Noname manuscript No.
(will be inserted by the editor)

Arithmetic of Congruence Monoids

Arielle Fujiwara · Joseph Gibson · Matthew O. Jenssen · Daniel Montealegre · Vadim Ponomarenko · Ari Tenzer

Abstract Let $\mathbb{N}$ represent the positive integers. Let $n \in \mathbb{N}$ and $\Gamma \subseteq \mathbb{N}$. Set $\Gamma_n = \{x \in \mathbb{N} : \exists y \in \Gamma,\ x \equiv y \pmod{n}\} \cup \{1\}$. If Γ_n is closed under multiplication, it is known as a *congruence monoid* or CM. A classical result of James and Niven [15] is that for each n, exactly one CM admits unique factorization into products of irreducibles, namely $\Gamma_n = \{x \in \mathbb{N} : \gcd(x, n) = 1\}$. In this paper, we examine additional factorization properties of CM's. We characterize CM's that contain primes, we determine elasticity for several classes of CM's and bound it for several others. Also, for several classes we characterize half-factoriality and determine whether the elasticity is accepted and whether it is full.

Keywords congruence monoid · nonunique factorization · elasticity · arithmetic congruence monoid · half-factorial

Mathematics Subject Classification (2000) 20M13, 11A51, 20M14

Arielle Fujiwara
Roosevelt University

Joseph Gibson
University of Texas at San Antonio

Matthew O. Jenssen
Queen's College, University of Cambridge

Daniel Montealegre
University of California at Los Angeles

Vadim Ponomarenko
San Diego State University, San Diego, CA 92182-7720
E-mail: vponomarenko@mail.sdsu.edu

Ari Tenzer
Washington University in Saint Louis

1 Introduction

Nonunique factorization theory studies the arithmetic properties of commutative, cancellative monoids and domains, where unique factorization fails to hold. For a general reference see any of [1,2,12]. One large class of such monoids are multiplicative submonoids of the natural numbers. This is quite broad in general, but a particular subclass called arithmetic congruence monoids (ACM's) have received considerable attention recently [4,6–10,16]. These ACM results are surveyed in the forthcoming [2]. The present work considers a generalization of ACM's, still contained within the natural numbers, called congruence monoids (CM's). The arithmetic properties of ACM's are fairly well-understood, and our intention is to determine these properties for CM's. Some previous results concerning CM's may be found in [5,13,15]. More generally, congruence monoids in Dedekind domains have been investigated in [11,14].

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{N}_0$ denote the set of nonnegative integers, and $\mathbb{P}$ denote the set of rational primes. Let us fix $n \in \mathbb{N}$, and let $[\cdot]_n$ denote the natural epimorphism from $\mathbb{N}$ to $\mathbb{Z}/n\mathbb{Z}$. Let $\Gamma \subseteq \mathbb{N}$ be nonempty, and set $[\Gamma]_n = \{[x]_n : x \in \Gamma\} \subseteq \mathbb{Z}/n\mathbb{Z}$. We define $\Gamma_n = \{x \in \mathbb{N} : [x]_n \in [\Gamma]_n\} \cup \{1\}$. If $[\Gamma]_n$ is multiplicatively closed, then Γ_n is a multiplicative submonoid of $\mathbb{N}$ and we call Γ_n a *congruence monoid* (CM). CM's were first introduced in [13], wherein they were called arithmetical congruence semigroups.

An *arithmetic congruence monoid* (ACM) is a congruence monoid with the added restriction that $|\Gamma| = 1$. They are commonly written as $M_{a,n}$, where $\Gamma = \{a\}$. The ACM's of the special type $M_{n,n} = \{1\} \cup n\mathbb{N}$ are of particular interest to us in the sequel, so we shall denote them more compactly as $M(n)$. The arithmetic properties of ACM $M_{a,n}$ are categorized broadly as follows. If $\gcd(a, n) = 1$, then in fact $a = 1$ and the ACM is called *regular*. Otherwise, the ACM is called *singular*. Singular ACM's are further subdivided based on whether $\gcd(a, n)$ is a prime power (called *local* ACM's), or otherwise (called *global* ACM's).

We now need to define various tools from the theory of nonunique factorization. For a full introduction, see the monograph [12]. For monoid M, let $M^\times$ denote its units and $M^\bullet$ denote its nonunits. We call M *reduced* if $|M^\times| = 1$. We call $x \in M^\bullet$ *irreducible* if it cannot be expressed as the product of two nonunits. We denote the set of all *irreducibles* of M by $\mathcal{A}(M)$. Given $x \in M^\bullet$, we call $x_1 x_2 \cdots x_k$ a *factorization of* x if each term is irreducible and their product is x. Monoid M is *atomic* if every $x \in M^\bullet$ has at least one factorization; all congruence monoids are reduced and atomic, being submonoids of $\mathbb{N}$. We call $x \in M^\bullet$ *prime* if $x|ab$ (in M) implies either $x|a$ (in M) or $x|b$ (in M). It is a standard result that every prime is irreducible; we call M *factorial* if every irreducible is prime.

Several important invariants are concerned with the quantity of irreducibles into which an element may be factored. For $x \in M^\bullet$, let $L(x)$ denote the maximum number of irreducibles in a factorization of x (in our context always finite), and let $l(x)$ denote the minimum number of irreducibles in a factorization of x. Let $\rho(x) = \frac{L(x)}{l(x)}$, called the *elasticity* of x. The *elasticity* of M is

defined as $\rho(M) = \sup\{\rho(x) : x \in M^\bullet\}$. If $\rho(M) = 1$ we call M *half-factorial*; at the other extreme we can have $\rho(M) = \infty$. If there is some $x \in M^\bullet$ such that $\rho(x) = \rho(M)$, we say that the elasticity of M is *accepted*. If for every rational $q \in [1, \rho(M))$, there is some $x_q \in M^\bullet$ with $\rho(x_q) = q$, we say that the elasticity of M is *full*, or M is *fully elastic*.

For general commutative, cancellative, reduced, atomic monoids M, N and monoid homomorphism $\sigma : M \to N$, we call σ a *transfer homomorphism* if

- $\sigma(x) \in N^\times$ if and only if $x \in M^\times$,
- σ is surjective, and
- If $x \in M$ and there are $a, b \in N$ such that $\sigma(x) = ab$, then there are $x', x'' \in M$ such that $x = x'x''$, $\sigma(x') = a$, and $\sigma(x'') = b$.

In particular, transfer homomorphisms preserve lengths; they are a common tool used in nonunique factorization theory, because the elasticity-related invariants for M coincide with those for N.

We now begin our study of congruence monoids with several classifying definitions. These are motivated in part by the following lemma.

Lemma 1 *Let Γ_n be a congruence monoid, and $x, y \in \Gamma_n$. Suppose that $[x]_n = [y]_n$. Then $\gcd(x, n) = \gcd(y, n)$.*

Proof We have $x = y + kn$ for some $k \in \mathbb{Z}$. Because $\gcd(x, n)$ divides x and n, $\gcd(x, n)$ also divides y and hence $\gcd(y, n)$. Reversing the roles of x, y we have $\gcd(y, n)$ divides $\gcd(x, n)$ and the result follows. □

The structure of ACM $M_{a,n}$ varies substantially depending on the invariant $\gcd(a, n)$. Similarly, the CM structure varies depending on two invariants, u, d, as defined below. For particular n and Γ, we factor $n = ur$, choosing r to be maximal such that $\gcd(r, g) = 1$ for all $g \in \Gamma$. We call r the *pRivate part* of n, and u the *pUblic part* of n, and observe that $\gcd(u, r) = 1$. Analogously, we call (rational) primes dividing r *private primes*, and primes dividing u *public primes*. Note that all primes dividing n are either private or public, but not both; also, for each public prime p there is some $g \in \Gamma$ with $p|g$. We call those rational primes that are neither public nor private *external primes*.

