Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

On the Delta Set of a Singular Arithmetical Congruence Monoid

par Paul Baginski, S. T. Chapman et George J. Schaeffer

Résumé. Si a et b sont des entiers positifs, avec $a \leq b$ et $a^2 \equiv a \bmod b$, nous appelons l'ensemble

$$M_{a,b} = \{x \in \mathbb{N} : x \equiv a \mod b \text{ ou } x = 1\}$$

un monoïde d'une congruence arithmetique (ACM). Pour chaque monoïde avec ses unités $M^\times$ et pour chaque $x \in M \backslash M^\times$, nous ditons que $t \in \mathbb{N}$ est une longueur de décomposition en facteurs de x si et seulement s'il y a des éléments irréductibles $y_1, \ldots, y_t \in M$ et $x = y_1 \cdots y_t$. Soit $\mathcal{L}(x) = \{t_1, \ldots, t_j\}$ l'ensemble des longeuers (avec $t_i < t_{i+1}$ pour $i < j$). Le Delta-ensemble d'un élément x est $\Delta(x) = \{t_{i+1} - t_i : 1 \leq i < j\}$ et le Delta-ensemble du monoïde M est $\Delta(M) = \bigcup_{x \in M \backslash M^\times} \Delta(x)$. Nous examinons $\Delta(M)$ quand $M = M_{a,b}$ est un ACM avec $\gcd(a, b) > 1$. Cet ensemble est caractérisé complètement quand $\gcd(a, b) = p^\alpha$, p est un nombre premier, et $\alpha > 0$. Quand $\gcd(a, b)$ a plus d'un facteur premier, nous trouvons des limites pour $\Delta(M)$.

Abstract. If a and b are positive integers with $a \leq b$ and $a^2 \equiv a \bmod b$, then the set

$$M_{a,b} = \{x \in \mathbb{N} : x \equiv a \bmod b \text{ or } x = 1\}$$

is a multiplicative monoid known as an arithmetical congruence monoid (or ACM). For any monoid M with units $M^\times$ and any $x \in M \setminus M^\times$ we say that $t \in \mathbb{N}$ is a *factorization length* of x if and only if there exist irreducible elements $y_1, \ldots, y_t$ of M and $x = y_1 \cdots y_t$. Let $\mathcal{L}(x) = \{t_1, \ldots, t_j\}$ be the set of all such lengths (where $t_i < t_{i+1}$ whenever $i < j$). The Delta-set of the element x is defined as the set of gaps in $\mathcal{L}(x)$: $\Delta(x) = \{t_{i+1} - t_i : 1 \leq i < k\}$ and the Delta-set of the monoid M is given by $\bigcup_{x \in M \backslash M^\times} \Delta(x)$. We consider the $\Delta(M)$ when $M = M_{a,b}$ is an ACM with $\gcd(a, b) > 1$. This set is fully characterized when $\gcd(a, b) = p^\alpha$ for p prime and $\alpha > 0$. Bounds on $\Delta(M_{a,b})$ are given when $\gcd(a, b)$ has two or more distinct prime factors.

The first author was supported by a Dept. of Homeland Security Graduate Fellowship.
The third author received support from the National Science Foundation, Grant #DMS-0353488.

1. Introduction

Throughout our work, $\mathbb{N}$ denotes the positive integers and $\mathbb{N}_0$ the non-negative integers. Let $\mathbb{P}$ denote the set of (positive) rational primes, and for any $x \in \mathbb{N}$, $\mathbb{P}(x)$ denotes the set of rational primes which divide x. If $S \subseteq \mathbb{N}$, then $\langle S \rangle_\times$ denotes the multiplicative closure of S in $\mathbb{N}$ (that is, $\langle S \rangle_\times$ is the free commutative monoid on S). Intervals will always be treated as subsets of $\mathbb{Z}$. Monoids are always assumed to be commutative, atomic (every element can be written as a finite product of irreducibles), and cancellative (for all $x, y, z \in M$, $xy = xz$ implies $y = z$).

For any $m > 0$ the set

$$H_m = \{x \in \mathbb{N} : x \equiv 1 \bmod m\} = 1 + m\mathbb{N}_0$$

is a monoid under the usual multiplication operation. Monoids of this form are called *Hilbert monoids* and generalize to a broader class of submonoids of $(\mathbb{N}, \times)$. Let $b \in \mathbb{N}$ and choose $a \in \mathbb{N}$ satisfying $0 < a \leq b$ and $a^2 \equiv a \bmod b$. The *arithmetical congruence monoid* (ACM) determined by this choice of a, b is defined as

$$M_{a,b} = \{x \in \mathbb{N} : x = 1 \text{ or } x \equiv a \bmod b\} = (a + b\mathbb{N}_0) \cup \{1\}.$$

Because $M_{a,b}$ is a submonoid of $(\mathbb{N}, \times)$ one easily verifies that it is commutative, atomic, and cancellative. In general, arithmetical congruence monoids do not possess unique factorization. Indeed, fixed elements of an ACM may have factorizations of different lengths. For example, in $M_{4,6}$ the elements $4, 10, 250$ are all irreducible, but $(10)^3 = (4)(250)$.

The value $d = \gcd M_{a,b} = \gcd(a, b)$ is very important to the factorization theory of $M_{a,b}$. If $d = 1$ then we call $M_{a,b}$ *regular* and if $d > 1$, we call it *singular*. An elementary argument (see [3, Lemma 2.1]) shows that regular ACMs are precisely the Hilbert monoids described above. Singular ACMs are further characterized as being either *local* or *global* depending on whether d has one or more distinct prime factors. An application of the Chinese Remainder Theorem shows that a global ACM can always be written uniquely as an intersection of local ACMs. Moreover, the local and global cases are also naturally distinguished by the structure of a certain characteristic submonoid (see Section 4).

Arithmetical congruence monoids have been addressed recently in the literature in [2] and [3] where the factorization properties of these monoids are explored. In particular, in [3, Theorem 2.4] and [6, Example 3.7.14] it is shown that the elasticity of factorization (see [1] or [6, Definition 1.4.1] for a definition) of $M_{a,b}$ is finite if and only if $M_{a,b}$ is regular or local. A more in-depth general analysis of congruence monoids can be found in [7]. Our purpose is to extend the work of [3] and provide a more precise examination of the factorization properties of the elements of $M_{a,b}$ into products of irreducible elements.

