EQUIDISTRIBUTION OF NUMERICAL SEMIGROUP GAPS MODULO $m$

CALEB MCKINLEY SHOR

Abstract. For a positive integer $m$, a finite set of integers is said to be equidistributed modulo $m$ if the set contains an equal number of elements in each congruence class modulo $m$. In this paper, we consider the problem of determining when the set of gaps of a numerical semigroup $S$ is equidistributed modulo $m$. Of particular interest is the case when the nonzero elements of an Apéry set of $S$ form an arithmetic sequence. We explicitly describe such numerical semigroups $S$ and determine conditions for which the sets of gaps of these numerical semigroups are equidistributed modulo $m$.

1. Introduction

Let $\mathbb{N}_0$ denote the set of non-negative integers, a monoid under addition, and let $\mathbb{N}$ denote the set of positive integers. A numerical semigroup $S$ is an additive submonoid of $\mathbb{N}_0$ with finite complement. Elements of the complement are called gaps. Any numerical semigroup can be written as the set of all finite non-negative linear combinations of a finite set $G = \{g_1, \ldots, g_k\} \subset \mathbb{N}$ with $\gcd(G) = 1$. We denote this by $S = \langle G \rangle$ or $S = \langle g_1, \ldots, g_k \rangle$.

In [10], Wang & Wang studied alternate Sylvester sums for numerical semigroups of the form $S = \langle a, b \rangle$ with $\gcd(a, b) = 1$. Among their results are formulas for the numbers of even gaps and odd gaps of $S$. In particular, they found that there are as many even gaps as there are odd gaps precisely when $a$ and $b$ are both odd. Put another way, they determined when $S$ has an equal number of gaps in each congruence class modulo 2.

In this paper, we consider the following problem: for a general numerical semigroup $S$ and $m \in \mathbb{N}$, do $S$ have an equal number of gaps in each congruence class modulo $m$? When this occurs, we say that the set of gaps of $S$ is equidistributed modulo $m$.

Our primary result (Proposition 3.9) states that for any nonzero $a \in S$ with $\gcd(a, m) = 1$, the set of gaps of $S$ is equidistributed modulo $m$ if and only if

$$\text{Ap}(S; a) \setminus \{0\} = \{1, 2, \ldots, a - 1\} \pmod{m},$$

where $\text{Ap}(S; a)$ denotes the Apéry set of $S$ relative to $a$ (Definition 3.1). With this, since $\{1, 2, \ldots, a - 1\}$ is an arithmetic sequence, we then investigate the case where $\text{Ap}(S; a) \setminus \{0\}$ is also an arithmetic sequence; i.e., where

$$\text{Ap}(S; a) \setminus \{0\} = \{\beta + \delta, \beta + 2\delta, \ldots, \beta + (a - 1)\delta\}$$

for some $\beta \in \mathbb{Z}$ and $\delta \in \mathbb{N}$. We obtain Theorem 4.5, which gives precise conditions to determine whether the set of gaps of such a numerical semigroup $S$ is equidistributed modulo $m$. It comes down to computing $\gcd(a\delta, m)$ and considering the congruence classes of $a$, $\beta$, and $\delta$ modulo $m$.

There is one family of numerical semigroups $S$ for which the nonzero terms of an Apéry set of $S$ form an arithmetic sequence: numerical semigroups of the form

$$S = \langle a, ha + d, ha + 2d, \ldots, ha + (a - 1)d \rangle,$$

with $h \geq 0$, $a, d \geq 1$, and $\gcd(a, d) = 1$. This family consists of two well-known subfamilies which correspond to the cases where $h = 0$ and $h > 0$. When $h = 0$, we have $S = \langle a, d \rangle$ (more commonly written $S = \langle a, b \rangle$ with $\gcd(a, b) = 1$), a numerical semigroup generated by at most two elements. The study of these numerical semigroups dates back to Sylvester [8]. When $h \geq 1$, $S$ is generated by a generalized arithmetic sequence Apéry sets.
of length $a$. Numerical semigroups generated by generalized arithmetic sequences (which may contain fewer than $a$ terms) have been investigated more recently, by Lewin [3], Selmer [7], Ritter [8], and Matthews [4].

Finally, we give specific conditions for which the sets of gaps of numerical semigroups in this family are equidistributed modulo $m$. In general (Corollary 5.6), the set of gaps of $S$ is equidistributed modulo $m$ if and only if $\gcd(ad, m) = 1$ and at least one of four congruences holds. We highlight two special cases here. When $h = 0$ (Corollary 5.8), we have $S = \langle a, b \rangle$ and the set of gaps of $S$ is equidistributed modulo $m$ precisely when $\gcd(ab, m) = 1$ and at least one of $a$ and $b$ is congruent to 1 modulo $m$. When $h = 1$ (Corollary 5.10), then $S$ is an numerical semigroup generated by a (purely) arithmetic sequence of length $a$, and the set of gaps of $S$ is equidistributed modulo $m$ if and only if $\gcd(ad, m) = 1$ and at least one of the following holds: $a \equiv 1 \pmod{m}$; or $d \equiv -1 \pmod{m}$.

1.1. **Organization.** This paper is organized as follows. In Section 2 we present preliminary results about equidistributed multisets, multiset congruence modulo $m$, and connections to congruences of associated generating functions modulo $(x^m - 1)\mathbb{Z}[x]$. In Section 3 we briefly describe numerical semigroups. Since the set of gaps of a numerical semigroup is finite, we can apply results from Section 2 to find a criterion in terms of an Apéry set of $S$ to determine if the set of gaps of $S$ is equidistributed modulo $m$.

In Section 4 we consider the case where $S$ has an Apéry set for which the nonzero terms form an arithmetic sequence. We completely determine when the set of gaps of $S$ is equidistributed modulo $m$ in Theorem 4.5. In Section 5 we determine the numerical semigroups $S$ which have a nonzero $a \in S$ for which $\operatorname{Ap}(S; a) \setminus \{0\}$ is an arithmetic sequence. We find that $S$ is in the family of numerical semigroups as described above. We conclude the paper by applying Theorem 4.5 to this family to get explicit results for when the set of gaps of a numerical semigroup in this family is equidistributed modulo $m$.

2. **Preliminaries**

In this paper, we will often work with intervals of integers. For $a, b \in \mathbb{Z}$ with $a \leq b$ we will let $[a, b] := \{n \in \mathbb{Z}: a \leq n \leq b\}$.

And since we will need to allow for repetition of elements in Section 4, we work with multisets, denoting them with curly braces. Multisets have the same properties as sets with one exception: repetition is allowed. For example, $\{0, 0, 1\} \neq \{0, 1\}$. As a result, if $A$ and $B$ are finite multisets of cardinalities $\#(A)$ and $\#(B)$, then the cardinality of their union is $\#(A \cup B) = \#(A) + \#(B)$.

2.1. **Equidistributed multisets.** Throughout this section, let $A$ and $B$ be finite multiset of integers, and let $m \in \mathbb{N}$.

We begin by defining a function which counts the number of elements of a finite multiset in a particular congruence class.

**Definition 2.1.** For $r \in \mathbb{Z}$, let $A_{r,m} := \{a \in A: a \equiv r \pmod{m}\}$, the submultiset of $A$ of elements which are congruent to $r$ modulo $m$; and let $n_{r,m}(A) := \#(A_{r,m})$, the number of elements of $A$ that are congruent to $r$ modulo $m$.

Since there are $m$ disjoint congruence classes modulo $m$, we have that the multisets $A_{1,m}, A_{2,m}, \ldots, A_{m,m}$ form a partition of $A$. Additionally, if $A$ and $B$ are finite multisets, then $(A \cup B)_{r,m} = (A_{r,m}) \cup (B_{r,m})$, and thus $n_{r,m}(A \cup B) = n_{r,m}(A) + n_{r,m}(B)$. (Put another way, $n_{r,m}$ is a monoid homomorphism from the monoid of finite multisets under multiset union to the monoid of nonnegative integers under addition.)

Next, we define multiset congruence modulo $m$.

**Definition 2.2.** Given finite multisets $A, B \subset \mathbb{Z}$, we say $A$ and $B$ are congruent multisets modulo $m$, denoted $A \equiv B \pmod{m}$, if $n_{r,m}(A) = n_{r,m}(B)$ for all $r$ in an interval of $m$ consecutive integers.

We will typically take the interval of $m$ consecutive integers to be $[1, m]$ or $[0, m - 1]$.

We will now some useful properties of multiset congruence. We’ll first show that two congruent multisets must have the same cardinality.

**Proposition 2.3.** If $A \equiv B \pmod{m}$, then $\#(A) = \#(B)$. 
Proof. We assume \( A \equiv B \pmod{m} \), which means \( n_{r,m}(A) = n_{r,m}(B) \) for \( r = 1, 2, \ldots, m \). Since \( A \) is partitioned by \( A_{1,m}, A_{2,m}, \ldots, A_{m,m} \), and since \( B \) is partitioned by \( B_{1,m}, B_{2,m}, \ldots, B_{m,m} \), we have
\[
\#(A) = \sum_{r=1}^{m} n_{r,m}(A) = \sum_{r=1}^{m} n_{r,m}(B) = \#(B).
\]
\( \square \)

Just as with the usual (integer) congruence modulo \( m \), multiset congruence modulo \( m \) is an equivalence relation. The proof of the following is straightforward.

**Proposition 2.4.** For finite multisets \( A, B, C \in \mathbb{Z} \) and any \( m \in \mathbb{N} \),
- \( A \equiv A \pmod{m} \);
- if \( A \equiv B \pmod{m} \), then \( B \equiv A \pmod{m} \); and
- if \( A \equiv B \pmod{m} \) and \( B \equiv C \pmod{m} \), then \( A \equiv C \pmod{m} \).

Multiset congruence behaves well with respect to multiset unions.

**Proposition 2.5.** Let \( A, B, C, D \) be finite multisets and suppose that \( C \equiv D \pmod{m} \). Then \( A \equiv B \pmod{m} \) if and only if \( A \cup C \equiv B \cup D \pmod{m} \).