If $u = 1$ we call Γ_n *regular*; in this case each $g \in \Gamma$ satisfies $\gcd(g, n) = 1$. If $\gcd(g, n) = 1$ for at least one $g \in \Gamma$ we call Γ_n *weakly regular*. When $|\Gamma| = 1$ these notions coincide, and agree with the established definition of regular ACM's.

We now define a related invariant $d = \gcd(\Gamma \cup \{n\})$. Note that $d|u$ and hence $1 \leq d \leq u$. In particular if Γ_n is regular then $u = d = 1$. If Γ_n is weakly regular then $d = 1$. The converse need not hold; for example $\Gamma = \{3, 4, 6\}$ with $n = 6$ has $d = 1$ but is not weakly regular.

If $d = u$ we call Γ_n a *J-monoid*. J-monoids are the closest direct generalization of ACM's; results for J-monoids are often similar to those for ACM's. If $d > 1$ we call Γ_n *singular*. If $d > 1$ and u is a prime power, then we call Γ_n *local*. These generalize the established definitions for singular and local ACM's. We call Γ_n *semi-regular* if it is weakly regular but not a J-monoid.

In particular, if Γ_n is semi-regular then $1 = d < u$. Hence all weakly regular CM's are either regular or semi-regular. Since ACM's are J-monoids, they are never semi-regular.

For $p \in \mathbb{P}$ and $x \in \mathbb{N}$, let $\nu_p(x)$ denote the largest power of p that divides x (as integers). By $\phi(x)$ we denote the Euler totient. By $a|b$ we mean a divides b as integers; if a, b are also members of a monoid, we will establish $\frac{b}{a}$ in the monoid separately. For $r \in \mathbb{N}$, we let $r^\perp = \{s \in \mathbb{N} : \gcd(s, r) = 1\}$.

The sequel contains the following results. First we recall that regular CM's are equivalent to other well-understood monoids, which largely determines their arithmetic properties. For all CM's, the presence of primes is characterized completely. For local J-monoids we compute elasticity, characterize half-factoriality, and in some cases determine accepted and full elasticity. More generally for singular J-monoids we present several transfer homomorphisms. For all local CM's, we have both an exact computation of elasticity (which is always finite) as well as several bounds using different invariants. Most generally, we determine whether elasticity is finite for many CM's. We conclude with two elasticity results for semi-regular CM's, and a family of semi-regular examples with infinite and full elasticity (a phenomenon that does not occur in ACM's).

2 Structural Results

We first consider regular congruence monoids. The following lemma, found in [2], shows that regular CM's are isomorphic to Krull monoids.

Lemma 2 *Let Γ_n be a regular congruence monoid. Then $[\Gamma]_n \leq (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof $[\Gamma]_n$ is closed by definition of congruence monoid. For $[x]_n \in [\Gamma]_n$, $\gcd(x, n) = 1$. Hence by Euler's theorem, $[x]_n^{\phi(n)-1}[x]_n = [1]_n$, and since $[\Gamma]_n$ is closed, all of these are in $[\Gamma]_n$. □

By [12, Example 5.3 (4)], we conclude from Lemma 2 that Γ_n is Krull with finite class group $(\mathbb{Z}/n\mathbb{Z})^\times/[\Gamma]_n$. Krull monoids are well-studied (e.g. in [12]), with finite and accepted elasticity equal to half of the Davenport constant of the block monoid of the class group. Half-factoriality is characterized by the class group being of order 1 or 2, which translates into the following result.

Proposition 1 *Regular congruence monoid Γ_n is half-factorial if and only if $|[\Gamma]_n| \geq \frac{\phi(n)}{2}$. It is factorial if and only if $|[\Gamma]_n| = \phi(n)$.*

We now turn our attention to prime elements of Γ_n. These are characterized in Theorem 1, which first requires the following lemma.

Lemma 3 *Let Γ_n be a weakly regular congruence monoid. Then $[1]_n \in [\Gamma]_n$.*

Proof Because Γ_n is weakly regular, there is some $g \in (\Gamma \cap n^\perp)$. By Euler's theorm, $1 \equiv g^{\phi(n)} \pmod{n}$ and $[g]_n^{\phi(n)} \in [\Gamma]_n$ since $[\Gamma]_n$ is closed. □

We now characterize congruence monoids that contain primes. Henceforth we will regularly make use, without further comment, of Dirichlet's theorem on primes in arithmetic progression.

Theorem 1 *Let Γ_n be a congruence monoid. If Γ_n is weakly regular, then it contains infinitely many primes; if not, then it contains no primes.*

Proof Let $p \in \mathbb{P}$ be arbitrary with $p \equiv 1 \pmod{n}$.

First, suppose that Γ_n is weakly regular. We will prove that p is prime in Γ_n. We have $[p]_n = [1]_n$ and, by Lemma 3, $[1]_n \in [\Gamma]_n$ so $p \in \Gamma_n$. Suppose now that $p|xy$, where $x, y \in \Gamma_n$. Since p is a rational prime, we may assume without loss that $p|x$; write $x = px'$ for some $x' \in \mathbb{N}$. Since $p \equiv 1 \pmod{n}$ we have $x \equiv x' \pmod{n}$ and hence $[x]_n = [x']_n$. Since $x \in \Gamma_n$ also $x' \in \Gamma_n$. Consequently, $p|x$ in Γ_n which completes the proof.

Now, suppose that Γ_n is not weakly regular. Let $x \in \Gamma_n^\bullet$ be arbitrary. Because $[x]_n = [xp]_n = [xp^2]_n$, both of $xp, xp^2 \in \Gamma_n$. However $p \notin \Gamma_n$ since $\gcd(p, n) = 1$ although, by Lemma 1, $\gcd(g, n) > 1$ for all $g \in \Gamma$. Now we have $x|(xp)(xp)$ in Γ_n because $x(xp^2) = (xp)(xp)$, but $x \nmid xp$ in Γ_n because $p \notin \Gamma_n$. Hence x is not prime in Γ_n. □

In [3] it is shown that monoids with accepted elasticity and at least one prime have full elasticity. Since regularity implies weak regularity, Theorem 1 implies that all regular congruence monoids have full elasticity.

We now produce an explicit element of Γ, based on the factorization $n = ur$.

Theorem 2 *Let Γ_n be a CM, with $n = ur$. Then $[u^{\phi(r)}]_n \in [\Gamma]_n$.*

Proof Write $u = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Because $p_1, p_2, \ldots, p_r$ are all public primes, there are some $g_1, g_2, \ldots, g_r \in \Gamma$ (not necessarily distinct) such that $p_1|g_1$, $p_2|g_2, \ldots$, $p_r|g_r$. Set $x = g_1^{a_1} g_2^{a_2} \cdots g_r^{a_r}$. Because $[\Gamma]_n$ is closed, $[x]_n \in [\Gamma]_n$. Hence, there is some $y \in \Gamma$ such that $[x]_n = [y]_n$. But $\gcd(x, n) = u$ so, by Lemma 2, $\gcd(y, n) = u$. Note that $[y^{\phi(r)}]_n \in [\Gamma]_n$. We have $y^{\phi(r)} \equiv 0 \equiv u^{\phi(r)} \pmod{u}$ because $u|y$. Also we have $y^{\phi(r)} \equiv 1 \equiv u^{\phi(r)} \pmod{r}$, via Euler's theorem, because $\gcd(y, r) = \gcd(u, r) = 1$. By the Chinese Remainder Theorem, $y^{\phi(r)}$ and $u^{\phi(r)}$ are congruent modulo $\operatorname{lcm}(u, r) = n$. Hence $[y^{\phi(r)}]_n = [u^{\phi(r)}]_n$ and the result follows. □

In the special case of ACM's, $|[\Gamma]_n| = 1$, so by Theorem 2 we see that $[\Gamma]_n = \{[u^{\phi(r)}]_n\}$. For fixed n, there are hence 2^t ACM's, where t denotes the number of distinct primes dividing n, and just one of these (corresponding to $u = 1$) is regular. This observation was Proposition 4.1 in [2].

