Arithmetic Congruence Monoids: A Survey

Paul Baginski and Scott Chapman

Abstract We consider multiplicative monoids of the positive integers defined by a single congruence. If a and b are positive integers such that $a \leq b$ and $a^2 \equiv a \mod b$, then such a monoid (known as an arithmetic congruence monoid or an ACM) can be described as $M_{a,b} = (a + b\mathbb{N}_0) \cup \{1\}$. In lectures on elementary number theory, Hilbert demonstrated to students the utility of the proof of the Fundamental Theorem of Arithmetic for $\mathbb{Z}$ by considering the arithmetic congruence monoid with $a = 1$ and $b = 4$. In $M_{1,4}$, the element 441 has a nonunique factorization into irreducible elements as $9 \cdot 49 = 21^2$. ACMs have appeared frequently in the mathematical literature over the last decade. While their structures can be understood merely with rational number theory, their multiplicative behavior can become quite complex. We show that all ACMs fall into one of three mutually exclusive classes: regular (relating to $a = 1$), local (relating to $\gcd(a,b) = p^k$ for some rational prime p), and global ($\gcd(a,b)$ is not a power of a prime). In each case, we examine the behavior of various invariants widely studied in the theory of nonunique factorizations. Our principal tool will be the construction of transfer homomorphisms from the $M_{a,b}$ to monoids with simpler multiplicative structure.

Key words: monoid, arithmetic progressions, nonunique factorization, elasticity of factorization, Krull monoids

Early in the study of number theory, one encounters the obstacle of nonunique factorization, since elements in many rings of algebraic integers do not always factor uniquely into products of irreducible elements. The multiplicative structure of these number rings has been classically used to demonstrate the prickly issue of nonunique factorization. However, we can also exhibit the phenomenon of nonunique factorization using a common object from additive number theory, arithmetic progressions. An **arithmetic congruence monoid (ACM)** is an arithmetic

Department of Mathematics and Statistics, Smith College, Northampton, MA 01063, USA.
Department of Mathematics and Statistics, Sam Houston State University, Huntsville, TX 77341, USA.

progression which naturally possesses a multiplicative structure. Specifically, an arithmetic congruence monoid is the monoid:[1]

$$M_{a,b} = (a + b\mathbb{N}_0) \cup \{1\} = \{1\} \cup \{a, a+b, a+2b, \ldots\},$$

where a and b are positive integers satisfying $0 < a \leq b$ and $a^2 \equiv a \mod b$. The congruence demanded upon a and b is both sufficient and necessary for the arithmetic progression $a + b\mathbb{N}_0$ to be closed under multiplication. The trivial values $a = 1$ or $a = b$ satisfy this congruence for any $b \geq 1$, but nontrivial pairs, such as $a = 4$ and $b = 6$, also exist. In general, for a given b, there are 2^r choices for a with $0 < a \leq b$, where r is the number of distinct primes dividing b (cf. Section 4).

As we shall describe in this survey, ACMs exhibit both unique and nonunique factorization of elements, exhibiting the widely varying behavior one encounters in algebraic number rings, as well as some more pathological behavior such as the *bifurcus* property (cf. Section 2). In contrast to number rings, however, very little mathematical background is necessary to grasp the idea of an ACM and uncover many of its factorization properties. As such, ACMs can be a valuable pedagogical tool, since arguments can often be phrased with elementary arithmetic and without resorting to norms or other mathematical machinery to determine, say, whether an element is irreducible. Despite the low barrier to initiating the study of ACMs, their factorization theory is surprisingly complex: many questions remain open and the finer study of the factorizations often requires more involved number theoretic and combinatorial arguments. We therefore present ACMs as both an alternative and a complement in number theory to the study of nonunique factorization in algebraic number rings.

After a brief section introducing terms and notation from the theory of nonunique factorizations, we proceed with the study of factorization in ACMs. ACMs naturally divide into three classes (regular, singular local, singular global), each exhibiting starkly different behavior due to their connections with other classes of monoids. In Section 2, we consider the class of ACMs where $a = b$. The special case where $a = b = p^r$, for p a rational prime, is fully described in Proposition 2.2. In Proposition 2.3 we generalize the argument to the case where $a = b$ is not a power of a prime. Section 3 considers the case of **regular** ACMs, which are those with $a = 1$. In Theorem 3.2, we show that these ACMs are special in the sense that they belong to the class of **Krull monoids** (cf. Definition 1.3). Using this Krull structure, Theorem 3.4 gives a striking overview of the factorization properties of these monoids. In Section 4, we consider the case where $a \neq 1$. Such ACMs are called **singular** and include the ACMs of Section 2. The singular ACMs break into two subclasses: 1) **local** ACMs where $\gcd(a,b) = p^k$ for p a rational prime, and 2) **global** ACMs where $\gcd(a,b)$ is not a power of a prime. After the development of some machinery applicable to all singular ACMs, we analyze the local case in Theorem 4.9. We show in Lemma 4.15 that for each global ACM $M_{a,b}$ there is a constant λ such that every

[1] Several authors define $M_{a,b}$ to equal just the arithmetic progression, so that it is a semigroup. We shall include a unity, since it does not affect the structure but allows the factorization-theoretic definitions to be simpler and coincide with the literature.

nonunit of $M_{a,b}$ has an irreducible factorization of length at most λ. While this behavior is more unruly than the behavior encountered in algebraic number rings, there are still commonalities. For example, in Theorem 4.17, we demonstrate that in a global ACM there is a finite bound N such that for every element, if we have two factorizations whose lengths differ by more than N, then there is a factorization of that element whose length lies between the two other lengths.

1 Terms and Notation

The following notation draws from the theory of nonunique factorizations of rings and monoids; see the monograph [18] of Geroldinger and Halter-Koch for comprehensive references and for undefined terms. The symbol $\mathbb{N}$ denotes the natural numbers $\{1,2,3,\ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. The integers are denoted $\mathbb{Z}$ and for $n \in \mathbb{Z}$, $\mathbb{Z}_n$ denotes the quotient ring $\mathbb{Z}/n\mathbb{Z}$. The image of $x \in \mathbb{Z}$ in $\mathbb{Z}_n$ shall be denoted $\bar{x}$. If $\gcd(k,n) = 1$, then $\mathrm{ord}_k(n)$ shall denote the order of $\overline{n}$ in the group of units of $\mathbb{Z}_k$, which we denote by $\mathbb{Z}_k^\times$. We use $\varphi(n)$ to denote the Euler totient function of n. We open by formally defining the objects we are about to study.

Definition 1.1 *Given $a,b \in \mathbb{N}$ with $0 < a \leq b$ and $a^2 \equiv a \mod b$, the* **arithmetic congruence monoid** *defined by a and b is,*

$$M_{a,b} := \{n \in \mathbb{N} \,|\, n \equiv a \mod b\} \cup \{1\}.$$

We note that for any a and b satisfying Definition 1.1, $M_{a,b}$ is both commutative and cancellative.

We state the main definitions and notation for the theory of nonunique factorizations in terms of a general commutative cancellative monoid. In such a general monoid M, if $x,y \in M$ then x divides y (written $x|y$) if there exists a $z \in M$ such that $xz = y$. We will write $|_M$ when we need to distinguish monoids; most commonly we will use $|_{\mathbb{N}}$ for the regular "divides" relation in the natural numbers and reserve $|$ for the "divides" relation in our arithmetic congruence monoids $M_{a,b}$. If M is a monoid, $M^\times$ will denote the units of M. A nonunit $x \in M$ is **irreducible** (or an **atom**) if whenever $x = yz$ for some $y,z \in M$, then either y or z is a unit. We write $\mathscr{A}(M)$ for the set of irreducibles of M. A nonunit $x \in M$ is **prime** if whenever $x|yz$ for some $y,z \in M$, either $x|y$ or $x|z$. As in the theory of integral domains, prime elements are irreducible but not vice versa.

A monoid M is **atomic** if every nonunit x can be written as a product of irreducibles of M. The Fundamental Theorem of Arithmetic states that $(\mathbb{N},\times)$ is atomic (and furthermore that the factorizations into irreducibles are unique). Since $M_{a,b}$ is a submonoid of the unique factorization monoid $(\mathbb{N},\times)$, its atomicity is immediate. Indeed, if $x \in M_{a,b}$, then $x = p_1 \cdots p_n$, a unique product of prime numbers in $\mathbb{N}$, and so x can be written as a product of at most n elements of $M_{a,b}$. For the rest of the article, all monoids will be assumed to be atomic.

If every nonunit $x \in M$ has a unique factorization into irreducibles of M, then M is said to be **factorial**. M is factorial if and only if all its irreducibles are prime. M is factorial if and only if it is isomorphic to the free abelian monoid over its irreducibles. When M is factorial, the greatest common divisor is well defined: given a finite, nonempty $X \subseteq M$, $\gcd(X)$ is the unique (up to associates) element $g \in M$ such that $g|x$ for all $x \in X$ but for each nonunit $h \in M$, there is an $x \in X$ such that $gh \not| x$.

For $x \in M \setminus M^\times$, we define

$$\mathscr{L}(x) = \{ n : \text{there are } \alpha_1, \ldots, \alpha_n \in \mathscr{A}(M) \text{ with } x = \alpha_1 \cdots \alpha_n \},$$

which is known as the **set of lengths of** x. We collect these sets together as $\mathscr{L}(M) = \{ \mathscr{L}(x) : x \in M \setminus M^\times \}$, the set of lengths of M. The ratio $\rho(x) = \sup \mathscr{L}(x) / \min \mathscr{L}(x)$ is called the **elasticity** of x. The elasticity of the monoid M is defined by

$$\rho(M) = \sup\{ \rho(x) : x \in M \setminus M^\times \}$$

(see [18, Chapter 1.4] or the survey paper [4]). If $\rho(M) = 1$, then M is called **half-factorial**. A survey of half-factorial integral domains and monoids can be found in [12]. M is said to be **fully elastic** if for every rational q with $1 \leq q < \rho(M)$, there exists an $x \in M \setminus M^\times$ such that $\rho(x) = q$. Many common objects of study in factorization theory are fully elastic (for instance, the ring of integer-valued polynomials [15]), but numerical monoids (cf. Definition 2.1) are not ([14]). If there exists an $x \in M \setminus M^\times$ such that $\rho(M) = \rho(x)$, then the elasticity of M is said to be **accepted**. Rings of algebraic integers have accepted elasticity. Non-examples also exist (see [10] and later our Example 4.10), even ones having rational elasticity that is not accepted. However, these non-examples do not abound in the literature.