Proof. Observe that \( n_{r,m}(A \cup C) - n_{r,m}(A) = n_{r,m}(C) \) and \( n_{r,m}(B \cup D) - n_{r,m}(B) = n_{r,m}(D) \). Since \( C \equiv D \pmod{m} \), we have \( n_{r,m}(C) = n_{r,m}(D) \) for all \( r \in [1, m] \). Hence
\[
n_{r,m}(A \cup C) - n_{r,m}(A) = n_{r,m}(B \cup D) - n_{r,m}(B)
\]
for all \( r \in [1, m] \). Rearranging,
\[
n_{r,m}(A \cup C) - n_{r,m}(B \cup D) = n_{r,m}(A) - n_{r,m}(B)
\]
for all \( r \in [1, m] \). This implies that \( n_{r,m}(A) = n_{r,m}(B) \) for all \( r \in [1, m] \) if and only if \( n_{r,m}(A \cup C) = n_{r,m}(B \cup D) \) for all \( r \in [1, m] \). The result follows. \( \square \)

In particular, if we have two elements \( \alpha \) and \( \beta \) which are congruent to each other modulo \( m \), then we can add them to or remove them from a pair of congruent multisets to obtain a new pair of congruent multisets. More specifically, applying Proposition 2.5 with \( C = \{\alpha\} \) and \( D = \{\beta\} \), we obtain the following.

**Corollary 2.6.** Let \( \alpha, \beta \in \mathbb{Z} \) with \( \alpha \equiv \beta \pmod{m} \). For finite multisets \( A, B \), we have \( A \equiv B \pmod{m} \) if and only if \( A \cup \{\alpha\} \equiv B \cup \{\beta\} \pmod{m} \).

We now define an equidistributed multiset modulo \( m \).

**Definition 2.7.** We say the multiset \( A \) is **equidistributed modulo** \( m \) if \( n_{r_1,m}(A) = n_{r_2,m}(A) \) for all \( r_1, r_2 \in [1, m] \).

**Lemma 2.8.** If \( A \) is equidistributed modulo \( m \), then \( m \mid \#(A) \). When this occurs, \( \#(A) = m \cdot n_{r,m}(A) \) for all \( r \in [1, m] \).

Proof. Suppose \( A \) is equidistributed modulo \( m \). Then \( n_{r,m}(A) = n_{1,m}(A) \) for all \( r \in [1, m] \). Since each element of \( A \) is in exactly one of the \( m \) congruence classes modulo \( m \),
\[
\#(A) = n_{1,m}(A) + n_{2,m}(A) + \cdots + n_{m,m}(A) = m \cdot n_{1,m}(A).
\]
Therefore, \( m \mid \#(A) \). \( \square \)

**Remark 2.9.** As in Definition 2.1, we can replace the interval \( [1, m] \) in Definition 2.7 and in Lemma 2.8 with any interval of \( m \) consecutive integers.

Next, we see that if \( A \) is equidistributed modulo \( m \), then \( A \) is equidistributed modulo all divisors of \( m \).

**Proposition 2.10.** For \( d, m \in \mathbb{N} \), if \( A \) is equidistributed modulo \( m \) and \( d \mid m \), then \( A \) is equidistributed modulo \( d \).
Proof. Suppose \( m = dk \) for \( k \in \mathbb{N} \). For \( n \in \mathbb{Z} \), we have \( n \equiv r \pmod{d} \) if and only if \( n \equiv r + id \pmod{m} \) for some \( i \in [1, k] \). In other words, \( n \in \mathcal{A}_{r,d} \) if and only if \( n \in \mathcal{A}_{r+id,m} \) for some \( i \in [1, k] \). Since \( \mathcal{A}_{r_1,m} \cap \mathcal{A}_{r_2,m} = \emptyset \) for \( r_1, r_2 \in [1, m] \) with \( r_1 \neq r_2 \),

\[
n_{r,d}(A) = \sum_{i=1}^{k} n_{r+id,m}(A).
\]

Now, if \( A \) is equidistributed modulo \( m \), then \( n_{r,m}(A) = \#(A)/m \) for all \( r \in [1, m] \). Thus

\[
n_{r,d}(A) = k \cdot n_{r,m}(A) = k \cdot \#(A)/m = \#(A)/d
\]

for all \( r \in [1, d] \). We therefore conclude that \( A \) is equidistributed modulo \( d \). \( \square \)

Example 2.11. Consider the set \( A = \{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\} \), which has \( \#(A) = 12 \). (This is the set of positive integers which cannot be written as a non-negative linear combination of 5 and 7.) By Lemma 2.8, if \( A \) is equidistributed modulo \( m \), then \( m \) is a divisor of 12. We immediately see that \( A \) is not equidistributed modulo 12 because \( A \) contains no element which is 0 modulo 12. However, \( A \) is equidistributed modulo 6 and modulo 4. By Proposition 2.10, \( A \) is also equidistributed modulo any divisor of 6 or 4. Thus, \( A \) is equidistributed modulo \( m \) for \( m \in \{1, 2, 3, 4, 6\} \).

In Example 2.10 we will revisit this set.

2.2. Generating functions. We now consider generating functions arising from multisets. For a finite multiset \( A \subset \mathbb{N}_0 \), consider the (polynomial) generating function

\[
P_A(x) := \sum_{a \in A} x^a \in \mathbb{Z}[x].
\]

For example, if \( A = \{3, 3, 4\} \), then \( P_A(x) = 2x^3 + x^4 \).

We have thus far worked with multiset congruences in \( \mathbb{Z}/m\mathbb{Z} \). The analogue for generating functions is to work with polynomial congruences. For any \( h(x) \in \mathbb{Z}[x] \), let \( \langle h(x) \rangle := h(x)\mathbb{Z}[x] \), the principal ideal generated by \( h(x) \). (In the introduction, we used angle brackets to denote the set of all finite non-negative linear combinations of a set of integers. For the remainder of this paper, the context will be clear.) As usual, for \( f(x), g(x), h(x) \in \mathbb{Z}[x] \), we write

\[
f(x) \equiv g(x) \pmod{h(x)}
\]

to mean \( f(x) - g(x) \in \langle h(x) \rangle \).

Now, we fix \( m \in \mathbb{N} \). In the polynomial ring \( \mathbb{Z}[x] \), consider the ideal \( \langle x^m - 1 \rangle \). We have a ring homomorphism

\[
\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]/\langle x^m - 1 \rangle
\]

\[
f(x) \mapsto f(x) + \langle x^m - 1 \rangle.
\]

Since \( (x^m - 1) \) is a monic polynomial and \( \mathbb{Z} \) is an integral domain, we can apply the polynomial division algorithm to any \( f(x) \in \mathbb{Z}[x] \) and \( (x^m - 1) \) to find a unique pair of polynomials \( q_f(x), r_f(x) \in \mathbb{Z}[x] \) for which

\[
f(x) = q_f(x) \cdot (x^m - 1) + r_f(x) \quad \text{where } \deg(r_f(x)) < m \text{ or } r_f(x) \text{ is the zero polynomial}.
\]

In other words, \( f(x) + \langle x^m - 1 \rangle = r_f(x) + \langle x^m - 1 \rangle \). The uniqueness of the pair means we can represent elements of \( \mathbb{Z}[x]/\langle x^m - 1 \rangle \) with polynomials \( r(x) \) of degree less than \( m \) along with the zero polynomial:

\[
\mathbb{Z}[x]/\langle x^m - 1 \rangle = \{ r(x) + \langle x^m - 1 \rangle : r(x) \in \mathbb{Z}[x], \deg(r(x)) < m \} \cup \{ 0 + \langle x^m - 1 \rangle \}.
\]

In particular, since \( x^m = 1 + (x^m - 1) \), we have \( x^m \equiv 1 \pmod{(x^m - 1)} \).

For this particular ideal, it is straightforward to take a polynomial \( f(x) \) of any degree and compute \( r_f(x) \). Suppose

\[
f(x) = \sum_{k=0}^{\infty} c_k x^k
\]

for integers \( c_0, c_1, \ldots \), where all but finitely many are 0. We obtain the image of \( f(x) \) in \( \mathbb{Z}[x]/\langle x^m - 1 \rangle \) by repeatedly replacing any instance of \( x^m \) with 1. (Put another way, we reduce the exponents modulo \( m \).) The result is a polynomial of degree less than \( m \). From the previous paragraph, we know there is only one such polynomial, so this reduction must be \( r_f(x) \). The coefficient of \( x^k \) in \( r_f(x) \) is the sum of the coefficients
of \(x^k, x^{k+m}, x^{k+2m}, \ldots\) of \(f(x)\). This is the sum of coefficients for which the index is congruent to \(k\) modulo \(m\). We have

\[r_f(x) = \sum_{k=0}^{m-1} \left( \sum_{i=0}^{\infty} c_{k+im} \right) x^k.\]

(All but finitely many of the \(c_{k+im}\) terms are zero.)

Now, suppose \(A\) is a finite multiset of nonnegative integers. Then, if we write \(P_A(x) = \sum_{k=0}^{\infty} c_k x^k\), we see that for any \(k \in [0, m - 1]\),

\[\sum_{i=0}^{\infty} c_{k+im} = c_k + c_{k+m} + c_{k+2m} + \cdots = \#(A_{k,m}) = n_{k,m}(A).\]

We immediately obtain the following lemma.

**Lemma 2.12.** If \(A\) is a finite multiset of nonnegative integers, then

\[P_A(x) = \sum_{a \in A} x^a \equiv \sum_{r=0}^{m-1} n_{r,m}(A)x^r \pmod{(x^m - 1)}.\]

We now describe a connection between congruence of multisets modulo \(m\) and congruence of generating functions modulo \((x^m - 1)\).

**Proposition 2.13.** For finite multisets \(A\) and \(B\) of nonnegative integers, \(A \equiv B \pmod{m}\) if and only if \(P_A(x) \equiv P_B(x) \pmod{(x^m - 1)}\).