A useful structural ACM result in [4] expresses each ACM as the intersection of a regular ACM and the singular ACM $M(u)$. This result is generalized in the following.

Theorem 3 *Let $\Gamma \subseteq \mathbb{N}$, Γ_n be a congruence monoid, and $n = ur$. Then Γ_r is a regular congruence monoid and*

$$M(u) \cap \Gamma_r \subseteq \Gamma_n \subseteq M(d) \cap \Gamma_r$$

Further, Γ_n is a J-monoid if and only if $M(u) \cap \Gamma_r = \Gamma_n$.

Proof We first prove that Γ_r is a regular congruence monoid. Let $x, y \in \Gamma$. Because $[\Gamma]_n$ is closed, there is some $z \in \Gamma$ such that $[x]_n[y]_n = [z]_n$. That is, $ur|(xy - z)$. But then $r|(xy - z)$, so $[x]_r[y]_r = [z]_r$. Hence $[\Gamma]_r$ is closed. If $\gcd(r, g) > 1$ for any $g \in \Gamma$, that would violate the definition of r; hence Γ_r is regular. Further, for $g \in \Gamma$, if $[x]_n = [g]_n$, then $n|(x - g)$ and hence $r|(x - g)$ and $[x]_r = [g]_r$. Consequently $\Gamma_n \subseteq \Gamma_r$.

The second inclusion is now clear. To prove the first inclusion, let $x \in (M(u) \cap \Gamma_r)^\bullet$. Then there is some $y \in \Gamma$ such that $x \equiv y \pmod r$. But $u^{\phi(r)} \equiv 1 \pmod r$ so also $x \equiv yu^{\phi(r)} \pmod r$. Hence $r|(x - yu^{\phi(r)}) = u(\frac{x}{u} - yu^{\phi(r)-1})$, but since $\gcd(r, u) = 1$ in fact $r|(\frac{x}{u} - yu^{\phi(r)-1})$ and hence $n = ru|(x - yu^{\phi(r)})$. Hence $[x]_n = [y]_n[u^{\phi(r)}]_n \in [\Gamma]_n$.

We now prove the last statement. If Γ_n is a J-monoid, then all the inclusions are equalities. If instead Γ_n is not a J-monoid, there is some $g \in \Gamma$ with $u \nmid g$. Then $(g + n) \in \Gamma_n^\bullet \setminus (M(u) \cap \Gamma_r)$. □

Corollary 1 *Let $x, y \in \Gamma_n$, a CM. If $\frac{x}{y} \in M(u)$ then $\frac{x}{y} \in \Gamma_n$.*

Proof By the second inclusion of Theorem 3, $x, y \in \Gamma_r$, which is regular. By Lemma 2, there is some $z \in \Gamma$ satisfying $[y]_r[z]_r = [1]_r$. Since $\frac{x}{y} \in M(u)$, $\frac{x}{y} \in \mathbb{N}$ and $[\frac{x}{y}]_r = [x]_r[z]_r \in [\Gamma]_r$. Hence $\frac{x}{y} \in M(u) \cap \Gamma_r$ and we apply the first inclusion of Theorem 3. □

The following generalizes Lemma 2 to non-regular congruence monoids. It shows that J-monoids have an implicit group structure.

Theorem 4 *Let Γ_n be a congruence monoid. Then $[(M(u) \cap \Gamma_r)^\bullet]_n$ is isomorphic to a subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$. Further, if Γ_n is a J-monoid, then $[\Gamma]_n = [(M(u) \cap \Gamma_r)^\bullet]_n$.*

Proof Consider $\psi : \Gamma_r \to (M(u) \cap \Gamma_r)^\bullet$ given by $\psi(x) = u^{\phi(r)}x$. Let $t : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/u\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z})$ be the natural isomorphism. Set $S = \{t([\psi(x)]_n) : x \in \Gamma_r\} \subseteq (\mathbb{Z}/u\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z})$. In fact, because $\psi(x) \equiv 0 \pmod u$ and $\psi(x) \equiv x \pmod r$, $S = \{0\} \times [\Gamma_r^\bullet]_r = \{0\} \times [\Gamma]_r$. By Theorem 3, Γ_r is a regular congruence monoid, so we apply Lemma 2 to get the first statement. The second statement follows from Theorem 3 and $[\Gamma_n^\bullet]_n = [\Gamma]_n$. □

Theorem 4 is illustrated by the following example.

Example 1 Let $n = 30$ and $\Gamma = \{1, 4, 14, 16, 26\}$. We have $d = 1, u = 2, r = 15$, so $[\Gamma]_{30}$ is semi-regular. We see that $[(M(2) \cap \Gamma_{15})^\bullet]_{30} = \{[4]_{30}, [14]_{30}, [16]_{30}, [26]_{30}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \leq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^\times$. The identity in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is the image of $[16]_{30}$.

Our last result of this section generalizes the analogous ACM result found in [4]. Its condition holds for all non-regular J-monoids, and hence for all non-regular ACM's.

Theorem 5 *Let Γ_n be a congruence monoid with $d^2 \nmid u$. If $x \in \Gamma_n^\bullet$ is reducible, then $x + n \in \Gamma_n$ is irreducible.*

Proof We have $x = yz$ for some $y, z \in \Gamma_n^\bullet$. By the second inclusion of Theorem 3, $d^2|x$. If also $x + n$ were reducible, then $d^2|(x + n)$ and hence $d^2|n$ but then $d^2|u$ contrary to hypothesis. □

Consequently, if Γ_n satisfies the conditions of Theorem 5 then

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

3 Elasticity

Recall that in the ACM context, if u is 1 (the regular case), or u is a prime power (the local singular case), the elasticity is finite. On the other hand, for all other u (the global singular case), the elasticity is infinite. We have similar results for congruence monoids, except instead of just u we are concerned with both u and d. For J-monoids, just as with ACM's, these constants coincide.

We recall the following result from [16].

Theorem 6 *Let Γ_n be a congruence monoid. Let $A = \{x \in \Gamma : \gcd(x, n) > 1\}$, and let $B = \{p \in \mathbb{P} : p|n, p^k \in \Gamma_n$ for some $k \in \mathbb{N}\}$. Then $\rho(\Gamma_n) < \infty$, if and only if, $\forall x \in A\ \exists p \in B$ with $p|x$.*

We first generalize the ACM finite elasticity result, via u. The following result handles all local CM's, as well as certain semi-regular CM's.

Theorem 7 *Let Γ_n be a congruence monoid. If $u = p^k$ for some $p \in \mathbb{P}$ and some $k \in \mathbb{N}_0$, then $\rho(\Gamma_n) < \infty$.*

Proof Let A, B be as in Theorem 6. By Theorem 2, $[u^{\phi(r)}]_n \in [\Gamma]_n$. Setting $s = k\phi(r)$ we have $p^s = u^{\phi(r)}$ so $[p^s]_n \in [\Gamma]_n$ and $p^s \in \Gamma_n$. Thus $p \in B$. Now let $x \in A$. We have $\gcd(x, u) = \gcd(x, n) > 1$, so $p|x$. Since $x \in A$ was arbitrary, the result follows. □

We now generalize the ACM infinite elasticity result, via d.

