeq \mathbb{Z}_L^* \rtimes \mathbb{Z}_L, \tag{5}$$

where  $\mathbb{Z}_L^*$  is the group of units in the ring  $\mathbb{Z}_L$  of integers modulo  $L$ . Note that  $|\text{Hol}(\mathbb{Z}_L)| = \phi(L)L$ . For brevity of notation, we let  $\mathcal{G} = \text{Hol}(\mathbb{Z}_L)$ .

**Remark 4.2.** More typically, a semidirect product is written using the notation  $A \rtimes B$ . However, it is more convenient here to use the isomorphic group  $B \rtimes A$ .

**Theorem 4.3.** *There is a natural (left) action of  $\mathcal{G}$  on  $\Gamma$ .*

*Proof.* Let  $g = (a, x) \in \mathcal{G}$  and  $C = \{(r_i, m_i) \mid 1 \leq i \leq t\} \in \Gamma$ . Define

$$g.C := \{(ar_i + x, m_i) \mid 1 \leq i \leq t\}.$$

We first show that  $g.C$  is indeed a covering. Let  $n$  be any integer. Since  $C$  is a covering, there exists  $j$  such that

$$a^{-1}(n - x) \equiv r_j \pmod{m_j}.$$

Hence,

$$n \equiv ar_j + x \pmod{m_j},$$

so that  $n$  is covered by  $g.C$ .

Note that  $(1, 0) \in \mathcal{G}$  is the identity element in  $\mathcal{G}$ , and that  $(1, 0).C = C$ . Next, let  $h \in \mathcal{G}$  with  $h = (b, y)$ . By the definition of the operation in  $\mathcal{G}$ , we have that

$$gh = (a, x)(b, y) = (ab, ay + x).$$

Thus,

$$\begin{aligned} (gh).C &= \left\{ (abr_i + ay + x, m_i) \mid 1 \leq i \leq t \right\} \\ &= \left\{ (a(br_i + y) + x, m_i) \mid 1 \leq i \leq t \right\} \\ &= g. \left\{ (br_i + y, m_i) \mid 1 \leq i \leq t \right\} \\ &= g.(h.C), \end{aligned}$$

which completes the proof. □

**Theorem 4.4.** *Let  $C = \{(r_i, m_i) \mid 1 \leq i \leq t\} \in \Gamma$ . Then*

$$|\text{orb}_{\mathcal{G}}(C)| \geq \kappa(L)\phi(L), \tag{6}$$

where  $\kappa(L)$  denotes the square-free kernel of  $L$ , and  $\phi$  is Euler's totient function. Moreover, equality holds in (6) if

$$\kappa(L)(r_i - r_j) \equiv 0 \pmod{\text{gcd}(m_i, m_j)} \quad \text{for all } i \text{ and } j. \tag{7}$$

*Proof.* Let  $g = (a, x) \in \text{stab}(C)$ . Then  $g.C = C$  and hence

$$(a - 1)r_i + x \equiv 0 \pmod{m_i}, \tag{8}$$

for all  $(r_i, m_i) \in C$ . Let  $p$  be a prime such that  $L \equiv 0 \pmod{p}$ , and let

$$C_p = \left\{ (r_i, m_i) \in C \mid m_i \equiv 0 \pmod{p} \right\}.$$

Since  $C$  is a covering, there exist  $i$  and  $j$ , with  $i \neq j$  and  $(r_i, m_i), (r_j, m_j) \in C_p$ , such that  $r_i \not\equiv r_j \pmod{p}$ . For this particular pair of congruences in  $C_p$ , we have by (8) that

$$(a-1)r_i + x \equiv (a-1)r_j + x \pmod{p}. \quad (9)$$

Rearranging (9) and using the fact that  $r_i \not\equiv r_j \pmod{p}$ , we get that  $a \equiv 1 \pmod{p}$ . Thus,

$$a \equiv 1 \pmod{\kappa(L)}. \quad (10)$$

There are exactly  $\phi(L)/\phi(\kappa(L)) = L/\kappa(L)$  distinct values of  $a \in \mathbb{Z}_L^*$  that satisfy (10). For each such value of  $a$ , we claim that there is at most one value of  $x \in \mathbb{Z}_L$  that satisfies all congruences in (8). To see this, we fix  $a$  and write  $a-1 = z\kappa(L)$  for some integer  $z$  with  $0 \leq z \leq L/\kappa(L) - 1$ . Then the system of congruences (8) can be rewritten as the following system of congruences in the variable  $x$ :

$$x \equiv -z\kappa(L)r_i \pmod{m_i}, \quad \text{for all } (r_i, m_i) \in C. \quad (11)$$

