Factorization Properties of Congruence Monoids

Arielle Fujiwara, Joseph Gibson, Matthew Jenssen,
Daniel Montealegre, Ari Tenzer

August 9, 2012

Abstract

Let $n \in \mathbb{N}$, $\Gamma \subseteq \mathbb{N}$ and define $\Gamma_n = \{\overline{x} \in \mathbb{Z}_n \mid x \in \Gamma\}$ the set of residues of elements of Γ modulo n. If Γ_n is multiplicatively closed we may define the following submonoid of the naturals: $H_{\Gamma_n} = \{x \in \mathbb{N} \mid \overline{x} = \overline{\gamma}, \overline{\gamma} \in \Gamma_n\} \cup \{1\}$ known as a *congruence monoid* (CM). Unlike the naturals, many CMs enjoy the property of non-unique factorization into irreducibles. This opens the door to the study of arithmetic invariants associated with non-unique factorization theory; most important to us will be the concept of *elasticity*. In particular we give a complete characterization of when a given CM has finite elasticity. Throughout we explore the arithmetic properties of H_{Γ_n} in terms of the arithmetic and algebraic properties of Γ_n.

1 Introduction and Preliminaries

By the Fundamental Theorem of Arithmetic each element of the set $\mathbb{N}$, the naturals, can be written uniquely as a product of primes (or irreducibles). For multiplicatively closed subsets of $\mathbb{N}$ containing 1, the corresponding property of unique factorization into irreducibles is not in general inherited from $\mathbb{N}$. In this paper we are interested in a certain class of subsets of $\mathbb{N}$ called Congruence Monoids. Before we begin studying the non-unique factorization theory of such objects, let us define some terms:

Definition 1. *A set S equipped with a binary operation is a **semigroup** if it is closed and associative with respect to that operation.*

Definition 2. *A **monoid** is a semigroup that contains an identity element.*

Definition 3. *Let M be a monoid, let $M^\times$ denote the set of units in M, and let $M^\bullet = M \backslash M^\times$. We say $x \in M^\bullet$ is **irreducible** if whenever $x = yz$ and $y, z \in M$, either $y \in M^\times$ or $z \in M^\times$. If x is not irreducible, it is **reducible**.*

Definition 4. *We say a monoid M is **atomic** if every non-unit can be factored into irreducibles.*

In a monoid that does not possess unique factorization into irreducibles, we may encounter elements that yield factorizations of different lengths. This motivates the following definition.

Definition 5. *We define the* ***length set*** *of x, $\mathcal{L}(x)$, to be:*

$$\mathcal{L}(x) = \left\{ m \in \mathbb{N} \mid x = \prod_{i=1}^{m} \alpha_i \right\}$$

where the α_i are irreducibles in M. Let $L(x) = \max\{\mathcal{L}(x)\}$ and $l(x) = \min\{\mathcal{L}(x)\}$. We define the ***elasticity*** *of x to be $\rho(x) = \frac{L(x)}{l(x)}$, and the* ***elasticity of the monoid*** *M to be:*

$$\rho(M) = \sup_{x \in M} \rho(x).$$

Let $n \in \mathbb{N}$, $\Gamma \subseteq \mathbb{N}$ and define $\Gamma_n = \{\overline{x} \in \mathbb{Z}_n \mid x \in \Gamma\}$, the set of residues of elements of Γ modulo n. If Γ_n is multiplicatively closed we may define the following submonoid of the naturals: $H_{\Gamma_n} = \{x \in \mathbb{N} \mid \overline{x} = \overline{\gamma}, \overline{\gamma} \in \Gamma_n\} \cup \{1\}$ known as a **congruence monoid** (CM). In the case where $\Gamma_n = \{a\}$ is a singleton we refer to H_{Γ_n} as an **Arithmetical Congruence Monoid** (ACM), which is denoted by $M_{a,n}$. ACMs have been the focus of much study in recent years. CMs are a natural generalization of ACMs.

Broadly speaking, one encounters different behaviors depending on whether Γ_n contains units or not. This leads us to introduce the following taxonomy:

1. We say that H_{Γ_n} is **regular** if $\Gamma_n = \Gamma_n^{\times}$
2. We say that H_{Γ_n} is **singular** if $\Gamma_n = \Gamma_n^{\bullet}$
3. We say that H_{Γ_n} is **semi-regular** otherwise.

A useful tool for showing that two distinct monoids have the same factorization properties (defined below) is the *transfer homomorphism* defined below.

Definition 6. *Let M and N be commutative, cancellative, atomic monoids and $\sigma : M \longrightarrow N$ be a monoid homomorphism. σ is a* ***transfer homomorphism*** *if:*

* *$\sigma(u) \in N^{\times}$ for any $u \in M^{\times}$*
* *$\sigma(u) \notin N^{\times}$ for any $u \notin M^{\times}$*
* *(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 $\sigma(z) = vb$.*

Transfer homomorphisms preserve the length sets of each element in the monoid. Therefore, they preserve all the information that can be deduced from these length sets. We shall refer to the properties of a monoid M preserved under a transfer homomorphism as the **factorization properties** of M. Below, we list some examples:

1. **Accepted elasticity**: We say a CM, M, has accepted elasticity if $\exists x \in M$ such that $\rho(x) = \rho(M)$.
2. **Full elasticity**: We say a CM, M, has full elasticity if $\forall q \in \mathbb{Q} \cap [1, \rho(M)), \exists x \in M$ such that $\rho(x) = q$.
3. **Delta set**: Order $\mathcal{L}(X) = \{\ell_1, ..., \ell_j\}$ with $\ell_i < \ell_{i+1}$ for $1 \leq i < j$. Denote $\Delta(x) = \{\ell_{i+1} - \ell_i \text{ for } 1 \leq i < j\}$. By the $\Delta - set$ of M, we mean

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

Definition 7. *Define $v_p(x)$, the **p-adic evaluation of x** to be the greatest integer k such that $p^k \mid x$.*

An important constant used in factorization theory is the Davenport constant.

Definition 8. *Let G be a finite abelian group. The* Davenport constant *of G is the length of the longest minimal zero-sum sequence of G and is denoted by $D(G)$.*

Definition 9. *Let $\Gamma_n = \{\gamma_1, \ldots, \gamma_m\}$ we define the **gcd-set** of H_{Γ_n} as $\mathcal{D}_{\Gamma_n} = \{\gcd(\gamma_1, n), \ldots, \gcd(\gamma_m, n)\}$*

2 General Congruence Monoids

In this section we consider what information we can glean from a general CM where we place no restrctions on Γ or n. From the gcd-set $\mathcal{D}_{\Gamma_n}$ we can determine two parameters d and δ which play an important role in the factorization theory of a CM: let $\delta = \text{lcm}(\mathcal{D}_{\Gamma_n})$ and $d = \gcd(\mathcal{D}_{\Gamma_n})$ and define $\zeta = n/\delta$. Before we continue we require a short lemma:

Lemma 1. *Let S be a semigroup and G a group. Suppose that $\theta : S \longrightarrow G$ is a bijection such that $\theta(s_1 s_2) = \theta(s_1)\theta(s_2)$ $\forall s_1, s_2 \in S$. Then S is in fact a group and $S \cong G$.*

Proof. It suffices to show that S contains an identity element and that each element of S has an inverse. Let e_G denote the identity element in G. Since θ is surjective, $\theta(e_S) = e_G$ for some $e_S \in S$. For $s \in S$,

$$\theta(e_S s) = \theta(e_S)\theta(s) = e_G\theta(s) = \theta(s)$$

hence by injectivity of θ, $e_S s = s$. Similarly $s e_S = s \ \forall s \in S$ so e_S is an identity element in S. Now, for $s \in S$ pick $s' \in S$ such that $\theta(s') = \theta(s)^{-1}$ (possible by surjectivity of θ).

$$\theta(ss') = \theta(s)\theta(s') = \theta(s)\theta(s)^{-1} = e_G = \theta(e_S)$$

hence $ss' = e_S$ by injectivity and similarly $s's = e_S$. s' is an inverse of s in S hence S is a group and θ is a group isomorphism. □

The following theorem is of great use in the study of singular CMs. We give the statement and proof here and return to it in a later section.