Theorem 8 *Let Γ_n be a congruence monoid. If $d = d_1 d_2$ for some $d_1, d_2 > 1$ with $\gcd(d_1, d_2) = 1$, then $\rho(\Gamma_n) = \infty$.*

Proof Let A, B be as in Theorem 6. We first prove that $B = \emptyset$; otherwise let $p^k \in B$. Then $[p^k]_n \in [\Gamma]_n$, so there is some $y \in \Gamma$ with $[p^k]_n = [y]_n$. By Lemma 1, $\gcd(y, n) = \gcd(p^k, n) = p^s$ for some $s \in \mathbb{N}$. But also $d| \gcd(y, n)$, which is a contradiction since d is not a prime power. We now observe that $A \neq \emptyset$, else $d = 1$, and the result follows. □

For J-monoids, Theorems 7 and 8 characterize finite elasticity. Otherwise, there is no simple way to close the gap, as the following two examples show. For particular cases one can always apply Theorem 6 directly, by calculating B and checking which elements of Γ have one of these as divisor.

Example 2 Set $n = 105 = 3{\cdot}5{\cdot}7$, and $\Gamma = \{1, 15\}$. We have $r = 7, u = 15, d = 1$ so Theorems 7 and 8 do not apply. Applying Theorem 6, we have $A = \{15\}$ yet $B = \emptyset$, hence $\rho(\Gamma_n) = \infty$.

Example 3 Set $n = 105$, and $\Gamma = \{1, 15, 85\}$. We again have $r = 7, u = 15, d = 1$ so Theorems 7 and 8 do not apply. Applying Theorem 6, we have $A = \{15, 85\}$; however this time $[85]_n = [5^{30}]_n$ so $B = \{5\}$. Hence $\rho(\Gamma_n) < \infty$.

We now sharpen Theorem 7 and compute elasticity for the local case. An upper bound for elasticity is computed in [16], but it is not particularly tight.

Theorem 9 *Let Γ_n be a local congruence monoid, $p \in \mathbb{P}$. Suppose that $u = p^\alpha, d = p^\gamma > 1$. Let $\delta = \sup\{\nu_p(x) : x \in \Gamma_n, x \text{ irreducible}\}$. Then $\rho(\Gamma_n) = \frac{\delta}{\gamma}$.*

Proof If δ is finite, set $\delta' = \delta$; otherwise set δ' to be an arbitrarily large element of $\{\nu_p(x) : x \in \Gamma_n, x \text{ irreducible}\}$. We now choose $s, t \in (\mathbb{P} \cap n^\perp)$ with $p^{\delta'}s, p^\gamma t$ both irreducibles in Γ_n. The former is guaranteed by the definition of δ', while the latter is guaranteed by the definition of d. Let $k \in \mathbb{N}$ be arbitrary, and consider the two factorizations $x = (p^{\delta'}s)^{\gamma\phi(n)k}(p^\gamma t^{\delta'\phi(n)k+1}) = (p^\gamma t)^{\delta'\phi(n)k}(p^\gamma t s^{\gamma\phi(n)k})$. We verify that $\nu_p(x) = \delta'\gamma\phi(n)k + \gamma$, $\nu_s(x) = \gamma\phi(n)k$, $\nu_t(x) = \delta'\phi(n)k + 1$, so indeed these are factorizations as integers. Because $t^{\phi(n)} \equiv 1 \equiv s^{\phi(n)} \pmod n$, by Euler's theorem we have $(p^\gamma t^{\delta'\phi(n)k+1}) \equiv p^\gamma t \equiv (p^\gamma t s^{\gamma\phi(n)k}) \pmod n$, so they are each in Γ_n. Further, they are each irreducibles because they have only γ copies of p, the minimum possible. Consequently, $L(x) \geq \delta'\phi(n)k + 1$ and $l(x) \leq \gamma\phi(n)k + 1$ so $\rho(x) \geq \frac{\delta'\phi(n)k+1}{\gamma\phi(n)k+1}$. Hence $\rho(\Gamma_n) \geq \frac{\delta'\phi(n)k+1}{\gamma\phi(n)k+1}$ for all $k \in \mathbb{N}$ so indeed $\rho(\Gamma_n) \geq \frac{\delta'}{\gamma}$.

If $\delta = \infty$ we are done, otherwise we need an upper bound for $\rho(\Gamma_n)$. For irreducible $z \in \Gamma_n$, we have $\gamma \leq \nu_p(z) \leq \delta$. For $y \in \Gamma_n$, $\gamma L(y) \leq \nu_p(y) \leq \delta l(y)$, which rearranges to $\rho(y) = \frac{L(y)}{l(y)} \leq \frac{\delta}{\gamma}$. Hence $\rho(\Gamma_n) \leq \frac{\delta}{\gamma}$. □

The invariant δ in Theorem 9 may be difficult to compute, so in the following result we bound $\rho(\Gamma_n)$ using other invariants. Note that because $u = p^\alpha$, by Theorem 2 there is some power of p that is Γ_n. Let β be minimal such that $p^\beta \in \Gamma_n$. We have $\gamma \leq \beta \leq \alpha\phi(r)$.

Theorem 10 *Let Γ_n be a local congruence monoid, $p \in \mathbb{P}$. Suppose that $u = p^\alpha, d = p^\gamma > 1$. Let β be minimal such that $p^\beta \in \Gamma_n$. Then*

$$\max\left(\left\lfloor \frac{\gamma + \beta - 1}{\gamma} \right\rfloor, \frac{\psi\beta + \gamma - 1}{\psi\gamma}\right) \leq \rho(\Gamma_n) \leq \frac{\alpha + \beta - 1}{\gamma}$$

where $\psi = \lceil \frac{\alpha - \gamma + 1}{\beta} \rceil$.

Proof Let $\delta = \max\{\nu_p(x) : x \in \Gamma_n, x \text{ irreducible}\}$, and let $x \in \Gamma_n$ be irreducible with $\nu_p(x) = \delta$. Suppose first that $\delta \geq \alpha + \beta$. We have $p^\beta \in \Gamma_n$ by definition of β. Set $y = xp^{-\beta} \in \mathbb{N}$. We have $\nu_p(y) \geq \alpha$ so $y \in M(u)$ and, by Corollary 1, $y \in \Gamma_n$. Hence x is reducible via $x = p^\beta y$, a contradiction. Hence $\delta \leq \alpha + \beta - 1$, which establishes the right inequality.

Set $c = \lfloor \frac{\beta-1}{\gamma} \rfloor$. Because $c \leq \frac{\beta-1}{\gamma}$, we have $\beta \geq c\gamma + 1$. Choose any $t \in n^{\perp}$ with $p^{\gamma}t \in \Gamma_n$; such a t must exist by definition of d. Let $s \in \mathbb{P} \setminus \{p\}$ satisfy $s \equiv t^{c+1} \pmod{n}$. Now, set $x = p^{\gamma(c+1)}s$. We have $[x]_n = [(p^{\gamma}t)^{c+1}]_n = [p^{\gamma}t]_n^{c+1}$. Because $[\Gamma]_n$ is closed, $x \in \Gamma_n$. Suppose x were reducible as $x = (p^a)(p^b s)$. By definition of d, $b \geq \gamma$ and hence $a \leq \gamma(c+1) - \gamma = \gamma c \leq \beta - 1$. This contradicts the definition of β. Hence x is irreducible and $\delta \geq \gamma(c+1)$; applying Theorem 9 gives $\rho(\Gamma_n) \geq \lfloor \frac{\gamma+\beta-1}{\gamma} \rfloor$.

We now turn to the last inequality. We assume without loss that there is some $q_1 \in (\mathbb{P} \cap n^{\perp})$ such that $p^{\gamma}q_1 \in \Gamma_n$. Choose $q_2 \in (\mathbb{P} \cap n^{\perp})$ such that $q_2 \equiv p^{-\psi\beta-\gamma+1} \pmod{r}$. We now show that $x = p^{\psi\beta+\gamma-1}q_2 \in \Gamma_n$. First, we have $\nu_p(x) = \psi\beta + \gamma - 1 \geq \alpha$, so $x \equiv 0 \pmod{p^{\alpha}}$. Second, we have $x \equiv 1 \pmod{r}$. Hence $[x]_n = [u^{\phi(r)}]_n \in [\Gamma]_n$, by Theorem 2.

