#A38 INTEGERS 17 (2017)

ON THE PERIODICITY OF IRREDUCIBLE ELEMENTS IN ARITHMETICAL CONGRUENCE MONOIDS

Jacob Hartzer
Mathematics Department, Texas A&M University, College Station, Texas
jmhartzer@tamu.edu

Christopher O'Neill
Mathematics Department, UC Davis, Davis, California
coneill@math.ucdavis.edu

Received: 6/1/16, Revised: 3/5/17, Accepted: 8/15/17, Published: 9/14/17

Abstract

Arithmetical congruence monoids, which arise in non-unique factorization theory, are multiplicative monoids $M_{a,b}$ consisting of all positive integers n satsfying the modular equation $n \equiv a \bmod b$. In this paper, we examine the asymptotic behavior of the set of irreducible elements of $M_{a,b}$, and characterize in terms of a and b when this set forms an eventually periodic sequence.

1. Introduction

Fix positive integers a and b, and consider the set $M_{a,b}$ of positive integers n satisfying the equation $n \equiv a \bmod b$. If $M_{a,b}$ is closed under multiplication, it is known as an *arithmetical congruence monoid* (Definition 1). Since their introduction [3], much of the literature concerning arithmetical congruence monoids has centered around their factorization structure [2, 3, 5], that is, the different ways in which monoid elements can be expressed as products of irreducible elements. Unlike the set $\mathbb{Z}_{\geq 1}$ of all positive integers, which admits unique factorization into primes, factorization of elements of $M_{a,b}$ need not be unique; see Example 1.

The class of arithmetical congruence monoids encompasses a wide range of factorization structures. Some are Krull monoids, which have particularly well-behaved factorization structure [6], while others are ill-behaved enough to have non-accepted elasticity [4], a pathological factorization property found in few "naturally occuring" monoids. Additionally, the factorization structure of arithmetical congruence monoids is strongly connected to prime factorization in the integers, one of the classical motivations of broader factorization theory. For a thorough overview of the arithmetical congruence monoid literature, see Baginski and Chapman's survey [1].

In this paper, we examine the distribution of irreducible elements in arithmetical congruence monoids. Our main result (Theorem 1) gives a complete answer to Question 1, which appeared as [1, Open Question 4.6] in the aforementioned survey.

Question 1. Is the set of irreducible elements of $M_{a,b}$ eventually periodic?

Theorem 1. *The irreducible elements of $M_{a,b}$ form a periodic sequence if and only if $a > 1$ and $a \mid b$. In all other cases, this sequence is not eventually periodic.*

The proof of Theorem 1 is split between Sections 3 and 4, each of which include one direction of the proof (Theorems 3 and 4, respectively). Initial investigations into Question 1, as well as the formation of several proofs, made use of a new software package for working with arithmetical congruence monoids (Remark 2).

2. Arithmetical Congruence Monoids

Definition 1. An *arithmetical congruence monoid* is a multiplicative submonoid of $(\mathbb{Z}_{\geq 1}, \cdot)$ of the form

$$M_{a,b} = \{1\} \cup \{n \in \mathbb{Z}_{\geq 1} : n \equiv a \bmod b\}$$

for positive integers $a, b \in \mathbb{Z}_{\geq 1}$ satisfying $a^2 \equiv a \bmod b$. A non-unit $u \in M_{a,b}$ is *irreducible* if it cannot be written as a product of two non-unit elements of $M_{a,b}$. A *factorization* of a given element $n \in M_{a,b}$ is an expression of the form

$$n = u_1 \cdots u_r$$

for irredudible elements $u_1, \ldots, u_r \in M_{a,b}$.

Remark 1. The condition $a^2 \equiv a \bmod b$ in Definition 1 simply ensures that $M_{a,b}$ is closed under multiplication. We include the identity element $1 \in M_{a,b}$, as doing so simplifies many statements without affecting the factorization structure.