Theorem 2. *Let H_{Γ_n} be a CM. Then*

$$M_{\delta,\delta} \cap H_{\Gamma_\zeta} \subseteq H_{\Gamma_n} \subseteq M_{d,d}$$

where H_{Γ_ζ} is regular and the following are equivalent:

1. $H_{\Gamma_n} = M_{\delta,\delta} \cap H_{\Gamma_\zeta}$
2. $\delta = d$
3. *Multiplication induces a group structure on Γ_n.*

Proof. Let $\Gamma_n = \{\gamma_1, \ldots, \gamma_m\}$ and $d_i = \gcd(\gamma_i, n)$. We begin by showing that H_{Γ_ζ} is regular. Note that $\overline{\gamma_1} \cdots \overline{\gamma_m} \in \Gamma_n$ since Γ_n is closed so without loss of generality let $\overline{\gamma_1} \cdots \overline{\gamma_m} = \overline{\gamma_1}$. Now, $\delta \mid \gamma_1 \cdots \gamma_m$ and $\delta \mid n$ hence $\gcd(\gamma_1 \cdots \gamma_m, n) \geq \delta$ however $\gcd(\gamma_1 \cdots \gamma_m, n) = \gcd(\gamma_1, n) = d_1 \leq \delta$ hence $d_1 = \delta$. It follows that $d_i \mid d_1 \ \forall i$ and in particular $\delta = d_1 = \max\{d_1, \ldots, d_m\}$. Suppose that $p \mid \zeta = n/\delta$ and $p \mid \gamma_i$ for some prime $p \in \mathbb{N}$ and $1 \leq i \leq m$. It follows that $p\delta \mid n$ and $p\delta \mid \gamma_i\gamma_1$ hence $\gcd(\gamma_i\gamma_1, n) \geq p\delta$ contradicting the maximality of d_1 since $\overline{\gamma_i}\overline{\gamma_1} \in \Gamma_n$. We conclude that $\gcd(\zeta, \gamma_i) = 1 \ \forall i$ and so $\Gamma_\zeta \subseteq \mathbb{Z}_\zeta^\times$ i.e. H_{Γ_ζ} is regular. It is also useful to note that $\gcd(\delta, \zeta) = 1$ since $\delta \mid \gamma_1$ and $\gcd(\gamma_1, \zeta) = 1$.

Let us now show the first inclusion in the above statement. Let $x \in (M_{\delta,\delta} \cap H_{\Gamma_\zeta})^\bullet$ so that $\delta \mid x$ and $x \equiv \gamma_j \pmod{\zeta}$ for some $1 \leq j \leq m$. Now, $\gamma_1 \in \mathbb{Z}_\zeta^\times$ hence $\gamma_1^k \equiv 1 \pmod{\zeta}$ for some $k \geq 1$ and so $x \equiv \gamma_j\gamma_1^k \pmod{\zeta}$ i.e. $x = \gamma_j\gamma_1^k + c\zeta$ for some $c \in \mathbb{Z}$. We have $\delta \mid x$ and $\delta \mid \gamma_j\gamma_1^k$ hence $\delta \mid c\zeta$ and so $n = \delta\zeta \mid c\zeta$, since $\gcd(\delta, \zeta) = 1$, thus $x \equiv \gamma_j\gamma_1^k \pmod{n}$ so $x \in H_{\Gamma_n}$ as required.

The second inclusion is straightforward: If $x \in H_{\Gamma_n}^\bullet$ i.e. $x \equiv \gamma_j \pmod{n}$ for some $1 \leq j \leq m$ then $x \equiv \gamma_j \pmod{f}$ so $x \in H_{\Gamma_f}$ and $x \in M_{d,d}$ since $d \mid n$ and $d \mid \gamma_j$ so $d \mid x$.

We shall now demonstrate the stated equivalences. It is simplest to show that (1) and (3) are both equivalent to (2).
(1) $\iff$ (2): Suppose that $\delta = d$. Then by the above, $M_{\delta,\delta} \cap H_{\Gamma_\zeta} \subseteq H_{\Gamma_n} \subseteq \overline{M_{\delta,\delta} \cap H_{\Gamma_n}}$. However, since $\zeta \mid n$ we have that $H_{\Gamma_n} \subseteq H_{\Gamma_\zeta}$ and so we must have

$M_{\delta,\delta} \cap H_{\Gamma_\zeta} = H_{\Gamma_n}$. For the converse suppose that $\delta \neq d$. Then $\delta \nmid \gamma_j$ for some j and so $\gamma_j + n \in H_{\Gamma_n}$ yet $\gamma_n + n \notin M_{\delta,\delta}$ (note that we consider $\gamma_j + n$ rather than just γ_j to account for the case where $\gamma_j = 1$). We conclude that if $\delta \neq d$ then $M_{\delta,\delta} \cap H_{\Gamma_\zeta} \subsetneq H_{\Gamma_n}$.

(2) $\iff$ (3): Suppose that $\delta = d$ and consider the map

$$\begin{array}{ccccc} & & \theta : \Gamma_n & \longrightarrow & \Gamma_\zeta \\ \gamma_i & (\text{mod } n) & \longmapsto & \gamma_i & (\text{mod } \zeta) \end{array}$$

θ is clearly well-defined and surjective. Suppose that $\gamma_i \equiv \gamma_j \pmod{\zeta}$ some $1 \leq i, j \leq m$ but $\delta = d$ so that $0 \equiv \gamma_i \equiv \gamma_j \pmod{\delta}$ hence $\gamma_i \equiv \gamma_j \pmod{n}$, since $n = \delta\zeta$ and $\gcd(\delta, \zeta) = 1$, thus θ is injective. Finally, for $\gamma_i, \gamma_j \in \Gamma$ we have $\theta(\gamma_i\gamma_j \mod n) = \gamma_i\gamma_j \pmod{\zeta} = \theta(\gamma_i \mod n)\theta(\gamma_j \mod n)$ so by Lemma 1 $(\Gamma_n, \cdot)$ is a group isomorphic to $\Gamma_\zeta \subseteq \mathbb{Z}_n^\times$.