Given $x \in M \setminus M^\times$, write its length set in increasing order as

$$\mathscr{L}(x) = \{n_1, n_2, \ldots, n_k\},$$

where $n_i < n_{i+1}$ for $1 \leq i \leq k-1$. The **delta set** of x is defined by $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq k$ and the **delta set** of M by

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

(see again [18, Chapter 1.4]). As with elasticity, the study of the delta sets of particular monoids has an active history, and various calculations in specific cases can be found in [7] and [11].

As in any field of mathematics, we wish to reduce the study of complex objects into questions about simpler objects. In the realm of factorization theory, the collapsing of structure is achieved using the concept of transfer homomorphisms.

Definition 1.2 *Let M and N be commutative, cancellative, atomic monoids and $\sigma : M \to N$ be a monoid homomorphism. The map σ is a* **transfer homomorphism** *if*

- $\sigma(u) \in N^\times$ *for any* $u \in M^\times$,

- $\sigma(x) \notin N^\times$ *for any* $x \notin M^\times$,
- *(Surjectivity up to associates) For every* $a \in N$, *there exists a unit* $u \in N^\times$ *and an* $x \in M$ *such that* $\sigma(x) = ua$, *and*
- *whenever* $x \in M$ *and* $a, b \in N$ *such that* $\sigma(x) = ab$, *there exist* $y, z \in M$ *and units* $u, v \in N^\times$ *such that* $x = yz$, $\sigma(y) = ua$, *and* $\sigma(z) = vb$.

Intuitively, a transfer homomorphism from M to N ensures that N has (up to noise from units) all the basic factorization theory of M. Specifically, divisibility relations from M are preserved in N and $\mathscr{L}_M(x) = \mathscr{L}_N(\sigma(x))$ for all $x \in M$, so that by surjectivity up to associates, $\mathscr{L}(M) = \mathscr{L}(N)$. The cost of a transfer homomorphism lies in forgetting which exact factors appear in factorizations. Indeed, for factorization properties not concerned solely with length sets, this can be a true concern. As we shall see in Section 2, the ACM $M_{2,2}$ (namely, the even numbers along with 1) is half-factorial but not factorial. Nonetheless, $M_{2,2}$ has a transfer homomorphism into the free monoid $(\mathbb{N}_0, +)$, which is factorial. A more surprising example occurs in Section 3, where the half-factorial ACM $M_{1,4}$ has a transfer homomorphism into the factorial monoid $\mathscr{B}(\mathbb{Z}_4^\times)$ (defined in that section). There are other factorization invariants, such as the catenary and tame degrees, which also require extra care under this caveat, but for the scope of the concepts under review in this survey, only the distinction between factoriality and half-factoriality merits vigilance. In all cases we shall encounter, the presence or lack of unique factorization can be easily verified. Thus for our purposes, other than this minor exception, one can consider transfer homomorphisms as indicating that M and N have the same factorization-theoretic properties.

As we shall see, many ACMs can be reduced to other better studied monoids in much the same way as the factorization theory of algebraic number rings transfers to simpler combinatorial monoids over the class group (see [5] for an introductory exposition on algebraic number rings from the perspective of nonunique factorization theory).

A similar concept to that of a transfer homomorphism is that of a divisor theory.

Definition 1.3 *Let* M *be a monoid. A* **divisor theory** *for* M *is a free commutative monoid* $\mathscr{F}(P)$ *and a monoid homomorphism* $\sigma : M \to \mathscr{F}(P)$ *satisfying the following properties:*

- $\sigma(u) = 1$ *for any* $u \in M^\times$.
- $\sigma(u) \neq 1$ *for any* $u \notin M^\times$.
- *For any nonunits* $x, y \in M$, $\sigma(x) | \sigma(y)$ *implies* $x | y$.
- *For every* $p \in P$, *there is a finite subset* $X \subseteq M$ *such that* $p = \gcd(\sigma(X))$.

A monoid M *which has a divisor theory is said to be a* **Krull monoid**. *The generators* P *are said to be the* **prime divisors** *of* M *and the quotient monoid* $\mathscr{F}(P)/\sigma(M)$ *(which can be shown to be an abelian group) is known as the* **class group** *of* M.

Krull monoids abound in mathematics. For instance, if D is a Dedekind domain, $D \backslash \{0\}$ is a Krull monoid under multiplication. Hence, the multiplicative monoid of a ring of algebraic integers is a Krull monoid. The definition of a Krull domain, usually given via v-ideals, can be restated more simply using Krull monoids as follows:

an integral domain is a Krull domain if and only if its multiplicative monoid is a Krull monoid (see [23]).

The distinctions between a divisor theory and a transfer homomorphism are subtle. First, a divisor theory need not be (and usually is not) surjective. More subtly, the property that $\sigma(x)|\sigma(y)$ implies $x|y$ is not a consequence of the last property of a transfer homomorphism. For both transfer homomorphisms and divisor theories, if $\sigma(x) \neq \sigma(y)$, then $\sigma(x)|\sigma(y)$ implies $\sigma(y)$ is reducible and thus so is y. Yet, unlike a divisor theory, a transfer homomorphism does not guarantee a choice of x as a witness to the reducibility of y in M.

2 Multiples

The simplest of all ACMs are those in which $a = b$ (i.e. $M_{a,b} = b\mathbb{N} \cup \{1\}$), the set of positive multiples of b along with the element 1. If $b = 1$, then $M_{a,b} = \mathbb{N}$, which has unique factorization, so let us assume $b > 1$. Our analysis shall divide into two cases, when b is a power of a prime and when it is not.

If $b = p^r$, where p is a prime and $r \geq 1$, then all nonunits of $M_{a,b}$ must be divisible in $\mathbb{N}$ by p^r. Therefore an element $x \in M_{a,b}$ is reducible if and only if $p^{2r}|_{\mathbb{N}} x$. This simple observation leads to a complete characterization of M_{p^r,p^r} in terms of another, well-studied monoid known as a numerical monoid.

Definition 2.1 *Given $x_1, \ldots, x_n \in \mathbb{N}$, the* **numerical monoid** *generated by $x_1, \ldots, x_n$, denoted $\langle x_1, \ldots, x_n \rangle$, is the set of nonnegative linear combinations of the x_i. In other words,*

$$\langle x_1, \ldots, x_n \rangle = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; a_i \in \mathbb{N}_0 \right\}.$$

Numerical monoids have deceptively complicated combinatorial structure. For instance, if the generators are minimal and have no common factor, there is a least integer not contained in the numerical monoid. This integer is known as the Frobenius number, and while formulas exist for the Frobenius number of a two- or three-generator numerical monoid, computation of the Frobenius number in general is NP-hard. The interested reader may consult [24], a recent reference work on numerical monoids and their occurrence in mathematics. For our purposes, we will only need to explore a particularly simple and very well-understood class of numerical monoids: those generated by a full interval of integers, $\{r, r+1, \ldots, 2r-1\}$. In this case, set

$$S_r := \langle r, r+1, \ldots, 2r-1 \rangle = (r + \mathbb{N}_0) \cup \{0\}.$$

The Frobenius number of S_r is clearly $r-1$. Though this monoid may resemble an ACM, bear in mind that the operation on numerical monoids is addition, while it is multiplication for ACMs.

Proposition 2.2 *Let p be prime and $r \geq 1$. The map*

$$\sigma : M_{p^r,p^r} \to S_r = \langle r, r+1, \ldots 2r-1 \rangle$$

defined by

$$\sigma(x) = \mathsf{v}_p(x),$$

where $\mathsf{v}_p(x)$ is the p-adic valuation of $x \in \mathbb{N}$, is a transfer homomorphism. Therefore we have the following.

1. *Given a nonunit $x \in M_{p^r,p^r}$,*

$$\mathscr{L}(x) = \left\{ \ell \in \mathbb{N} \;\middle|\; \left\lceil \frac{\mathsf{v}_p(x)}{2r-1} \right\rceil \leq \ell \leq \left\lfloor \frac{\mathsf{v}_p(x)}{r} \right\rfloor \right\}.$$

2. *The elasticity is given by $\rho(M_{p^r,p^r}) = \frac{2r-1}{r}$ and is accepted.*
3. *M_{p^r,p^r} is not fully elastic, unless $r = 1$.*
4. *M_{p^r,p^r} is half-factorial if and only if $r = 1$. However it is never factorial.*
5. *$\Delta(M_{p^r,p^r}) = \{1\}$ if $r > 1$ and $\Delta(M_{p^r,p^r}) = \emptyset$ if $r = 0$.*
6. *M_{p^r,p^r} has no prime elements.*

Proof. This function σ is clearly a monoid homomorphism and $\sigma(x) = 0$ if and only if $x = 1$. Based on the membership criterion for M_{p^r,p^r}, σ clearly maps surjectively onto the numerical monoid $N = \langle r, \ldots, 2r-1 \rangle$. We now demonstrate that σ is a transfer homomorphism. Since neither M_{p^r,p^r} nor the numerical monoid have any units other than their respective identities, we have only one condition left to verify. Suppose $x \in M_{p^r,p^r}$ and $n, m \in \langle r, r+1, \ldots, 2r-1 \rangle$ such that $\sigma(x) = n+m$. By the definition of σ, $p^{n+m}|_{\mathbb{N}} x$. Since $n, m \geq r$, we find that $p^n \in M_{p^r,p^r}$ and $x/p^n \in M_{p^r,p^r}$. Thus $x = p^n(x/p^n)$, $\sigma(p^n) = n$, $\sigma(x/p^n) = m$, and σ is a transfer homomorphism.

Since σ is a transfer homomorphism, for every nonunit $x \in M_{p^r,p^r}$, $\mathscr{L}_{M_{p^r,p^r}}(x) = \mathscr{L}_N(\sigma(x)) = \mathscr{L}_N(\mathsf{v}_p(x))$. Yet for any $k \geq r$ (in particular $k = \mathsf{v}_p(x)$), the length set of k in N can easily be computed to be equal to the set on the right hand of claim 1. Such a basic computation appears in [11], where it is immediately concluded that $\rho(N) = \frac{2r-1}{r}$, so that N is half-factorial if and only if $r = 1$. When $r = 1$, clearly $\Delta(N) = \emptyset$, while $\Delta(N) = \{1\}$ when $r > 1$ (see [2] or [11]). Because σ is a transfer homomorphism, the values of all these invariants are identical for M_{p^r,p^r} and M_{p^r,p^r} is half-factorial if and only if $r = 1$. However $M_{p,p}$ is never factorial, for if q is a prime different than p, then $(pq)(pq) = p(pq^2)$ in $M_{p,p}$ and all these factors are irreducible. We note that, alternately, claim 4 follows from the main proposition of [9].