**Proof.** Suppose \(A \equiv B \pmod{m}\). We equivalently have \(n_{r,m}(A) = n_{r,m}(B)\) for all \(r\). Since the polynomials

\[\sum_{r=0}^{m-1} n_{r,m}(A)x^r \text{ and } \sum_{r=0}^{m-1} n_{r,m}(B)x^r\]

have degree less than \(m\), these polynomials are congruent modulo \((x^m - 1)\) precisely when their coefficients are equal, which means \(n_{r,m}(A) = n_{r,m}(B)\) for all \(r\). Finally, by Lemma 2.12 these polynomials are congruent, respectively, to \(P_A(x)\) and \(P_B(x)\) modulo \((x^m - 1)\). Thus, \(A \equiv B \pmod{m}\) if and only if \(P_A(x) \equiv P_B(x) \pmod{(x^m - 1)}\). \(\Box\)

By Lemma 2.13, a finite multiset \(A\) is equidistributed modulo \(m\) if and only if \(n_{r,m}(A) = \#(A)/m\) for all \(r\). Combined with Lemma 2.12 we obtain the following.

**Corollary 2.14.** \(A\) is equidistributed modulo \(m\) if and only if

\[P_A(x) \equiv \#(A) \sum_{r=0}^{m-1} x^r \pmod{(x^m - 1)}.\]

The summation in the above corollary will come up in a few contexts moving forward, so we give it a name. For any \(n \in \mathbb{N}\), let

\[C_n(x) := \frac{x^n - 1}{x - 1} = \sum_{r=0}^{n-1} x^r \in \mathbb{Z}[x].\]

**Proposition 2.15.** \(A\) is equidistributed modulo \(m\) if and only if

\[(x - 1)P_A(x) \equiv 0 \pmod{(x^m - 1)}.\]

**Proof.** For the forward direction, suppose \(A\) is equidistributed modulo \(m\). Since

\[(x - 1) \sum_{r=0}^{m-1} x^r = x^m - 1 \equiv 0 \pmod{(x^m - 1)},\]

we use Corollary 2.14 to conclude that

\[(x - 1)P_A(x) \equiv (x - 1) \frac{\#(A)}{m} \sum_{r=0}^{m-1} x^r \equiv 0 \pmod{(x^m - 1)},\]
as desired.

For the reverse direction, suppose

\[(x - 1) P_A(x) \equiv 0 \pmod{(x^m - 1)}\].

Thus, \[(x - 1) P_A(x) = (x^m - 1) h(x)\] for some \(h(x) \in \mathbb{Z}[x]\). Dividing through by \((x - 1)\), we find \(P_A(x) = C_m(x) h(x)\). We then apply the division algorithm to \(h(x)\) and \((x - 1)\) (which is valid in \(\mathbb{Z}[x]\) because \((x - 1)\) is monic) to find

\[h(x) = (x - 1) q(x) + h(1)\]

for some \(q(x) \in \mathbb{Z}[x]\). Thus

\[P_A(x) = C_m(x) h(1) + (x^m - 1) q(x),\]

so \(P_A(x) \equiv C_m(x) h(1) \pmod{(x^m - 1)}\). We therefore have \(n_{r,m}(A) = h(1)\) for all \(r \in [1, m]\). Thus, \(A\) is equidistributed modulo \(m\). \(\square\)

3. Numerical semigroups and sets of gaps

Numerical semigroups were briefly described in the introduction. We provide more details here. For a thorough treatment, see [6].

A numerical semigroup is a submonoid of \(\mathbb{N}_0\) under addition with finite complement. In other words, a numerical semigroup is a set \(S \subseteq \mathbb{N}_0\) that is closed under addition, contains 0, and has finite complement in \(\mathbb{N}_0\). Let \(H(S) = \mathbb{N}_0 \setminus S\), the set of gaps of \(S\). The genus of \(S\) is \(g(S) = \#(H(S))\), the number of gaps of \(S\). Since \(H(S)\) is a finite set,

\[P_{H(S)}(x) = \sum_{n \in H(S)} x^n \in \mathbb{Z}[x].\]

We call \(P_{H(S)}(x)\) the gap polynomial of \(S\).

For any set \(G \subseteq \mathbb{N}_0\), let \(\langle G \rangle\) denote the set of all finite \(\mathbb{N}_0\)-linear combinations of elements of \(G\). If \(G = \{g_1, \ldots, g_k\}\), then we let \(\langle g_1, \ldots, g_k \rangle = \langle G \rangle\). It is a standard result that \(\langle G \rangle\) is a numerical semigroup if and only if \(\gcd(G) = 1\). For any numerical semigroup \(S\), there is a finite set \(G \subseteq \mathbb{N}\) such that \(S = \langle G \rangle\). Further, there is a unique minimal (relative to set inclusion) generating set \(G\). The embedding dimension of \(S\), denoted \(e(S)\), is the cardinality of the minimal generating set \(G\) (which is necessarily finite). The least nonzero element of \(S\), which is also the least element of its minimal generating set \(G\), is the multiplicity of \(S\), denoted \(m(S)\).

An Apéry set of a numerical semigroup is an incredibly useful object. We have the following definition.

Definition 3.1 ([1]). For \(S\) a numerical semigroup and any nonzero \(a \in S\), the Apéry set of \(S\) relative to \(a\) is

\[\text{Ap}(S; a) = \{s \in S : s - a \notin S\}.\]

Put another way, \(\text{Ap}(S; a)\) consists of the least element of \(S\) in each congruence class modulo \(a\). Hence, \(#(\text{Ap}(S; a)\) = \(a\).

3.1. Detecting an equidistributed set of gaps via an Apéry set. In the introduction of this paper, we mentioned the work of Wang & Wang [10] from which, for a numerical semigroup of the form \(S = \langle a, b \rangle\) with \(\gcd(a, b) = 1\), one can determine whether or not \(H(S)\) is equidistributed modulo 2. Their work was based on the following result of Tuenter.

Theorem 3.2 ([3], Theorem 2.1)). For \(S = \langle a, b \rangle\) and any function \(f\) defined on \(\mathbb{N}_0\),

\[\sum_{n \in H(S)} |f(n + a) - f(n)| = \sum_{n=1}^{a-1} [f(nb) - f(n)].\]

Still with \(S = \langle a, b \rangle\), Wang & Wang used Theorem 3.2 and the function \(f(n) = (-1)^n\) to derive an expression ([10], Theorem 4.1) for the alternate Sylvester sum

\[T_m(S) = \sum_{n \in H(S)} (-1)^n n^m\]
for $m \in \mathbb{N}_0$. In particular, when $m = 0$, they found

$$\sum_{n \in H(S)} (-1)^n = \begin{cases} 0 & \text{for } a, b \text{ odd, } \\ -b - 1 \over 2 & \text{a even, } b \text{ odd.} \end{cases}$$

(Note that $a$ and $b$ are interchangeable. Since they cannot both be even, we may assume that $b$ is odd.) Thus, the numerical semigroup $S = (a,b)$ has as many even gaps as odd gaps precisely when $a$ and $b$ are odd. Otherwise, there are more odd gaps than even gaps.

Our goal here is to determine when the set of gaps of a numerical semigroup is equidistributed modulo $m$. We take a similar approach, beginning with a generalization of Tuenter’s result.

**Theorem 3.3 (Theorem 2.3).** For $S$ a numerical semigroup, any nonzero $a \in S$, and any function $f$ defined on $\mathbb{N}_0$,

$$\sum_{n \in H(S)} [f(n + a) - f(n)] = \sum_{n \in Ap(S; a)} f(n) - \sum_{n = 0}^{a-1} f(n).$$

Since $-1$ is a 2nd root of unity, the function $f(n) = (-1)^n$ is useful for understanding the congruence classes of the gaps modulo 2. In order to understand the congruence classes of the gaps of a numerical semigroup modulo $m$, we should therefore consider $m$th roots of unity. For $\zeta_m$ a primitive $m$th root of unity, we can use $f(n) = \zeta_m^n$. However, since we do not need any particular properties of the cyclotomic ring $\mathbb{Z}[\zeta_m]$, we will stick with polynomials, using $f(n) = x^n$ and working modulo $(x^m - 1)$.

In Proposition 2.15 we found that a finite multiset $A$ is equidistributed modulo $m$ if and only if

$$(x - 1) P_A(x) \equiv 0 \pmod{(x^m - 1)}.$$  

Since $(x - 1) \mid (x^a - 1)$ in $\mathbb{Z}[x]$, we can combine that result with Corollary 3.4 to say something about when the set of gaps of $S$ is equidistributed modulo $m$.

**Corollary 3.4.** For $S$ a numerical semigroup and any nonzero $a \in S$,

$$(x^a - 1) P_{H(S)}(x) = \sum_{n \in Ap(S; a)} x^n - \sum_{n = 0}^{a-1} x^n.$$  

In Proposition 2.15 we found that a finite multiset $A$ is equidistributed modulo $m$ if and only if

$$(x - 1) P_A(x) \equiv 0 \pmod{(x^m - 1)}.$$  

Since $(x - 1) \mid (x^a - 1)$ in $\mathbb{Z}[x]$, we can combine that result with Corollary 3.4 to say something about when the set of gaps of $S$ is equidistributed modulo $m$.

**Corollary 3.5.** For $S$ a numerical semigroup with some nonzero $a \in S$, if $H(S)$ is equidistributed modulo $m$, then

$$\sum_{n \in Ap(S; a)} x^n \equiv \sum_{n = 0}^{a-1} x^n \pmod{(x^m - 1)},$$

which we may equivalently write as $Ap(S; a) \equiv [0, a - 1] \pmod{m}$.

**Proof.** Suppose $H(S)$ is equidistributed modulo $m$. By Proposition 2.15

$$(x - 1) P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}.$$  

Thus,

$$(x^a - 1) P_{H(S)}(x) = C_a(x)(x - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}.$$  

By Corollary 3.4 we conclude that

$$\sum_{n \in Ap(S; a)} x^n \equiv \sum_{n = 0}^{a-1} x^n \pmod{(x^m - 1)},$$

as desired.