Before describing the contents of our paper, some definitions and notation are necessary. For any monoid M the set of units will be denoted by $M^\times$ and the set of irreducible elements will be denoted by $\mathcal{A}(M)$. If $x \in M \setminus M^\times$ set

$$\mathcal{L}(x) = \{l \in \mathbb{N}_0 : \text{there exist } x_1, \ldots, x_l \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_l\}.$$

Order $\mathcal{L}(x) = \{l_1, \ldots, l_j\}$ with $l_i < l_{i+1}$ for $1 \leq i < j$ and define

$$\Delta(x) = \{l_{i+1} - l_i : i \in [1, j)\}.$$

Finally, we define the Δ-*set* of M by

$$\Delta(M) = \bigcup_{x \in M \setminus M^\times} \Delta(x).$$

Note that M is half-factorial (i.e., $|\mathcal{L}(x)| = 1$ for each $x \in M \setminus M^\times$) if and only if $\Delta(M) = \varnothing$.

Determining the Δ-set of a given monoid is no simple task, and in fact, very few specific calculations are known. For instance, the Δ-set of the Hilbert monoid H_m (which is a Krull monoid) is equivalent to that of the block monoid on $(\mathbb{Z}/m\mathbb{Z})^\times$ (see [6, Proposition 2.11.6]), and in general, little can be said about the Δ-set of a block monoid on a finite abelian group unless it is cyclic. The Δ-set of a numerical monoid (an additive submonoid of $\mathbb{N}_0$) has been analyzed rigorously in [4] where the authors characterize $\Delta(S)$ when S is a numerical monoid with equally spaced generators. In particular, if $S = \langle a, a + k, a + 2k, \ldots, a + wk \rangle$ then $\Delta(S) = \{k\}$.

In our paper, we will examine the Δ-set of a singular ACM. By [6, Theorem 2.11.8], ACMs are examples of a larger class of arithmetically motivated monoids known as C-monoids (H is a C-monoid if and only if it is a submonoid of a factorial monoid F such that $H \cap F^\times = H^\times$ and the reduced class semigroup of H in F is finite, see [8]). The Δ-set of a C-monoid is finite [6, Theorem 1.6.3]; hence we can always assume by a Theorem of Geroldinger [6, Proposition 1.4.4] that

$$\Delta(M_{a,b}) \subseteq \{s, 2s, \ldots, qs\}$$

where $s = \min \Delta(M_{a,b})$ and q is a positive integer.

We will completely determine the Δ-set of a local ACM (Theorem 3.1). We will also characterize a property of global ACMs which gives an upper bound on the Δ-set in this case (Theorem 4.2).

An overview of basic ACM structure in Section 2 culminates with a useful membership criterion. This allows us to note that if $M_{a,b}$ is local with $d = \gcd(a, b) = p^\alpha$, then there exists $\beta \geq \alpha$ such that $p^\beta \in M_{a,b}$. Section 3 contains the proof of Theorem 3.1, which fully characterizes the Δ-set of a local ACM according to the values of α and β. Section 4 closes with some

provocative remarks on the structure of ACMs, including Theorem 4.2 and some of its corollaries.

Many important factorization properties of ACMs have already been investigated; in particular, questions of factoriality, half-factoriality, and elasticity are covered extensively in [3] and [6]. Most relevant to our discussion will be the following results from [3] (Theorem 2.4 and Theorem 2.7).

Theorem 1.1. *Let $M_{a,b}$ be an arithmetical congruence monoid.*

(1) $\Delta(M_{a,b}) = \varnothing$ *(that is, $M_{a,b}$ is half-factorial) if and only if either*
   a. $M_{a,b} = H_m$ *where $\varphi(m) \leq 2$, or*
   b. $a \equiv p \bmod b$, *where p is a rational prime dividing b.*

(2) *If $\Delta(M_{a,b}) \neq \varnothing$, then $1 \in \Delta(M_{a,b})$.*

2. Basic structure theory of ACMs

Since an arithmetical congruence monoid is determined by the choice of a, b, it is logical to begin our discussion with the possible choices. In the process, we also determine a membership criterion for $M_{a,b}$.

Theorem 2.1. *Let $a, b \in \mathbb{N}$, $0 < a \leq b$, $a^2 \equiv a \mod b$, $d = \gcd(a, b)$ and $m = b/d$. Then $\gcd(a, m) = \gcd(d, m) = 1$ and*

$$M_{a,b} = (d\mathbb{N} \cap H_m) \cup \{1\}.$$

Conversely, let $d, m \in \mathbb{N}$ with $\gcd(d, m) = 1$ and set $b = dm$. Then there is a unique $a \in \mathbb{N}$ such that $0 < a \leq b$, $a^2 \equiv a \mod b$, and $d = \gcd(a, b)$. In this case, $M_{a,b}$ has the form above.

Proof. Let $0 < a \leq b$ and $a^2 \equiv a \mod b$. Then $b \mid a(a-1)$. Since a and $a-1$ are relatively prime, we have $v_p(a) \geq v_p(b)$ for any prime p dividing d. But $d = \gcd(a, b)$, so for such p we have $v_p(b) = v_p(d)$ and $v_p(m) = 1$. This yields that $\gcd(a, m) = \gcd(d, m) = 1$.

Since $m \mid b$ we have $a^2 \equiv a \mod m$; but $\gcd(a, m) = 1$, so a is a unit modulo m. Therefore $a \equiv 1 \mod m$. Every $x \neq 1$ in $M_{a,b}$ is of the form $a + kb$, so $d|x$ and we have $x \equiv 1 \mod m$. Thus $x \in d\mathbb{N} \cap H_m$ and $M_{a,b} \subseteq (d\mathbb{N} \cap H_m) \cup \{1\}$. For the reverse inclusion, suppose $x \equiv 1 \mod m$ and $d|x$. Since $a \equiv 1 \mod m$, we have $x = a + km$ for some k. But since $d|x$, $d|a$ and $\gcd(d, m) = 1$, we must have $d|k$. So $x = a + b(k/d) > 0$ and therefore $x \in M_{a,b}$ by definition.

Now we show the converse. Let $d, m \in N$ with $\gcd(d, m) = 1$ and set $b = dm$. Since $\gcd(d, m) = 1$, we may choose integers u, v such that $ud - vm = 1$. Therefore:

$$(ud)^2 = ud(1 + vm) = ud + buv \equiv ud \mod b$$

If a is the least positive residue of ud modulo b, then $0 < a \leq b$ and $a^2 \equiv a \mod b$. Also, $a = ud + kb$ for some k, so $d|a$. But $ud \equiv 1 \mod m$, so $a \equiv 1 \mod m$ and $\gcd(a, m) = 1$. Therefore $\gcd(a, b) = d$.