Example 1. Consider the arithmetical congruence monoid $M_{1,4}$, known as the *Hilbert monoid*. Any prime integer p satisfying $p \equiv 1 \bmod 4$ is irreducible in $M_{1,4}$, but these are not the only irreducible elements of $M_{1,4}$. For instance, $9, 21, 49 \in M_{1,4}$ are all irreducible, since each is the product of two prime integers that lie outside of $M_{1,4}$. As a result, some elements of $M_{1,4}$ have multiple distinct factorizations (in the sense of Definition 1). For example, $441 \in M_{1,4}$ has two distinct factorizations:

$$441 = 9 \cdot 49 = 21^2.$$

Non-unique factorizations occur in every arithmetical congruence monoid, with the exception of $M_{1,1}$ and $M_{1,2}$.

Remark 2. Proving results involving arithmetical congruence monoids often requires locating monoid elements with specific factorization properties (see, for instance, the proofs of [1, Theorems 4.8 and 4.9], or Proposition 1 in this paper). To aid in this process, the authors developed a Sage [7] package for computing factorizations in arithmetical congruence monoids. This package is now publicly available under the MIT license, and can be downloaded from the following webpage:

`http://www.math.ucdavis.edu/∼coneill/acms`

This package was used for initial investigations into Question 1, and to aid in locating sequences of elements necessary to prove Proposition 1. It was also used to generate the plots included in Figures 1 and 2. It is the authors' hope that others interested in studying the factorization properties of arithmetical congruence monoids will find this package useful as well.

We conclude this section by recalling the following elementary fact from number theory, which will be used in the proof of Theorem 4.

Theorem 2 (Dirichlet). *If a and b are relatively prime positive integers, then there are infinitely many primes p satisfying $p \equiv a \bmod b$.*

3. The Periodic Case

The main result of this section is Theorem 3, which proves the direction of Theorem 1 concerning arithmetical congruence monoids whose irreducible elements form an eventually periodic sequence. Most of the argument is contained in Lemma 1, which gives two modular conditions (one necessary and one sufficient) for reducibility in any arithmetical congruence monoid. Lemma 1 will also be used in the proof of Theorem 4, which proves the other direction of Theorem 1.

Example 2. Consider the arithmetical congruence monoid $M_{7,42}$, whose irreducible and reducible elements are depicted in Figure 1. As is readily visible from the plot, exactly one in every 7 elements is reducible, namely the following elements:

$$49, 343, 637, 931, 1225, \ldots$$

In particular, the reducible elements of $M_{7,42}$ form an arithmetic sequence with step size $7 \cdot 42 = 294$, which is the period guaranteed by Theorem 3. Moreover, every reducible element is congruent to $7^2 = 49$ modulo 294, as guaranteed by Lemma 1.

Lemma 1. *Fix an arithmetical congruence monoid $M_{a,b}$, and let $g = \gcd(a, b)$.*

(a) Any reducible element $n \in M_{a,b}$ satisfies $n \equiv a^2 \bmod bg$.

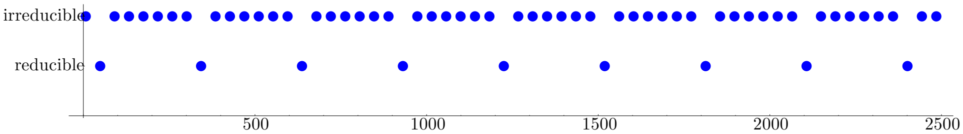

Figure 1: A plot depicting the irreducible elements of $M_{7,42}$ from Example 2.

(b) If $a > 1$, then any positive integer $n \equiv a^2 \bmod ab$ lies in $M_{a,b}$ and is reducible.

Proof. For $q_1, q_2 \in \mathbb{Z}_{\geq 0}$, multiplying the elements $a + q_1 b, a + q_2 b \in M_{a,b}$ yields

$$\begin{aligned}(a + bq_1)(a + bq_2) &= a^2 + ab(q_1 + q_2) + b^2 q_1 q_2 \\ &= a^2 + bg(\tfrac{a}{g}(q_1 + q_2) + \tfrac{b}{g} q_1 q_2)\end{aligned}$$

which is congruent to a^2 modulo bg. This proves part (a). Next, suppose $a > 1$ and fix $n = a^2 + abq$. Notice that $n \in M_{a,b}$ since $n \equiv a^2 \equiv a \bmod b$. Since $a \neq 1$,

$$n = a^2 + abq = a(a + bq)$$

expresses n as a product of nonunits, thus proving n is reducible. □

Theorem 3. *Fix an arithmetical congruence monoid $M_{a,b}$ satisfying $a > 1$ and $a \mid b$. An element $n \in M_{a,b}$ is reducible if and only if $n \equiv a^2 \bmod ab$.*