It is a general fact that all finitely-generated monoids have accepted elasticity [3, Thm. 7]; in this case, the element $2r^2 - r$ witnesses the accepted elasticity of N and hence any preimage under σ, such as p^{2r^2-r}, witnesses the accepted elasticity for M_{p^r,p^r}. Using the transfer homomorphism, we obtain that M_{p^r,p^r} is not fully elastic for $r \geq 2$ by [14, Theorem 2.2]; $M_{p,p}$ is trivially fully elastic since it is half factorial.

Lastly, we show that M_{p^r,p^r} has no prime elements. If x were a prime element of M_{p^r,p^r}, then x would be irreducible and hence have the form $p^s k$ for some $r \leq s \leq 2r-1$ and integer $k \geq 1$ relatively prime to p. Let $m, n > 1$ be integers relatively prime to x. Then $x | p^{r+s} nmk$, but x does not divide either $p^s m$ or $p^r nk$. □

Note that the prime p plays no role in the factorization properties of the monoids M_{p^r,p^r}; all the invariants can be characterized solely in terms of r, the exponent. Indeed, for any two primes p and q, $M_{p^r,p^r} \cong M_{q^r,q^r}$. This isomorphism is just the restriction to M_{p^r,p^r} of the isomorphism $\sigma : \mathbb{N} \to \mathbb{N}$ given by

$$\sigma(x) = xp^{\mathsf{v}_q(x)-\mathsf{v}_p(x)}q^{\mathsf{v}_p(x)-\mathsf{v}_q(x)},$$

which swaps all instances of p and q in the prime factorization of x. The case M_{p^r,p^r} generalizes to a corresponding prime power case in Section 4.1, known as the class of local ACMs. Even there we shall see that the prime p plays a minimal role in the factorization properties of the ACM.

In contrast, when b is not a power of a prime, factorization in $M_{b,b}$ becomes quite wild. As we shall see in Proposition 2.3, we can exploit the trick from the previous proof, which showed that M_{p^r,p^r} contains no prime elements, to show that for $M_{b,b}$ with b not a prime power, any reducible element has a factorization of length 2. These monoids are natural examples of the pathological class known as *bifurcus monoids* [1].

In the prime power case, we discovered that $M_{b,b}$ has a transfer homomorphism to a translate $r+\mathbb{N}_0$ of the unique factorization monoid $(\mathbb{N}_0,+)$. Similarly, in the case where b is not a power of a prime, we shall show the existence of a transfer homomorphism from $M_{b,b}$ to a translate $(v_1,\dots,v_n)+\mathbb{N}_0^n$ of the additive, unique-factorization monoid $(\mathbb{N}_0^n,+)$, for an appropriate $n \geq 1$.

Proposition 2.3 *Let b be a positive integer which is not a prime power. In $\mathbb{N}$, write b as $p_1^{e_1}\cdots p_n^{e_n}$, where the p_i are distinct primes and the $e_i \geq 1$ and set $N = (e_1,\dots,e_n)+\mathbb{N}_0^n$. The map*

$$\sigma : M_{b,b} \to N$$

defined by

$$\sigma(x) = (\mathsf{v}_{p_1}(x),\dots,\mathsf{v}_{p_n}(x))$$

is a transfer homomorphism. Therefore we have the following.

1. *Given a nonunit $x \in M_{b,b}$, write it in $\mathbb{N}$ as $b^k m$, with $k \geq 1$ and $b \nmid_{\mathbb{N}} m$. If x is reducible, then*
$$\mathscr{L}(x) = \{\ell \in \mathbb{N} \,|\, 2 \leq \ell \leq k\}.$$
2. *$\rho(M_{b,b}) = \infty$.*
3. *$M_{b,b}$ is not fully elastic.*
4. *$\Delta(M_{b,b}) = \{1\}$.*
5. *$M_{b,b}$ has no prime elements.*

Proof. Let $b = p_1^{e_1}\cdots p_n^{e_n}$ and N be as in the hypotheses. Clearly the map σ is a monoid homomorphism and $\sigma(x) = (0,\dots,0)$ if and only if $x = 1$. Since every element of $M_{b,b}$ is divisible by b, σ maps into N; conversely, given $(v_1,\dots,v_n) \in N$, we know that $v_i \geq e_i$ for all i and hence $x = p_1^{v_1}\cdots p_n^{v_n} \in M_{b,b}$ is a preimage of $(v_1,\dots,v_n)$ under σ. Thus σ is surjective onto N. Since $M_{b,b}$ and N have no

units besides the identity, to show σ is a transfer homomorphism, we take an arbitrary $x = p_1^{v_1} \cdots p_n^{v_n} m \in M_{b,b}$, where $\gcd(m,b) = 1$. Then $\sigma(x) = (v_1, \ldots, v_n)$. Suppose $(v_1, \ldots, v_n) = (w_1, \ldots, w_n) + (u_1, \ldots, u_n)$, where $w_i, u_i \geq e_i$ for all i. Then $y = p_1^{w_1} \cdots p_n^{w_n} m$ and $z = p_1^{u_1} \cdots p_n^{u_n}$ are preimages of $(w_1, \ldots, w_n)$ and $(u_1, \ldots, u_n)$, respectively, in $M_{b,b}$ and $x = yz$. So σ is indeed a transfer homomorphism.

All the remaining claims may be computed in N, using σ, however we shall argue them directly in $M_{b,b}$. Let p be a prime of $\mathbb{N}$ that divides b and set $v = \mathsf{v}_p(b)$. Given a nonunit $x \in M_{b,b}$, with $x = b^k m$ for some m not divisible by b, we can factor x as $b \cdots b \cdot (bm)$, a product of k irreducibles. No factorizations of x in $M_{b,b}$ may be longer, since each irreducible must be divisible by b in $\mathbb{N}$. If x is reducible, then $b^2 |_{\mathbb{N}} x$, so we write

$$x = \left(\frac{x}{b p^{\mathsf{v}_p(x) - 2v}} \right) (b p^{\mathsf{v}_p(x) - 2v}).$$

Both factors on the right are in $M_{b,b}$ since they are divisible in $\mathbb{N}$ by b. However they are irreducibles; the factor on the right is clear because b is not a power of p, while the factor on the left has a p-adic valuation of v, so it can be divisible by b exactly once. Therefore we have shown every reducible element of $M_{b,b}$ can be written as a product of two irreducibles. Now, if x is reducible, then for any $2 < \ell < k$, we can factor x as $b \cdots b \cdot y_1 \cdot y_2$, where $y_1 y_2$ is a factorization of $b^{k-\ell+2} m$ as a product of two irreducibles (note $b^{k-\ell+2} m \in M_{b,b}$ is reducible). Thus we have produced a factorization of x of length ℓ and the length set of x has the prescribed form.

From this explicit description of the length set, the values of the elasticity and delta set of $M_{b,b}$ are immediate. It is also clear that $M_{b,b}$ is not fully elastic since $\rho(x) = k/2$ for some $k \geq 2$ for any nonunit $x \in M_{b,b}$. If $x \in M_{b,b}$ is a nonunit, then $x | (p_1 x)(p_2 x)$ but $x \nmid p_1 x$ and $x \nmid p_2 x$ since b is not a power of a prime. So $M_{b,b}$ has no prime elements. $\square$

Despite being submonoids of the unique factorization monoid $(\mathbb{N}, \times)$, these $M_{b,b}$ exhibit factorization properties very unlike the uniqueness enjoyed by $\mathbb{N}$. Yet far from being unusual submonoids of $\mathbb{N}$, these $M_{b,b}$ possess a particularly simple form. They can even be expressed as finite intersections of the more well-behaved M_{p^r,p^r}, as stated in the proposition below, whose proof is clear. In particular, by Proposition 2.2, for b a squarefree composite number, the badly behaved monoid $M_{b,b}$ can be expressed as a finite intersection of half-factorial monoids $M_{p,p}$.

Proposition 2.4 *If $b = p_1^{e_1} \cdots p_n^{e_n} \in \mathbb{N}$, where all the p_i are distinct and prime and $e_i \geq 1$ for all $1 \leq i \leq n$, then*

$$M_{b,b} = \bigcap_{i=1}^{n} M_{p_i^{e_i}, p_i^{e_i}}.$$

Proposition 2.4 will parallel Proposition 4.14 below, just as the local/global dichotomy of Section 4 parallels the dichotomy in this section between b a power of a prime and b not a power of a prime.

3 Regular Arithmetic Congruence Monoids

The case $a = 1$ bears attention not only mathematically, but historically. The ACMs $M_{1,b}$ are sometimes called Hilbert monoids in honor of David Hilbert's early use of $M_{1,4}$ to demonstrate the occurrence of nonunique factorization in natural number-theoretic settings (see [8]). Mathematically, they merit distinction from other ACMs as they are the ACMs which fall into the important class of Krull monoids, a generalization of Dedekind domains. Our primary goal for this section will be to demonstrate the Krull property for these monoids. We begin with an elementary, yet key, observation.

Lemma 3.1 *Let $x, y, z \in \mathbb{N}$ such that $x = yz$. If $x, y \in M_{1,b}$ then $z \in M_{1,b}$.*

Proof. We have $1 \equiv x = yz \equiv z \mod b$, so $z \in M_{1,b}$. □

In more compact notation, for any $x, y \in M_{1,b}$, if $x|_{\mathbb{N}} y$, then we already have $x|y$. In factorization theory parlance, we say that $M_{1,b}$ is **saturated** in $\mathbb{N}$. Note that the saturation of $M_{1,b}$ is in stark contrast to $M_{b,b}$ where, for instance, $2|_{\mathbb{N}} 6$ but $2 \not| 6$ in $M_{2,2}$.

Note that if $x \in M_{1,b}$ and p is prime in $\mathbb{N}$ with $p|_{\mathbb{N}} x$, then $\gcd(p,b) = 1$. Indeed, since $x \equiv 1 \mod b$, p must be invertible modulo b. Therefore, p belongs to the set of primes $P = \{p \in \mathbb{N} \mid p \text{ is prime and } \gcd(p,b) = 1\}$. Let $\mathscr{F}(P)$ be the free commutative monoid generated by P, which we identify with its isomorphic copy in $(\mathbb{N}, \times)$. Under this identification, $M_{1,b}$ will be a submonoid of $\mathscr{F}(P)$. This observation allows us to prove the following theorem, first shown by Halter-Koch [21].