By Proposition 2.15 this conclusion is equivalent to the statement that $Ap(S; a) \equiv [0, a - 1] \pmod{m}$. □

We illustrate this result with an example.
Example 3.6. Let \( S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, 9, 10, \ldots \} \), a numerical semigroup with \( H(S) = \{1, 2, 4, 7\} \). Observe that \( n_{r,4}(H(S)) = 1 \) for each \( r \in \{0, 3\} \), which means \( H(S) \) is equidistributed modulo 4. By Corollary 3.5 Ap(\( S; a \)) \( \equiv [0, a - 1] \pmod 4 \) for all \( a \in S \).

We verify this for a few elements of \( S \):
- \( \text{Ap}(S; 3) = \{0, 5, 10\}; \)
- \( \text{Ap}(S, 5) = \{0, 3, 6, 9, 12\}; \) and
- \( \text{Ap}(S; 14) = \{0, 3, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 18, 21\} \).

If we look at each of these multisets modulo 4, we find
- \( \text{Ap}(S; 3) \equiv \{0, 1, 2\} \equiv [0, 2] \pmod 4 \),
- \( \text{Ap}(S; 5) \equiv \{0, 3, 2, 1, 0\} \equiv [0, 4] \pmod 4 \), and
- \( \text{Ap}(S; 14) \equiv \{0, 3, 1, 2, 0, 1, 2, 3, 0, 1, 3, 2, 1, 1\} \equiv [0, 13] \pmod 4 \).

Next, we have a non-example.

Example 3.7. Let \( S \) be a numerical semigroup of genus \( g(S) = g \geq 0 \) with \( g \in S \). Then \( \text{Ap}(S; g) \) is a set of \( g \) elements, each in its own congruence class modulo \( g \). Hence, \( \text{Ap}(S; g) \equiv [0, g - 1] \pmod g \). By Lemma 2.8 if \( H(S) \) is equidistributed modulo \( g \), then
\[
\frac{n_{0,g}(H(S))}{g} = \frac{\#(H(S))}{g} = 1.
\]

However, since \( 0 \cdot g, 1 \cdot g, 2 \cdot g, \ldots \) are all in \( S \), \( n_{0,g}(H(S)) = 0 \). Thus, \( H(S) \) is not equidistributed modulo \( g \).

For a concrete non-example, let \( S = \langle 4, 5, 11 \rangle \). The set of gaps of \( S \) is \( H(S) = \{1, 2, 3, 6, 7\} \) and \( g(S) = 5 \in S \). Observe that \( \text{Ap}(S; 5) = \{0, 4, 8, 11, 12\} \), which has \( \text{Ap}(S; 5) \equiv [0, 4] \pmod 5 \), yet \( H(S) \) is not equidistributed modulo 5.

Thus, the converse of Corollary 3.5 is false. However, if we further include the assumption that \( \gcd(a, m) = 1 \), then the converse holds. We will prove it after stating the following lemma, which is well-known.

Lemma 3.8. Let \( a, b \in \mathbb{N} \). Then \( \gcd(x^a - 1, x^b - 1) = x^\gcd(a,b) - 1 \).

Proposition 3.9. For \( S \) a numerical semigroup, any nonzero \( a \in S \), and any \( m \in \mathbb{N} \) with \( \gcd(a, m) = 1 \), the following statements are equivalent.

1. \( H(S) \) is equidistributed modulo \( m \).
2. \( \Phi_{H(S)}(x) \in \langle C_m(x) \rangle \).

3. \( \sum_{n \in \text{Ap}(S; a)} x^n \equiv \sum_{n=0}^{a-1} x^n \pmod (x^m - 1) \).

4. \( \sum_{n \in \text{Ap}(S; a) \setminus \{0\}} x^n \equiv \sum_{n=1}^{a-1} x^n \pmod (x^m - 1) \).

5. \( \text{Ap}(S; a) \equiv [0, a - 1] \pmod m \).

6. \( \text{Ap}(S; a) \setminus \{0\} \equiv [1, a - 1] \pmod m \).

Proof. By Proposition 2.13 (1) \( \iff \) (2). Since \( 0 \in \text{Ap}(S; a) \), (3) \( \iff \) (4) and (5) \( \iff \) (6). By Proposition 2.13 (3) \( \iff \) (5). It is therefore enough to show (3) \( \iff \) (1).

Since \( \gcd(a, m) = 1 \), by Lemma 3.8 \( \gcd(x^a - 1, x^m - 1) = x^1 - 1 \). Therefore, \( C_a(x) \) is a unit modulo \( (x^m - 1) \).

Now, suppose
\[
\sum_{n \in \text{Ap}(S; a)} x^n \equiv \sum_{n=0}^{a-1} x^n \pmod (x^m - 1) \).
\]

By Corollary 3.3 \( (x^a - 1) \Phi_{H(S)}(x) \equiv 0 \pmod (x^m - 1) \). Therefore
\[
C_a(x)(x - 1) \Phi_{H(S)}(x) \equiv 0 \pmod (x^m - 1) \).
\]

Since \( C_a(x) \) is a unit modulo \( (x^m - 1) \), we conclude that \( (x - 1) \Phi_{H(S)}(x) \equiv 0 \pmod (x^m - 1) \). By Proposition 2.13 we conclude that \( H(S) \) is equidistributed modulo \( m \). □

This leads to the following interesting result.
Corollary 3.10. For any nonzero $a, b \in S$ with $\gcd(ab, m) = 1$, $Ap(S; a) \equiv [0, a - 1] \pmod{m}$ if and only if $Ap(S; b) \equiv [0, b - 1] \pmod{m}$.

Before moving on, we make one more remark regarding $m$th roots of unity. By Proposition 2.15, $H(S)$ is equidistributed modulo $m$ if and only if $(x - 1)^k P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}$, which is to say $C_m(x)$ divides the gap polynomial $P_{H(S)}(x)$. For $\zeta_m$ a primitive $m$th root of unity,

$$C_m(x) = \prod_{i=1}^{m-1} (x - \zeta_m^i).$$

Thus, $H(S)$ is equidistributed modulo $m$ if and only if $P_{H(S)} \left( \zeta_m^i \right) = 0$ for all $i = 1, 2, \ldots, m - 1$.

3.2. Numerical semigroups with maximal embedding dimension. We turn our attention to numerical semigroups of maximal embedding dimension.

Let $S$ be a numerical semigroup. Then $S$ is generated by a minimal set $A$ of cardinality $e(S)$. By Proposition 2.10, $e(S) \leq m(S)$. If $e(S) = m(S)$, then $S$ has maximal embedding dimension. Let $b \in A$ and $s \in S \setminus \{0, b\}$. By the minimality of $A$, $b - s \notin A$ and therefore $b \in Ap(S; s)$. In particular, if $a \in A$, then $(A \setminus \{a\}) \subset Ap(S; a)$. For $S$ with maximal embedding dimension, we can describe $Ap(S; a)$ in the case where $a = m(S)$.

Proposition 3.11 ([4, Proposition 3.1]). For $S$ generated by the minimal set $A$, let $a = m(S)$. Then $S$ has maximal embedding dimension if and only if

$$Ap(S; a) \setminus \{0\} = A \setminus \{a\}.$$

We combine Proposition 3.11 with Proposition 3.9 for a simple criterion to determine when the gaps of a numerical semigroup of maximal embedding dimension are equidistributed modulo $m$.

Corollary 3.12. Suppose $S$ is a numerical semigroup of maximal embedding dimension with minimal generating set $A$. For $a = m(S) = e(S)$ and $m \in \mathbb{N}$ with $\gcd(a, m) = 1$, $H(S)$ is equidistributed modulo $m$ if and only if

$$A \setminus \{a\} \equiv [1, a - 1] \pmod{m}.$$

3.3. Numerical semigroups with small multiplicity. We conclude this section by completely determining when the set of gaps of a numerical semigroup of multiplicity 2 or 3 is equidistributed modulo $m$.

To begin, suppose $m(S) = 2$. Then $g(S) > 0$, $1 \notin S$, and $2 \in S$. Therefore, $e(S) = 2$, which means $S$ is a semigroup of maximal embedding dimension. In particular, $S = \langle 2, b \rangle$ for odd $b \geq 3$. We can then determine when $H(S)$ is equidistributed modulo $m$.

Proposition 3.13. Suppose $m(S) = 2$. Then $S = \langle 2, b \rangle$ for some odd integer $b \geq 3$, and $H(S)$ is equidistributed modulo $m$ if and only if $m$ is an odd divisor of $g(S) = (b - 1)/2$.

Proof. Suppose $m(S) = 2$. Then $e(S) = 2$. We have $S = \langle 2, b \rangle$ for some $b > 1$ with $\gcd(b, 2) = 1$. In other words, $b$ is an odd integer with $b \geq 3$. The set of gaps of $S$ is $H(S) = \{1, 3, 5, \ldots, b - 2\}$, a set of cardinality $(b - 1)/2$. (Thus, $g(S) = (b - 1)/2$.)

Now, we wish to determine when $H(S)$ is equidistributed modulo $m$. Since $\#(H(S)) = (b - 1)/2$, it is a necessary condition (by Lemma 3.8) that $m \mid (b - 1)/2$. We consider the cases of $m$ even and $m$ odd separately.

First, consider $H(S)$ modulo 2. Since $H(S)$ contains zero even elements,

$$n_{0,2}(H(S)) = 0 \neq (b - 1)/2 = n_{1,2}(H(S)).$$

Therefore, $H(S)$ is not equidistributed modulo 2. By the contrapositive of Proposition 2.10, $H(S)$ is not equidistributed modulo $m$ for even.