Conversely, suppose that $(\Gamma_n, \cdot)$ is a group with identity element $\overline{\gamma_i}$. For $1 \leq j \leq m$ we have $\gamma_j\gamma_i \equiv \gamma_j \pmod{n}$ and $d_i \mid \gamma_i, n$ hence $d_i \mid \gamma_j$ so that $d_i \mid d_j$. On the other hand $\gamma_j\gamma_k \equiv \gamma_i \pmod{n}$ for some k (γ_k is the inverse of γ_j in $(\Gamma_n, \cdot)$) and $d_j \mid \gamma_j, n$ hence $d_j \mid \gamma_i$ so $d_j \mid d_i$. We conclude that $d_i = d_j$ and since j was arbitrary we have $d_1 = d_2 = \ldots = d_m$ hence $\delta = d$ as required. □

The above theorem hinges on information contained in the gcd-set $\mathcal{D}_{\Gamma_n}$. It is a surprising fact that the information afforded by the gcd-set also allows us to answer the fundamental question of whether a given CM has finite elasticity. Before we present a result to this effect we must set up some machinery:

Definition 10. *Let $S \subseteq \mathbb{N}$. We say that a set T is* S-essential *if $T = \{p : p$ prime and $p \mid x\}$ for some $x \in S$.*

Lemma 3. *Let $n \in \mathbb{N}$ and let $T = \{p_1, \ldots, p_m\}$ be a set of rational primes. Then $\exists r$ such that $p_i^{2r} \equiv p_i^r \pmod{n}$ for all $1 \leq i \leq m$.*

Proof. Let $v_i = v_{p_i}(n)$ then for $r \geq v_i$:

$$p_i^{2r} \equiv p_i^r \pmod{n} \iff p_i^{2r-v_i} \equiv p_i^{r-v_i} \pmod{np_i^{-v_i}}$$

$$\iff p_i^r \equiv 1 \pmod{np_i^{-v_i}}$$

where we've used the fact that $\gcd(p_i, np_i^{-v_i}) = 1$. The above shows that $r = \text{lcm}(\varphi(np_1^{-v_1}), \ldots, \varphi(np_m^{-v_m}))$ has the required property for the lemma. □

The following lemma is a restatement of Lemma 1.4.9 of p.27 [11].

Lemma 4. *Let $(A, \cdot)$ be a finite abelian group, $x = a_1 \cdots a_k$ a product of elements of A, and D the Davenport constant of A. If $k \geq D + 1$ then $a_{i_1} \cdots a_{i_l} = e_A$ for some $1 \leq i_1, \ldots, i_l \leq k$ and $l \leq D$.*

Definition 11. *For $z \in \mathbb{N}$, let $\wp(z)$ denote the multiset of prime divisors of z in $\mathbb{N}$.*

Corollary 5. *Let H_{Γ_n} be a congruence monoid and let $x \in H_{\Gamma_n}$. If $\Gamma_n^\times \neq \emptyset$ and $\wp(x)$ contains more than $D(\mathbb{Z}_n^\times/\Gamma_n^\times)$ elements coprime to n, then x is reducible in H_{Γ_n}.*

Proof. Let $D = D(\mathbb{Z}_n^\times/\Gamma_n^\times)$. By hypothesis there exist rational primes $p_1, \ldots, p_k$ (not necessarily distinct) coprime to n such that $p_1 \cdots p_k \mid x$ and $k > D$. By Lemma 4, $\overline{p_{i_1}}\Gamma_n^\times \cdots \overline{p_{i_l}}\Gamma_n^\times = \Gamma_n^\times$ for some $1 \leq i_1, \ldots, i_l \leq k$ and $l \leq D$ i.e. $\overline{p_{i_1}} \cdots \overline{p_{i_l}} \in \Gamma_n^\times$. It follows that $u = p_{i_1} \cdots p_{i_l} \in H_{\Gamma_n}$ and we write $x = uy$ where $1 < y \in \mathbb{N}$. Now, u is a unit modulo n and $y \equiv xu^{-1} \pmod{n}$ hence $y \in H_{\Gamma_n}$ by multiplicative closure of Γ_n. Thus x is reducible as claimed. □

Remark: Letting $G = \mathbb{Z}_n^\times/\Gamma_n^\times$, we could replace $D(G)$ in the above by $|G|^2$ and lose the need for Lemma 4. This is because given $|G|^2$ elements of G, at least $|G|$ must be the same (equal to g, say) and $g^{|G|} = e_G = \Gamma_n^\times$.

Theorem 6. *A congruence monoid H_{Γ_n} has finite elasticity if and only if every minimal H_{Γ_n}-essential set is a singleton.*

Proof. $\Rightarrow$) Suppose that $T = \{p_1, \ldots, p_m\}$ is a minimal H_{Γ_n}-essential set that is not a singleton i.e. $m \geq 2$. Since T is H_{Γ_n}-essential, $\exists e_1, \cdots, e_m \geq 1$ such that $p_1^{e_1} \cdots p_m^{e_m} \in H_{\Gamma_n}$. By Lemma 3 we can pick r such that $p_i^{2r} \equiv p_i^r \pmod{n}$ $\forall i$. Note that for $k_1 \ldots, k_m \geq 1$ we have $p_1^{k_1 r} \cdots p_m^{k_m r} \in H_{\Gamma_n}$ since:

$$p_1^{k_1 r} \cdots p_m^{k_m r} \equiv p_1^r \cdots p_m^r \equiv (p_1^{e_1} \cdots p_m^{e_m})^r \pmod{n}$$

Consequently, letting $a = p_1 \cdots p_m$, the following expressions are factorizations in H_{Γ_n} for $k \geq 1$:

$$x = (p_1^r \cdots p_m^r)^{k(t-1)+1} = \prod_{i=1}^{m} p_i^r \left(\frac{a}{p_i}\right)^{rk}$$

The LHS factors into at least $k(t-1)+1$ irreducibles whereas the RHS factors into at most rm irreducibles since each irreducible must be divisible by $p_1, \ldots, p_m$ by minimality of T. It follows that

$$\rho(x) \geq \frac{k(t-1)+1}{rm}$$

and $(k(t-1)+1)/rm \to \infty$ as $k \to \infty$ since $t \geq 2$.

$\Leftarrow$) Assume that every minimal H_{Γ_n}-essential set is a singleton. Let $Q = \{q \in \mathbb{N} : q \text{ prime}, q \mid n \text{ and } \{q\} \text{ an } H_{\Gamma_n}\text{-essential set}\}$, $Q = \{q_1, \ldots, q_t\}$ say. For each $q_i \in Q$, $\exists k_i \geq 1$ such that $p_i^{k_i} \in H_{\Gamma_n}$. By Lemma 3 we can pick r_i minimal such that $p_i^{2r_i} \equiv p_i^{r_i} \pmod{n}$. $p_i^{r_i} \in H_{\Gamma_n}$ since $p_i^{r_i} \equiv (p_i^{k_i})^{r_i} \pmod{n}$. Suppose now that $yp_i^c \in H_{\Gamma_n}$ where $c \geq 2r_i$, $c = 2r_i + c'$ say. $yp_i^c = (p_i^{r_i})(yp_i^{c-r_i})$ and

$yp_i^{c-r_i} \in H_{\Gamma_n}$ since $yp_i^c = yp_i^{2r_i+c'} \equiv yp_i^{r_i+c'} = yp_i^{c-r_i} \pmod{n}$. We conclude that any irreducible in H_{Γ_n} can have p_i-adic evaluation at most $2r_i - 1$.

Define $P = \{p \in \mathbb{N} : p \text{ prime and } p \nmid n\}$ and let $x \in H^\bullet_{\Gamma_n}$ have longest factorization into irreducibles $x = u_1 \cdots u_L$ and shortest factorization $x = v_1 \cdots v_\ell$. Suppose that $u \in H_{\Gamma_n}$where $\wp(u)$ contains no element of P then since each minimal H_{Γ_n}-essential set is a singleton, $\wp(u)$ must contain an element of Q. It follows that $\wp(u_i)$ contains an element of P or Q for $1 \leq i \leq L$ and hence $\wp(x)$ contains λL elements of P and μL elements of Q where $\lambda + \mu \geq 1$. In the special case where $\Gamma_n^\times = \emptyset$ then $\gcd(z, n) > 1$ for all $z \in H^\bullet_{\Gamma_n}$ hence no power of $p \in P$ can appear in H_{Γ_n}. Consequently, $\wp(u_i)$ contains an element of Q for all i and so $\mu \geq 1$.