Theorem 3.2 *Let $P = \{p \in \mathbb{N} \mid p \text{ is prime and } \gcd(p,b) = 1\}$. The free monoid $\mathscr{F}(P) \leq (\mathbb{N}, \times)$ and the homomorphism $\iota : M_{1,b} \hookrightarrow \mathscr{F}(P)$ form a divisor theory for $M_{1,b}$. Thus $M_{1,b}$ is Krull.*

Proof. Since ι is injective, for any $u \in M_{1,b}$, $\iota(u) = 1$ if and only if $u = 1$. Furthermore, if for some nonunits $x, y \in M_{1,b}$ we have $\iota(x)|\iota(y)$, then $x|y$ in $\mathbb{N}$, so Lemma 3.1 gives us that $x|y$ in $M_{1,b}$. Lastly, we must show that for every $p \in P$ there is a finite subset $X \subseteq M$ such that $p = \gcd(\iota(X))$. Let such a p be given. By Dirichlet's Theorem, we may choose two distinct primes $q_1, q_2 \in \mathbb{N}$ distinct from p such that $q_1 \equiv q_2 \equiv p^{-1} \mod b$ (here we use $\gcd(p,b) = 1$). Therefore $q_1, q_2 \in P$; $pq_1, pq_2 \in M_{1,b}$; and $p = \gcd(pq_1, pq_2) = \gcd(\iota(pq_1), \iota(pq_2))$. □

In fact, $M_{1,b}$ being Krull is an instance of a general theorem that all saturated submonoids of factorial monoids are Krull [18, Prop. 2.4.4 (3)]. All other ACMs besides $\mathbb{N}$ are not Krull. For ACMs that are multiples, this is due to their correspondence with numerical monoids and translates of $(\mathbb{N}^n, +)$, both of which are not Krull; for general singular ACMs this shall be proven in Theorem 4.8.

A thorough reference for the theory of Krull monoids can be found in [18]; a gentle introduction to this theory can be found in [5], where most of the facts below involving block monoids are developed in detail for algebraic number rings, a particularly well-behaved class of Krull monoids. We shall summarize these facts from

the theory of Krull monoids without further citation until we return to dealing with regular ACMs again specifically.

As mentioned in the discussion of divisor theories and the Krull property in Section 1, Krull monoids have a notion of class group. Namely, for a Krull monoid M with divisor theory $\sigma : M \to \mathscr{F}(P)$, the quotient monoid $\mathscr{F}(P)/\sigma(M)$ forms an abelian group G generated (as a monoid) by a subset S equal to the image of P under this quotient. The Krull monoid M can then be related to a combinatorial structure built out of G and S, known as the *block monoid*.

Definition 3.3 *Let G be an abelian multiplicative group and $S \subseteq G$ be nonempty. Let $\mathscr{F}(S)$ be the free commutative monoid generated by S, with elements written as $[s_1]^{e_1} \cdots [s_n]^{e_n}$. Let E be the identity of $\mathscr{F}(S)$. Given $A = [s_1]^{e_1} \cdots [s_n]^{e_n} \in \mathscr{F}(S)$, the* **length** *of A, denoted $|A|$, is $\sum_{i=1}^{n} e_i$.*

There is a natural evaluation map $\theta : \mathscr{F}(S) \to G$ given by $\theta([s_1]^{e_1} \cdots [s_n]^{e_n}) = s_1^{e_1} \cdots s_n^{e_n}$. The **block monoid of G over S** *is the monoid defined as:*

$$\mathscr{B}(G,S) = \left\{ [s_1]^{e_1} \cdots [s_n]^{e_n} \in \mathscr{F}(S) \,|\, \theta([s_1]^{e_1} \cdots [s_n]^{e_n}) = 1 \right\}.$$

In other words, the block monoid $\mathscr{B}(G,S)$ corresponds to all unordered sequences over S, such that the product of these terms in G yields the identity. The set $\mathscr{B}(G,S)$ is clearly a submonoid of $\mathscr{F}(S)$ and hence is atomic since $\mathscr{F}(G,S)$ is. Moreover, it is a *saturated* submonoid of $\mathscr{F}(S)$. Block monoids have been studied extensively in the literature and numerous factorization-theoretic properties of them are known (see [5] and [18]). For example, the elasticity of $\mathscr{B}(G,S)$ relates to an important value known as the **Davenport constant**, $D(G,S)$, of G with respect to S. The Davenport constant is defined as the maximal length of an irreducible of $\mathscr{B}(G,S)$. When G is an infinite group and $S = S^{-1}$, for example, then $D(G,S) = \infty$, but for finite groups it is easily shown that $D(G,S) \leq |G|$. For any group G and subset $S \subseteq G$, it is known that $\rho(\mathscr{B}(G,S)) \leq \max\{1, D(G,S)/2\}$, with equality in many cases, such as when $S = G$.

If M is Krull, there is a transfer homomorphism $\phi : M \to \mathscr{B}(G,S)$, where $G = \mathscr{F}(P)/\sigma(M)$ is the class group of M and $S = \{p\sigma(M) \,|\, p \in P\}$ is the subset of classes which contain elements of P. For each $m \in M$, we can consider the corresponding element $\sigma(m) = [p_1]^{e_1} \cdots [p_n]^{e_n}$ of $\sigma(M) \leq \mathscr{F}(G)$. Using this expression, we now are able to define ϕ compactly as:

$$\phi(m) = [s_1]^{e_1} \cdots [s_n]^{e_n},$$

where for each i, s_i is the image of p_i in G. In the next theorem, we explicitly determine the class group G and subset S for a regular ACM $M_{1,b}$. We shall then use the natural transfer homomorphism to the block monoid $\mathscr{B}(G,S)$ to conclude many factorization-theoretic properties of $M_{1,b}$.

The identity of the class group G is easy to surmise based on our previous knowledge. Let $x \in M_{1,b}$ be given and factor x in $\mathbb{N}$ as $p_1^{e_1} \cdots p_n^{e_n}$. We know all the $p_i \in P$. Since $x \equiv 1 \mod b$, each $\overline{p}_i$ is necessarily an invertible element of $\mathbb{Z}_b$, i.e. $\overline{p}_i \in \mathbb{Z}_b^\times$. Conversely, if we have primes $p_i \in P$, then $\overline{p}_i \in \mathbb{Z}_b^\times$ for all i. If, fur-

thermore, $\overline{p}_1^{e_1} \cdots \overline{p}_n^{e_n} = \overline{1}$, then $x = p_1^{e_1} \cdots p_n^{e_n}$ belongs to $M_{1,b}$. Thus our class group is $G = \mathbb{Z}_b^\times$, as we shall now verify.

Theorem 3.4 *The class group G of $M_{1,b}$ is $\mathbb{Z}_b^\times$ and the corresponding subset S also equals $\mathbb{Z}_b^\times$. The map*

$$\phi : M_{1,b} \to \mathscr{B}(\mathbb{Z}_b^\times, \mathbb{Z}_b^\times)$$

defined by

$$\phi(x) = \phi(p_1^{e_1} \cdots p_n^{e_n}) = [\overline{p}_1]^{e_1} \cdots [\overline{p}_n]^{e_n},$$

is a transfer homomorphism. Thus, we have the following.

1. *$M_{1,b}$ is half-factorial if and only if $b = 2, 3, 4, 6$.*
2. *$M_{1,b}$ is factorial if and only if $b = 2$.*
3. *The elasticity is $\rho(M_{1,b}) = \frac{D(\mathscr{B}(\mathbb{Z}_b^\times))}{2}$.*
4. *The elasticity of $M_{1,b}$ is accepted.*
5. *$M_{1,b}$ has full elasticity.*
6. *$\Delta(M_{1,b}) = \{1, \ldots, c\}$ for some $c \in \mathbb{N}$.*
7. *$M_{1,b}$ contains infinitely many prime elements.*

Proof. We use the notation of Theorem 3.2. As shown in that theorem, $\mathscr{F}(P)$ and the map $\iota : M_{1,b} \hookrightarrow \mathscr{F}(P)$ form a divisor theory for $M_{1,b}$. Here $\mathscr{F}(P)$ is being identified with its isomorphic copy in $(\mathbb{N}, \times)$. Set $\sigma = \iota$. Let $n, n' \in \mathscr{F}(P)$ be given such that $n \equiv n' \mod b$. By Dirichlet's Theorem, we may choose a prime $q \in \mathbb{N}$ distinct from n and n' (if they were prime) such that $q \equiv n^{-1} \mod b$. Then nq and $n'q$ are both elements of $M_{1,b}$, so $\sigma(n)$ and $\sigma(n')$ are equivalent modulo $\sigma(M_{1,b})$. Conversely, if $n, n' \in \mathscr{F}(P)$ and $n \not\equiv n' \mod b$, then for no $m \in \mathscr{F}(P)$ do we have both $nm \in M_{1,b}$ and $n'm \in M_{1,b}$. Therefore G is isomorphic to the image of $\mathscr{F}(P)$ in $(\mathbb{Z}_b, \times)$. By Dirichlet's Theorem, for every $\omega \in Z_b^\times$, there is a $p \in P$ such that $\overline{p} = \omega$, so $S \supseteq \mathbb{Z}_b^\times$. Yet we observed prior to this theorem that a product $p_1 \cdots p_k$ of primes in $\mathbb{N}$ is an element of $M_{1,b}$ if and only if $\gcd(p_i, b) = 1$ for all i and $p_1 \cdots p_k \equiv 1 \mod b$. In other words, G is contained in $Z_b^\times$ and thus $G = S = \mathbb{Z}_b^\times$.

Therefore we have our transfer homomorphism $\phi : M_{1,b} \to \mathscr{B}(\mathbb{Z}_b^\times, \mathbb{Z}_b^\times)$, and all factorization properties relating to lengths are identical for $M_{1,b}$ and $\mathscr{B}(\mathbb{Z}_b^\times, \mathbb{Z}_b^\times)$.

It is well-known (see [18] or [5], for example) that if G is a finite abelian group, then $\mathscr{B}(G, G)$ is half-factorial if and only if $|G| = 1$ or 2. For other finite abelian groups, $\rho(\mathscr{B}(G, G)) = D(G)/2$, where $D(G)$ is the Davenport constant of G. In both cases, the elasticity is accepted. Thus $M_{1,b}$ is half-factorial if and only if $|\mathbb{Z}_b^\times| \leq 2$, which is the case precisely when $b = 2, 3, 4$, or 6. The case $M_{1,2}$ is the odd numbers, which is factorial by the Fundamental Theorem of Arithmetic. For all other b, one can easily construct a product with distinct factorizations. For example: $4 \times 25 = 10 \times 10$ in $M_{1,3}$; $9 \times 49 = 21 \times 21$ in $M_{1,4}$; and $25 \times 121 = 55 \times 55$ in $M_{1,6}$.

Geroldinger and Yuan [20, Theorem 1] recently determined that if G is a finite abelian group, then $\Delta(\mathscr{B}(G, G))$ is the set of consecutive integers $\{1, 2, \ldots, c\}$ up to some integer $c \geq 1$. For many finite groups G, they give an explicit value of c in terms of another factorization invariant of $\mathscr{B}(G, G)$ known as the catenary degree. Namely, for those groups c is 2 less than the catenary degree.