Next, factor out all powers of 2 from $(b - 1)/2$ to write $(b - 1)/2 = 2^kl$ for $k \in \mathbb{N}$ and $l$ odd. Then $b = 1 + 2^{k+1}l$ and $\gcd(2, l) = 1$. By Corollary 3.12 since $A \setminus \{2\} \equiv \{b\} \equiv \{1\} \pmod{l}$, $H(S)$ is equidistributed modulo $l$. If $m$ is any odd divisor of $(b - 1)/2$, then $m$ is a divisor of $l$. Therefore, by Proposition 2.10, $H(S)$ is equidistributed modulo $m$.

We conclude that $H(S)$ is equidistributed modulo $m$ if and only if $m$ is an odd divisor of $\#(H(S)) = (b - 1)/2$, as desired.
Remark 3.14. We note that the previous proposition is a special case of a more general result concerning
the equidistribution of sets of gaps of numerical semigroups of embedding dimension 2. (See Corollary 5.8)

Next, we consider the case where \( m(S) = 3 \).

Proposition 3.15. Suppose \( m(S) = 3 \). Then \( e(S) = 2 \) or \( 3 \).

If \( e(S) = 2 \), then \( S = \langle 3, b \rangle \) for some \( b \geq 3 \) with \( \gcd(3, b) = 1 \), and \( H(S) \) is equidistributed modulo \( m \) if
and only if \( \gcd(3, m) = 1 \) and \( m \) is a divisor of \( b - 1 \).

If \( e(S) = 3 \), then \( S = \langle 3, b, c \rangle \) for some \( b, c \) and \( \gcd(3, bc) = 1 \) and \( 3 < b < c < 2b \), and \( H(S) \) is
equidistributed modulo \( m \) if and only if \( \gcd(3, m) = 1 \) and \( m \) is a divisor of either \( \gcd(b - 1, c - 2) \) or
\( \gcd(b - 2, c - 1) \).

Proof. Suppose \( H(S) \) is equidistributed modulo \( m \). Since \( 1 \notin S \), \( e(S) > 1 \), and since \( e(S) \leq m(S) = 3 \), we
conclude that \( e(S) = 2 \) or \( 3 \). Since \( 3 \in S \), \( H(S) \) contains no multiples of \( 3 \). Thus \( H(S) \) is not equidistributed
modulo \( m \) for \( m \) a multiple of \( 3 \). We therefore have \( \gcd(3, m) = 1 \).

If \( e(S) = 2 \), then \( S = \langle 3, b \rangle \) for \( b > 3 \) and \( \gcd(b, 3) = 1 \). Note that \( A_p(3, \delta) \) and \( \beta \)
seems reasonable to assume that we can get explicit results when \( A_p(\delta) \) and \( \beta \)
Lemma 4.1. \{ \}

Remark 3.16. Note that if \( m(S) = e(S) = 3 \), then \( S = \langle 3, b, c \rangle \) for \( 3 < b < c < 2b \), \( \gcd(3, bc) = 1 \), and
\( b \neq c \) (mod \( 3 \)). Since there
are only two nonzero congruence classes modulo \( 3 \), \( 2b \equiv c \) (mod \( 3 \)), and thus we must have \( c < 2b \). As this is
a maximal embedding numerical semigroup, by Corollary 3.12 \( H(S) \) is equidistributed modulo \( m \) if and
only if \( \{ b, c \} \equiv \{ 1, 2 \} \) (mod \( 3 \)). We must have one of the following: \( b \equiv 1 \) (mod \( m \)) and \( c \equiv 2 \) (mod \( m \));
or \( b \equiv 2 \) (mod \( m \)) and \( c \equiv 1 \) (mod \( m \)). For the first case, we equivalently have that \( m \) divides \( b - 1 \) and \( c - 2 \),
which occurs precisely when \( m \) divides \( \gcd(b - 1, c - 2) \). The second case gives the other condition. \( \square \)

4. Apéry sets where the nonzero terms form an arithmetic sequence

By Proposition 3.9, for \( S \) a numerical semigroup with some nonzero \( a \in S \), \( H(S) \) is equidistributed
modulo \( m \) if and only if \( \gcd(3, bc) = 1 \) and \( b \neq c \) (mod \( m \)). Then \( 2b - c = 3h \) for some \( h \in \mathbb{N} \). Let \( d = c - b \in \mathbb{N} \). Then \( S = \langle 3, 3h + d, 3h + 2d \rangle \). In other
cwords, \( S \) is a numerical semigrou of maximal embedding dimension generated by a generalized arithmetic
sequence with \( m(S) = 3 \). In Section 5 we will find explicit results for such semigroups of any multiplicity.
(See Corollary 5.6)

(1) Apéry sets where the nonzero terms form an arithmetic sequence

By Proposition 3.9, for \( S \) a numerical semigroup with some nonzero \( a \in S \), \( H(S) \) is equidistributed
modulo \( m \) if and only if \( \gcd(3, bc) = 1 \) and \( b \neq c \) (mod \( m \)). Then \( 2b - c = 3h \) for some \( h \in \mathbb{N} \). Let \( d = c - b \in \mathbb{N} \). Then \( S = \langle 3, 3h + d, 3h + 2d \rangle \). In other
cwords, \( S \) is a numerical semigrou of maximal embedding dimension generated by a generalized arithmetic
sequence with \( m(S) = 3 \). In Section 5 we will find explicit results for such semigroups of any multiplicity.
(See Corollary 5.6)
for which $\beta + i\delta \equiv 1 \pmod{a}$ and $\beta + j\delta \equiv 2 \pmod{a}$. Taking the difference, we have $(j - i)\delta \equiv 1 \pmod{a}$, and thus $\gcd(a, \delta) = 1$.

Next, since $\gcd(a, \delta) = 1$, $\delta$ is a generator of $\mathbb{Z}/a\mathbb{Z}$. In particular, $\{i\delta : 1 \leq i \leq a - 1\} \equiv [1, a - 1] \pmod{a}$.

Therefore

$$[\beta + 1, \beta + a - 1] \equiv \{\beta + i\delta : 1 \leq i \leq a - 1\} \equiv \text{Ap}(S; a) \setminus \{0\} \equiv [1, a - 1] \pmod{a},$$

implying $\beta \equiv 0 \pmod{a}$ and hence $a \mid \beta$.

Finally, since $\beta + \delta \in S$, $2(\beta + \delta) \in S$ as well. Also, $\beta + 2\delta \in \text{Ap}(S; a) \subset S$. We have $a \mid \beta$ and, thus $\beta + 2\delta \equiv 2(\beta + \delta) \equiv 2\delta \pmod{a}$. Since $\beta + 2\delta \in \text{Ap}(S; a)$, $\beta + 2\delta$ is the smallest element of $S$ in its congruence class modulo $a$. Thus, $\beta + 2\delta \leq 2(\beta + \delta)$, from which we conclude $0 \leq \beta$. $\square$

Now, if $\text{Ap}(S; a) \setminus \{0\}$ is an arithmetic sequence, then by Corollary 3.4 we have

$$\text{(2)} \quad (x^a - 1)P_{H(S)}(x) = x^\beta \sum_{j=1}^{a-1} x^{\beta j} - \sum_{j=1}^{a-1} x^j.$$ 

Each summation is a finite geometric series, so we may equivalently write

$$\text{(3)} \quad (x^a - 1)P_{H(S)}(x) = x^\beta \frac{x^{\beta a} - x^\beta}{x^\beta - 1} - \frac{x^a - x^1}{x - 1},$$

which is equivalent to the polynomial equation

$$\text{(4)} \quad (x - 1)(x^a - 1)(x^\delta - 1)P_{H(S)}(x) = x^\beta (x - 1)(x^{\beta a} - x^\beta) - (x^a - x)(x^\delta - 1).$$

We will use these equations to show that if $H(S)$ is equidistributed modulo $m$, then $\gcd(\delta, m) = 1$ and $\gcd(a, m) = 1$.

**Proposition 4.2.** Suppose $H(S)$ is equidistributed modulo $m$. Then $\gcd(\delta, m) = 1$.

**Proof.** If $a = 1$, then $\delta = 1$ and hence $\gcd(\delta, m) = 1$.

For the rest of this proof, we assume $a \geq 2$. By Proposition 2.15 if $H(S)$ is equidistributed modulo $m$, then $(x - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}$. Thus, by Eq. (2),

$$x^\beta (x^\delta + x^{2\delta} + \cdots + x^{(a-1)\delta}) \equiv x^1 + x^2 + \cdots + x^{a-1} \pmod{(x^m - 1)}.$$ 

Equivalently,

$$\{\beta + \delta, \beta + 2\delta, \ldots, \beta + (a - 1)\delta\} \equiv \{1, 2, 3, \ldots, a - 1\} \pmod{m}.$$ 

If $a = 2$, then $\beta + \delta \equiv 1 \pmod{m}$. Since $\beta = 0$, this implies $\gcd(\delta, m) = 1$.

If $a \geq 3$, we must have some $i, j \in [1, a - 1]$ such that $\beta + i\delta \equiv 1 \pmod{m}$ and $\beta + j\delta \equiv 2 \pmod{m}$. In particular, $(j - i)\delta \equiv 1 \pmod{m}$, from which we conclude that $\gcd(\delta, m) = 1$. $\square$

**Proposition 4.3.** Suppose $H(S)$ is equidistributed modulo $m$. Then $\gcd(a, m) = 1$.

**Proof.** Suppose $H(S)$ is equidistributed modulo $m$. By Lemma 4.1 $a \mid \beta$. Thus, $\beta = al$ for some $l \in \mathbb{Z}$. By the division algorithm in $\mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ for which $l = qm + r$ with $1 < r \leq m + 1$. (It will be helpful to have $r \geq 2$.) It follows that $\beta \equiv ar \pmod{m}$.