For uniqueness, suppose a, a' both satisfy the conditions, with $a \leq a'$. Then we may write $a = kd$ and $a' = k'd$ for some $0 < k \leq k' \leq m$. Since $\gcd(a, b) = \gcd(a', b) = d$, we must have $a \equiv a' \equiv 1 \mod m$. So $m|(a' - a) = (k' - k)d$. Since $\gcd(d, m) = 1$, we conclude $m|k' - k$ and so $k' = k$. Therefore $a = a'$.□

We will later find the following corollary to be very useful.

Corollary 2.2. *Let $x, y \in M_{a,b}$ be such that $x, y \neq 1$ and $y \mid_{\mathbb{N}} x$.*

- *If $d \mid_{\mathbb{N}} (x/y)$, then $x/y \in M_{a,b}$.*
- *If $x \in \mathcal{A}(M_{a,b})$, then $y \in \mathcal{A}(M_{a,b})$.*

Proof. For the first claim it is enough to note that $x \equiv y \equiv 1 \bmod m$ so that $x/y \equiv 1 \bmod m$.

For the second claim, suppose that y is reducible and z is an irreducible factor of y. Then $y/z \in M_{a,b}$, so $d \mid_{\mathbb{N}} (y/z)$. Since $y \mid_{\mathbb{N}} x$, we see $d \mid_{\mathbb{N}} (x/z)$. By the first claim, $x/z \in M_{a,b}$ and so $x = z(x/z)$ is reducible in $M_{a,b}$ as well. □

We close this section with an interesting observation concerning the irreducible elements of a singular ACM.

Theorem 2.3. *If M is a singular ACM and $x \in M$ is reducible, then $x + b \in \mathcal{A}(M)$.*

Proof. If x is reducible, then $x = x_1 x_2$ for some nontrivial $x_1, x_2 \in M_{a,b}$. Therefore $d \mid_{\mathbb{N}} x_1$ and $d \mid_{\mathbb{N}} x_2$ so $d^2 \mid_{\mathbb{N}} x$. But $d^2 \nmid_{\mathbb{N}} b$ since $\gcd(d, m) = 1$. Therefore $d^2 \nmid_{\mathbb{N}} x + b$ and so $x + b$ is necessarily irreducible in $M_{a,b}$. □

This suggests that if M is a singular ACM, then

$$\varsigma(M) = \limsup_{k \to \infty} \frac{|\mathcal{A}(M) \cap [1, k]|}{|M \cap [1, k]|} \geq \frac{1}{2}.$$

For example, since a positive integer x in $M_{2,2}$ is irreducible if and only if $2 \mid x$ but $4 \nmid x$, it follows that $\varsigma(M_{2,2}) = 1/2$. On the other hand, it is possible to force ς to be arbitrarily close to 1. To see this, let p be an odd prime and consider $\varsigma(M_{p,2p})$. We claim that $\varsigma(M_{p,2p}) = (p - 1)/p$. In $\varsigma(M_{p,2p})$, $x \in M$ is irreducible if and only if $p \mid x$ but $p^2 \nmid x$. Thus, dividing through by p we see that $\varsigma(M)$ is equal to the density of odd numbers which are not divisible by p, which is as claimed.

3. The Δ-set of a local ACM

Throughout this section, M will denote a local ACM with $d = p^\alpha$ for $p \in \mathbb{P}$ and $\alpha > 0$. By Theorem 2.1 $\gcd(p, m) = 1$ so we may choose the least integer greater $\beta \geq \alpha$ such that $p^\beta \equiv 1 \bmod m$. By the membership criterion, p^β is the smallest power of p which is an element of M and, of course, $p^\beta \in \mathcal{A}(M)$. The main theorem of this section is the following:

Theorem 3.1. *Let M be a local ACM.*

- *If $\alpha = \beta = 1$, $\Delta(M) = \varnothing$.*
- *If $\alpha = \beta > 1$, then $\Delta(M) = \{1\}$.*
- *If $\alpha < \beta$, then $\Delta(M) = [1, \beta/\alpha)$.*

The first of these results is an immediate consequence of Theorem 1.1. Observe that when $\alpha = \beta = 1$, $p \in M_{a,b}$. Since a is minimal among the nonunits of M and $p \mid a$, it follows that $a = p$, so a is a prime divisor of b.

It is natural in the local case to classify elements of the ACM by their p-adic values. Note that if $x \in M$ and $v_p(x) < 2\alpha$, x is irreducible. Similarly, if $v_p(x) \geq \alpha + \beta$, x is reducible:

$$x = p^{\alpha+\beta} y = (p^\beta)(p^\alpha y),$$

where $p^\beta \in M$ by hypothesis and $p^\alpha y \in M$ by Corollary 2.2. Hence, if $x \in \mathcal{A}(M)$, $v_p(x) \in [\alpha, \alpha + \beta)$. Moreover, by Dirichlet's Theorem there are infinitely many irreducibles of M which have p-adic value γ for each $\gamma \in [\alpha, \alpha + \beta)$.

3.1. Bounding $\Delta(M)$ in the local case. Let $\mathbf{F}$ be the set of all nonnegative integral vectors indexed by the interval $[\alpha, \alpha + \beta)$. We consider $\mathbf{F}$ as a monoid under coordinate-wise addition and write $\mathbf{f}' \leq \mathbf{f}$ if and only if $f'_\gamma \leq f_\gamma$ for all $\gamma \in [\alpha, \alpha + \beta)$. We also set $|\mathbf{f}| = f_\alpha + \cdots + f_{\alpha+\beta-1}$.

Given $x \in M \setminus M^\times$, we write that $\mathbf{f} \in \mathbf{F}(x)$ if and only if x has a factorization into $|\mathbf{f}|$-many irreducibles of M such that f_γ of these factors have p-adic value γ, for each γ. We say in this case that $\mathbf{f}$ is a *factorization scheme for x*. Clearly if $\mathbf{f}$ is a factorization scheme for x, then $|\mathbf{f}| \in \mathcal{L}(x)$.