Lastly, we demonstrate that $M_{1,b}$ contains infinitely many prime elements. By Dirichlet's Theorem, there are infinitely many primes $p \in \mathbb{N}$ which are equivalent to 1 modulo b. These are all prime by Lemma 3.1. From the existence of prime elements and accepted elasticity, we conclude $M_{1,b}$ is fully elastic by [6, Corollary 2.2]. □

Example 3.5 Notice that the use of Dirichlet's Theorem in the first part of the proof of Theorem 3.4 indicates that each divisor class of the the class group $\mathbb{Z}_b^\times$ of $M_{1,b}$ contains countably many prime divisors. Hence, by part 2 above, $M_{1,3}$, $M_{1,4}$ and $M_{1,6}$ are half-factorial Krull monoids with class groups isomorphic to $\mathbb{Z}_2$ and equal distributions of prime divisors in each divisor class. Since all three of these monoids are reduced, by [18, Theorem 2.5.4] it follows that $M_{1,3} \cong M_{1,4} \cong M_{1,6}$. Hence, ACMs with different defining moduli can still be isomorphic.

Example 3.6 Consider the special case implied by Theorem 3.4 when $b = p$ where p is a rational prime. Then $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ is a cyclic group, and since $D(\mathscr{B}(\mathbb{Z}_{p-1})) = p-1$, it follows that $\rho(M_{1,p}) = \frac{p-1}{2}$. It is easy here to construct a factorization where the elasticity is attained. Let x be a primitive root modulo p. By Dirichlet's Theorem, choose distinct primes p_1 and p_2 so that in $\mathbb{Z}_p^\times$ we have $\overline{x} = \overline{p_1}$ and $\overline{x}^{-1} = \overline{p_2}$. Then p_1p_2, p_1^{p-1} and p_2^{p-1} are all atoms of $M_{1,p}$. Moreover $z = (p_1p_2)^{p-1} = p_1^{p-1}p_2^{p-1}$ yields $\rho(z) = \frac{p-1}{2}$. That the class group is cyclic yields even further results. For instance, by [13, Proposition 5.3.3], $\Delta(\mathscr{B}(\mathbb{Z}_n)) = \{1,2,\ldots,n-2\}$ for all $n \in \mathbb{N}$. Taking $n = p-1$ we have $\Delta(M_{1,p}) = \{1,2,\ldots,p-3\}$.

4 Singular Arithmetic Congruence Monoids

If $a \neq 1$, the ACM is known as **singular**. We have already encountered one example of a singular ACM in Section 2, namely $a = b$. However, for a given modulus b, there are generally many singular ACMs.

Proposition 4.1 *Let $b > 1$ be given and factor $b = p_1^{e_1} \cdots p_r^{e_r}$ as a product of primes in $\mathbb{N}$. There are 2^r choices of a with $0 < a \leq b$ such that $M_{a,b}$ is an ACM. In particular, $2^r - 1$ of them will be singular.*

Proof. Suppose $M_{a,b}$ is an ACM for this fixed b. For each $1 \leq i \leq r$, we have $a^2 \equiv a \mod p_i^{e_i}$, so $p_i^{e_i} | a(a-1)$. Since p_i is prime, we conclude $p_i^{e_i} | a$ or $p_i^{e_i} | a-1$. Thus, each a for which $M_{a,b}$ is an ACM satisfies the system of linear congruences:

$$\begin{aligned} a &\equiv c_1 \mod p_1^{e_1} \\ &\vdots \\ a &\equiv c_r \mod p_r^{e_r}, \end{aligned}$$

where for each i, c_i is either 1 or $p_i^{e_i}$. Conversely, by the Chinese Remainder Theorem, for all choices of $c_1, \ldots, c_r$, where each c_i is either 1 or $p_i^{e_i}$, we obtain an a with

$0 < a \leq b$ such that $a^2 \equiv a \mod b$, i.e., $M_{a,b}$ is an ACM. There are 2^r such choices for the c_i and only one of them (all $c_i = 1$) produces the regular ACM $M_{1,b}$.

The structure of a singular ACM depends heavily upon the factors in common between a and b. Let $d = \gcd(a,b)$ and $f = b/d$. It is easy to see from the congruence $a^2 \equiv a \mod b$ (or the previous proof) that $d = 1$ if and only if $a = 1$, so a singular ACM must always have $d > 1$. The arithmetic congruence monoids of the form $M_{b,b}$ studied in Section 2 fall into the class of singular ACMs. In the initial exposition for this section, we shall allow ACMs of multiples as possibilities, even though we have already studied many of their properties in Section 2. One of the goals of this initial exposition is to show that singular ACMs are not Krull, a fact which we did not yet demonstrate for ACMs of multiples.

Singular ACMs are divided into two subclasses depending on d: a **local** ACM has d a power of prime, while a **global** ACM has d divisible by at least two distinct primes. In the later subsections on local and global singular ACMs, we shall exclude the possibility that $a = b$.

Lemma 4.2 *[7, Thm. 2.1] Let $a,b \in \mathbb{N}$ with $0 < a \leq b$ and $a^2 \equiv a \mod b$. Suppose $d = \gcd(a,b) > 1$ and set $f = b/d$. Then $\gcd(a,f) = \gcd(d,f) = 1$ and*

$$M_{a,b} = M_{d,d} \cap M_{1,f}\,.$$

Conversely, given $d, f \in \mathbb{N}$ with $d > 1$, $f \geq 1$ and $\gcd(d,f) = 1$, then there exists a unique $a \in \mathbb{N}$ such that $0 < a < df$ and $\gcd(a,df) = d$, so that $M_{a,df}$ is a singular ACM satisfying the above intersection.

Proof. As in the proof of Proposition 4.1, let $b = p_1^{e_1} \cdots p_r^{e_r}$. For each $1 \leq i \leq r$, we have $a \equiv c_i \mod p_i^{e_i}$, where $c_i = 1$ or $c_i = p_i^{e_i}$. In either case, we have $M_{a,b} \subseteq M_{c_i,p_i^{e_i}}$ and by the Chinese Remainder Theorem,

$$M_{a,b} = \bigcap_{i=1}^{r} M_{c_i,p_i^{e_i}}\,.$$

Let $I = \{1 \leq i \leq r \,|\, c_i = 1\}$ and $J = \{1,\ldots,r\}\backslash I$. For each $i \in I$, $c_i = 1$ and so $p_i \not|_{\mathbb{N}}\, a$. Hence $p_i^{e_i}|_{\mathbb{N}} f$. Conversely, for each $i \in J$, $c_i = p_i^{e_i}$. Since $a \equiv c_i \mod p_i^{e_i}$, we have $p_i^{e_i}|_{\mathbb{N}} a$ and thus $p_i^{e_i}|_{\mathbb{N}} d$. Together, we find $f = \prod_{i\in I} p_i^{e_i}$ and $d = \prod_{i\in J} p_i^{e_i}$ and that $\gcd(a,f) = \gcd(d,f) = 1$. By the Chinese Remainder Theorem,

$$\bigcap_{i\in J} M_{c_i,p_i^{e_i}} = \bigcap_{i\in J} M_{p_i^{e_i},p_i^{e_i}} = M_{d,d} \quad \text{and} \quad \bigcap_{i\in I} M_{c_i,p_i^{e_i}} = \bigcap_{i\in I} M_{1,p_i^{e_i}} = M_{1,f}$$

Thus $M_{a,b} = M_{d,d} \cap M_{1,f}$, as desired. The converse claim follows immediately from the proof of Proposition 4.1 by taking $b = df = p_1^{e_i} \cdots p_r^{e_r}$ and having $a \equiv p_i^{e_i} \mod p_i^{e_i}$ if $p_i|_{\mathbb{N}} d$ and $a \equiv 1 \mod p_i^{e_i}$ if $p_i|_{\mathbb{N}} f$. The uniqueness of a is guaranteed by the Chinese Remainder Theorem. □

We already saw in Lemma 3.1 that regular ACMs are saturated in $\mathbb{N}$. Using the above characterization of singular ACMs as intersections of a regular ACM with an

ACM of multiples, we are able to demonstrate a weak form of saturation for singular ACMs.

Lemma 4.3 *[7, Corollary 2.2] Let $a,b,d = \gcd(a,b)$, and f have the usual assumptions. Let $x,y \in M_{a,b}$ with $y|_{\mathbb{N}} x$. Then:*

1. *$x/y \in M_{a,b}$ if and only if $d|_{\mathbb{N}} x/y$, and*
2. *if $x \in \mathscr{A}(M_{a,b})$, then $y \in \mathscr{A}(M_{a,b})$.*

Proof. For the proof of (1), by Lemma 4.2, $x,y \in M_{1,f}$ so by Lemma 3.1 $x/y \in M_{1,f}$. By Lemma 4.2 again, $x/y \in M_{a,b}$ if and only if $x/y \in M_{d,d}$, which is equivalent to $d|_{\mathbb{N}} x/y$. Claim (2) is immediate from (1). □

Proposition 4.4 *Let $a,b,d = \gcd(a,b)$, and $f = b/d$ have the usual assumptions for a singular ACM. Then $M_{a,b}$ has no prime elements.*

Proof. Let q be a prime number in $\mathbb{N}$ with $\gcd(q,d) = 1$ and $q \equiv 1 \mod f$. By Lemma 4.2, for any $x \in M_{a,b}$ with $x > 1$, we must have $xq \in M_{a,b}$ and $xq^2 \in M_{a,b}$. Now let such an x be given. Since $q \notin M_{a,b}$, we cannot have $x|xq$ in $M_{a,b}$. Yet $x(xq^2) = (xq)(xq)$, so x cannot be prime in $M_{a,b}$. □

Although $M_{a,b}$ has no primes, it has infinitely many irreducibles as shown by the following simple argument from [7].

Proposition 4.5 *Let $a,b,d = \gcd(a,b)$, and $f = b/d$ have the usual assumptions. If $x \in M_{a,b}$ is reducible, then $x+b$ is irreducible.*

Proof. If $x = yz$ in $M_{a,b}$, then by Lemma 4.2 $d^2|_{\mathbb{N}} x$. If $x+b$ is also irreducible, then $d^2|_{\mathbb{N}} x+b$, so $d^2|_{\mathbb{N}} b$. But $\gcd(d,b/d) = \gcd(d,f) = 1$ by Lemma 4.2, a contradiction. □

In the singular ACM $M_{p,2p}$, we can easily show that x is irreducible if and only if $p^2|x$, so in this monoid the irreducibles are periodic with period p.