$\wp(v_j)$ must contain at least $\mu L/\ell$ elements of Q for some j. Indeed, suppose that $\wp(v_j)$ contains $\geq 2t \max\{r_1, \ldots, r_t\}$ elements of Q then $\wp(v_j)$ must contain $\geq 2r_k$ copies of p_k for some k hence v_j is reducible by the above, a condradiction. We conclude that

$$\frac{\mu L}{\ell} < 2t \max\{r_1, \ldots, r_t\}$$

If $\Gamma_n^\times = \emptyset$ then $\rho(x) = L/\ell \leq \mu L/\ell < 2t \max\{r_1, \ldots, r_t\}$. This bound is independent of x hence $\rho(H_{\Gamma_n}) < \infty$ and we're done. Suppose then that $\Gamma_n^\times \neq \emptyset$:

$\wp(v_i)$ contains at least $\lambda L/\ell$ elements of P for some i. v_i is irreducible hence by Corollary 5, $\wp(v_i)$ contains $\leq D(\mathbb{Z}_n^\times/\Gamma_n^\times)$ elements of P hence:

$$\frac{\lambda L}{\ell} \leq D\left(\frac{\mathbb{Z}_n^\times}{\Gamma_n^\times}\right)$$

It follows that

$$\rho(x) = \frac{L}{\ell} \leq (\lambda + \mu)\frac{L}{\ell} < 2t \max\{r_1, \ldots, r_t\} + D\left(\frac{\mathbb{Z}_n^\times}{\Gamma_n^\times}\right)$$

The last bound is independent of x hence the elasticity of the monoid is finite. □

Lemma 7. *A minimal H_{Γ_n}-essential set contains only primes that divide n*

Proof. Suppose that $x = p_1 \cdots p_r q_1 \cdots q_l \in H_{\Gamma_n}$ where the p_i, q_j's are (not necessarily distinct) rational primes such that $p_i \mid n$, $q_j \nmid n$. We have that $x^{\varphi(n)} \equiv (p_1 \cdots p_r)^{\varphi(n)} \pmod{n}$ and so $(p_1 \cdots p_r)^{\varphi(n)} \in H_{\Gamma_n}$. It follows that if $l \geq 1$, the set of primes dividing x is not minimal H_{Γ_n}-essential. □

Although the above theorem gives a characterization of when a given CM has finite elasticity, we would like a simple test to determine this property. As mentioned above the salient information with regards to this problem lies in the gcd-set:

Theorem 8. *H_{Γ_n} has finite elasticity if and only if every minimal $\mathcal{D}_{\Gamma_n}$-essential set is a singleton.*

Proof. By Theorem 8 it suffices to show that a set is minimal $\mathcal{D}_{\Gamma_n}$-essential if and only if it is minimal H_{Γ_n}-essential. To this end it suffices to show that a minimal H_{Γ_n}-essential set is $\mathcal{D}_{\Gamma_n}$-essential and every $\mathcal{D}_{\Gamma_n}$-essential set is H_{Γ_n}-essential.

Suppose that $T = \{p_1, \ldots, p_t\}$ is minimal H_{Γ_n}-essential with $p_1^{e_1} \cdots p_t^{e_t} \equiv \gamma_1 \pmod{n}$ say. By Lemma 7, each p_i divides n hence the given congruence ensures that T is the set of primes dividing $d_1 = \gcd(\gamma_1, n)$ and so T is $\mathcal{D}_{\Gamma_n}$-essential.

Finally suppose that $S = \{q_1, \ldots, q_s\}$ is $\mathcal{D}_{\Gamma_n}$-essential, $d_2 = q_1^{f_1} \cdots q_s^{f_s}$ say. It follows that γ_2 can be written as $\gamma_2 = q_1^{\alpha_1} \cdots q_s^{\alpha_s} r_1^{\beta_1} \cdots r_l^{\beta_l}$ where $\alpha_i \geq 1$ and r_j a rational prime not dividing n. Note that $\gamma_2^{\varphi(n)} \equiv (q_1^{\alpha_1} \cdots q_s^{\alpha_s})^{\varphi(n)} \pmod{n}$ and so $(q_1^{\alpha_1} \cdots q_s^{\alpha_s})^{\varphi(n)} \in H_{\Gamma_n}$ hence S is H_{Γ_n}-essential.

□

We mention a couple of simple corollaries that apply in later sections of the paper, yet can be understood here.

Corollary 9. *Let $(\Gamma_n, \cdot)$ be a group and $(\overline{\Gamma}_n, \cdot)$ a subgroup then H_{Γ_n} has finite elasticity iff $H_{\overline{\Gamma}_n}$ has finite elasticity.*

Proof. By Theorem 2, $\mathcal{D}_{\Gamma_n}$ and $\mathcal{D}_{\overline{\Gamma}_n}$ are singletons and they are equal since $\overline{\Gamma}_n$ is a subset of Γ_n. The result now follows by Theorem 8. □

Corollary 10. *Let $\Gamma_n^\bullet \neq \emptyset$ then H_{Γ_n} has finite elasticity if and only if $H_{\Gamma_n^\bullet}$ has finite elasticity*

Proof. Note that $\mathcal{D}_{\Gamma_n} = \mathcal{D}_{\Gamma_n^\bullet} \cup \{1\}$, the result then follows from Theorem 8. □

3 Regular Congruence Monoids

When $\Gamma_n = \Gamma_n^\times$, it follows that Γ_n is a normal subgroup of $\mathbb{Z}_n^\times$, the set of units modulo n. This makes the quotient group:

$$G_{\Gamma_n} = \mathbb{Z}_n / \Gamma_n$$

well defined. The structure of G_{Γ_n} plays a large role in determining the factorization properties of H_{Γ_n}. First we define the block monoid over an abelian group.

Definition 12. *Let G be an abelian group, and let $\mathcal{B}(G)$ be the set of all zero-sums G. We call $\mathcal{B}(G)$ the* **block monoid over G.**

Theorem 11. *Let n be a fixed modulus, Γ be a finite subset of $\mathbb{N}$ such that Γ_n is multiplicatively closed, and $\Gamma_n = \Gamma_n^\times$. Then there exists a transfer homomorphism from H_{Γ_n} to $\mathcal{B}(G_{\Gamma_n})$.*