Factoring $x = (p^{s_0}q_2)(p^{s_1})(p^{s_2}) \cdots (p^{s_t})$ into as many irreducibles as possible, we have $\psi\beta + \gamma - 1 = \nu_p(x) = s_0 + s_1 + \cdots + s_t \geq \gamma + t\beta$. Rearranging, we get $t < \psi$ and hence $L(x) = t + 1 \leq \psi$. Now, we set $\phi = \phi(n)$ and choose (large) $k \in \mathbb{N}$. We now consider

$$y = (p^{\psi\beta+\gamma-1}q_2)^{k\phi\gamma}(p^{\gamma}q_1^{k\phi(\psi\beta+\gamma-1)+1}) = (p^{\gamma}q_1)^{k\phi(\psi\beta+\gamma-1)}(p^{\gamma}q_2^{k\phi\gamma}q_1)$$

Note that since $q_1^{\phi} \equiv q_2^{\phi} \equiv 1 \pmod{n}$, we have $[p^{\gamma}q_1^{k\phi(\psi\beta+\gamma-1)+1}]_n = [p^{\gamma}q_1]_n = [p^{\gamma}q_2^{k\phi\gamma}q_1]_n$, so these terms are in Γ_n. Since γ is minimal, these terms are irreducible. We now compute

$$\rho(y) \geq \frac{k\phi(\psi\beta+\gamma-1)+1}{k\phi\gamma L(x)+1} \geq \frac{k\phi(\psi\beta+\gamma-1)+1}{k\phi\gamma\psi+1}$$

Since $\rho(\Gamma_n) \geq \rho(y)$ for arbitrary k, the desired bound follows. □

In the special case of local J-monoids, $\alpha = \gamma$ and $\psi = 1$ in Theorem 10, giving the exact result $\rho(\Gamma_n) = \frac{\alpha+\beta-1}{\alpha}$. This generalizes a result in [6] for local singular ACM's.

Another consequence of Theorem 10 is the following necessary condition for half-factoriality in local CM's. An exact characterization of this property for J-monoids appears in Proposition 2, and for regular congruence monoids in Proposition 1. For other congruence monoids the problem remains open. Congruence monoids with the stronger property of factoriality were characterized 60 years ago in [15].

Corollary 2 *Let Γ_n be a local congruence monoid. If Γ_n is half-factorial, then $\gamma = \beta = 1$.*

Proof We have $1 = \rho(\Gamma_n) \geq \frac{\beta}{\gamma} + \frac{\gamma-1}{\psi\gamma} \geq 1+0$. All inequalities are equalities. □

Proposition 2 *Let Γ_n be a local J-monoid. Then Γ_n is half-factorial if and only if*

1. *u is prime, and*
2. *$[u]_n \in [\Gamma]_n$.*

Proof By Theorem 10, we have $1 = \rho(\Gamma_n) = \frac{\alpha+\beta-1}{\alpha}$, if and only if $\beta = 1$ (i.e. $[u]_n \in [\Gamma]_n$). If $\beta = 1$, then since $1 \leq \gamma \leq \beta$, $\gamma = 1$, and since Γ_n is a J-monoid, $\alpha = \gamma = 1$ and hence u is prime. For the other direction, if u is prime and $[u]_n \in [\Gamma]_n$, then $\beta = 1$. □

Half-factoriality of J-monoids is therefore completely characterized by Propositions 1 and 2, and Theorem 8.

The following examples show that both lower bounds of Theorem 10 are meaningful, and that the upper bound is sometimes, but not always, met.

Example 4 Let $n = 128$, $\Gamma = \{16, 20, 64, 128\}$. We have $p = 2, \gamma = 2, \beta = 4, \alpha = 7$, and $\psi = 2$. Theorem 10 gives us $\max(2, 2.25) \leq \rho(\Gamma_n) \leq 5$.

Example 5 Let $n = 1280$, $\Gamma = \{32, 188, 192, 256, 512, 768, 784, 896, 1024\}$. We have $p = 2, \gamma = 2, \beta = 5, \alpha = 8$, and $\psi = 2$. Theorem 10 gives us $\max(3, 2.75) \leq \rho(\Gamma_n) \leq 6$.

Example 6 Let $n = p^\alpha$, $\Gamma = \{p, p^2, \ldots, p^\alpha\}$. Theorem 10 gives $1 \leq \rho(\Gamma_n) \leq \alpha$. If $p \neq 2$, then $2p^\alpha$ is irreducible (since, for $r < \alpha$, $2p^r$ is not congruent to any element of Γ, modulo p^α). Hence by Theorem 9, $\rho(\Gamma_n) = \alpha$. If instead $p = 2$, then $3p^{\alpha-1} = p^{\alpha-1} + p^\alpha \in \Gamma_n$, and is irreducible (since, for $r < \alpha - 1$, $3p^r$ is not congruent to any element of Γ, modulo p^α). Hence $\rho(\Gamma_n) \geq \alpha - 1$, and we will prove equality. If we had $\rho(\Gamma_n) = \alpha$ then some for some $c \in \mathbb{N}$, cp^α would be irreducible, but $(p)(\frac{c}{2}p^\alpha)$ or $(p)(p^{\alpha-1} + \frac{c-1}{2}p^\alpha)$ are factorizations for c even or odd, respectively.

4 Singular J-Monoids

In the case of singular J-monoids, the factorization structure is determined by the interplay between public and external primes. Motivated by Theorem 4, we make the following definitions. For singular J-monoid Γ_n, we define abelian group $G = G(\Gamma_n) = (\mathbb{Z}/r\mathbb{Z})^\times/[\Gamma]_r$. We write $G = \{g_1, g_2, \ldots, g_m\}$, where g_1 is the identity, and let $\sigma : r^\perp \to G$ denote the natural epimorphism.

We factor $u = u_1^{a_1} u_2^{a_2} \cdots u_k^{a_k}$, where $u_1, \ldots, u_k \in \mathbb{P}$ and $a_1, \ldots, a_k \in \mathbb{N}$. Let $\{e_i\}$ denote the standard basis vectors. We now define $\theta : r^\perp \to \mathbb{N}_0^k \times \mathbb{N}_0^m$ as follows:

$$\theta(u_i) = (e_i, 0), \text{ for } u_i \in \{u_1, u_2, \ldots, u_k\}$$
$$\theta(p) = (0, e_{\sigma(p)}), \text{ for } p \in (\mathbb{P} \cap n^\perp)$$
$$\theta(xy) = \theta(x) + \theta(y), \text{ for } x, y \in r^\perp$$

For $z \in r^\perp$, we consider $\theta(z) = (z', z'') = ((z'_1, \ldots, z'_k), (z''_1, \ldots, z''_m))$. We have $z \in M(u)$ if and only if $z'_i \geq a'_i$ (for each $1 \leq i \leq k$). We have $z \in \Gamma_r$ if and only if

$$\sigma(u_1)^{z'_1} \cdots \sigma(u_k)^{z'_k} g_1^{z''_1} \cdots g_m^{z''_m} = g_1$$

That is, if we consider the sequence in G formed by the images of all the primes dividing z, that sequence must be zero-sum for $[z]_r \in [\Gamma]_r$ and hence $z \in \Gamma_r$. These observations lead to the following result.