Open Question 4.6 *Determine the distribution of the irreducibles in $M_{a,b}$. Are they (eventually) periodic?*

Our remaining goal for this introductory exposition on singular ACMs is to show they are not Krull. This fact was originally proven by Halter-Koch [21, Thm. 1] and our proof shall follow similar lines. Since $\gcd(d,f) = 1$, the integer $\gamma = \mathrm{ord}_f(d) \geq 1$ exists. Thus $d^\gamma \equiv 1 \mod f$ and $d^\gamma \in M_{a,b}$ by Lemma 4.2. This element d^γ shall be central to our analysis of $M_{a,b}$ due to the following proposition.

Proposition 4.7 *Let $\gamma = ord_f(d)$. For all nonunits $x_1,\ldots,x_{\gamma+1} \in M_{a,b}$, we have $d^\gamma | x_1 \cdots x_{\gamma+1}$.*

Proof. Let nonunits $x_1,\ldots,x_{\gamma+1} \in M_{a,b}$ be given. Write each x_i as $d^{k_i} m_i$, where $d \not| _{\mathbb{N}} m_i$ for all i and let $K = \sum_{i=1}^{\gamma+1} k_i$. Since $k_i \geq 1$ for all $1 \leq i \leq r$ by Lemma 4.2, $K - \gamma \geq 1$ and so $d|_{\mathbb{N}} d^{K-\gamma} m_1 \cdots m_{\gamma+1}$. Because $x_1 \cdots x_{\gamma+1} = (d^\gamma)(d^{K-\gamma} m_1 \cdots m_{\gamma+1})$, by Lemma 4.3 we conclude $d^\gamma | x_1 \cdots x_{\gamma+1}$. □

Theorem 4.8 *Let $a,b \in \mathbb{N}$ with $0 < a \leq b$ such that $M_{a,b}$ is a singular ACM. Then $M_{a,b}$ is not Krull.*

Proof. Let $d = \gcd(a,b) > 1$ and let $\gamma = \mathrm{ord}_f(d)$. Then $d^\gamma \in M_{a,b}$. Suppose that $M_{a,b}$ is Krull. By definition, there is a free commutative monoid $\mathscr{F}(P)$ and a monoid homomorphism $\sigma : M_{a,b} \to \mathscr{F}(P)$ yielding a divisor theory. Consider $X = \sigma(d^\gamma)$ and write $X = P_1^{e_1} \cdots P_n^{e_n}$. By Proposition 4.7, $d^\gamma | x^{\gamma+1}$ for any nonunit $x \in M_{a,b}$ and thus X must divide $\sigma(x)^{\gamma+1}$.

Consider a. By Lemma 4.2, we know $a \equiv 1 \mod f$ and we can write $a = d^k m$, for some $k,m \in \mathbb{N}$ with $d \not|_{\mathbb{N}} m$. Note that $k \leq \gamma$ since $d^\gamma \in M_{a,b}$ and a is the least element of $M_{a,b}$ greater than 1. Since $\gcd(a,f) = 1$, by Dirichlet's Theorem we may pick a prime $q \in \mathbb{N}$ such that $q \equiv m^{-1} \mod f$ and $\gcd(d,q) = 1$. For all $v \geq 1$,

$$(d^{\gamma-k}qa)^{v\gamma+1} = (d^\gamma qm)^{v\gamma+1} = (d^\gamma)^{v\gamma}(d^\gamma q^{v\gamma+1} m^{v\gamma+1}).$$

By the choice of q and γ, we have $d^\gamma qm \in M_{1,f}$ and $d^\gamma q^{v\gamma+1} m^{v\gamma+1} \in M_{1,f}$. Since $d|_{\mathbb{N}} d^\gamma q^{v\gamma+1} m^{v\gamma+1}$, we conclude $d^\gamma q^{v\gamma+1} m^{v\gamma+1} \in M_{a,b}$ by Lemma 4.2. Similarly $d^{\gamma-k}qa \in M_{a,b}$, so in $M_{a,b}$ we find $(d^\gamma)^{v\gamma} | (d^{\gamma-k}qa)^{v\gamma+1}$ for all $v \geq 1$. Let $B = \sigma(d^{\gamma-k}qa) = \sigma(d^\gamma qm)$. Since $X|B^{\gamma+1}$ and we are working in a free commutative monoid, we can write B as

$$B = P_1^{g_1} \cdots P_n^{g_n} Q_1^{h_1} \cdots Q_t^{h_t},$$

where $g_i \geq 1$ for all $1 \leq i \leq n$ and $P_i \neq Q_j$ for any $1 \leq i \leq n$ and $1 \leq j \leq t$. Because σ is a monoid homomorphism and $(d^\gamma)^{v\gamma} | (d^{\gamma-k}qa)^{v\gamma+1}$ for all $v \geq 1$, we find $X^{v\gamma} | B^{v\gamma+1}$ for all $v \geq 1$. In other words, for all $1 \leq i \leq n$ and all $v \geq 1$,

$$v\gamma e_i \leq (v\gamma+1) g_i.$$

Since $v \geq 1$ arbitrary and $e_i, g_i \in \mathbb{N}$, we conclude $e_i \leq g_i$ for all i. Thus $X|B$. But σ is a divisor theory, so in $M_{a,b}$ we find $d^\gamma | d^\gamma qm$. Therefore $qm \in M_{a,b}$, but this is a contradiction by Lemma 4.2 since $d \not|_{\mathbb{N}} qm$. So no such divisor theory exists and $M_{a,b}$ is not Krull. □

This concludes the general statements we can make about singular ACMs. For the remaining two subsections, assume $a < b$.

4.1 Local Arithmetic Congruence Monoids

In this section, we shall assume $d = p^\alpha$, for p prime and $\alpha \geq 1$. Since $\gcd(d,f) = 1$, p has finite order $\mathrm{ord}_f(p)$ modulo f. Choose a least $\beta \geq \alpha$ such that $p^\beta \equiv 1 \mod f$; by Lemma 4.2, p^β is the least power of p in $M_{a,b}$. In the previous section we had chosen a least $\gamma \geq 1$ such that $d^\gamma \equiv 1 \mod f$; since $d = p^\alpha$, we conclude $\gamma = \mathrm{ord}_f(p^\alpha)$ and $\gamma |_{\mathbb{N}} \mathrm{ord}_f(p)$. Furthermore, β is a multiple of $\mathrm{ord}_f(p)$, so $\gamma |_{\mathbb{N}} \beta$ but

they need not be equal. The invariants α and β shall prove to be pivotal for many of the factorization properties of $M_{a,b}$.

Theorem 4.9 *Let $M_{a,b}$ be a singular ACM with $d = \gcd(a,b) = p^\alpha$ for some $p \in \mathbb{N}$ prime and $\alpha \geq 1$. Let $\beta \geq \alpha$ be minimal such that $d^\beta \in M_{a,b}$.*

1. *[9, Theorem 2.4 (1)] The elasticity of $M_{a,b}$ is*

$$\rho(M_{a,b}) = \frac{\alpha+\beta-1}{\alpha}.$$

2. *[9, Theorem 2.4 (4)] $\rho(M_{a,b}) < 2$ if and only if $a = p^\alpha$.*
3. *[9, Theorem 2.4 (3)] $M_{a,b}$ is half factorial if and only if $a = p$.*
4. *[7, Theorem 3.1] The Delta set of $M_{a,b}$ is*

$$\Delta(M_{a,b}) = \begin{cases} \emptyset & \text{if } \alpha = \beta = 1 \\ \{1\} & \text{if } \alpha = \beta > 1 \\ \mathbb{N} \cap [1, \frac{\beta}{\alpha}) & \text{if } \beta > \alpha. \end{cases}$$

Proof. (1). If $x \in M_{a,b}$ and $\mathsf{v}_p(x) \geq \alpha+\beta$, then $x = (p^\beta)(x/p^\beta)$. By Lemma 4.2, $x, p^\beta \in M_{1,f}$ and so by Lemma 3.1, $x/p^\beta \in M_{1,f}$ as well. Furthermore, $p^\alpha|_{\mathbb{N}} x/p^\beta$, so by Lemma 4.2, $x/p^\beta \in M_{a,b}$. Thus x is reducible. Hence all irreducibles x of $M_{a,b}$ have $\mathsf{v}_p(x) \leq \alpha+\beta-1$. On the other hand, all irreducibles x of have $\mathsf{v}_p(x) \geq \alpha$ by Lemma 4.2. Consequently, if $y \in M_{a,b}$ with $y > 1$, then any factorization of y into irreducibles involves at most $\mathsf{v}_p(y)/\alpha$ irreducibles and at least $\mathsf{v}_p(y)/(\alpha+\beta-1)$ irreducibles. Thus for all nonunit $y \in M_{a,b}$,

$$\rho(y) \leq \frac{\frac{\mathsf{v}_p(y)}{\alpha}}{\frac{\mathsf{v}_p(y)}{\alpha+\beta-1}} = \frac{\alpha+\beta-1}{\alpha}.$$

To show that this fraction equals $\rho(M_{a,b})$, we must find elements y whose elasticities approach this value. By Dirichlet's Theorem, there exist primes q and r distinct from p such that $q \equiv p^{\beta-\alpha+1} \mod f$ and $r \equiv p^{\beta-\alpha} \mod f$. By Lemma 4.2, both $p^{\alpha+\beta-1}q$ and $p^\alpha r$ are elements of $M_{a,b}$. Since $p^\alpha|_{\mathbb{N}} x$ for all nonunits $x \in M_{a,b}$ and p^β is the least power of p in $M_{a,b}$, both $p^{\alpha+\beta-1}q$ and $p^\alpha r$ are irreducible. Note that $q^\beta \equiv r^\beta \equiv 1 \mod f$ since $p^\beta \equiv 1 \mod f$, so for similar reasons as above, both $p^\alpha q^{\beta k} r$ and $p^\alpha r^{\beta k+1}$ are irreducibles of $M_{a,b}$ for any $k \geq 0$. Therefore we have for all $k \geq 1$:

$$(p^{\alpha+\beta-1}q)^{k\alpha\beta}(p^\alpha r^{\beta k(\alpha+\beta-1)+1}) = (p^\alpha r)^{k\beta(\alpha+\beta-1)}(p^\alpha q^{\beta k\alpha} r).$$

The factorization on the left has $k\alpha\beta+1$ irreducibles, while the one on the right has $k\beta(\alpha+\beta-1)+1$ irreducibles, so the elasticity of $M_{a,b}$ is bounded below by:

$$\rho((p^{\alpha+\beta-1}q)^{k\alpha\beta}(p^\alpha r^{k\beta(\alpha+\beta-1)+1})) \geq \frac{k\beta(\alpha+\beta-1)+1}{k\alpha\beta+1},$$

which goes to $(\alpha+\beta-1)/\alpha$ as k goes to infinity.