Proof. Let $x \in H_{\Gamma_n}$ and suppose $x = \prod_{i=1}^{k} p_i^{\alpha_i}$ is its prime factorization in $\mathbb{N}$. Note that $\bar{x} = \prod_{i=1}^{k} \bar{p}_i^{\alpha_i} \in \Gamma_n$ where multiplication is in $\mathbb{Z}_n$, hence in G_{Γ_n} we have that $\Gamma_n = \bar{x}\Gamma_n = \prod_{i=1}^{k} (\bar{p}_i\Gamma_n)^{\alpha_i}$. It follows that we have a map $\phi : H_{\Gamma_n} \longrightarrow \mathcal{B}(G_{\Gamma_n})$ defined by $\phi(x) = [\bar{p}_1\Gamma_n]^{\alpha_1}[\bar{p}_2\Gamma_n]^{\alpha_2}\cdots[\bar{p}_k\Gamma_n]^{\alpha_k}$ where $x = \prod_{i=1}^{k} p_i^{\alpha_i}$ as above. We claim that ϕ is a transfer homomorphism. The fact that ϕ is a monoid homomorphism is clear. Note that the only units in H_{Γ_n} and $\mathcal{B}(G_{\Gamma_n})$ are 1 and $[\Gamma_n]$ respectively, thus is suffices to show (i) that ϕ is surjective, and (ii) if $x \in H_{\Gamma_n}$ and $a, b \in \mathcal{B}(G_{\Gamma_n})$ such that $\phi(x) = ab$ then $\exists y, z \in H_{\Gamma_n}$ such that $x = yz$ and $\phi(y) = a$, $\phi(z) = b$.
(i) Let $\beta = [\overline{u_1}\Gamma_n]^{\alpha_1}[\overline{u_2}\Gamma_n]^{\alpha_2}\cdots[\overline{u_k}\Gamma_n]^{\alpha_k} \in \mathcal{B}(G_{\Gamma_n})$. For $1 \le i \le k$, $u_i \in \mathbb{Z}_n^{\times}$ i.e $\gcd(u_i, n) = 1$, hence by Dirichlet's theorem we may pick a prime $p_i \in \mathbb{N}$ congruent to u_i modulo n. Let $x = \prod_{i=1}^{k} p_i^{\alpha_i}$. Then $\bar{x} = \prod_{i=1}^{k} \bar{p}_i^{\alpha_i} = \prod_{i=1}^{k} \overline{u_i}^{\alpha_i} \in \Gamma_n$ since $\beta \in \mathcal{B}(G_{\Gamma_n})$. Thus $x \in H_{\Gamma_n}$ and $\phi(x) = [\overline{u_1}\Gamma]^{\alpha_1}[\overline{u_2}\Gamma_n]^{\alpha_2}\cdots[\overline{u_k}\Gamma_n]^{\alpha_k}$.
(ii) Suppose that $x = \prod_{i=1}^{k} p_i^{\alpha_i} \in H_{\Gamma_n}$ and that $\phi(x) = [\bar{p}_1\Gamma_n]^{\alpha_1}[\bar{p}_2\Gamma_n]^{\alpha_2}\cdots[\bar{p}_k\Gamma_n]^{\alpha_k} = ab$ where $a, b \in \mathcal{B}(G_{\Gamma_n})$ (note that it may be the case that $\bar{p}_i = \bar{p}_j$ for $i \neq j$). Write $a = [\bar{p}_1\Gamma_n]^{\beta_1}[\bar{p}_2\Gamma_n]^{\beta_2}\cdots[\bar{p}_k\Gamma_n]^{\beta_k}$, $b = [\bar{p}_1\Gamma_n]^{\gamma_1}[\bar{p}_2\Gamma_n]^{\gamma_2}\cdots[\bar{p}_k\Gamma_n]^{\gamma_k}$ where $0 \le \beta_i, \gamma_i \le \alpha_i$ and $\beta_i + \gamma_i = \alpha_i$ for $1 \le i \le k$. Since $a \in \mathcal{B}(G_{\Gamma_n})$ we have that $\prod_{i=1}^{k} \bar{p}_i^{\beta_i} \in \Gamma_n$ i.e $y = \prod_{i=1}^{k} p_i^{\beta_i} \in H_{\Gamma_n}$. Similarly $z = \prod_{i=1}^{k} p_i^{\gamma_i} \in H_{\Gamma_n}$. Hence $x = yz$ where $y, z \in H_{\Gamma_n}$, $\phi(y) = a$ and $\phi(z) = b$. □

Example : Let $\Gamma = \{1, 7, 11\}$ and $n = 19$. Then:

$$G_{\Gamma_n} = \mathbb{Z}_{19}^{\times}/\Gamma_n = \{\Gamma_n, \overline{2}\Gamma_n, \overline{4}\Gamma_n, \overline{8}\Gamma_n, \overline{16}\Gamma_n, \overline{13}\Gamma_n\} \simeq \mathbb{Z}_6.$$

First we map each coset into the free monoid over $\mathbb{Z}_6$:

$$\Gamma_n \mapsto [0], \overline{2}\Gamma_n \mapsto [1], \overline{4}\Gamma_n \mapsto [2], \overline{8}\Gamma_n \mapsto [3], \overline{16}\Gamma_n \mapsto [4], \overline{13}\Gamma_n \mapsto [5].$$

Now let's say we want to factor a number like 1343545157637423 in H_{Γ_n}. First we factor our number over the naturals:

$$1343545157637423 = 3^5 \cdot 13^3 \cdot 17^1 \cdot 23^6.$$

We note that $\overline{3} \in \overline{2}\Gamma_n$,$\overline{13} \in \overline{13}\Gamma_n$,$\overline{17} \in \overline{16}\Gamma_n$, and $\overline{23} \in \overline{4}\Gamma_n$. Hence with our mapping, we have:

$$3^5 \cdot 13^3 \cdot 17^1 \cdot 23^6 \longmapsto [1]^5[5]^3[4]^1[2]^6 \in \mathcal{B}(\mathbb{Z}_6).$$

Now we can focus on factorizations within the block monoid. Some factorizations of $[1]^5[5]^3[4]^1[2]^6$ are:

* $([1][5])^3([1]^2[2]^2)([2][4])([2]^3)$
* $([1][5])^3([1]^2[4])([2]^3)^2$
* $([1][5])([2][4])([2][5]^2)([1]^4[2])([2]^3)$

Looking back in H_{Γ_n}, we obtain these different factorizations into irreducibles:

* $(3 \cdot 13)^3(3^2 \cdot 23^2)(23 \cdot 17)(23^3) = 39^3 \cdot 4761 \cdot 391 \cdot 12167$

* $(3 \cdot 13)^3(3^2 \cdot 17)(23^3)^2 = 39^3 \cdot 153 \cdot 12167^2$

* $(3 \cdot 13)(23 \cdot 17)(23 \cdot 13^2)(3^4 \cdot 23)(23^3) = 39 \cdot 391 \cdot 3887 \cdot 1863 \cdot 12167$

Since transfer homomorphism preserves factorization properties, we immediatly obtain the following results.

Corollary 12. *Let H_{Γ_n} be a regular congruence monoid, $\mathcal{B}(G_{\Gamma_n})$ be the block monoid over G_{Γ_n}, and $\sigma : H_{\Gamma_n} \longrightarrow \mathcal{B}(G_{\Gamma_n})$ be a transfer homomorphism. Then:*

1. *For all $x \in H_{\Gamma_n}$, x is irreducible iff $\sigma(x) \in \mathcal{B}(G_{\Gamma_n})$ is irreducible.*
2. *For all $x \in H_{\Gamma_n}$, $\mathcal{L}(x) = \mathcal{L}(\sigma(x))$ and $\rho(x) = \rho(\sigma(x))$.*
3. *$\rho(H_{\Gamma_n}) = \rho(\mathcal{B}(G_{\Gamma_n})) = \frac{D(G_{\Gamma_n})}{2}$.*

Proof. These properties follow straight from the definition of a transfer homomorphism. □

With a little more machinery, we also obtain results about full and accepted elasticity.

Lemma (Unit-Primes Lemma). *If $\Gamma_n^\times$ is not empty, then H_{Γ_n} contains infinitely many primes.*

Proof. Let $\Gamma \subseteq \mathbb{N}$ such that Γ_n contains a unit, a, and is multiplicatively closed. The modulus and the the unit a are coprime, so by Dirichlet, there exist infinitely many rational primes $p \equiv a \pmod{n}$. Choose one such rational prime, p, and let $x, y \in H_{\Gamma_n}$. Suppose $p \mid xy$ in H_{Γ_n}, then without loss of generality, $p \mid x$ in $\mathbb{N}$, and therefore, $x = pk$ in $\mathbb{N}$. Because $p \in H_{\Gamma_n}$, and H_{Γ_n} is multiplicatively closed, there must exist some p^k such that $p^k = 1$ for some $k \geq 1$. Then clearly $p \cdot p^{k-1} = 1$ and the inverse of p is in H_{Γ_n} as well. Multiplying $x = pk$ by the inverse gives us $p^{-1}x = k$ and then, because H_{Γ_n} is multiplicatively closed, k must also be in H_{Γ_n}. Therefore $p \mid x$ in the monoid and p must be prime. It can be concluded that there are infinitely many primes in H_{Γ_n} when Γ_n contains a unit. □

We also note that block monoids over finite abelian groups have accepted elasticy (Theorem 7, [1]) and monoids that have accepted elasticity and a prime element also have full elasticy (Corollary 2.2, [4]). These two theorems along with the Unit-Primes Lemma give us the following result.