Proof. Both directions follow from Lemma 1 since $\gcd(a, b) = a$ in this case. □

Corollary 1. *For each $a \geq 2$, there exists an arithmetical congruene monoid $M_{a,b}$ with asymptotic density $1 - \frac{1}{a}$, that is,*

$$\lim_{n\to\infty} \frac{|\mathcal{A}(M_{a,b}) \cap [1, n]|}{|M_{a,b} \cap [1, n]|} = 1 - \frac{1}{a}.$$

Proof. Apply Theorem 3 to $M_{a,b}$ for $b = a(a - 1)$. □

4. The Aperiodic Case

In this section, we complete the proof of Theorem 1 by showing that the set of irreducible elements of any arithmetical congruence monoid not covered by Theorem 3 is not eventually periodic (Theorem 4). The main idea of the proof is given in Proposition 1, which produces arbitrarily long sequences of reducible elements in any such arithmetical congruence monoid.

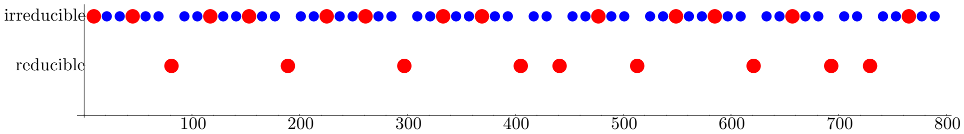

Figure 2: A plot depicting the irreducible elements of $M_{9,12}$ from Example 3.

Example 3. Depicted in Figure 2 are the irreducible elements of the arithmetical congruence monoid $M_{9,12}$. The large red dots indicate elements of the set

$$A = \{n \in M_{9,12} : n \equiv 9^2 \bmod 36\}$$

defined in Proposition 1. Notice that every element of $M_{9,12}$ that lies outside of A (represented by a small blue dot) is irreducible, as predicted by Lemma 1(b).

Proposition 1 provides the first step in the proof of Theorem 4 by locating arbitrarily long sequences of reducible elements in the set A. For $M_{9,12}$, the following sequence of $k = 4$ consecutive elements of A is identified.

$$\begin{array}{ll} 31995873 = 21 \cdot 1523613 & 31995909 = 33 \cdot 969573 \\ 31995945 = 45 \cdot 711021 & 31995981 = 57 \cdot 561333 \end{array}$$

The remainder of the proof of Theorem 4 demonstrates that, under certain conditions, the set A also contains infinitely many irreducible elements.

Proposition 1. *Fix an arithmetical congruence monoid $M_{a,b}$, and let $g = \gcd(a, b)$. The set*

$$A = \{n \in M_{a,b} : n \equiv a^2 \bmod bg\} \subset M_{a,b}$$

contains arbitrarily long sequences of consecutive elements that are reducible.

Proof. Fix $k \geq 2$, and consider the sequence $n_1, \ldots, n_k$ given by

$$n_j = bgj + ga + (a + b - g) \prod_{i=1}^{k} (bi + a)$$

for $j = 1, \ldots, k$. We first verify that $n_j \in A$ for each $j \leq k$. Since $a^2 \equiv a \bmod b$, we have $a^k = a + bq$ for some $q > 0$. This implies

$$\begin{array}{rcl} n_j & \equiv & ga + (a + b - g)a^k \bmod bg \\ & \equiv & a^{k+1} + g(a - a^k) \bmod bg \\ & \equiv & a(a + bq) \bmod bg \\ & \equiv & a^2 \bmod bg, \end{array}$$

meaning $n_j \in A$. Now, to prove that each n_j is reducible in $M_{a,b}$, we express n_j as

$$n_j = (bj + a)\left(g + (a + b - g)\prod_{i \neq j}(bi + a)\right).$$

Clearly the first factor lies in $M_{a,b}$. Moreover, b divides $a(a-1)$ and $a^2 \equiv a \bmod b$, so b also divides $g(a-1)$ since $\gcd(\frac{a}{g}, b) = 1$. This means the second factor satisfies