The monoid $\mathbf{F}$ gives us a way to track factorizations of elements in M. If $\mathbf{f} \in \mathbf{F}(y)$ and $\mathbf{g} \in \mathbf{F}(z)$ then $\mathbf{f} + \mathbf{g} \in \mathbf{F}(yz)$ (i.e., $\mathbf{F}(y) + \mathbf{F}(z) \subseteq \mathbf{F}(yz)$). Conversely, suppose $\mathbf{f} \in \mathbf{F}(x)$ and $\mathbf{f}' < \mathbf{f}$. Fix a factorization of x corresponding to $\mathbf{f}$. For each γ choose f'_γ-many irreducible factors of x with p-adic valuation γ and multiply all the chosen irreducibles together to yield an element $y \in M$. Then $\mathbf{f}' \in \mathbf{F}(y)$, $x/y \in M$, and $\mathbf{f} - \mathbf{f}' \in \mathbf{F}(x/y)$.

Lastly, we define a homomorphism $r : \mathbf{F} \to \mathbb{Z}$ by:

$$r(\mathbf{f}) = \sum_{i=\alpha}^{\alpha+\beta-1} (\beta - i) f_i = \sum_{i=1-\alpha}^{\beta-\alpha} i f_{\beta-i}.$$

Note that if $\mathbf{f} \in \mathbf{F}(x)$ then $r(\mathbf{f}) = \beta|\mathbf{f}| - v_p(x)$. We now establish two lemmas about values of r in relation to the partial ordering on F.

Lemma 3.2. *Let* $\mathbf{f} \in \mathbf{F}$.

- *If* $r(\mathbf{f}) \leq R < 0$ *there is* $\mathbf{f}' \leq \mathbf{f}$ *such that* $r(\mathbf{f}') \in [R+1, R+\alpha-1]$.
- *If* $r(\mathbf{f}) \geq R > 0$ *there is* $\mathbf{f}' \leq \mathbf{f}$ *such that* $r(\mathbf{f}') \in [R+\alpha-\beta, R-1]$.

Proof. If $r(\mathbf{f}) < 0$ then there is some $\gamma > \beta$ such that $f_\gamma > 0$. Let $\mathbf{e}_\gamma$ be the vector which has 1 in the γ-th coordinate and 0 in all other coordinates. Then $\mathbf{f} - \mathbf{e}_\gamma \leq \mathbf{f}$ and $r(\mathbf{f} - \mathbf{e}_\gamma) = r(\mathbf{f}) - (\beta - \gamma)$. Thus we have found an $\mathbf{f}'$ such that $r(\mathbf{f}) < r(\mathbf{f}') \leq r(\mathbf{f}) + \alpha - 1$. Proceeding inductively, we are able to find an $\mathbf{f}' \leq \mathbf{f}$ with $r(\mathbf{f}')$ in any subinterval of $[r(\mathbf{f}), \alpha - 2]$ of size $\alpha - 1$.

The proof for the second claim is analogous, with $\gamma < \beta$ and intervals of size $\beta - \alpha$ instead. □

The above lemma is crucial in that it illustrates a level of uniformity to the distribution of values taken by r.

Lemma 3.3. *Fix* $x \in M$, $\mathbf{f} \in \mathbf{F}(x)$, *and suppose that* $r(\mathbf{f}) \leq -\alpha$. *Then there exists* $\mathbf{g} \in \mathbf{F}(x)$ *such that* $|\mathbf{g}| = |\mathbf{f}| + 1 \in \mathcal{L}(x)$.

Proof. Using Lemma 3.2 for the case when $r(\mathbf{f}) \leq 1 - 2\alpha$, we are always able to choose $\mathbf{f}' \leq \mathbf{f}$ such that $r(\mathbf{f}') \in [2 - 2\alpha, -\alpha]$. Pick $y \in M$ such that $\mathbf{f}' \in \mathbf{F}(y)$ and $x/y \in M$.

Since $v_p(y) - \beta|\mathbf{f}'| = -r(\mathbf{f}') \geq \alpha$, by Corollary 2.2 we know that $z = y/p^{\beta|\mathbf{f}'|} \in M$. Furthermore, since $v_p(z) = -r(\mathbf{f}') < 2\alpha$ we find that z is irreducible. Thus $(p^\beta)^{|\mathbf{f}'|}z$ is a factorization of y into $|\mathbf{f}'| + 1$ irreducibles. Since $|\mathbf{f} - \mathbf{f}'| \in \mathcal{L}(x/y)$, we have shown that $|\mathbf{f}| + 1 \in \mathcal{L}(x)$. □

Corollary 3.4. *If* $\alpha = \beta > 1$, *then* $\Delta(M) = \{1\}$.

Proof. Let $x \in M$ be a nonunit. Since M is not half-factorial, we may take x such that $\Delta(x) \neq \varnothing$. Let $\mathbf{f} \in \mathbf{F}(x)$ be given. If $|\mathbf{f}| \neq \max \mathcal{L}(x)$ then

$$|\mathbf{f}| + 1 \leq \max \mathcal{L}(x) \leq \frac{v_p(x)}{\alpha}$$

Since $\alpha = \beta$ this implies $r(\mathbf{f}) \leq -\alpha$. By Lemma 3.3, $|\mathbf{f}| + 1 \in \mathcal{L}(x)$. □

Lemma 3.5. *Let* M *be a local ACM with* $\alpha < \beta$. *Fix* $x \in M$, $\mathbf{f} \in \mathbf{F}(x)$, *and suppose that*

$$r(\mathbf{f}) \geq K = (\beta - \alpha)\left\lceil \frac{\beta}{\alpha} \right\rceil + 1$$

Then $|\mathbf{f}| - k \in \mathcal{L}(x)$ *for some* $0 < k < \beta/\alpha$.

Proof. By Lemma 3.2 there exists $\mathbf{f}' \leq \mathbf{f}$ with $r(\mathbf{f}') \in [K, K + (\beta - \alpha) - 1]$. Set $r = r(\mathbf{f}')$ and write $r = t\beta - \alpha + s$ for some $0 \leq s < \beta$. Note that

$$(\lceil \beta/\alpha \rceil - 2)\,\beta - \alpha + (\beta - 1) < K$$

since $\alpha\lceil \beta/\alpha \rceil < \beta + \alpha + 2$, and thus $t \geq \lceil \beta/\alpha \rceil - 1$. Also,

$$\beta \left\lceil \frac{\beta}{\alpha} \right\rceil - \alpha \geq K + (\beta - \alpha) - 1,$$

with equality holding if and only if α divides β. Thus, we always have $t = \lceil \beta/\alpha \rceil - 1$, with one possible exceptional case: α divides β, $t = \beta/\alpha$ and $s = 0$.

Set $q = \lceil (\alpha + r)/\beta \rceil$, so that $q = t$ if $s = 0$ and $q = t + 1$ if $s > 0$. We claim that $r > q(\beta - \alpha)$. If $s = 0$, the desired inequality reduces to $t > 1$. Since $\beta - \alpha < K$, we cannot have $r = \beta - \alpha$ and so $t > 1$.