By Proposition 4.2 $\gcd(\delta, m) = 1$. Thus, $(x - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}$ if and only if

$$(x - 1)(x^\delta - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}.$$ 

Since $H(S)$ is equidistributed modulo $m$, by Eq. (3),

$$\frac{x^\beta (x - 1)(x^{\beta a} - x^\beta) - (x^a - x)(x^\delta - 1)}{x^a - 1} \equiv 0 \pmod{(x^m - 1)}.$$ 

Since $\beta \equiv ar \pmod{m}$, we expand and regroup to find

$$\frac{x(x^{r+\delta}a - 1)}{x^a - 1} + \frac{x^a + \delta(x^{r-1}a - 1)}{x^a - 1} \equiv \frac{x^a(x^{r+\delta-1}a - 1)}{x^a - 1} + \frac{x^a + 1(x^ra - 1)}{x^a - 1} \pmod{(x^m - 1)}.$$ 

Each quotient is a finite geometric series. (Note that $r + \delta, r - 1, r + \delta - 1, r$ are all positive integers. This is why we wanted $r \geq 2$ earlier.) The left side expands out as

$$L(x) = x \left(1 + x^a + x^{2a} + \cdots + x^{(r-1)a}\right) + x^{a+\delta} \left(1 + x^a + x^{2a} + \cdots + x^{(r-2)a}\right)$$

and the right side expands out as

$$R(x) = x^a \left( 1 + x^2a + \cdots + x^{(r+\delta-2)a} \right) + x^{\delta+1} \left( 1 + x^2a + \cdots + x^{(r-1)a} \right).$$

Now, since $L(x) \equiv R(x) \pmod{(x^m - 1)}$, for the corresponding multisets

$$M_L = \{ 1 + ia : 0 \leq i \leq r + \delta - 1 \} \cup \{ \delta + ja : 1 \leq j \leq r - 1 \}$$

and

$$M_R = \{ ia : 0 \leq i \leq r + \delta - 1 \} \cup \{ \delta + ja : 0 \leq j \leq r - 1 \},$$

we have $M_L \equiv M_R \pmod{m}$. In particular, since $1 \in M_L$, some element of $M_R$ is congruent to 1 modulo $m$. Thus, we have two cases: either $ia \equiv 1 \pmod{m}$ for some $i \in [1, r + \delta - 1]$; or $\delta + ja \equiv 1 \pmod{m}$ for some $j \in [0, r - 1]$.

In the first case, we have that $a$ is a unit modulo $m$ and hence $\gcd(a, m) = 1$, as desired.

In the second case, we have two subcases. If $j = 0$, then $\delta + 1 \equiv 1 \pmod{m}$, which implies $\delta \mid m$. Since $\gcd(\delta, m) = 1$, this implies $m = 1$, and thus $\gcd(a, m) = 1$. If $j > 0$, then $\delta + ja \equiv 1 \pmod{m}$. Since $\gcd(\delta, m) = 1$, $\delta$ is a unit modulo $m$ and thus $-\delta^{-1}ja \equiv 1 \pmod{m}$. Therefore, $a$ is also a unit modulo $m$, and hence $\gcd(a, m) = 1$. □

In the above proof, $M_L$ and $M_R$ may have repeated elements. For this reason, as well as for similar reasons in subsequent results in this section, we have chosen to work with multisets in this paper rather than sets.

**Proposition 4.4.** $H(S)$ is equidistributed modulo $m$ if and only if $\gcd(a\delta, m) = 1$ and we have the multiset congruence

$$\{ a, a\delta + \beta + 1, \beta + \delta, \delta + 1 \} \equiv \{ a + \delta, a\delta + \beta, \beta + \delta + 1, 1 \} \pmod{m}.$$

**Proof.** For the forward direction, suppose $H(S)$ is equidistributed modulo $m$. By Proposition 4.2 and Proposition 4.3 $\gcd(\delta, m) = \gcd(a, m) = 1$. By Proposition 2.15 $(x - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}$, and hence

$$(x - 1)(x^a - 1)(x^\delta - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}.$$  

By Eq. (4),

$$x^\beta(x - 1)(x^{a\delta} - x^\delta) - x^a(x^\delta - 1) \equiv 0 \pmod{(x^m - 1)}.$$  

Expanding out and moving terms so that all leading coefficients are +1, we have

$$x^a + x^{a\delta + \beta + 1} + x^{\beta + \delta} + x^{\delta + 1} \equiv x^a + x^{a\delta + \beta} + x^{\beta + \delta + 1} + x^1 \pmod{(x^m - 1)}.$$  

By Proposition 2.15

$$\{ a, a\delta + \beta + 1, \beta + \delta, \delta + 1 \} \equiv \{ a + \delta, a\delta + \beta, \beta + \delta + 1, 1 \} \pmod{m},$$

as desired.

Now we prove the converse. Suppose

$$\{ a, a\delta + \beta + 1, \beta + \delta, \delta + 1 \} \equiv \{ a + \delta, a\delta + \beta, \beta + \delta + 1, 1 \} \pmod{m}$$

and $\gcd(a\delta, m) = 1$. Reversing our steps from the proof of the forward implication, the multiset congruence implies

$$(x - 1)(x^a - 1)(x^\delta - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)}.$$  

Since $\gcd(a\delta, m) = 1$, we use Lemma 3.8 to get

$$\gcd((x - 1)(x^a - 1), x^m - 1) = \gcd((x - 1)^3, x^m - 1) = x - 1.$$  

We therefore have that

$$(x - 1)P_{H(S)}(x) \equiv 0 \pmod{(x^m - 1)},$$

which, with Proposition 2.15 implies that $H(S)$ is equidistributed modulo $m$, as desired. □

We are now ready to state the main result. The proof follows from our work above along with tracking through specific cases.
Theorem 4.5. For $S$ a numerical semigroup, any nonzero $a \in S$, and

$$\text{Ap}(S; a) = \{0\} \cup \{\beta + i\delta : i \in [1, a - 1]\}$$

for some $\beta \geq 0$ and $\delta > 0$, $H(S)$ is equidistributed modulo $m$ if and only if $\gcd(a\delta, m) = 1$ and one of the following occurs:

1. $a \equiv 1 \pmod{m}$; or
2. $a \equiv 2 \pmod{m}$ and $\beta + \delta \equiv 1 \pmod{m}$; or
3. $\delta \equiv 1 \pmod{m}$ and $\beta \equiv 0 \pmod{m}$; or
4. $\delta \equiv -1 \pmod{m}$ and $\beta \equiv a \pmod{m}$.

(Recall that $\beta$ and $\delta$ are uniquely determined when $a \geq 3$. For $a = 1$, we take $\beta = 0$ and $\delta = 1$. For $a = 2$, we take $\beta = 0$ and $\delta$ odd.)

Proof. We begin with the forward implication. If $H(S)$ is equidistributed modulo $m$, then by Proposition 4.4, $\gcd(a\delta, m) = 1$ and

$$\{a, a\delta + \beta + 1, \beta + \delta, \delta + 1\} \equiv \{a + \delta, a\delta + \beta, \beta + \delta + 1, 1\} \pmod{m}.$$ 

In particular, $a$ is congruent modulo $m$ to one of the following elements: $a + \delta; a\delta + \beta; \beta + \delta + 1; a$ or 1. We consider these four cases separately.

1. If $a \equiv a + \delta \pmod{m}$, then $\delta \equiv 0 \pmod{m}$. Since $\gcd(\delta, m) = 1$, we have $m = 1$. All four conclusions therefore hold.

2. If $a \equiv a\delta + \beta \pmod{m}$, then $\beta \equiv a - a\delta \pmod{m}$. We use Corollary 2.6 looking at the remaining elements in the multisets to find $\{a + 1, a - a\delta + \delta, \delta + 1\} \equiv \{a + \delta, a - a\delta + \delta + 1, 1\} \pmod{m}$. Next, $a + 1$ is congruent modulo $m$ to one of the following elements: $a - a\delta + \delta + 1; a + \delta$ or 1. We consider these cases separately.
   (a) If $a + 1 \equiv a + \delta \pmod{m}$, then $\delta \equiv 1 \pmod{m}$, which then implies $\beta \equiv 0 \pmod{m}$.
   (b) If $a + 1 \equiv a - a\delta + \delta + 1 \pmod{m}$, then $a\delta \equiv \delta \pmod{m}$. Since $\gcd(\delta, m) = 1$, we get $a \equiv 1 \pmod{m}$, which is the first concluding case.
   (c) If $a + 1 \equiv 1 \pmod{m}$, then $m \mid a$. Since $\gcd(a, m) = 1$, we have $m = 1$. All four concluding cases occur.

3. If $a \equiv \beta + \delta + 1 \pmod{m}$, we have $\beta \equiv a - \delta - 1 \pmod{m}$. We use Corollary 2.6 looking at the remaining elements in the multisets to find $\{a + a\delta - \delta, a - 1, \delta + 1\} \equiv \{a + \delta, a + a\delta - \delta - 1, 1\} \pmod{m}$. We see that $a - 1$ is congruent modulo $m$ to one of $a + \delta, a + a\delta - \delta - 1, 1$. We consider these cases separately.
   (a) If $a - 1 \equiv a + \delta \pmod{m}$, then $\delta \equiv -1 \pmod{m}$. Since $\beta \equiv a - \delta - 1 \pmod{m}$, we have $\beta \equiv a \pmod{m}$.
   (b) If $a - 1 \equiv a + a\delta - \delta - 1 \pmod{m}$, then $a\delta \equiv \delta \pmod{m}$ and hence $a \equiv 1 \pmod{m}$. This is the first concluding case.
   (c) If $a - 1 \equiv 1 \pmod{m}$, then $a \equiv 2 \pmod{m}$. Since $\beta \equiv a - \delta - 1 \pmod{m}$, we have $\beta + \delta \equiv 1 \pmod{m}$.

4. If $a \equiv 1 \pmod{m}$, then we are done. This is the first concluding case.

Now we prove the converse. For each of the four concluding cases, we need to show

$$\{a, a\delta + \beta + 1, \beta + \delta, \delta + 1\} \equiv \{a + \delta, a\delta + \beta, \beta + \delta + 1, 1\} \pmod{m}.$$ 

Along with the condition that $\gcd(a\delta, m) = 1$, we will use Proposition 4.4 to conclude that $H(S)$ is equidistributed modulo $m$.