Corollary 13. *If H_{Γ_n} is a regular congruence monoid, then the elasticity of H_{Γ_n} is accepted and full.*

Proof. Since H_{Γ_n} is regular, by Theorem 11 we know there exists a transfer homomorphism to $\mathcal{B}(G_{\Gamma_n})$. Because G_{Γ_n} is a finite abelian group, it follows that the elasticity of $\mathcal{B}(G_{\Gamma_n})$ is accepted, hence the elasticity of H_{Γ_n} is also accepted. Since Γ_n is regular, it contains at least one unit. Therefore, by the Unit-Primes Lemma, H_{Γ_n} contains infinitely many primes. Therefore, because H_{Γ_n} has accepted elasticity and a prime element, it follows that the elasticity is also full. □

4 Singular Congruence Monoids

Recall Theorem 2 from the section on general congruence monoids:

Theorem. *Let H_{Γ_n} be a CM then*

$$M_{\delta,\delta} \cap H_{\Gamma_\zeta} \subseteq H_{\Gamma_n} \subseteq M_{d,d}$$

where H_{Γ_ζ} is regular and the following are equivalent:

1. $H_{\Gamma_n} = M_{\delta,\delta} \cap H_{\Gamma_\zeta}$
2. $\delta = d$
3. *Multiplication induces a group structure on Γ_n.*

In light of this theorem it is natural to consider CMs for which $d = \delta$, i.e. $(\Gamma_n, \cdot)$ is a group), let us call such CMs J-monoids. This is a natural generalization of the concept of an ACM since ACMs correspond to the case where $(\Gamma_n, \cdot)$ is the trivial group. In the regular case $\Gamma_n \subseteq \mathbb{Z}_n^\times$ we have $d = \delta = 1$ hence (1) is satisfied in Theorem 2 vacuously. However it is important to note that there exist interesting groups of non units e.g. $\Gamma_{30} = \{4, 14, 16, 26\} \cong C_2 \times C_2$ where 16 acts as the identity, $\Gamma_{62} = \{2, 4, 8, 16, 32\} \cong C_5$ where 32 acts as the identity. The proof of Theorem 2 shows that if $(\Gamma_n, \cdot)$ is a group then it is in fact isomorphic to a subgroup of $\mathbb{Z}_\zeta^\times$.

Theorem 2 suggests that d and δ are important parameters in the study of the factorization theoretic porperties of a CM. With this in mind, we present some results that rely on certain properties of d, δ.

Corollary 14. *Let $x, y \in H_{\Gamma_n}$ with $y \mid_{\mathbb{N}} x$ and $x \neq y$ then:*
$\delta \mid_{\mathbb{N}} x/y \implies y \mid x$ *in* H_{Γ_n}.

Proof. By Theorem 2 $x, y \in H_{\Gamma_\zeta}$ where H_{Γ_ζ} is regular. Let $x = ky$ for $k \in \mathbb{N}$ then $x \equiv ky \pmod{\zeta}$. y is a unit modulo ζ and Γ_ζ is multiplicatively closed hence $xy^{-1} \equiv k \pmod{\zeta}$ and $k \in H_{\Gamma_\zeta}$. By the first inclusion of Theorem 2 $\delta \mid_{\mathbb{N}} x/y \implies x/y = k \in H_{\Gamma_n}$. □

Corollary 15. *Let Γ_n be such that $d^2 \nmid \delta$ then:*

1. *H_{Γ_n} contains no prime elements.*

2. *If x is reducible then $x+n$ is irreducible.*

Proof. (1) Let $x \in H^{\bullet}_{\Gamma_n}$. By the proof of Theorem 2 $\gcd(\delta,\zeta)=1$, hence $\delta/d \in \mathbb{Z}_\zeta^\times$, and the residue of x modulo ζ lies $\mathbb{Z}_\zeta^\times$. Let p be a rational prime such that $p \nmid d$ and $p \equiv (x\delta/d)^{-1} \pmod{\zeta}$ and set $y = p\delta/d$. Note that by the second inclusion of Theorem 2, $d \mid x$ hence $\delta \mid xy$. Noting also that $\bar{x}\bar{y}, \bar{x}\bar{y}^2 \in \Gamma_\zeta$, since $\bar{y} = \bar{x}^{-1} \in \Gamma_\zeta \subseteq \mathbb{Z}_\zeta^\times$, we have $xy, xy^2 \in H_{\Gamma_n}$ by the first inclusion of Theorem 2. Now $d \nmid y = p\delta/d$ since $\gcd(d,p)=1$ and $d^2 \nmid \delta$ by assumption. It follows from Theorem 2 again that $y \notin H_{\Gamma_n}$. Finally note that $x \mid x(xy^2) = (xy)(xy)$ but $x \nmid xy$ and so x is not prime.

(2) If $x = yz$ for some $y, z \in H^{\bullet}_{\Gamma_n}$ then by the second inclusion of Theorem 2, $d^2 \mid_{\mathbb{N}} x$. If $x+n$ is also reducible then $d^2 \mid_{\mathbb{N}} x+n$ and so $d^2 \mid_{\mathbb{N}} n$. However, $d \mid \delta$ and $n = \delta\zeta$ where $\gcd(\delta,\zeta)=1$ hence $d^2 \mid \delta$ contrary to assumption. □

Remarks:

- The above hypotheses cover the case when $(\Gamma_n, \cdot)$ is a group of non-units since in this case $d = \delta > 1$.

- Let H_{Γ_n} satisfy the hypotheses of the above corollary and let $\mathcal{A}(H_{\Gamma_n}) = \{x \in H_{\Gamma_n} : x \text{ is irreducible}\}$. It follows from (2) that

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

When studying the ACM $M_{a,b}$ it is useful to consider the case when $\gcd(a,b)$ is a power of a prime. Analogously we may consider the case when $\delta = p^\alpha$ is a power of a prime in which case $d = p^\gamma$ for some $\gamma \leq \alpha$ since $d \mid \delta$.

Theorem 16. *Let Γ_n be such that $\delta = p^\alpha$, $d = p^\gamma$ for some prime $p \in \mathbb{N}$ and $\gamma \geq 1$. Let $\beta \geq 0$ be minimal such that $p^\beta \in H_{\Gamma_n}$ then:*

$$\frac{\alpha+\beta-1}{c\gamma} \leq \rho(H_{\Gamma_n}) \leq \frac{\alpha+\beta-1}{\gamma}$$

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

Proof. Let $x \in H_{\Gamma_n}$ such that $v_p(x) \geq \alpha+\beta$. By assumption $p^\beta \in H_{\Gamma_n}$ hence $x, p^\beta \in H_{\Gamma_\zeta}$ a fortiori. Now, $p^\alpha \mid_{\mathbb{N}} xp^{-\beta}$ hence by Corollary 14, $xp^{-\beta} \in H_{\Gamma_n}$ and so $x = (p^\beta)(xp^{-\beta})$ is reducible. We conclude that all irreducibles in H_{Γ_n} have p-adic value at most $\alpha+\beta-1$. On the other hand, all irreducibles have p-adic value greater than γ by the second inclusion of Theorem 2. It follows

that if $y \in H^{\bullet}_{\Gamma_n}$ then the number of irreducibles in any factorization of y lies in the interval $[v_p(y)/(\alpha+\beta-1), v_p(y)/\gamma]$ hence

$$\rho(y) \leq \frac{v_p(y)/\gamma}{v_p(y)/(\alpha+\beta-1)} = \frac{\alpha+\beta-1}{\gamma}$$

This demonstrates the upper bound in the statement of the proposition. To deal with the lower bound we find a sequence of elements $x_k \in H_{\Gamma_n}$ such that $\rho(x_k) \geq c_k$ where $c_k \to (\gamma+\beta-1)/\gamma$ as $k \to \infty$.