On the other hand, if $s > 0$ then the desired inequality reduces to showing that $s > \beta - t\alpha$. Recall that in this case $t = \lceil \beta/\alpha \rceil - 1$, so we must show that $s > \beta + \alpha - \alpha\lceil \beta/\alpha \rceil$. But

$$(\beta - \alpha) \left\lceil \frac{\beta}{\alpha} \right\rceil < K \leq r = \left(\left\lceil \frac{\beta}{\alpha} \right\rceil - 1 \right) \beta - \alpha + s$$

from which we obtain our desired inequality. Thus $q < r/(\beta - \alpha) \leq |\mathbf{f}'|$.

Pick a factor y of x such that $\mathbf{f}' \in \mathbf{F}(y)$. Then $v_p(y) = \beta|\mathbf{f}'| - r = \beta(|\mathbf{f}'| - q) + q\beta - r$ and

$$y = (p^\beta)^{|\mathbf{f}'| - q} z,$$

where $v_p(z) = q\beta - r \geq \alpha$. Hence we can factor y into $|\mathbf{f}'| - q + k$ irreducibles, for some $1 \leq k \leq \lfloor (q\beta - r)/\alpha \rfloor$. But x/y can be factored into $|\mathbf{f} - \mathbf{f}'|$ many irreducibles so we have a factorization of x of length $|\mathbf{f}| - (q - k)$.

We are left with verifying that $0 < q - k < \beta/\alpha$. First, observe that when $s = 0$, $q - k \leq q - 1 = t - 1 < \lceil \beta/\alpha \rceil$. When $s > 0$, $q - k \leq q - 1 = t < \lceil \beta/\alpha \rceil$ since the exceptional case when $t = \beta/\alpha$ occurs precisely when $s = 0$. Thus $q - k < \beta/\alpha$. For the other inequality, recall that $q < r/(\beta - \alpha)$, and so $(q\beta - r)/\alpha < q$. Applying the floor function to both sides, we still have a strict inequality (since $q \in \mathbb{Z}$), so

$$q - k \geq q - \left\lfloor \frac{q\beta - r}{\alpha} \right\rfloor > 0.$$

Therefore $0 < q - k < \beta/\alpha$, as desired. □

Theorem 3.6. *If M is a local ACM and $\alpha < \beta$, then $\Delta(M)$ is nonempty and* $\max \Delta(M) < \beta/\alpha$.

Proof. $\Delta(M)$ is nonempty since $\beta > 1$. Let K be defined as in Lemma 3.5 and fix $x \in M$. Since the values of r on $\mathbf{F}(x)$ depend only on $v_p(x)$ and the

length of a given factorization, we will treat r as a function on $\mathcal{L}(x)$. Set

$$\mathcal{L}_+(x) = \{l \in \mathcal{L}(x) : r(l) \geq K\} = \left\{ l \in \mathcal{L}(x) : l \geq \frac{v_p(x)+K}{\beta} \right\}, \text{ and}$$
$$\mathcal{L}_-(x) = \{l \in \mathcal{L}(x) : r(l) \leq -\alpha\} = \left\{ l \in \mathcal{L}(x) : l \leq \frac{v_p(x)-\alpha}{\beta} \right\},$$

and let $\mathcal{L}_0(x)$ be the complement of $\mathcal{L}_+(x) \cup \mathcal{L}_-(x)$ in $\mathcal{L}(x)$.

If $\mathcal{L}_+(x)$ is nonempty, then Lemma 3.5 implies that consecutive values in $\mathcal{L}_+(x)$ are spaced less that β/α apart. This lemma also shows in this case that $\mathcal{L}_0(x) \neq \varnothing$ and the distance between $\min \mathcal{L}_+(x)$ and $\max \mathcal{L}_0(x)$ is less than β/α. If $\mathcal{L}_-(x)$ is nonempty, then Lemma 3.3 actually implies $[\min \mathcal{L}_-(x), \max \mathcal{L}_-(x) + 1] \subseteq \mathcal{L}(x)$. In particular, $\mathcal{L}_0(x) \neq \varnothing$ since in this case $\max \mathcal{L}_-(x) + 1 \in \mathcal{L}_0(x)$. Lastly, note that

$$\mathcal{L}_0(x) \subseteq \left(\frac{v_p(x)-\alpha}{\beta}, \frac{v_p(x)+K}{\beta} \right),$$

which is an open interval in $\mathbb{R}$ of length strictly less than $\lceil \beta/\alpha \rceil$. Therefore any values in $\mathcal{L}_0(x)$ are less than β/α apart. All these cases combine to show that $\max \Delta(x) < \beta/\alpha$. □

3.2. The Determination of $\Delta(M)$ in the local case. In the previous section it was proven that if M is a local ACM with $\alpha = \beta$ then either $\Delta(M) = \varnothing$ or $\Delta(M) = \{1\}$ (depending on whether $\alpha = \beta = 1$ or $\alpha = \beta > 1$, respectively). Moreover, we found a general upper bound for $\Delta(M)$ when M is a local ACM. It remains then to prove only the last claim of Theorem 3.1. Throughout this section we will assume that $\alpha < \beta$ and we will also denote the multiplicative order of p modulo m by ω.

Lemma 3.7. *If $\beta = \omega$ then $[1, \delta] \subseteq \Delta(M)$ where $\delta = \lceil \beta/\alpha \rceil - 1$.*

Proof. Let $\gamma \in [\alpha, \beta)$ and choose distinct rational primes q, r which are not equal to p and such that $q \equiv p^{-\alpha} \bmod m$ and $r \equiv p^{-\gamma} \bmod m$. Set

$$t = \left\lceil \frac{\beta - \gamma}{\alpha} \right\rceil + 1,$$

so that $\alpha t - \beta + \gamma \in [\alpha, 2\alpha)$. Consider $x = p^{\alpha t + \gamma} q^t r$ and note that $x \in M$. Furthermore, we have irreducible factorizations

$$x = (p^\alpha q)^t (p^\gamma r) = (p^\beta)(p^{\alpha t - \beta + \gamma} q^t r)$$

which are of lengths $t + 1$ and 2, respectively.