Theorem 11 *Let Γ_n be a singular J-monoid. Let $N_1 = ((a_1, \ldots, a_k) + \mathbb{N}_0^k) \times \mathbb{N}_0^m$. Let $N_2 = \{(z', z'') \in \mathbb{N}_0^k \times \mathbb{N}_0^m : \prod_{i=1}^k \sigma(u_i)^{z_i'} \prod_{j=1}^m g_j^{z_j''} = g_1\}$. Then $N = (N_1 \cap N_2) \cup \{(0,0)\}$ is a monoid under addition, and θ is a transfer homomorphism from Γ_n to N.*

Proof First, since $N_1 \cup \{(0,0)\}$ and $N_2 \cup \{(0,0)\}$ are each submonoids of $\mathbb{N}_0^k \times \mathbb{N}_0^m$ under addition, their intersection is. The map $\theta : \Gamma_n \to N$ is a monoid homomorphism by construction, and $\theta(x) = (0,0)$ if and only if $x = 1$. We may choose external primes $q_1, \ldots, q_m$ such that $\sigma(q_i) = g_i$. Hence for $(z', z'') \in N$, we take $z = \prod_{i=1}^k u_i^{z_i'} \prod_{j=1}^m q_j^{z_j''}$ and have $\theta(z) = (z', z'')$. Thus θ is surjective. Now, let $z = u_1^{f_1} \cdots u_k^{f_k} p_1 \cdots p_s$, where the p_i are not necessarily distinct external primes. Suppose now that $\theta(z) = ((f_1, \ldots, f_k), z'') = (x', x'') + (y', y'')$, a factorization in N. For each $g_j \in G$, exactly z_j'' of the $\{p_1, \ldots, p_s\}$ are preimages under σ. Arbitrarily choose x_j'' of these, and let v_j denote their product. Let w_j denote the product of the remaining y_i'' of them. Now set $x = \prod_{i=1}^k u_i^{x_i'} \prod_{j=1}^m v_j$, $y = \prod_{i=1}^k u_i^{y_i'} \prod_{j=1}^m w_j$. We have $x, y \in \Gamma_n$ by Theorem 3, and $\theta(x) = (x', x''), \theta(y) = (y', y'')$ as desired. □

For regular J-monoids, $u = 1$ and the problem reduces to the study of zero-sum sequences as before. For singular J-monoids, the public primes are distinguished and there are minimal requirements for their quantity; the presence of external primes affects which quantities are permitted.

Example 7 Let $n = 1860$ and $\Gamma = \{124, 496, 1364, 1736\}$. We have $u = 31 \cdot 2^2$, $r = 15$, $[\Gamma]_{15} = \{[1]_{15}, [4]_{15}, [-4]_{15}, [-1]_{15}\}$ and $G = (\mathbb{Z}/15\mathbb{Z})^\times / [\Gamma]_{15} \cong (\mathbb{Z}/2\mathbb{Z})$. For $p \in (\mathbb{P} \cap r^\perp)$, we have $\sigma(p) = g_1$ if p is congruent to one of $\{\pm 1, \pm 4\}$ modulo 15, and $\sigma(p) = g_2$ otherwise. We have $N^\bullet \cong \{(a,b,c,d) \in \mathbb{N}_0^4 : a \geq 1, b \geq 2$, and $2|(b+d)\}$. Element (a,b,c,d) is irreducible exactly when $a = 1$ or $b \in \{2,3\}$.

In some sense the opposite extreme of the regular case is where $\sigma(u_1) = \cdots = \sigma(u_k) = g_1$; in this case the zero-sum sequence component of the problem is irrelevant. In the context of ACM's, this corresponds to the case of $M_{xd,yd}$ where $\gcd(x,y) = 1$ and each divisor of d is congruent to 1 modulo y.

Theorem 12 *Let Γ_n be a singular J-monoid. Suppose that $\sigma(u_1) = \cdots = \sigma(u_k) = g_1$. Then there is a transfer homomorphism $\tau : \Gamma_n \to M$ given by $\tau(x) = (\nu_{u_1}(x), \ldots, \nu_{u_k}(x))$, where $M = \big((a_1, \ldots, a_k) + \mathbb{N}_0^k\big) \cup \{0\}$.*

Proof The map τ is a monoid homomorphism by construction, and $\tau(x) = 0$ if and only if $x = 1$. For $z \in M$, we take $x = \prod_{i=1}^k u_i^{z_i}$ and have $\tau(x) = z$; thus τ is surjective. Now, let $x = m \prod_{i=1}^k u_i^{z_i} \in \Gamma_n$, where $\gcd(m,n) = 1$. Since $\sigma(x) = g_1 = \sigma(u_1) = \cdots = \sigma(u_k)$, we have $\sigma(m) = g_1$ as well. Now, suppose

that $z = \tau(x) = (z_1, \ldots, z_k) = z' + z''$, where $z', z'' \in M$. Set $x' = m\prod_{i=1}^{k} u_i^{z_i'}$, $x'' = \prod_{i=1}^{k} u_i^{z_i''}$. We have $x', x'' \in \Gamma_n$ by Theorem 3, and $\tau(x') = z', \tau(x'') = z''$, as desired. □

Recall that in [2] a transfer homomorphism was demonstrated from $M(u)$ to the same $(a_1, \ldots, a_k) + \mathbb{N}_0^k$. Consequently, $M(u)$ and Γ_n share the same factorization invariants if $\sigma(u_1) = \cdots = \sigma(u_k) = g_1$.

In the remainder of this section, we consider local J-monoids, and with three choices of restrictions we determine full and/or accepted elasticity. Our first restriction is that $\beta = \alpha$.

Theorem 13 *Let Γ_n be a J-monoid with $u = p^\alpha$. Suppose that $u \in \Gamma_n$. Then $\rho(\Gamma_n) = \frac{2\alpha-1}{\alpha}$, and it is accepted. Further, if $p^k \notin \Gamma_n$ for all $\alpha < k < 2\alpha$, then Γ_n has full elasticity.*

Proof Theorem 10 gives $\rho(\Gamma_n) = \frac{\alpha+\beta-1}{\alpha}$. Let $q \in (\mathbb{P} \cap n^\perp)$ such that $\sigma(q) = \sigma(p)$. Consider the factorization $(2\alpha-2)(\alpha,0) + (\alpha, \alpha e_{\sigma(q)}) = \alpha(2\alpha-1, e_{\sigma(q)})$ in $\mathbb{N}_0 \times \mathbb{N}_0^m$, which has elasticity $\frac{2\alpha-1}{\alpha}$, as desired.

Now, let $\frac{s}{t} \in [1, \frac{2\alpha-1}{\alpha})$. Let $x \in \Gamma_n$ have the two factorizations given by

$$(p^\alpha)^{t(2\alpha-1)-s\alpha}(p^{2\alpha-1}q)^{\alpha(s-t)} = (p^\alpha)^{s\alpha-s-1}(p^\alpha q^{\alpha(s-t)})$$

Because $\nu_p(y) \geq \alpha$ for all irreducibles y, $L(x) \leq \lfloor \frac{\nu_p(x)}{\alpha} \rfloor = s\alpha - s$, as represented on the right. Now, express any factorization of x as $x_p x_q$, where x_p is a product of irreducibles that are pure powers of p, while x_q is a product of irreducibles that are multiples of q. We have $|x| = |x_p| + |x_q|$ and $\nu_p(x) \leq \alpha|x_p| + (2\alpha-1)|x_q|$ since $\nu_p(y) = \alpha$ if $y \in x_p$ and $\nu_p(y) \leq 2\alpha - 1$ if $y \in x_q$. We have $|x_q| \leq \nu_q(x) = \alpha(s-t)$. We now have $|x| \geq \frac{\nu_p(x)-(2\alpha-1)|x_q|}{\alpha} + |x_q| = \frac{1}{\alpha}(\nu_p(x) - (\alpha-1)|x_q|) \geq \frac{1}{\alpha}(\nu_p(x) - (\alpha-1)\alpha(s-t)) = \alpha t - t$. Hence the minimal length factorization is represented on the left. Combining, we have $\rho(x) = \frac{\alpha s - s}{\alpha t - t} = \frac{s}{t}$, as desired. □

Our next restriction is that $\alpha = 1$.