Now, $\delta = p^{\alpha} = \text{lcm}(d_1, \ldots, d_m)$ which forces $d_i = p^{k_i}$ for some $\gamma \leq k_i \leq \alpha$ in which case $\delta = p^{\alpha} = \max\{p^{k_1}, \ldots, p^{k^m}\}$ and $d = p^{\gamma} = \gcd(p^{k_1}, \ldots, p^{k^m}) = \min\{p^{k_1}, \ldots, p^{k^m}\}$. Assume without loss of generality that $k_1 = \gamma$ and $k_m = \alpha$. It follows that $\gcd(\gamma_1 p^{-\gamma}, f) = 1$ so by Dirichlet's Theorem we can pick a rational prime r coprime to n, such that $r \equiv \gamma_1 p^{-\gamma} \pmod{f}$ i.e. $p^{\gamma} r \equiv \gamma_1 \pmod{n}$. Note that $p^{\gamma} r \in H_{\Gamma_n}$ and is irreducible since $d^2 = p^{2\gamma} \nmid_{\mathbb{N}} x$ for all reducibles $x \in H_{\Gamma_n}$. The proof of Theorem 2 shows that $\gcd(\delta, \zeta) = 1$ hence $\gcd(p, \zeta) = 1$ and so we can find a rational prime q coprime to n such that $q \equiv p^{\beta-\alpha+1} \pmod{\zeta}$. $\delta \mid p^{\alpha+\beta-1} q$ and $p^{\alpha+\beta-1} q \equiv 1 \pmod{\zeta}$ hence $p^{\alpha+\beta-1} q \in H_{\Gamma_n}$ by Theorem 2.

Let $\varphi = \varphi(n)$ the Euler totient function of n. r and q are units modulo n hence for $k \in \mathbb{N}$, $p^{\gamma} r^{k\varphi+1} \equiv p^{\gamma} r \equiv p^{\gamma} q^{k\varphi} r \pmod{n}$ and so $p^{\gamma} r^{k\varphi+1}, p^{\gamma} q^{k\varphi} r \in H_{\Gamma_n}$. Furthermore $p^{\gamma} r^{k\varphi+1}, p^{\gamma} q^{k\varphi} r$ are both irreducible since they do not contain $p^{2\gamma}$ as a factor in $\mathbb{N}$. For $k \geq 1$ w have:

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

Suppose that $p^{\alpha+\beta-1} q$ can be factored into more than c irreducibles in H_{Γ_n} i.e. $p^{\alpha+\beta-1} q = (p^{r_1}) \ldots (p^{r_c})(p^{r_{c+1}} q)$. $r_i \geq \beta$ for $1 \leq i \leq c$ by definition of β hence $r_{c+1} < \alpha + \beta - 1 - c\beta < \gamma$ so $d \nmid (p^{r_{c+1}} q)$ a contradiction. We conclude that $(p^{r_{c+1}} q)$ can be factored into at most c irreducibles. Consequently, the factorization on the left of the above has at most $ck\varphi\gamma + 1$ irreducibles, while the one on the right has $k\varphi(\alpha+\beta-1)+1$ irreducibles so:

$$\rho(H_{\Gamma_n}) \geq \frac{k\varphi(\alpha+\beta-1)+1}{ck\varphi\gamma+1}$$

which tends to $(\alpha+\beta-1)/c\gamma$ as $k \to \infty$ □

Remarks:

- Note that if $(\Gamma_n, \cdot)$ is a group then $c = 1$ hence $\rho(H_{\Gamma_n}) = (\alpha+\beta-1)/\alpha$. In particular, the above generalizes the result that gives the elasticity of a local singular ACM.
- Other conditions such as $\alpha - \gamma < \beta$ force c to equal 1.

- It is interesting to note that the two inclusions of Theorem 2 translate to bounds on the elasticity of the monoid. Furthermore the more Γ_n behaves as a group i.e. the closer α and γ become, the tighter the bounds become.

- Below we shall see that if $\Gamma = \{p, p^2, \ldots, p^r\}$, $n = p^r$ then for $p \neq 2$, $\rho(H_{\Gamma_n}) = r$ so the upper bound is met even when c is large for the monoid. Furthermore if $p = 2$ then $\rho(H_{\Gamma_n}) = r - 1$ which shows that the upper bound is not always met.

The last remark motivates us to analyze conditions under which we have equality in the upper bound of Theorem 16 more closely. In the context of Theorem 16 we have the following:

Proposition 17. *If $\exists$ a rational prime q such that $\bar{p}^{\alpha-1}\bar{q} \in \Gamma_\zeta$ and $p^{\alpha-j}q \notin H_{\Gamma_n}$ for all $1 \leq j \leq \alpha - \gamma$ for which $p^{\beta+j-1} \in H_{\Gamma_n}$ then:*

$$\rho(H_{\Gamma_n}) = \frac{\alpha + \beta - 1}{\gamma}$$

Proof. Let $q \in \mathbb{N}$ be as in the statement of the proposition. We begin by showing that $p^{\alpha+\beta-1}q \in H_{\Gamma_n}$ and that it is irreducible. Since $p^\beta \in H_{\Gamma_n}$ we have $\bar{p}^\beta \in \Gamma_\zeta$ and by assumption $\bar{p}^{\alpha-1}\bar{q} \in \Gamma_\zeta$ hence $\bar{p}^{\alpha+\beta-1}\bar{q} \in \Gamma_\zeta$. Moreover $\delta = p^\alpha \mid p^{\alpha+\beta-1}q$ so that $p^{\alpha+\beta-1}q \in H_{\Gamma_n}$ by Theorem 2.

Suppose that $p^{\alpha+\beta-1}q$ is reducible in H_{Γ_n}. Since β is minimal such that $p^\beta \in H_{\Gamma_n}$ and $d = p^\gamma$ divides each element of H_{Γ_n}, $p^{\alpha+\beta-1}q$ must factorize in H_{Γ_n} as $(p^{\beta+j-1})(p^{\alpha-j}q)$ for some $1 \leq j \leq \alpha - \gamma$ contradicting the assumptions of the proposition. We conclude that $p^{\alpha+\beta-1}q$ is irreducible.

Now, returning to equation 1 of Theorem 16 we see that the factorization on the left has at most $k\varphi\gamma + 1$ irreducibles, while the one on the right has $k\varphi(\alpha + \beta - 1) + 1$ irreducibles so:

$$\rho(H_{\Gamma_n}) \geq \frac{k\varphi(\alpha + \beta - 1) + 1}{k\varphi\gamma + 1}$$

which tends to $(\alpha + \beta - 1)/\gamma$ as $k \to \infty$. However, by Theorem 16, $\rho(H_{\Gamma_n}) \leq (\alpha + \beta - 1)/\gamma$ and so we must have equality. □

Remarks:

- The hypotheses of this proposition give a characterization for when one can find a rational prime q such that $p^{\alpha+\beta-1}q \in H_{\Gamma_n}$ is irreducible.