Suppose that y is an irreducible factor of x in M and write $y = p^v q^i r^j$ where $i \in [0, t]$ and $j \in [0, 1]$. Since $y \equiv 1 \bmod m$ and β is the order of p modulo m by hypothesis we must also have $v \equiv i\alpha + j\gamma \bmod \beta$. From this we infer the following:

- If $i = j = 0$, then $v = \beta$ and $y = p^\beta$.
- If $i = 0$ and $j = 1$, then $v = \gamma$ and $y = p^\gamma r$.
- If $i > 0$ then $v < 2\alpha$. Otherwise $p^\alpha q$ properly divides y in M.

Assume that $i > 0$ so that $v \in [\alpha, 2\alpha)$. Let S be the set of residue classes $[\alpha, 2\alpha) + \beta\mathbb{Z}$ and note that we must have $\alpha i + \gamma j + \beta\mathbb{Z} \in S$. We have two cases:

- If $j = 0$, then $\alpha i + \beta\mathbb{Z} \in S$, so either $i = 1$ or $\alpha i \geq \alpha + \beta$. In the latter case, we see that since $i \leq t$, $\alpha t \geq \alpha + \beta$, but this contradicts the choice of t, as then $\alpha t - \beta + \gamma \geq 2\alpha$.
- If on the other hand $j = 1$, then $\alpha i + \gamma + \beta\mathbb{Z} \in S$. Since $\gamma \geq \alpha$, we have $\alpha i + \gamma \geq \alpha + \beta$, and it follows that $i \geq \frac{1}{\alpha}(\beta - \gamma) + 1$, whence $i = t$ by the choice of t.

Combining all of these arguments we find that the irreducible divisors of x in M are precisely $p^\gamma r$, $p^\alpha q$, p^β, and $p^{\alpha t - \beta + \gamma} q^t r$. It is clear from counting r's and q's that the only two factorizations of x are the two already described. Therefore $\Delta(x) = \{t - 1\}$.

We conclude that

$$\left\{ \left\lceil \frac{\beta - \gamma}{\alpha} \right\rceil : \gamma \in [\alpha, \beta) \right\} \subseteq \Delta(M),$$

but the set on the left-hand side is exactly $[1, \delta]$, as desired. □

Lemma 3.8. *If $\beta \geq 2\alpha - 1$ then $\beta = \omega$.*

Proof. Set $\beta = k\omega$. By the minimality of $\beta \geq \alpha$, $(k-1)\omega \leq \alpha - 1$. Combining this with the assumed bound on β,

$$\omega = k\omega - (k-1)\omega \geq (2\alpha - 1) - (\alpha - 1) = \alpha$$

so that $\beta = \omega$. □

Theorem 3.9. *If $\alpha < \beta$ then $\Delta(M) = [1, \beta/\alpha)$.*

Proof. Let $\delta = \lceil \beta/\alpha \rceil - 1$ so that $[1, \delta] = [1, \beta/\alpha)$. By Theorem 3.6, $\Delta(M) \subseteq [1, \delta]$. If $\beta = \omega$, then $[1, \delta] \subseteq \Delta(M)$ by Lemma 3.7.

If on the other hand $\beta \neq \omega$, we see that $\beta \leq 2(\alpha - 1)$ by Lemma 3.8, so $\delta = 1$. Because $\Delta(M)$ is nonempty (as $1 \leq \alpha < \beta$), equality must hold in the inclusion $\Delta(M) \subseteq [1, \delta] = \{1\}$. □

4. The Δ-set of a global ACM

Any singular ACM can be decomposed as an intersection of local ACMs. In particular, if we factor $\gcd(a, b) = d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ then

$$M_{a,b} = \bigcap_{i=1}^{n} M_{a_i, b/q_i}$$

where $q_i = \prod_{j \neq i} p_j^{\alpha_j}$, and a_i is the least positive residue of a modulo b/q_i. Each of the terms in this intersection is easily seen to be local by results in Section 2. Furthermore, this local decomposition is unique by the Chinese Remainder Theorem. Though this decomposition always exists, a mathematical relationship between $\Delta(M \cap N)$ and $\Delta(M), \Delta(N)$ may not exist. If N is a general submonoid of M, the factorization properties of M and N might be substantially different, since it is not always the case, for example, that $\mathcal{A}(N) = \mathcal{A}(M) \cap N$. However, $\mathcal{A}(N) = \mathcal{A}(M) \cap N$ if N is divisor-closed in M.

In Section 3 we often made use of the fact that p^β is irreducible in the local ACM M. In the global case we will employ a similar strategy. For any monoid M let $\mathfrak{s}_M$ be the set of all $x \in M$ such that for all $y \in M \setminus M^\times$ there exists $t \in \mathbb{N}$ with $x \mid_M y^t$; this is the *singularity* of M. One can check that $\mathfrak{s}_M$ is a divisor-closed submonoid of M. In fact, if N is a divisor-closed submonoid of M and $M^\times \leq N \leq \mathfrak{s}_M$, then either $N = M^\times$ or $N = \mathfrak{s}_M$. Hence, if $\mathfrak{s}_M \neq M^\times$, $\mathfrak{s}_M$ is the minimal nontrivial divisor-closed submonoid of M.

Now, if M is an ACM and N is a divisor-closed submonoid of M, then $N = \langle P \rangle_\times \cap M$ where $\mathbb{P}(d) \subseteq P \subseteq \mathbb{P} \setminus \mathbb{P}(m)$. In particular, $\mathfrak{s}_M = \langle \mathbb{P}(d) \rangle_\times \cap M$. Thus, $\mathfrak{s}_M = M^\times = \{1\}$ when M is a regular ACM. In a local ACM, $\mathfrak{s}_M$ is nontrivial and finitely generated since

$$\mathcal{A}(\mathfrak{s}_M) = \mathcal{A}(M) \cap \mathfrak{s}_M = \{p^{\beta + k\omega} : 0 \leq k < \alpha/\omega\}.$$

In the global case, $\mathcal{A}(\mathfrak{s}_M)$ is actually infinite, as we will see below. This provides an algebraically significant distinction between the regular, local, and global cases as they correspond precisely to when $\mathfrak{s}_M$ is trivial, finitely generated, or not finitely generated.

For the remainder of this section we will assume that $M = M_{a,b}$ is a global ACM where $d = \gcd(a,b) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $n > 1$, $p_1, \ldots, p_n \in \mathbb{P}$ are distinct and $\alpha_i > 0$ for each i. As before, we note that p_i does not divide m, so for each i we will fix ω_i to be the multiplicative order of p_i modulo m; $\beta_i \geq \alpha_i$ will again be minimal such that $\omega_i \mid \beta_i$.