By the generalized Chinese remainder theorem, the system (11) has a solution  $x \in \mathbb{Z}_L$ , and it is unique, if and only if

$$z\kappa(L)(r_i - r_j) \equiv 0 \pmod{\gcd(m_i, m_j)}$$

for all  $i$  and  $j$ . Thus, we have shown that

$$|\text{stab}_{\mathcal{G}}(C)| \leq \frac{L}{\kappa(L)}.$$

Consequently, since  $|\mathcal{G}| = \phi(L)L$ , we have that

$$|\text{orb}_{\mathcal{G}}(C)| = [\mathcal{G} : \text{stab}_{\mathcal{G}}(C)] \geq \kappa(L)\phi(L).$$

Moreover, if

$$\kappa(L)(r_i - r_j) \equiv 0 \pmod{\gcd(m_i, m_j)}$$

for all  $i$  and  $j$ , then

$$z\kappa(L)(r_i - r_j) \equiv 0 \pmod{\gcd(m_i, m_j)}$$

for any fixed  $z$  and all  $i$  and  $j$ . Thus, in this case, the system (11) has a unique solution, and so equality holds in (6).  $\square$

The following corollary is immediate from Theorem 4.4.

**Corollary 4.5.** *Let  $C = \{(r_i, m_i) \mid 1 \leq i \leq t\} \in \Gamma$ . If (7) holds and  $\mathcal{G}$  acts transitively on  $\Gamma$ , then*

$$|\Gamma| = |\text{orb}_{\mathcal{G}}(C)| = \kappa(L)\phi(L). \tag{12}$$

Condition (7) alone is not sufficient to deduce (12). For example, let  $L = 36$  and  $M = [2, 3, 4, 6, 9, 18, 36]$ . Then, computer computations show that  $|\Gamma| = 144$  and each  $C \in \Gamma$  satisfies (7). Also, there are two orbits of size  $\kappa(L)\phi(L) = 72$ , so that  $\mathcal{G}$  does not act transitively on  $\Gamma$ . Thus, in this case, we see that  $|\Gamma| = 2\kappa(L)\phi(L)$ .

**Corollary 4.6.** *If  $L$  is square-free, then equality holds in (6) for all  $C \in \Gamma$ .*

*Proof.* Since  $|\text{orb}_{\mathcal{G}}(C)|$  divides  $|\mathcal{G}| = L\phi(L)$ , we have that  $|\text{orb}_{\mathcal{G}}(C)| \leq L\phi(L)$ . Since  $L$  is square-free,  $\kappa(L) = L$ , and therefore by Theorem 4.4, we deduce that

$$L\phi(L) \geq |\text{orb}_{\mathcal{G}}(C)| \geq \kappa(L)\phi(L) = L\phi(L). \quad \square$$

If we want to utilize Theorem 4.4 to determine  $|\Gamma|$ , then the question of transitivity of the action of  $\mathcal{G}$  on  $\Gamma$  is a main concern. Unfortunately, we have been unable to find a way to determine when this occurs in general. For certain values of  $L$  and certain lists  $M$ , we used a computer to determine  $|\Gamma|$  and  $|\text{orb}_{\mathcal{G}}(C)|$ . This information is given in Table 1. We denote the number of orbits as  $\#$ . A complete set of orbit representatives for each example given in Table 1 is available upon request. Note that, in Table 1,  $L \in S$  only for  $L = 80$  and  $L = 90$ .

$L$	$M$	$\#$	$ \text{orb}(C) $	$ \Gamma $
36	[2, 3, 4, 6, 9, 18, 36]	2	72	144
60	[2, 3, 4, 5, 6, 10, 15, 20, 30]	6	480	2880
72	[2, 3, 4, 6, 9, 24, 36, 72]	2	144	288
80	[2, 4, 5, 8, 10, 16, 20, 40, 80]	6	320	1920
90	[2, 3, 9, 5, 6, 10, 15, 18, 30, 45]	12	720	8640
108	[2, 3, 4, 6, 9, 18, 27, 54, 108]	4	216	864
120	[2, 3, 4, 5, 8, 10, 12, 30, 40, 60]	6	960	5760

TABLE 1. Data concerning the action of  $\mathcal{G}$  on  $\Gamma$

The examples in Table 1 are all such that  $M$  is minimal, and the cardinality of each orbit under the action of  $\mathcal{G}$  is the same. However, there

are examples of lists of moduli such that the cardinalities of the orbits are different. Although we cannot make it precise, there seems to be a connection between this difference in the cardinalities of the orbits and the following phenomenon.