Theorem 14 *Let Γ_n be a J-monoid with $u = p$. Then $\rho(\Gamma_n) = \beta$, and Γ_n has full elasticity.*

Proof Theorem 10 gives $\rho(\Gamma_n) = \beta$. Let $q \in (\mathbb{P} \cap n^\perp)$ such that $\sigma(q) = \sigma(p)^{-1}$. Let $\frac{s}{t} \in [1, \beta)$. Let $x \in \Gamma_n$ have the two factorizations given by

$$(pq)^{\beta s-\beta t+1}(p^\beta)^{\beta t-s-1} = (p^\beta)^{\beta t-t-1}(pq^{\beta s-\beta t+1})$$

By Theorem 9, $\nu_p(y) \leq \beta$ for all irreducibles y. Hence $l(x) \geq \lceil \frac{\nu_p(x)}{\beta} \rceil = \beta t - t - 1$, as represented on the right. Now, express any factorization of x as $x_p x_q$, where x_p is a product of irreducibles that are pure powers of p, while x_q is a product of irreducibles that are multiples of q. We have $|x| = |x_p| + |x_q|$ and $\nu_p(x) \geq \beta|x_p| + |x_q|$ since $\nu_p(y) \geq \beta$ if $y \in x_p$ and $\nu_p(y) \geq \alpha = 1$ if $y \in x_q$. We have $|x_q| \leq \nu_q(x) = \beta s - \beta t + 1$. We now have $|x| \leq \frac{\nu_p(x)-|x_q|}{\beta} + |x_q| =$

$\frac{1}{\beta}(\nu_p(x) + (\beta-1)|x_q|) \leq \frac{1}{\beta}(\nu_p(x) + (\beta-1)(\beta s - \beta t + 1)) = \beta s - s$. Hence the maximal length factorization is represented on the left. Combining, we have $\rho(x) = \frac{\beta s - s}{\beta t - t} = \frac{s}{t}$, as desired. □

In general the question of accepted elasticity in local ACM's (and hence local J-monoids) is difficult; see, e.g. [10]. We give one more result in this direction, under a restriction based on $\sigma(p)$ and the structure of G.

Theorem 15 *Let Γ_n be a J-monoid with $u = p^\alpha$ and set $g = \sigma(p)^{-1}$. Suppose there is some $h \in G$ such that $|h| = |g| = \beta$ and $\langle h \rangle \cap \langle g \rangle = g_1$. Then the elasticity of Γ_n is accepted.*

Proof Let $q \in (\mathbb{P} \cap n^\perp)$ such that $\sigma(q) = h$, and let $r \in (\mathbb{P} \cap n^\perp)$ such that $\sigma(r) = h^{-1}g$.

We have the factorization

$$\alpha(\alpha+\beta-1, (\alpha+2\beta-1)e_{\sigma(q)} + (\alpha-1)e_{\sigma(r)}) +$$

$$+\alpha(\alpha+\beta-1, (\alpha-1)e_{\sigma(q)} + (\alpha+2\beta-1)e_{\sigma(r)}) =$$

$$= (2\alpha+2\beta-2)(\alpha, \alpha(e_{\sigma(q)} + e_{\sigma(r)}))$$

We first show that each term is in N. $(\alpha+\beta-1, (\alpha+2\beta-1)e_{\sigma(q)} + (\alpha-1)e_{\sigma(r)})$ corresponds to $(g^{-1})^{\alpha+\beta-1}h^{\alpha+2\beta-1}(h^{-1}g)^{\alpha-1} = g^{-\beta}h^{2\beta} = g_1$. The next term is similar, and the last corresponds to $(g^{-1})^\alpha h^\alpha (h^{-1}g)^\alpha = g_1$. We now show that $p^{\alpha+\beta-1}q^{\alpha+2\beta-1}r^{\alpha-1}$ is irreducible in Γ_n. Suppose we factor it as xy; then $\nu_p(x) \in [\alpha, \beta-1]$. But since $\sigma(x) = g_1$, $\nu_r(x) \equiv \nu_p(x) \pmod{|g|}$, which is impossible since $\nu_r(x) \leq \alpha - 1$. Similarly, $p^{\alpha+\beta-1}q^{\alpha-1}r^{\alpha+2\beta-1}$ is irreducible and hence this factorization has elasticity $\frac{2\alpha+2\beta-2}{2\alpha} = \rho(\Gamma_n)$.

□

5 Semi-Regular Γ_n

We conclude with some rather meager results on semi-regular congruence monoids. This class of CM's has very rich structure, is disjoint from ACM's, and has the most opportunity for further work.

Of our earlier elasticity results, only Theorems 6 and 7 apply for semi-regular CM's, which determine when elasticity is infinite. To refine this, for semi-regular CM Γ_n we define $\Gamma^\perp = \Gamma \cap n^\perp$ and $\Gamma^\circ = \Gamma \setminus \Gamma^\times = \Gamma \setminus n^\perp$; each must be nonempty since $\{[1]_n, [u^{\phi(r)}]_n\} \subseteq [\Gamma]_n$, by Lemma 3 and Theorem 2 respectively. We now use this notation to present two lower bounds for $\rho(\Gamma_n)$, in Theorems 16 and 17.

Theorem 16 *Let Γ_n be a semi-regular congruence monoid. Then $\Gamma_n^\perp$ is a regular congruence monoid, and $\rho(\Gamma_n) \geq \rho(\Gamma_n^\perp)$.*

Proof First, let $g_1, g_2 \in \Gamma_n^{\perp} \subseteq \Gamma_n$. Hence $g_1 g_2 \in \Gamma_n$; but also $g_1 g_2 \in n^{\perp}$ so in fact $g_1 g_2 \in \Gamma_n^{\perp}$ and hence $\Gamma_n^{\perp}$ is a congruence monoid. By construction, $\Gamma_n^{\perp}$ is regular.

Suppose that $x = yz$ with $x, y, z \in \Gamma_n$, and further $x \in \Gamma_n^{\perp}$. Then also $y, z \in \Gamma_n^{\perp}$, because otherwise y (say) has $y \notin n^{\perp}$. Then, some public prime divides y and hence x, a contradiction. Hence $\rho(x)$ in Γ_n agrees with $\rho(x)$ in $\Gamma_n^{\perp}$. Since this holds for all $x \in \Gamma_n^{\perp}$, the conclusion follows. □

Consequently, if Γ_n is a half-factorial semi-regular CM, then $\Gamma_n^{\perp}$ is a half-factorial regular CM and Proposition 1 applies.

Theorem 17 *Let Γ_n be a semi-regular congruence monoid. Then Γ_n° is a congruence monoid that is not weakly regular. Further, if Γ_n° is a J-monoid, then*

1. *If $u = p^{\alpha}$ is a prime power, then $\rho(\Gamma_n) \geq \frac{\alpha+\beta-1}{\beta}$, where β is minimal such that $p^{\beta} \in \Gamma_n$.*
2. *If u is not a prime power, then $\rho(\Gamma_n) = \infty$.*

Proof First, let $g_1, g_2 \in \Gamma_n^{\circ} \subseteq \Gamma_n$. Hence $g_1 g_2 \in \Gamma_n$; but also $g_1 g_2 \notin n^{\perp}$ so in fact $g_1 g_2 \in \Gamma_n^{\circ}$ and hence Γ_n° is a congruence monoid. By construction, Γ_n° is not weakly regular, and shares u, r (though not necessarily d) with Γ_n. If Γ_n° is a local J-monoid, then it also shares α, β with Γ_n.