Call $y \in \mathcal{A}(\mathfrak{s}_M)$ a p_i-*amenable* irreducible if and only if $p_i^{k\omega_i} y \in \mathcal{A}(\mathfrak{s}_M)$ for each $k \in \mathbb{N}_0$. It is actually relatively easy to demonstrate the existence of such irreducibles: given $j \in [1,n]$, choose $y \in \mathcal{A}(\mathfrak{s}_M)$ of minimal p_j-adic value. If $i \neq j$, then y is p_i-amenable. Thus p_i-amenable irreducibles exist and, as a corollary, $\mathcal{A}(\mathfrak{s}_M)$ is infinite. This is precisely the feature of the global case which we will use to our advantage.

We are able to give a general condition on a monoid under which we can bound the Δ-set. Let

$$\Lambda = \{\min \mathcal{L}(x) : x \in M \setminus M^\times\}.$$

If M is not a group then this set is nonempty. If it is bounded, then we say that $\lambda = \max \Lambda + 1$ is the *critical length* of M.

Lemma 4.1. *Let M be a monoid which is not a group. If the critical length λ exists then $\Delta(M)$ is nonempty and finite with* $\max \Delta(M) \leq \lambda - 2$.

Proof. Note that any $x \in M \setminus M^\times$ with $\max \mathcal{L}(x) \leq \lambda$ has $\Delta(x) = \varnothing$ or $\max \Delta(x) \leq \lambda - 2$, so assume $\max \mathcal{L}(x) > \lambda$. Let $x_1 \cdots x_\mu$ be any factorization of x where $\mu \geq \lambda$. By the definition of λ, there is some $2 \leq k < \lambda$ and $y_1, \ldots, y_k \in \mathcal{A}(M)$ such that $x_1 \cdots x_\lambda = y_1 \cdots y_k$. Thus, $x = y_1 \cdots y_k x_{\lambda+1} \cdots x_\mu$ is an irreducible factorization of x and $\mu, \mu - (\lambda - k) \in \mathcal{L}(x)$. Since $\lambda - k \leq \lambda - 2$, the result now follows. □

If the critical length exists, then the above proof also shows that the catenary degree of M, denoted $\mathrm{c}(M)$ (see [6, Definition 1.6.1]), satisfies $\mathrm{c}(M) \leq \lambda$. Indeed, the proof shows that any factorization of some $x \in M$ can be connected by a λ-chain to a factorization of length less than λ.

Theorem 4.2. *Let M be a non-local ACM, $j \in [1, n]$, and y a p_j-amenable irreducible. Choose λ satisfying*

$$\lambda \geq \max_i \left(\frac{v_{p_i}(y)}{\alpha_i} \right) + 1, \quad \textit{and} \quad \lambda \geq \frac{2\alpha_j + \omega_j}{\alpha_j}.$$

Then $\lambda > \min \mathcal{L}(x)$ for all $x \in M \setminus M^\times$ and so M has a critical length. Furthermore, this critical length does not exceed λ.

Proof. Let $x \in M \setminus M^\times$ such that $l \in \mathcal{L}(x)$ for $l \geq \lambda$. Of course $v_{p_i}(x) \geq \lambda \alpha_i$ for each i. By the first bound on λ, $v_{p_i}(x) \geq \alpha_i + v_{p_i}(y)$ for each i and therefore $v_{p_i}(x/y) \geq \alpha_i$. We infer that $x/y \in M$ by the membership criterion.

Now find k such that $\alpha_j \leq v_{p_j}(x/y) - k\omega_j \leq \alpha_j + \omega_j - 1$. By the usual arguments, $x/p_j^{k\omega_j} y \in M$ and since

$$v_{p_j}\left(\frac{x}{p_j^{k\omega_j} y} \right) \leq \alpha_j + \omega_j - 1,$$

any factorization of $x/p_j^{k\omega_j} y$ has at most k irreducible factors where

$$k \leq \frac{\alpha_j + \omega_j - 1}{\alpha_j}.$$

Moreover, $k + 1 \in \mathcal{L}(x)$ since $p_j^{k\omega_j} y$ is irreducible in M (as y was chosen to be p_j-amenable). By the second bound on λ, $\lambda > k + 1$, so $\min \mathcal{L}(x) < \lambda$. □

The above theorem does not apply to the local case because in the local case $\mathcal{A}(\mathfrak{s}_M)$ is finite. We will now demonstrate the usefulness of Theorem

4.2 in formulating bounds for $\Delta(M)$ where M is non-local and singular. For instance, we can derive the following corollaries:

Corollary 4.3. *Let M be an ACM with $a = d = p_1p_2$. Then $\max \Delta(M) = \omega$ where ω is the order of p_1 (and p_2) modulo m.*

Proof. Note that in this case, $a = p_1p_2$ is p_1-amenable (and p_2-amenable) and since $a \equiv 1 \pmod{m}$, p_1 and p_2 necessarily have the same multiplicative order, ω, modulo m. Applying Theorem 4.2 with $y = a$ shows us that the critical length of M is less than or equal to $\lambda = \omega + 2$. Therefore, by Lemma 4.1, $\max \Delta(M) \leq \omega$. However, the element $x = p_1^{\omega+2}p_2^{\omega+2}$ has exactly two irreducible factorizations:

$$x = (p_1p_2)^{\omega+2} = (p_1^{\omega+1}p_2)(p_1p_2^{\omega+1}).$$

Hence $\Delta(x) = \{\omega\}$ and $\max \Delta(M) = \omega$. □

Corollary 4.4. *Let M be a non-local ACM. Furthermore, assume that $p_1^{\gamma_1} \cdots p_n^{\gamma_n} \in M$ where $\gamma_i \in [\alpha_i, 2\alpha_i)$ for each i and that for some j we have $\omega_j \leq \alpha_j$. Then $\Delta(M) = \{1\}$*

Proof. Set $y = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ and note that since $\gamma_i < 2\alpha_i$, y is irreducible and p_i-amenable for all $i \in [1, n]$. Applying Theorem 4.2 we see that $\lambda = 3$ is the critical length for M. Since the Δ-set of a non-local ACM is nonempty, $\Delta(M) = \{1\}$ by Lemma 4.1. □

Corollary 4.5. *Let M be a singular ACM with $a = b$. Then*

$$\Delta(M) = \begin{cases} \varnothing & \text{if } b \text{ is prime,} \\ \{1\} & \text{if } b \text{ is composite.} \end{cases}$$

Proof. This is simply a combination of results; specifically Theorem 3.1 and Corollary 4.4. □