Part (3) clearly follows from (1) as the following statements are equivalent:

1. $M_{a,b}$ is half factorial,
2. $\rho(M_{a,b}) = 1$,
3. $\beta = 1$,
4. $p \in M_{a,b}$, and
5. $a = p$ by minimality of a.

For part (2), observe that if $\beta > \alpha$, then $\rho(M_{a,b}) \geq (\alpha+(\alpha+1)-1)/\alpha = 2$. So $\rho(M_{a,b}) < 2$ implies $\beta = \alpha$, so that $d = p^\alpha \in M_{a,b}$. By minimality of a, we conclude $a = d = p^\alpha$. Conversely, if $a = d = p^\alpha$, then $\alpha = \beta$ and $\rho(M_{a,b}) < 2$.

The proof of part (4) is involved; the interested reader should consult [7]. □

To this point, we have seen that whenever an ACM has finite (and rational) elasticity, its elasticity is accepted. This is no longer the case for local ACMs, as the following example testifies.

Example 4.10 Consider $M_{4,6}$. Then $p = 2$, $\alpha = 1$, and $\beta = 2$ since clearly $4 \in M_{4,6}$. By Theorem 4.9, $\rho(M_{4,6}) = 2$. We also know $d = p$ and $f = 3$, so by Lemma 4.2, $M_{4,6} = M_{2,2} \cap M_{1,3}$. Consequently, we may characterize the irreducibles of $M_{4,6}$. If $4m \in M_{4,6}$, then $m \equiv 1 \mod 3$. If $m = m_1 m_2$ where $m_1, m_2 \equiv 2 \mod 3$, then $4m = (2m_1)(2m_2)$ in $M_{4,6}$. Thus $4m$ is irreducible if (and only if) m is a product of primes, all equivalent to 1 modulo 3. Call irreducibles of this form type "A" irreducibles.

We are left with considering $x \in M_{4,6}$ of the form $x = 2m$, where m is odd and, necessarily, $m \equiv 2 \mod 3$. Any such x is irreducible since it is not divisible (in $\mathbb{N}$) by 4. Call irreducibles of this form type "B" irreducibles.

Suppose $x \in M_{4,6}$ with $\rho(x) = 2$. Fix a longest factorization of x and suppose it has s type "A" irreducibles and t type "B" irreducibles. Then $\mathsf{v}_2(x) = 2s+t$. Fix a shortest factorization of x and suppose it has u type "A" irreducibles and v type "B" irreducibles. Then $\mathsf{v}_2(x) = 2u+v$. But $2 = \rho(x) = (s+t)/(u+v)$, so

$$s+t = 2(u+v) = \mathsf{v}_2(x)+v = 2s+t+v.$$

Thus $v+s = 0$ and so $v = s = 0$. The elasticity tells us $2u = t$, i.e. x may be written as a product of u many irreducibles of type "A", and also as a product of $2u$ irreducibles of type "B". As the former product, $x = 4^u m$, where m is a product of primes, all equivalent to 1 modulo 3. As the latter product, $x = 2^{2u} m_1 \cdots m_{2u}$, where each m_i is odd and $m_i \equiv 2 \mod 3$. But this is absurd, since each m_i would consist of a product of odd primes all equivalent to 1 modulo 3. Thus there is no $x \in M_{4,6}$ with $\rho(x) = 2$.

Note that $M_{4,6}$ falls into the third class of local ACMs with respect to their Delta sets. Here $\alpha = 1$ and $\beta = 2$ so $\Delta(M_{4,6}) = \{1,2\}$.

Although there exist examples of local ACMs without accepted elasticity, Banister, Chaika, Chapman, and Meyerson have demonstrated a large class of local ACMs which do have accepted elasticity.

Theorem 4.11 *[10, Theorem 1] Let $M_{a,b}$ be a singular, local ACM with $d = \gcd(a,b) = p^\alpha$ for some prime $p \in \mathbb{N}$ and some $\alpha \geq 1$. Set $f = b/d$ and choose $\beta \geq \alpha$ minimal such that $p^\beta \in M_{a,b}$. Let ω be the least residue of α modulo $ord_f(p)$. Suppose $a \neq d$ and p is a primitive root modulo f, so that $ord_f(p) = \varphi(f)$. Then $M_{a,b}$ has accepted elasticity if and only if*

1. $\varphi(f) > 5$, *and*
2. $\omega \geq 1 + \frac{\varphi(f)}{2}$.

Example 4.12 Suppose $M_{a,b}$ satisfies the hypotheses of Theorem 4.11 and assume $M_{a,b}$ has accepted elasticity. Since p is a primitive root modulo f, $\text{ord}_f(p) = \varphi(f) > 5$ by condition 1. Condition 2 then forces $\alpha \geq 4$. Hence, for $\alpha = 1, 2$ or 3, the elasticity of an $M_{a,b}$ satisfying the hypotheses of Theorem 4.11 is not accepted. Examples of accepted and non-accepted elasticity of monoids of this type can easily be constructed, even in the case where $\alpha = 4$. For instance, it is easy to show that $M_{2^4 9, 2^4 11}$ does not satisfy condition 2 above since $\omega = \alpha = 4 < 1 + \varphi(11)/2$. Hence $M_{2^4 9, 2^4 11}$does not have accepted elasticity. The ACM $M_{2^4 4, 2^4 9}$ does satisfy conditions 1 and 2 and hence has accepted elasticity. In this case, $\alpha = 4$ and $\beta = \varphi(9) = 6$ yields that $\rho(M_{2^4 4, 2^4 9}) = \frac{9}{4}$ which is realized by the irreducible factorization $[(2^4)(17)(5)]^9 = [(2^9)(17^9)][(2^9)(5^3)]^3$.

While not much is known about singular ACMs which are fully elastic, we do have one partial result.

Theorem 4.13 *[9, Corollary 3.3] Let $M_{a,b}$ be a local singular ACM with $d = p^\alpha$. Suppose $\rho(M_{a,b}) < 2$. Then $M_{a,b}$ is fully elastic if and only if $\alpha = ord_f(p)$.*

Proof. By Theorem 4.9.2, $\rho(M_{a,b}) < 2$ if and only if $a = d = p^\alpha$. By Lemma 4.2, since $a = p^\alpha \in M_{a,b}$, we must have $p^\alpha \equiv 1 \mod f$ so $\text{ord}_f(p)$ divides α. Conversely, if $\text{ord}_f(p)$ divides α, then $p^\alpha \in M_{a,b}$ by Lemma 4.2. Since $d = p^\alpha$ divides every element of $M_{a,b}$, we find that $a = d = p^\alpha$ by the minimality of a. Thus we have established that we are in the exact situation proscribed by Corollary 3.3 of [9], from which we conclude that $M_{a,b}$ is fully elastic if and only if $\alpha = \text{ord}_f(p)$.

4.2 Global Arithmetic Congruence Monoids

We begin by observing that every global ACM can be written in terms of local ACMs.

Proposition 4.14 *[7, Section 4] A global ACM $M_{a,b}$ is a finite, unique intersection of local ACMs. Specifically, if $d = \gcd(a,b) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $f = b/d$, then*

$$M_{a,b} = \bigcap_{i=1}^{n} M_{a_i, f p_i^{\alpha_i}}$$

where a_i is the least reside of a modulo $f p_i^{\alpha_i}$.

Proof. The proof follows easily using the Chinese Remainder Theorem. □

Though this observation may appear to be valuable upon first glance, it is actually of little utility for questions of nonunique factorization. As we saw in Section 2 with $M_{b,b}$ for b not a power of a prime, the intersection of a finite number of well-behaved ACMs can still result in an ACM with poorly behaved factorization theory. Similarly here, we may find $M_{a,b}$ to be an intersection of local ACMs all of which have finite elasticity, yet the intersection $M_{a,b}$ will never have finite elasticity due to the following lemma.

Lemma 4.15 *[7, Theorem 4.2][9, Theorem 2.3] Let $M_{a,b}$ be a global ACM. There exists $\lambda \geq 3$ such that for all nonunits $x \in M_{a,b}$, $\min \mathscr{L}(x) < \lambda$.*

In particular, if $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, then

$$\lambda \leq \min \left\{ \gamma + 1 + \left\lceil \frac{ord_f(p_i)}{\alpha_i} \right\rceil \;\middle|\; 1 \leq i \leq n \right\}$$

Proof. This result was proven in both [7] and [9], with [7] giving a constructive method for obtaining small (occasionally sharp) values of λ. Our proof differs from both of these proofs in the interest of simplicity.

By Lemma 4.2, $M_{a,b} = M_{d,d} \cap M_{1,f}$ where $\gcd(d, f) = 1$, and so there exists a least $\gamma \geq 1$ such that $d^\gamma \equiv 1 \mod f$. Write $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where $n \geq 2$ and $\alpha_i \geq 1$ for all $i \leq n$. We shall prove the existence of γ and its bound using p_1; the proof for other $1 \leq i \leq n$ is analogous.

We may choose a minimal $1 \leq v \leq \gamma$ such that there exists $u \geq 0$ with $d^v p_1^u \in M_{a,b}$. For this v, choose the minimal $u \geq 0$; then $d^v p_1^u$ is irreducible in $M_{a,b}$. Since $p_1^{\mathrm{ord}_f(p_1)} \equiv 1 \mod f$, we must have $0 \leq u < \mathrm{ord}_f(p_1)$.