**Definition 4.7.** Let  $M$  be a list of moduli such that  $\Gamma_M \neq \emptyset$  and, to avoid a trivial situation, that some  $C \in \Gamma_M$  is minimal. We say that  $M$  is *quasi-minimal* if there exist  $C_1, C_2 \in \Gamma_M$  such that  $C_1$  is minimal, but  $C_2$  is not.

We give an example to illustrate that quasi-minimal  $M$  do exist.

**Example 4.8.** *The list*

$$M = [3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120]$$

is quasi-minimal since the covering

$$C_1 = \{(0, 3), (0, 4), (0, 5), (1, 6), (6, 8), (3, 10), (5, 12), (11, 15), \\ (7, 20), (10, 24), (2, 30), (34, 40), (59, 60), (98, 120)\}$$

is minimal, but the covering

$$C_2 = \{(2, 3), (0, 4), (0, 5), (3, 6), (2, 8), (7, 10), (6, 12), (1, 15), \\ (19, 20), (22, 24), (13, 30), (0, 40), (49, 60), (0, 120)\}$$

is not minimal. Note that the elements  $(0, 40)$  and  $(0, 120)$  can be removed from  $C_2$  and the remaining set  $\widehat{C}_2$  is a covering; in fact, it is minimal.

**Remark 4.9.** The covering  $C_1$  in Example (4.8) is due to Erdős [8], while the covering  $\widehat{C}_2$  is due to Krukenberg [33].

To illustrate the possible connection between quasi-minimality and the difference in the cardinalities of the orbits, we give examples of two coverings using  $M$  from Example 4.8 where the cardinalities of the orbits under the action of  $\mathcal{G}$  are different. The covering

$$C_3 = \{(1, 3), (2, 4), (0, 5), (3, 6), (4, 8), (1, 10), (0, 12), (8, 15), \\ (7, 20), (8, 24), (29, 30), (11, 40), (17, 60), (13, 120)\}$$

is not minimal since removing the set of congruences  $\{(11, 40), (13, 120)\}$  from  $C_3$  gives a covering. Examining the orbit of  $C_3$  under  $\mathcal{G}$ , we see that  $|\text{orb}_{\mathcal{G}}(C_3)| = 3840$ . However, the covering

$$C_4 = \{(0, 3), (3, 4), (3, 5), (2, 6), (5, 8), (6, 10), (10, 12), (4, 15), \\ (0, 20), (17, 24), (22, 30), (25, 40), (37, 60), (1, 120)\}$$

is minimal and  $|\text{orb}_{\mathcal{G}}(C_4)| = 1920$ .

## 5. Final comments

Until now, no attempt had been made to impose an algebraic structure on the set of all coverings with a fixed list of moduli. While our results do not provide an answer in the most general situation, they do indicate that a rich and useful algebraic structure does indeed exist, and it is worthy of further pursuit.