Example 4.6. Consider $M_{6,30}$. In particular, we note that $m = 5$ and $d = 6 = (2)(3) \equiv 1 \bmod 5$. This exactly the situation in which Corollary 4.3 applies. Since 2 has multiplicative order 4 modulo 5, we see that $\max \Delta(M_{6,30}) = 4$. It is pretty easy to find witnesses to $1, 2, 3 \in \Delta(M_{6,30})$, and so $\Delta(M_{6,30}) = [1, 4]$. The local decomposition of $M_{6,30}$ is $M_{6,10} \cap M_{6,15}$, both of which have Δ-set equal to $[1, 3]$ by Theorem 3.1.□

Example 4.7. Let $M_{96,480}$. We have $d = 96$, $m = 5$, $\mathbb{P}(d) = \{2, 3\}$, $\boldsymbol{\alpha} = (5, 1)$, and $\boldsymbol{\omega} = (4, 4)$ (where $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$ are vectors defined in the obvious manner). Since $d = 96 \in M_{96,480}$ and $4 = \omega_1 \leq \alpha_1 = 5$, we can conclude by Corollary 4.4 that $\Delta(M_{96,480}) = \{1\}$. Again, we decompose M into local ACMs: $M_{96,480} = M_{96,160} \cap M_{6,15}$. Applying Theorem 3.1, $\Delta(M_{96,160}) = \{1\}$ and $\Delta(M_{6,15}) = [1, 3]$.□

In the local case, the values α and ω are sufficient to retrieve $\Delta(M)$. Thus, one might hope that $\Delta(M)$ is determined by $\boldsymbol{\alpha}, \boldsymbol{\omega}$ in the global case. This is not the case as the next example illustrates.

Example 4.8. Let $M = M_{56,70}$ and $N = M_{6,30}$. Making the usual preliminary calculations, we see that $(\boldsymbol{\alpha}_M, \boldsymbol{\omega}_M, m_M) = (\boldsymbol{\alpha}_N, \boldsymbol{\omega}_N, m_N)$. Despite these similarities, we claim that

$$\max \Delta(M) < 4 = \max \Delta(N).$$

Proof. Using Theorem 4.2 with $y = 56 = 2^3 7$ (which is 2-amenable), we see that the critical length for M is at most 6. Suppose we have an $x \in M$ and an $l \geq 2$ such that $l, l+4 \in \mathcal{L}(x)$. We wish to show that $l+1$, $l+2$, or $l+3$ is also in $\mathcal{L}(x)$. Let $x_1 \cdots x_{l+4}$ be a factorization of length $l+4$ and let y be the product of the first 6 irreducibles in this factorization.

By the definition of λ, $\min \mathcal{L}(y) < 6$. If y has a factorization of length $5, 4$ or 3, then we are done because that yields a factorization of x of a desired length. So let us assume that y has a factorization of length 2, say $y = y_1 y_2$.

For $x \in M \setminus M^\times$, let $\mu(x) = \min\{v_2(x), v_7(x)\}$. Then since $2^2 7^2$ is an element of M (and in fact is irreducible) and $\boldsymbol{\alpha} = (1, 1)$, we conclude that $\mu(x) \leq 2$ for all $x \in \mathcal{A}(M)$. Moreover, since $2^3 7$ and $2 \cdot 7^3$ are also both (irreducible) elements of M, if $x \in \mathcal{A}(M)$ and $\mu(x) = 2$, then

$$\big(v_2(x), v_7(x)\big) \in \{(2,2), (2,3), (3,2)\}.$$

Observe that $v_2(y) = v_2(y_1) + v_2(y_2) \geq 6$ and $v_7(y) = v_7(y_1) + v_7(y_2) \geq 6$. Suppose for contradiction that $\mu(y_1) = 2$ and without loss of generality, assume $v_2(y_1) = 2$. Then $v_2(y_2) \geq 4$, so it must be that $\mu(y_2) = 1$. This implies that $v_7(y_2) = 1$ and so $v_7(y_1) \geq 5$, which contradicts the irreducibility of y_1. Therefore $\mu(y_1) = \mu(y_2) = 1$. Without loss, assume $v_2(y_1) = 1$ so that $v_7(y_1), v_2(y_2) \geq 5$. We may therefore write $y_1 = 2^4 z_1$ and $y_2 = 7^4 z_2$. Note that $14 \mid_{\mathbb{N}} z_1, z_2$ and $2^4 \equiv 7^4 \equiv 1 \mod 5$, so we infer that $z_1, z_2 \in \mathcal{A}(M)$ by Corollary 2.2. Therefore $y = (14^2)^2 z_1 z_2$ is a factorization of y of length 4, completing the argument. □

From the preceding example we may conclude that the values of $\boldsymbol{\alpha}, \boldsymbol{\omega}, m$ are insufficient to determine $\Delta(M)$. This suggests that the case breakdown involved in determining the Δ-set of an arithmetical congruence monoid becomes rather intricate as n grows.

Acknowledgment

The authors wish to thank the referee for many helpful comments and suggestions.

References

[1] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189**(1997), 1–29.

[2] M. Banister, S. T. Chapman, J. Chaika, and W. Meyerson, On a result of James and Niven concerning unique factorization in congruence semigroups, to appear in *Elemente der Mathematik*.

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

[4] C. Bowles, S.T. Chapman, N. Kaplan, and D. Reiser. On Δ-sets of numerical monoids, *J. Pure Appl. Algebra* **5**(2006), 1–24.

[5] S. T. Chapman and A. Geroldinger, Krull domains and their monoids, their sets of lengths, and associated combinatorial problems, *Lecture Notes in Pure and Applied Mathematics* **189**(1997), 73–112.

[6] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

[7] A. Geroldinger and F. Halter-Koch, Congruence monoids, *Acta Arith.* **112**(2004), 263–296.

[8] F. Halter-Koch, C-monoids and congruence monoids in Krull domains, *Lect. Notes Pure Appl. Math.* **241**(2005), 71-98.

[9] R. D. James and I. Niven, Unique factorization in multiplicative systems, *Proc. Amer. Math. Soc.* **5**(1954), 834–838.

University of California at Berkeley, Department of Mathematics, Berkeley, California 94720
E-mail : `baginski@math.berkeley.edu`

Trinity University, Department of Mathematics, One Trinity Place, San Antonio, TX. 78212-7200
E-mail : `schapman@trinity.edu`

Carnegie Mellon University, Department of Mathematical Sciences, Pittsburgh, PA 15213
E-mail : `gschaeff@andrew.cmu.edu`