Next, suppose that Γ_n° is a J-monoid, and $u = u_1 u_2$ for some $u_1, u_2 > 1$ with $\gcd(u_1, u_2) = 1$. For each $m \in \mathbb{N}$, set $x_m = (u^{\phi(r)} u_1^{m\phi(r)})(u^{\phi(r)} u_2^{m\phi(r)}) = (u^{\phi(r)})^{(m+2)}$. Note that since x_m consists entirely of public primes, all irreducibles dividing x_m in Γ_n, must actually be contained in Γ_n° (and hence $\rho(x_m)$ is the same in both). By Theorem 3, each of $(u^{\phi(r)} u_1^{m\phi(r)})$, $(u^{\phi(r)} u_2^{m\phi(r)})$, $(u^{\phi(r)}) \in \Gamma_n^{\circ}$, although they might not be irreducible. However, $L(u^{\phi(r)} u_1^{m\phi(r)}) \leq \phi(r)$ and $L(u^{\phi(r)} u_2^{m\phi(r)}) \leq \phi(r)$, by considering the primes in u_2, u_1 respectively, since u must divide every irreducible. Hence $2 \leq l(x_m) \leq 2\phi(r)$, while $L(x_m) \geq m+2$, we conclude that $\rho(x_m) \geq \frac{m+2}{2\phi(r)}$. Letting $m \to \infty$ we conclude that $\rho(\Gamma_n) = \rho(\Gamma_n^{\circ}) = \infty$.

Next, suppose that Γ_n° is a J-monoid, with $u = p^{\alpha}$. By the comments following Theorem 10, we have $\rho(\Gamma_n^{\circ}) = \frac{\alpha+\beta-1}{\alpha}$. By Theorem 9, there is some irreducible $z \in \Gamma_n^{\circ}$ with $\nu_p(z) = \alpha + \beta - 1$. Suppose first that $p^{\alpha+\beta-1} \equiv 1 \pmod{r}$. Then we consider $x = (p^{\alpha+\beta-1})^{\beta} = (p^{\beta})^{\alpha+\beta-1}$. Since all factors of x are public primes, every irreducible dividing x is from Γ_n°. Hence the elasticity of x in Γ_n agrees with the elasticity of x in Γ_n°, which is $\frac{\alpha+\beta-1}{\beta}$. Lastly, we consider the case where $p^{\alpha+\beta-1} \not\equiv 1 \pmod{r}$. We may write $z = p^{\alpha+\beta-1} s$, for some $s \in (\mathbb{P} \cap n^{\perp})$ and $s \not\equiv 1 \pmod{r}$. Now, set $x = (p^{\alpha+\beta-1} s)^{\phi(n)\beta} = (p^{\beta})^{\phi(n)(\alpha+\beta-1)} (s^{\phi(n)})^{\beta}$. Within Γ_n, factors of $(p^{\alpha+\beta-1} s)$ must of necessity be both from Γ_n°, apart from $(p^{\alpha+\beta-1})(s)$, which is excluded since $p^{\alpha+\beta-1} \notin \Gamma_n^{\circ}$. Hence $p^{\alpha+\beta-1}$ is irreducible in Γ_n and thus $l(x) \leq \phi(n)\beta$. Each of $p^{\beta}, s^{\phi(n)} \in \Gamma_n$, and hence $L(x) \geq \phi(n)(\alpha + \beta - 1) + \beta$. Combining, we have $\rho(x) \geq \frac{\phi(n)(\alpha+\beta-1)+\beta}{\phi(n)\beta} > \frac{\alpha+\beta-1}{\beta}$. □

Note that Theorem 17 leaves open the possibility that Γ_n° is a J-monoid and $\frac{\alpha+\beta-1}{\beta} \leq \rho(\Gamma_n) < \rho(\Gamma_n^\circ) = \frac{\alpha+\beta-1}{\alpha}$. We wonder if this is possible.

We conclude with a variation of Theorem 17 that provides a family of examples that have infinite and full elasticity; in contrast, it was shown in [6] that no ACM has infinite and full elasticity.

Theorem 18 *Let Γ_n be a semi-regular congruence monoid. Suppose that $u \in \Gamma_n$, and that Γ_n° is a J-monoid with infinite elasticity. Then Γ_n has infinite and full elasticity.*

Proof Since Γ_n° is a J-monoid with infinite elasticity, we must have $u = u_1u_2$ for some $u_1, u_2 > 1$ with $\gcd(u_1, u_2) = 1$. Set $x_m = (uu_1^{2m\phi(r)})(uu_2^{2m\phi(r)}) = (u)^{2m\phi(r)+2}$. Since x_m consists entirely of public primes, all irreducibles dividing x_m must actually be contained in Γ_n°, and $\rho(x_m)$ agrees in both. By Theorem 3, each of $(uu_1^{2m\phi(r)})$, $(uu_2^{2m\phi(r)}) \in \Gamma_n^\circ$. Further, by considering the primes in u_2, u_1 respectivly, each is irreducible, as is u. Therefore $L(x_m) = 2m\phi(r)+2$ and $l(x_m) = 2$. Now, by Theorem 1, there is some prime $\pi \in \Gamma_n$. Let $\frac{s}{t} \geq 1$. We consider $x = \pi^{2t\phi(r)-2}x_{s-t}$. We have $\rho(x) = \frac{L(x_{s-t})+2t\phi(r)-2}{l(x_{s-t})+2t\phi(r)-2} = \frac{s}{t}$, as desired. □

Many problems involving arithmetic of congruence monoids remain open:

1. Characterizing half-factoriality for non-regular, non-J-monooids.
2. Computing elasticity (or even good bounds) when d is a prime power but u is not.
3. Computing elasticity (or even good bounds) for semi-regular CM's.
4. Computing elasticity (or even good bounds) for CM's that are not semi-regular, but have $d = 1$.
5. Determining accepted and full elasticity, apart from the several classes considered above.
6. Determining various other nonunique factorization invariants such as delta sets, catenary degree, etc.

Acknowledgements This research was supported in part by NSF REU grant 1061366.

References

1. D. D. Anderson and Jonathan Preisser. Factorization in integral domains without identity. *Results Math.*, 55(3-4):249–264, 2009.
2. Paul Baginski and Scott T. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory: Contributions from CANT 2011*. Springer, forthcoming.
3. Paul Baginski, Scott T. Chapman, Christopher Crutchfield, K. Grace Kennedy, and Matthew Wright. Elastic properties and prime elements. *Results Math.*, 49(3-4):187–200, 2006.
4. Paul Baginski, Scott T. Chapman, and George J. Schaeffer. On the delta set of a singular arithmetical congruence monoid. *J. Théor. Nombres Bordeaux*, 20(1):45–59, 2008.

5. 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(2):68–72, 2007.
6. M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math.*, 108(1):105–118, 2007.
7. M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. A theorem on accepted elasticity in certain local arithmetical congruence monoids. *Abh. Math. Semin. Univ. Hambg.*, 79(1):79–86, 2009.
8. M. Banister, J. Chaika, and W. Meyerson. Technical report, Trinity University REU, 2003.
9. S. T. Chapman and David Steinberg. On the elasticity of generalized arithmetical congruence monoids. *Results Math.*, 58(3-4):221–231, 2010.
10. Lorin Crawford, Vadim Ponomarenko, Jason Steinberg, and Marla Williams. Accepted elasticity in local arithmetic congruence monoids. under review.
11. Alfred Geroldinger and Franz Halter-Koch. Congruence monoids. *Acta Arith.*, 112(3):263–296, 2004.
12. Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.
13. Franz Halter-Koch. Arithmetical semigroups defined by congruences. *Semigroup Forum*, 42(1):59–62, 1991.
14. Franz Halter-Koch. C-monoids and congruence monoids in Krull domains. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 71–98. Chapman & Hall/CRC, Boca Raton, FL, 2005.
15. R. D. James and Ivan Niven. Unique factorization in multiplicative systems. *Proc. Amer. Math. Soc.*, 5:834–838, 1954.
16. Matthew Jenssen, Daniel Montealegre, and Vadim Ponomarenko. Irreducible Factorization Lengths and the Elasticity Problem within $\mathbb{N}$. *Amer. Math. Monthly*, 120(4):322–328, 2013.