### References

- [1] B. Banks, C. Finch, F. Luca, C. Pomerance and P. Stănică, *Sierpiński and Carmichael Numbers*, Trans. Amer. Math. Soc. (to appear)
- [2] Y.G. Chen, *On integers of the form  $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$* , Proc. Amer. Math. Soc. **128** (2000), 1613–1616.
- [3] Y.G. Chen, *On integers of the form  $k2^n + 1$* , Proc. Amer. Math. Soc. **129** (2001) 355–361.
- [4] Y.G. Chen, *On integers of the forms  $k - 2^n$  and  $k2^n + 1$* , J. Number Theory **89** (2001) 121–125.
- [5] Y.G. Chen, *On integers of the forms  $k^r - 2^n$  and  $k^r 2^n + 1$* , J. Number Theory **98** (2003) 310–319
- [6] Y.G. Chen, *On integers of the forms  $k \pm 2^n$  and  $k2^n \pm 1$* , J. Number Theory **125** (2007) 14–25.
- [7] F. Cohen and J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comput. **29** (1975), 79–81.
- [8] P. Erdős, *On integers of the form  $2^k + p$  and some related problems*, Summa Brasil. Math., (1950), 113–123.
- [9] M. Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, Number theory for the millennium, II (2002) 1–24.
- [10] M. Filaseta, C. Finch and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac’s conjecture*, J. Number Theory **128** (2008) 1916–1940.
- [11] M. Filaseta, K. Ford and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. **44** (2000) 633–643.
- [12] M. Filaseta, K. Ford, S. Konyagin, C. Pomerance and G. Yu, *Sieving by large integers and covering systems of congruences*, J. Amer. Math. Soc. **20** (2007), no. 2, 495–517.
- [13] M. Filaseta and J. Harrington, *A polynomial investigation inspired by work of Schinzel and Sierpiński*, Acta Arith. **155** (2012), no. 2, 149–161.
- [14] M. Filaseta, M. Kozek, C. Nicol and John Selfridge, *Composites that remain composite after changing a digit*, J. Comb. Number Theory **2** (2010), no. 1, 25–36.
- [15] C. Finch, J. Harrington and L. Jones, *Nonlinear Sierpiński and Riesel numbers*, J. Number Theory **133** (2013), no. 2, 534–544.
- [16] C. Finch and L. Jones, *Perfect Power Riesel Numbers* (submitted).

- 
- [17] P.-H. Fuss, *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIII Ème Siècle*, **I, II**, Johnson Reprint, New York, 1968.
- [18] J. Grantham, W. Jarnicki, J. Rickert and S. Wagon, *Repeatedly appending any digit to generate composite numbers*, Amer. Math. Monthly (to appear).
- [19] Song Guo and Zhi-Wei Sun, *On odd covering systems with distinct moduli*, Adv. in Appl. Math. **35** (2005), no. 2, 182–187.
- [20] B. Hough, *Solution of the minimum modulus problem for covering systems*, Ann. of Math. (2) **181** (2015), no. 1, 361–382.
- [21] A.S. Izotov, *A note on Sierpiński numbers*, Fibonacci Quart. **33** (1995) 206–207.
- [22] Scott Jenkin and Jamie Simpson, *Composite covering systems of minimum cardinality*, Integers **3** (2003), A13, 11 pp.
- [23] L. Jones, *Fibonacci variations of a conjecture of Polignac*, Integers **12** (2012), no. 4, 659–667.
- [24] L. Jones, *Polynomial variations on a theme of Sierpiński*, Int. J. Number Theory **5** (2009) 1–17.
- [25] L. Jones, *Using Lucas sequences to generalize a theorem of Sierpiński*, Acta Arith. **152** (2012), no. 3, 307–322.
- [26] L. Jones, *Variations on a theme of Sierpiński*, J. Integer Seq. **10** (2007) Article 07.4.4, 15 pp. (electronic).
- [27] L. Jones, *When does appending the same digit repeatedly on the right of a positive integer generate a sequence of composite integers?*, Amer. Math. Monthly, **118** (2011), 153–160.
- [28] L. Jones and A. Lamarche, *Generating  $d$ -composite sandwich numbers* (submitted).
- [29] L. Jones and M. Markovich, *Generating composite sequences by appending digits to special types of integers*, The Fibonacci Quarterly (to appear).
- [30] L. Jones and D. White, *Appending digits to generate an infinite sequence of composite numbers*, J. Integer Seq. **14** (2011), no. 5, Article 11.5.7, 12 pp.
- [31] L. Jones and D. White, *On primitive covering numbers*, <http://arxiv.org/abs/1406.6851>.
- [32] L. Jones and D. White, *Sierpinski numbers in imaginary quadratic fields*, Integers **12** (2012), no. 6, 1265–1278.
- [33] C. E. Krukenberg, *Covering sets of the integers*, Ph.D. thesis, University of Illinois, Urbana-Champaign, (1971).
- [34] P. Nielsen, *A covering system whose smallest modulus is 40*, J. Number Theory **129** (2009), no. 3, 640–666.
- [35] Hao Pan and Zhi-Wei Sun, *A sharp result on  $m$ -covers*, Proc. Amer. Math. Soc. **135** (2007), no. 11, 3515–3520 (electronic).
- [36] A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris Math., **29** (1849) 397–401, 738–739.
- [37] Š. Porubský, *Covering systems, Kubert identities and difference equations*, Math. Slovaca **50** (2000), no. 4, 381–413.