For the following, let $L = \{a, a\delta + \beta + 1, \beta + \delta, \delta + 1\}$ and $R = \{a + \delta, a\delta + \beta, \beta + \delta + 1, 1\}$. It is therefore enough to verify that $L \equiv R \pmod{m}$ in each case.

1. If $a \equiv 1 \pmod{m}$, then
   $$L \equiv \{1, \delta + \beta + 1, \beta + \delta, \delta + 1\} \pmod{m}$$
   and
   $$R \equiv \{1 + \delta, \delta + \beta, \beta + \delta + 1, 1\} \pmod{m}.$$
We begin by describing two well-known families of numerical semigroups. The first family consists of numerical semigroups for which the nonzero terms of an Apéry set form an arithmetic sequence. When numerical semigroups generated by generalized arithmetic sequences appear in the literature, h is taken to be a positive integer. (See, e.g., [3], [7], [5], and [4].) If we allow h = 0 as a degenerate case of the family of numerical semigroups that are generated by generalized arithmetic sequences.

As before, we suppose \(\langle{a, h, d}\rangle\) is a numerical semigroup that is generated by at most two integers. We can think of the numerical semigroups \(\langle{a, h, d}\rangle\) as subfamilies.

5. Explicit numerical semigroups and results

In the previous section, we focused on numerical semigroups for which had an Apéry set whose nonzero elements formed an arithmetic sequence, and we derived explicit conditions to determine when such a numerical semigroup is equidistributed modulo \(m\). In this section, we will explicitly describe the numerical semigroups that have such an Apéry set.

As before, we suppose \(S\) is a numerical semigroup with some nonzero \(a \in S\) for which \(\text{Ap}(S; a) \setminus \{0\}\) is an arithmetic sequence. In other words,

\[
\text{Ap}(S; a) = \{0\} \cup \{\beta + \delta \cdot i : i \in [1, a - 1]\}
\]

for some \(\beta, \delta \in \mathbb{Z}\). Recall that (by Lemma 5.1) we have \(\beta \geq 0, \delta > 0, a \mid \beta, \text{ and } \gcd(a, \delta) = 1\).

5.1. Numerical semigroups for which the nonzero terms of an Apéry set form an arithmetic sequence. We begin by describing two well-known families of numerical semigroups. The first family consists of numerical semigroups generated by at most two integers.

Proposition 5.1 ([7, Section 3.I]). Suppose \(S = \langle{a, b}\rangle\) with \(\gcd(a, b) = 1\). Then \(\text{Ap}(S; a) = \{0\} \cup \{ib : i \in [1, a - 1]\}\) and \(g(S) = (a - 1)(b - 1)/2\). If \(a = 1\) or \(b = 1\), then \(e(S) = 1\). Otherwise, \(e(S) = 2\).

The second family consists of numerical semigroups generated by generalized arithmetic sequences, which are sequences of the form \(\{a, ha + d, ha + 2d, \ldots, ha + kd\}\) for \(a \geq 2\) and \(h, d, k \geq 1\). In general, it is enough to consider \(k \in [1, a - 1]\). For our work, we are interested in the case of maximal embedding dimension, which occurs when \(k = a - 1\).

Proposition 5.2 ([8, Section 3.III,IV]). Suppose \(S = \langle{\{a\} \cup \{ha + id : i \in [1, a - 1]\}\} with a, h, d \in \mathbb{N} and \gcd(a, d) = 1\). Then \(e(S) = a\) and \(\text{Ap}(S; a) = \{0\} \cup \{ha + id : i \in [1, a - 1]\}\). Furthermore, \(g(S) = (a - 1)(2h + d - 1)/2\).

Remark 5.3. When numerical semigroups generated by generalized arithmetic sequences appear in the literature, \(h\) is taken to be a positive integer. (See, e.g., [8], [9], [10], and [11]). If we allow \(h = 0\), then

\[
S = \langle{\{a\} \cup \{id : i \in [1, a - 1]\}\} = \langle{a, d}\rangle,
\]
a numerical semigroup that is generated by at most two integers. We can think of the numerical semigroups with \(h = 0\) as a degenerate case of the family of numerical semigroups that are generated by generalized arithmetic sequences.

For the remainder of this paper, we will work with the family of numerical semigroups of the form

\[
S = \langle{\{a\} \cup \{ha + id : i \in [1, a - 1]\}\}
\]

where \(h \geq 0, a, d \geq 1\), and \(\gcd(a, d) = 1\). This family contains the two families described above (in Proposition 5.1 and Proposition 5.2) as subfamilies.
We now have a lemma which says Proposition 5.1 and Proposition 5.2 are “if and only if” statements. If we know an Apéry set, then we know the semigroup.

**Lemma 5.4.** Let $S$ and $T$ be numerical semigroups with some nonzero $a \in S \cap T$. If $\text{Ap}(S; a) = \text{Ap}(T; a)$, then $S = T$.

**Proof.** Each element of $\text{Ap}(S; a)$ is the minimal element of $S$ in its congruence class modulo $a$. Thus, 

$$H(S) = \{ w - ka : w \in \text{Ap}(S; a), k \in \mathbb{N}, w - ka > 0 \}.$$

Since $\text{Ap}(S; a) = \text{Ap}(T; a)$, $H(S) = H(T)$, and thus $S = T$. □

We are now able to explicitly describe the numerical semigroups where the nonzero terms of an Apéry set form an arithmetic sequence.

**Proposition 5.5.** Suppose $S$ is a numerical semigroup with some nonzero $a \in S$, and suppose $\text{Ap}(S; a) \setminus \{0\}$ is an arithmetic sequence consisting of at least one term. Then $a \geq 2$ and

$$S = \langle\{a\} \cup \{ha + id : i \in [1, a - 1]\}\rangle$$

for some $h \geq 0$, $d \geq 1$, and $\gcd(a, d) = 1$.

If $h = 0$ and $d = 1$, then $e(S) = 1$. If $h = 0$ and $d > 1$, then $e(S) = 2$. If $h \geq 1$, then $e(S) = a$.

**Proof.** Since $\#(\text{Ap}(S; a)) = a$, if $\text{Ap}(S; a) \setminus \{0\}$ contains at least one term, then $a \geq 2$. We consider the cases of $a = 2$ and $a \geq 3$ separately.

If $a = 2$, then $S = \langle 2, b \rangle$ for some odd positive integer $b$. If $b = 1$, then $S = \langle 2, 1 \rangle = \langle 1 \rangle = \mathbb{N}_0$, in which case we have $e(S) = 1, h = 0$, and $d = 1$. If $b > 1$, then by Proposition 5.1 $e(S) = 2$ and we can write

$$S = \langle 2, b \rangle = \langle\{2\} \cup \{0a + ib : i \in [1, 1]\}\rangle.$$

Hence, we have $h = 0, d = b > 1$, and $\gcd(a, d) = \gcd(2, b) = 1$.

If $a \geq 3$, and $\text{Ap}(S; a) \setminus \{0\}$ is an arithmetic sequence, then

$$\text{Ap}(S; a) \setminus \{0\} = \{\beta + i\delta : i \in [1, a - 1]\}$$

for $\beta \geq 0, \delta > 0, a \mid \beta$, and $\gcd(a, \delta) = 1$. Let $\beta = la$ for some $l \in \mathbb{N}_0$. We have two cases based on $l$.

If $l = 0$, then

$$\text{Ap}(S; a) \setminus \{0\} = \{i\delta : i \in [1, a - 1]\}.$$

By Proposition 5.1 and Lemma 5.4, $S = \langle a, \delta \rangle$ with $\gcd(a, \delta) = 1$. If $\delta = 1$, then $S = \langle a, 1 \rangle = \langle 1 \rangle = \mathbb{N}_0$, in which case we have $e(S) = 1, h = 0$, and $d = \delta = 1$. If $\delta > 1$, then by Proposition 5.1 $e(S) = 2$ and we can write

$$S = \langle a, \delta \rangle = \langle\{a\} \cup \{0a + i\delta : i \in [1, a - 1]\}\rangle.$$

Hence, we have $h = 0, d = \delta > 1$, and $\gcd(a, d) = \gcd(a, \delta) = 1$.

If $l > 0$, then

$$\text{Ap}(S; a) \setminus \{0\} = \{la + i\delta : i \in [1, a - 1]\}.$$

By Proposition 5.2 and Lemma 5.4

$$S = \langle\{a\} \cup \{ha + id : i \in [1, a - 1]\}\rangle$$

for $h = l$ and $d = \delta$. We have $h > 0, d > 0, \gcd(a, d) = 1$, and $e(S) = a$. □

### 5.2. Explicit criteria for this family of numerical semigroups.

Now that we can explicitly describe the numerical semigroups $S$ for which the nonzero terms of an Apéry set of $S$ form an arithmetic sequence, we can use the description to determine when the set of gaps of $S$ is equidistributed modulo $m$.

**Corollary 5.6.** Suppose $S$ is a numerical semigroup with some nonzero $a \in S$, and suppose $\text{Ap}(S; a) \setminus \{0\}$ is an arithmetic sequence consisting of at least one term. Then $S = \langle\{a\} \cup \{ha + id : i \in [1, a - 1]\}\rangle$ for $a \geq 2, h \geq 0, d \geq 1$, and $\gcd(a, d) = 1$. We have that $H(S)$ is equidistributed modulo $m$ if and only if $\gcd(ad, m) = 1$ and at least one of the following occurs:

1. $a \equiv 1 \pmod{m}$; or
2. $a \equiv 2 \pmod{m}$ and $2h + d \equiv 1 \pmod{m}$; or
3. $d \equiv 1 \pmod{m}$ and $h \equiv 0 \pmod{m}$; or
4. $d \equiv -1 \pmod{m}$ and $h \equiv 1 \pmod{m}$. 