Now let $x \in M_{a,b}$ and write $x = d^k m$, where $d \nmid_{\mathbb{N}} m$. Clearly, $\max \mathscr{L}(x) \leq k$ since every irreducible factor of x must be divisible by d in $\mathbb{N}$ by Lemma 4.2. Thus, if $k \leq \gamma + \lceil \mathrm{ord}_f(p_1)/\alpha_1 \rceil$, we are done. Let us assume $k > \gamma + \lceil \mathrm{ord}_f(p_1)/\alpha_1 \rceil$, so that $k \geq \gamma + 1 + \mathrm{ord}_f(p_1)/\alpha_1 > v + 1 + u/\alpha_1$. Write $m = p_1^s \ell$, where $p_1 \nmid_{\mathbb{N}} \ell$ and $s \geq 0$. Thus $\mathsf{v}_{p_1}(x) = k\alpha_1 + s$. Since $k > v + 1 + u/\alpha_1$, the integer

$$z = \left\lfloor \frac{(k - v - 1)\alpha_1 + s - u}{\mathrm{ord}_f(p_1)} \right\rfloor$$

is nonnegative. We have the following equation,

$$x = d^k p_1^s \ell = (d^v p_1^{z \,\mathrm{ord}_f(p_1) + u})(p_1^{(k-v)\alpha_1 + s - z \,\mathrm{ord}_f(p_1) - u} p_2^{(k-v)\alpha_2} \cdots p_n^{(k-v)\alpha_n} \ell).$$

Set $y = p_1^{(k-v)\alpha_1 + s - z \,\mathrm{ord}_f(p_1) - u} p_2^{(k-v)\alpha_2} \cdots p_n^{(k-v)\alpha_n} \ell$. Then $x = (d^v p_1^{z \,\mathrm{ord}_f(p_1) + u}) y$. By the choice of u and v, $d^v p_1^{z \,\mathrm{ord}_f(p_1) + u} \in M_{a,b}$. In fact, by the minimality of v, this element is irreducible in $M_{a,b}$. By the choice of z, we have

$$\alpha_1 \leq (k - v)\alpha_1 + s - z \,\mathrm{ord}_f(p_1) - u < \alpha_1 + \mathrm{ord}_f(p_1). \tag{1}$$

Since $k-v \geq 1$, we find that $d|_{\mathbb{N}} y$, so Lemma 4.3 tells us $y \in M_{a,b}$. Since $\gcd(p_1, \ell) = 1$, $\mathsf{v}_{p_1}(y) = ((k-v)\alpha_1 + s - z \operatorname{ord}_f(p_1) - u)/\alpha_1$ and y is divisible by d in $\mathbb{N}$ at most $\mathsf{v}_{p_1}(y)/\alpha_1$ times. Yet by Equation (1) we know $\mathsf{v}_{p_1}(y) \leq 1 + (\operatorname{ord}_f(p_1) - 1)/\alpha_1$. So y can be written as a product of at most $1 + \lfloor (\operatorname{ord}_f(p_1) - 1)/\alpha_1 \rfloor$ irreducibles of $M_{a,b}$. Note that $1 + \lfloor (\operatorname{ord}_f(p_1) - 1)/\alpha_1 \rfloor \leq \lceil \operatorname{ord}_f(p_1)/\alpha_1 \rceil$. So $x = (d^v p_1^{z \operatorname{ord}_f(p_1)+u})y$ can be factored as product of at most $1 + \lceil \operatorname{ord}_f(p_1)/\alpha_1 \rceil \leq \gamma + \lceil \operatorname{ord}_f(p_1)/\alpha_1 \rceil$ irreducibles of $M_{a,b}$. $\square$

This lemma is perhaps not surprising considering that global ACMs are analogous to ACMs of multiples $M_{b,b}$, where b was not a power of a prime. In that case, Proposition 2.3 (1), demonstrated that $\lambda = 3$ sufficed; indeed, since $f = 1$ and hence $\gamma = 1$ in this case, our present lemma predicts the same value of λ. An immediate corollary of this lemma is the following:

Corollary 4.16 *[9, Theorem 2.3] Let $M_{a,b}$ be a global ACM, so that $d = \gcd(a,b)$ is not a power of a prime. The elasticity $\rho(M_{a,b}) = \infty$ and $M_{a,b}$ is not fully elastic.*

Hence global ACMs are never half-factorial and never have accepted elasticity. The last invariant we have considered, the delta set, has not been determined fully for all global ACMs. However, it is known to be a finite (in contrast to the elasticity) and moreover the constant λ from above plays an important role as a bound.

Theorem 4.17 *[7, Theorem 4.2] Let $M_{a,b}$ be a global ACM and $d = \gcd(a,b) = p_1^{\alpha_i} \cdots p_n^{\alpha_n}$. Let $\lambda \geq 3$ be such that $\lambda > \min \mathscr{L}(x)$ for all nonunits $x \in M_{a,b}$. Then $\Delta(M_{a,b})$ is finite and $\max \Delta(M_{a,b}) \leq \lambda - 2$.*

We shall add that explicit bounds for the λ of Lemma 4.15 have been computed in [7], which are sharp in several cases and listed as corollaries in that paper. These bounds are obtained by finding certain irreducibles which are special relative to the factors p_i (finding such irreducibles is not difficult) and then computing explicit numbers in terms of: the p_i-adic values of these irreducibles; the exponents α_i on the p_i; and least residues of the p_i modulo $f = b/d$. Combining what we have shown here with the observations made earlier in Theorems 3.4 and 4.9 concerning Delta sets in the regular and local cases raises the following open problem.

Open Question 4.18 *Let $M_{a,b}$ be an ACM which is not half-factorial. Does there exist a positive integer c so that $\Delta(M_{a,b}) = \{1, 2, \ldots, c\}$?*

5 Conclusions: Some Known Generalizations

Arithmetic congruence monoids are examples of objects which lead to a more general definition. We first extend this through $\mathbb{N}$ as follows. Let $\Gamma \subseteq \mathbb{Z}_b$ be closed under multiplication. Set $M_\Gamma = \{n \in \mathbb{N} \,|\, \exists a \in \Gamma \; n \equiv a \mod b\} \cup \{1\}$. Clearly, M_Γ forms a multiplicative submonoid of $\mathbb{N}$ known as a **congruence monoid**. If Γ is a

multiplicative subgroup of $\mathbb{Z}_b^\times$, then M_Γ is Krull with class group $\mathbb{Z}_b^\times/\Gamma$ [19, Example 5.3 (4)]. Interest in these monoids reaches back over 60 years. In [22], James and Niven prove that a congruence monoid M is factorial if and only if there exists a positive integer n such that M consists of all positive integers relatively prime to n. On the other hand, the main result of [8] shows that the congruence monoid made up of all positive integers not relatively prime to a fixed integer n (appended to 1) is not factorial but is half-factorial.

The definition of a congruence monoid in $\mathbb{N}$ can be generalized even further. Congruence monoids in general Dedekind domains have been considered in [17] and we shall define them here in that specific case. Let D be a Dedekind domain, let $\mathfrak{f}$ be a nontrivial ideal of D and write $[a]_\mathfrak{f}$ for the image of $a \in D$ in $D/\mathfrak{f}$. A **congruence monoid** M in D is a monoid of the form:

$$M = \{a \in D \,|\, [a]_\mathfrak{f} \in \Gamma\}$$

for some multiplicatively closed subset Γ of $D/\mathfrak{f}$. The ideal $\mathfrak{f}$ is called an **ideal of definition** of M. In their main theorem (Theorem 3.6 of [17]), Geroldinger and Halter-Koch demonstrate that if D is a Dedekind domain with finite ideal class group, and $D/\mathfrak{f}$ is finite, then several strong factorization properties hold for any congruence monoid M with $\mathfrak{f}$ as an ideal of definition. Among these properties, there is a structure theorem for the length sets for elements of M, which states that such length sets are essentially arithmetic (multi-)progressions.

We close by noting that a natural extension of the ACM property (namely that $a^2 \equiv a \mod b$, but no assumption is made on the size of a relative to b) has been considered in detail in [16].

Acknowledgements The first author was supported by NSF IRFP grant #0853293.

References

1. D. Adams, R. Ardila, D. Hannasch, A. Kosh, H. McCarthy, V. Ponomarenko, R. Rosenbaum. *Bifurcus Semigroups and Rings*. Involve **2** (3) 2009, pp. 351–356.
2. J. Amos, S. T. Chapman, N. Hine, J. Paixao, *Sets of lengths do not characterize numerical monoids*, Integers **7** (2007), #A50.
3. D. D. Anderson, D. F. Anderson, S. T. Chapman, and W. W. Smith. *Rational elasticity of factorizations in Krull domains*, Proc. Amer. Math. Soc. **117** (1993), no. 1, 37–43.
4. D. F. Anderson, *Elasticity of factorizations in integral domains: a survey*, Factorization in integral domains (Iowa City, IA, 1996), 1–29, Lecture Notes in Pure and Appl. Math., **189**, Dekker, New York, 1997.
5. P. Baginski and S. T. Chapman. *Factorizations of algebraic integers, block monoids, and additive number theory*, to appear in Amer. Math. Monthly.
6. P. Baginski, S. T. Chapman, C. Crutchfield, K. G. Kennedy, and M. Wright. *Elastic properties and prime elements*, Results Math. 49 (2006), 187–200.
7. P. Baginski, S. T. Chapman, and G. Schaeffer. *On the delta-set of a singular arithmetical congruence monoid*, J. Théor. Nombres Bordeaux **20** (2008), pp. 45–59.

8. M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. *On a result of James and Niven concerning unique factorization in congruence semigroups*, Elem. Math. **62** (2007), pp. 68–72.
9. M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. *On the Arithmetic of Arithmetical Congruence Monoids*, Colloq. Math. **108** (2007), pp. 105–118.
10. M. Banister, J. Chaika, S. T. Chapman and W. Meyerson. *A Theorem on Accepted Elasticity in Certain Local Arithmetical Congruence Monoids*, Abh. Math. Sem. Univ. Hamburg **79** (2009), pp. 79–86.
11. C. Bowles, S. T. Chapman, N. Kaplan, S. Reiser. *On Delta sets of numerical monoids*, Journal Algebra Appl. **5** (2006), pp. 1–24.
12. S. T. Chapman and J. Coykendall, *Half-factorial domains, a survey*, Non-Noetherian commutative ring theory, 97–115, Math. Appl., **520**, Kluwer Acad. Publ., Dordrecht, 2000.
13. S. T. Chapman and A. Geroldinger, *Krull domains and monoids, their sets of lengths, and associated combinatorial problems*, Factorization in integral domains (Iowa City, IA, 1996), 73–112, Lecture Notes in Pure and Appl. Math., **189**, Dekker, New York, 1997.
14. S. T. Chapman, M. Holden and T. Moore, *On full elasticity in atomic monoids and integral domains*, Rocky Mountain J. Math. **36** (2006), 1437–1455.
15. S. T. Chapman and B. McClain, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra **293** (2005), 595–610.
16. S. T. Chapman and D. Steinberg, *Elasticity in generalized arithmetical congruence monoids*, Results Math. **58** (2010), 221–231.
17. A. Geroldinger and F. Halter-Koch. *Congruence Monoids*, Acta Arith. **112** (2004), pp. 263-296.
18. A. Geroldinger and F. Halter-Koch, *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
19. A. Geroldinger and F. Halter-Koch. *Non-unique factorizations: a survey*, Multiplicative ideal theory in commutative algebra, Springer, New York, 2006, pp. 207–226.
20. A. Geroldinger and P. Yuan. *The Set of Distances in Krull Monoids*, preprint.
21. F. Halter-Koch. *Arithmetical Semigroups Defined by Congruences*, Semigroup Forum **42** (1991), pp. 59–62.
22. R. D. James and I. Niven, *Unique factorization in multiplicative systems*, Proc. Amer. Math. Soc. **5** (1954), 834–838.
23. U. Krause, *On monoids of finite real character*, Proc. Amer. Math. Soc. **105** (1989), 546–554.
24. J.C. Rosales and P.A. García-Sánchez. *Numerical Semigroups,* Developments in Mathematics, **20**. Springer, New York, 2009.