$$\begin{aligned} g + (a + b - g)\prod_{i \neq j}(bi + a) &\equiv g + (a - g)a \bmod b \\ &\equiv a^2 + g(1 - a) \bmod b \\ &\equiv a \bmod b \end{aligned}$$

and thus also lies in $M_{a,b}$. This completes the proof. □

Remark 3. Resume notation from the proof of Proposition 1 above. The given sequence of reducible elements can be easily generalized. In particular, for each $c \geq 0$, the elements given by

$$bgj + g(bc + a) + (a + b - g)\prod_{i=1}^{k}(bi + bc + a)$$

for $j = 1, \ldots, k$ also form a sequence of consecutive reducible elements in A. The proof of this fact is analogous to the proof of Proposition 1 given above, where the given sequence coincides with the special case $c = 0$.

Remark 4. Proposition 1 makes no assumptions on the arithmetical congruence monoid $M_{a,b}$. In particular, if $a > 1$ and $a \mid b$ as in Theorem 3, then every element of A is reducible by Lemma 1. In all other cases, however, one can find infinitely many irreducible elements in the set A. This is the content of Theorem 4 below.

Theorem 4. *Fix an arithmetical congruence monoid $M_{a,b}$, and let $g = \gcd(a, b)$. If either $a = 1$ or $g < a$, then the irredudible elements of $M_{a,b}$ do not form an eventually periodic sequence.*

Proof. Let A denote the set defined in Proposition 1. By Lemma 1(a), every element of $M_{a,b} \setminus A$ is irreducible, and by Proposition 1, the set A contains arbitrarily long sequences of reducible elements of $M_{a,b}$. To complete the proof, it suffices to show that A also contains infinitely many irreducible elements of $M_{a,b}$.

Fix a prime integer of the form $p = (\frac{a}{g})^2 + \frac{b}{g}q$ for $q \in \mathbb{Z}_{\geq 0}$. If $a = 1$, then $p = 1 + bq$ lies in A and is clearly irredudible in $M_{a,b}$. Otherwise, consider the monoid element

$$n = g^2 p = a^2 + bgq \in M_{a,b}.$$

The above expression implies $n \in A$, and since every element of $M_{a,b}$ is divisible by g, the only possible factorization of n in $M_{a,b}$ is $n = (g)(gp)$, the first factor of which lies outside of $M_{a,b}$ by assumption. As such, n is irreducible in $M_{a,b}$.

We now complete the proof by applying Theorem 2, which ensures there are infinitely many primes p satisfying $p \equiv (\frac{a}{g})^2 \bmod \frac{b}{g}$ since $\gcd((\frac{a}{g})^2, \frac{b}{g}) = 1$. □

Together, Theorems 3 and 4 provide a complete proof of Theorem 1.

Proof of Theorem 1. Apply Theorems 3 and 4. □

References

[1] P. Baginski and S. Chapman, Arithmetic congruence monoids: a survey, in *Combinatorial and additive number theory - CANT 2011 and 2012*, Springer Proc. Math. Stat., vol. 101, New York, 15-38.

[2] P. Baginski, S. Chapman, and G. Schaeffer, On the delta set of a singular arithmetical congruence monoid, *J. Théor. Normbres Bordeaux* 20 (2008), 45–59.

[3] M. Banister, J. Chaika, S. Chapman, and W. Meyerson, On the arithmetic of arithmetical congruence monoids, *Colloq. Math.* 108 (2007), 105–118.

[4] M. Banister, J. Chaika, S. Chapman, and W. Meyerson, A theorem of accepted elasticity in certain local arithmetical congruence monoids, *Abh. Math. Semin. Univ. Hambg.* 79 (1), 79–86 (2009).

[5] S. Chapman and D. Steinberg, On the elasticity of generalized arithmetical congruence monoids, *Results Math.* 58 **3** (2010), 221–231.

[6] A. Geroldinger, F. Halter-Koch, *Nonunique factorization: Algebraic, Combinatorial, and Analytic Theory*, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[7] SageMath, the Sage Mathematics Software System (Version 7.3), The Sage Developers, 2016, `http://www.sagemath.org`.