Proof. If \( Ap(S; a) \setminus \{0\} = \{\beta + i\delta : i \in [1, a - 1]\} \) is an arithmetic sequence consisting of at least one term, then by Proposition 5.5 we must have \( S = \{a\} \cup \{ha + id : i \in [1, a - 1]\} \) for \( a \geq 2, h \geq 0, d \geq 1, \) and \( \gcd(a, d) = 1 \). (As before, \( \beta = ha \) and \( \delta = d \).)

By Theorem 4.15, \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(a\delta, m) = 1 \) and any of the four cases from Theorem 4.5 occur. For \( n = 1, 2, 3, 4 \), we will assume Case \( n \) of Theorem 4.5 and show that it is equivalent to Case \( n \) of this corollary.

- **n = 1:** Both cases have \( a \equiv 1 \mod m \), so we are done.
- **n = 2:** Suppose \( a \equiv 2 \mod m \) and \( \beta + \delta \equiv 1 \mod m \). Since \( \beta = ha \equiv 2h \mod m \) and \( \delta = d \), we equivalently have \( a \equiv 2 \mod m \) and \( 2h + d \equiv 1 \mod m \). These two cases are equivalent.
- **n = 3:** Suppose \( \delta \equiv 1 \mod m \) and \( \beta \equiv 0 \mod m \). Since \( \beta = ha \) and \( \delta = d \), we equivalently have \( d \equiv 1 \mod m \) and \( ha \equiv 0 \mod m \). The latter congruence is equivalent to the congruence \( h \equiv 0 \mod m \) because \( \gcd(a, m) = 1 \). These two cases are equivalent.
- **n = 4:** Suppose \( \delta \equiv -1 \mod m \) and \( \beta \equiv a \mod m \). Since \( \beta = ha \) and \( \delta = d \), we equivalently have \( d \equiv -1 \mod m \) and \( ha \equiv a \mod m \). The latter congruence is equivalent to the congruence \( h \equiv 1 \mod m \) because \( \gcd(a, m) = 1 \). These two cases are equivalent.

\( \square \)

**Remark 5.7.** We can revisit Proposition 3.15 where we determined conditions for \( S \) a numerical semigroup of multiplicity 3. In particular, when \( e(S) = m(S) = 3 \), we have \( S = \langle 3, b, c \rangle \), and \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(3, m) = 1 \) and \( m \) divides either \( \gcd(b - 1, c - 2) \) or \( \gcd(b - 2, c - 1) \). In Remark 3.10 we note that the numerical semigroup \( S = \langle 3, b, c \rangle \), with \( b < c \), can be written as \( S = \langle 3, 3h + d, 3h + 2d \rangle \) for \( h \equiv (2b - c)/3 \equiv d = c - b \). By Corollary 5.6, \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(3d, m) = 1 \) and one of four conditions holds. As expected, working through the four conditions, we recover the same results that we obtained in Proposition 3.15.

We can specialize to the case where \( e(S) = 2 \).

**Corollary 5.8.** Suppose \( e(S) = 2 \), so \( S = \langle a, b \rangle \) for \( a, b > 1 \) with \( \gcd(a, b) = 1 \). Then \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(ab, m) = 1 \) and at least one of the following holds:

1. \( a \equiv 1 \mod m \); or
2. \( b \equiv 1 \mod m \).

**Proof.** If \( e(S) = 2 \), then by Proposition 5.1 we have \( S = \langle a, b \rangle \) for \( a, b > 1 \) with \( \gcd(a, b) = 1 \). Thus, \( S = \{a\} \cup \{ha + id : i \in [1, a - 1]\} \) for \( h = 0 \) and \( d = b \). Plugging these into the four cases of Corollary 5.6 we find that either \( a \equiv 1 \mod m \) or \( b \equiv 1 \mod m \). Hence \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(ab, m) = 1 \) at least one of \( a \) and \( b \) is 1 modulo \( m \). \( \square \)

Put another way, for \( S = \langle a, b \rangle \), \( H(S) \) is equidistributed modulo \( m \) if and only if \( m \) is a divisor of \( a - 1 \) with \( \gcd(b, m) = 1 \), or if \( m \) is a divisor of \( b - 1 \) with \( \gcd(a, m) = 1 \). (Note that we can allow \( a = 1 \) or \( b = 1 \) here as well.)

**Example 5.9.** Let \( S = \langle 5, 7 \rangle \). Then \( H(S) = \{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\} \). In Example 2.11 we determined that this set is equidistributed modulo \( m \) for \( m \in \{1, 2, 3, 4, 6\} \). We will revisit this example now that we have Corollary 5.6. The divisors of \( 5 - 1 \) are each relatively prime to \( 7 \). The divisors of \( 7 - 1 \) are each relatively prime to \( 5 \). Thus, \( H(S) \) is equidistributed modulo any divisor of \( 4 \) or \( 6 \), which is to say \( H(S) \) is equidistributed modulo \( 1, 2, 3, 4, \) and \( 6 \).

For a numerical semigroup \( S \) of maximal embedding dimension generated by a (purely) arithmetic sequence, we have \( S = \langle a, a + d, a + 2d, \ldots, a + (a - 1)d \rangle \) for \( a, d \geq 1 \). We can obtain results for such a numerical semigroup by plugging \( h = 1 \) into Corollary 5.6. Note that the third case can now only occur if \( m = 1 \), and the second case is now a special case of the fourth case. We therefore have two cases: \( a \equiv 1 \mod m \) or \( d \equiv -1 \mod m \).

**Corollary 5.10.** Suppose \( S \) is a numerical semigroup of maximal embedding dimension generated by an arithmetic sequence. Then \( S = \{a + id : i \in [0, a - 1]\} \) for \( a \geq 1, d \in \mathbb{N}, \) and \( \gcd(a, d) = 1 \). We have that \( H(S) \) is equidistributed modulo \( m \) if and only if \( \gcd(ad, m) = 1 \) and at least one of the following occurs:

1. \( a \equiv 1 \mod m \); or
2. \( d \equiv -1 \mod m \).
5.3. Observations. Finally, we make a few observations.

For \( e(S) = 2 \), \( g(S) = (a-1)(b-1)/2 \). By Corollary 5.8 H(S) is equidistributed modulo \( m \) if and only if \( \gcd(ab,m) = 1 \) and either \( m \mid (a-1) \) or \( m \mid (b-1) \).

In the purely arithmetic case, \( g(S) = (a-1)(d+1)/2 \). By Corollary 5.10 H(S) is equidistributed modulo \( m \) if and only if \( \gcd(ad,m) = 1 \) and either \( m \mid (a-1) \) or \( m \mid (d+1) \).

These two cases have a very similar feel. The generalized arithmetic case is similar, though we don’t quite get an “if and only if” result.

In the generalized arithmetic case, \( g(S) = (a-1)(2h+d-1)/2 \). By Corollary 5.6 if H(S) is equidistributed modulo \( m \), then \( \gcd(ad,m) = 1 \) and either \( m \mid (a-1) \) or \( m \mid (2h+d-1) \), the latter congruence implied by, but not equivalent to, cases 2, 3, 4 of Corollary 5.6.

Acknowledgments

The author wishes to thank the anonymous referees for their detailed reports. Their suggestions were incredibly helpful. The author also wishes to thank Pieter Moree for suggesting the phrase ‘equidistribution modulo \( m \).

References

[1] R. Apéry. Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris*, 222:1198–1200, 1946.

[2] T. A. Gassert and C. M. Shor. Characterizations of numerical semigroup complements via Apéry sets. *Semigroup Forum*, 98(1):31–47, Feb 2019. ISSN 1432-2137. doi: 10.1007/s00233-018-9935-4. URL https://doi.org/10.1007/s00233-018-9935-4

[3] M. Lewin. An algorithm for a solution of a problem of Frobenius. *J. Reine Angew. Math.*, 276:68–82, 1975. ISSN 0075-4102. doi: 10.1515/crll.1975.276.68. URL https://doi.org/10.1515/crll.1975.276.68

[4] G. L. Matthews. On numerical semigroups generated by generalized arithmetic sequences. *Comm. Algebra*, 32(9):3459–3469, 2004. ISSN 0092-7872. doi: 10.1081/AGB-120039623. URL https://doi.org/10.1081/AGB-120039623

[5] S. M. Ritter. On a linear Diophantine problem of Frobenius: extending the basis. *J. Number Theory*, 69(2):201–212, 1998. ISSN 0022-314X. doi: 10.1006/jnth.1997.2219. URL https://doi.org/10.1006/jnth.1997.2219

[6] J. C. Rosales and P. A. García-Sánchez. *Numerical Semigroups*, volume 20 of *Developments in Mathematics*. Springer-Verlag New York, 2009. ISBN 978-1-4419-0159-0. doi: 10.1007/978-1-4419-0160-6.

[7] E. S. Selmer. On the linear diophantine problem of Frobenius. *J. Reine Angew. Math.*, 0293:0294:1–17, 1977. doi: 10.1515/crll.1977.293-294.1. URL https://doi.org/10.1515/crll.1977.293-294.1

[8] J. J. Sylvester. On subvariants, i.e. semi-invariants to binary quantics of an unlimited order. *Amer. J. Math.*, 5(1):79–136, 1882. ISSN 00029327, 10806377. doi: 10.2307/2369536. URL https://doi.org/10.2307/2369536

[9] H. J. H. Tuenter. The Frobenius problem, sums of powers of integers, and recurrences for the Bernoulli numbers. *J. Number Theory*, 117(2):376–386, 2006. ISSN 0022-314X. doi: 10.1016/j.jnt.2005.06.015. URL http://dx.doi.org/10.1016/j.jnt.2005.06.015

[10] W. Wang and T. Wang. Alternate Sylvester sums on the Frobenius set. *Comput. Math. Appl.*, 56(5):1328–1334, 2008. ISSN 0898-1221. doi: 10.1016/j.camwa.2008.02.031. URL http://dx.doi.org/10.1016/j.camwa.2008.02.031

Department of Mathematics, Western New England University, Springfield, MA 01119

Email address: cshor@wne.edu