- In the case where $\Gamma = \{p, p^2, \ldots, p^r\}$, $n = p^r$ Proposition 17 determines the elasticity of H_{Γ_n} where Theorem 16 fails to do so.

- Let $\gamma_i' = \gamma_i / v_p(\gamma_i)$. A weaker but simpler condition for the above equality to hold is

$$\bar{p}^{1-\alpha}\Gamma_\zeta \not\subset \{\overline{\gamma_1'} \ldots \overline{\gamma_m'}\}$$

We've seen that it's common for H_{Γ_n} to saturate the upper bound of Theorem 16 even when $(\Gamma_n, \cdot)$ is not a group. However, we still have the following:

Proposition 18. *Suppose the upper bound of Theorem* 16 *is met for* H_{Γ_n} *then:*

1. H_{Γ_n} *is half-factorial if and only if* $(\Gamma_n, \cdot)$ *is a group and* $\min\{\Gamma_n\} = p$
2. $\rho(H_{\Gamma_n}) < 2$ *if and only if* $(\Gamma_n, \cdot)$ *is a group and* $\min\{\Gamma_n\} = p^\gamma$

Proof. (1): H_{Γ_n} is half-factorial $\iff (\alpha + \beta - 1)/\gamma = 1 \iff \alpha - \gamma = 1 - \beta$. Now, $\alpha - \gamma \geq 0$ and $\beta \geq 1$ hence $\alpha - \gamma = 1 - \beta \iff \alpha = \gamma$ and $\beta = 1$. By the proof of Theorem 2 we have $\alpha = \gamma \iff (\Gamma_n, \cdot)$ is a group. Finally $\beta = 1 \iff p \in H_{\Gamma_n}$, but p divides all non units in H_{Γ_n} hence $p \in H_{\Gamma_n} \iff p$ is the least element of $H^\bullet_{\Gamma_n} \iff p = \min\{\Gamma_n\}$.

(2): $(\alpha+\beta-1)/\gamma < 2 \iff \alpha-\gamma < \gamma-\beta+1$. Note that $\alpha-\gamma \geq 0$ and $\gamma-\beta \leq 0$ hence $\alpha - \gamma < \gamma - \beta + 1 \iff \alpha = \gamma = \beta$. Again, by the proof of Theorem 2 we have $\alpha = \gamma \iff (\Gamma_n, \cdot)$ is a group. Furthermore $\beta = \gamma \iff p^\gamma \in H_{\Gamma_n}$, but $d = p^\gamma$ divides all non units in H_{Γ_n} hence $p^\gamma \in H_{\Gamma_n} \iff p^\gamma$ is the least element of $H^\bullet_{\Gamma_n} \iff p^\gamma = \min\{\Gamma_n\}$. □

Having analyzed the case where d and δ are prime powers it is natural to consider the case where d and δ are composite.

Theorem 19. *Let* Γ_n *be such that* d, δ *are composite and share the same prime factors then* $\exists \lambda > 0$ *such that* $\ell(x) < \lambda \ \forall x \in H_{\Gamma_n}$.

Proof. Let $d = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, $\delta = p_1^{\beta_1} \cdots p_t^{\beta_t}$ be the prime factorizations of d, δ in $\mathbb{N}$, we're assuming that $t \geq 2$. Let $r \geq \beta_i/\alpha_i$ be such that $p_i^r \equiv 1 \pmod{\zeta}$ for all i ($r = \lceil \beta_i/(\alpha_i \varphi(\zeta)) \rceil \varphi(\zeta)$ suffices).

Let $x \in H^\bullet_{\Gamma_n}$. By Theorem 2, d must divide all non-units in H_{Γ_n} so we may write $x = p_1^{m_1} \cdots p_t^{m_t} y$ where $m_i \geq \alpha_i$, $y \in \mathbb{N}$ and $p_i \nmid y$. If $m_i < 3\alpha_i r$ for some i then $\ell(x) \leq v_d(x) < 3r$ so assume that $m_i \geq 3\alpha_i r$ for all i. Write $m_i = \alpha_i r l + m_i'$ where $2 \leq l \in \mathbb{N}$ and $\alpha_i r \leq m_i' < 2\alpha_i r$. We have $x = x_1 x_2 x_3$ where $x_1 = p_1^{\alpha_1 r} p_2^{\alpha_2 r(l-1)} \cdots p_t^{\alpha_t r(l-1)}$, $x_2 = p_1^{\alpha_1 r(l-1)} p_2^{\alpha_2 r} \cdots p_t^{\alpha_t r}$ and $x_3 = p_1^{m_1'} \cdots p_t^{m_t'} y$. Theorem 2 dictates that $x_1 \in H_{\Gamma_n}$ since $\delta \mid x_1$ and $x_1 \equiv 1 \pmod{\zeta}$, similarly $x_2 \in H_{\Gamma_n}$. $x_3 \in H_{\Gamma_n}$ since $\delta \mid x_3$ and $x_3 \equiv x \pmod{\zeta}$.

Finally note that $\ell(x_1), \ell(x_2) \leq r$ and $\ell(x_3) < 2r$ hence $\ell(x) < 4r$. □

Remark: If $(\Gamma_n, \cdot)$ is a group then $d = \delta$ and so d, δ trivially share the same prime factors.

Corollary 20. *Let* Γ_n *be as in Theorem* 19 *then* H_{Γ_n} *has infinite elasticity and the elasticity is not full.*

Indeed if Γ_n is such that d is composite then H_{Γ_n} has infinite elasticity. This is a simple corollary of Theorem 8.

We have explored what impact the parameters d and δ have on the factorization properties of H_{Γ_n}. For the remainder of this section let us assume that $(\Gamma_n, \cdot)$ is a group where $d = \delta = p_1^{e_1} \dots p_k^{e_k}$ for p_i distinct primes and the $e_i \geq 1$ and that $H_{\Gamma_n} = M_{\delta,\delta} \cap H_{\Gamma_\zeta}$ as in Theorem 2:

Theorem 21. *If $p_i \in H_{\Gamma_\zeta}$ $\forall i$ then*

$$\begin{aligned} \sigma : \quad H_{\Gamma_n} &\longrightarrow (e_1, \dots, e_k) + \mathbb{N}_0^k \\ x &\longmapsto (v_{p_1}(x), \dots, v_{p_k}(x)) \end{aligned}$$

is a transfer homomorphism.

Proof. Let $N = (e_1, \dots, e_k) + \mathbb{N}_0^k$. Since $H_{\Gamma_n} = M_{\delta,\delta} \cap H_{\Gamma_\zeta}$, each element of H_{Γ_n} is divisible by δ and so σ maps into N. σ is clearly a monoid homomorphism, let us show that it is surjective: Let $(v_1, \dots, v_k) \in N$. By the proof of Thoerem 2 we know that $\gcd(\delta, \zeta) = 1$ hence $\exists m \in \mathbb{N}$ such that $x := p_1^{v_1} \cdots p_k^{v_k} m \equiv 1 \pmod{\zeta}$. Note that we can choose m such that it is coprime to δ. We know that $v_i \geq e_i$ for all i hence $\delta \mid x$. It follows that $x \in H_{\Gamma_n}$ and $\sigma(x) = (v_1, \dots, v_k)$.

Let $x \in H_{\Gamma_n}$ be arbitrary where we write $x = p_1^{v_1} \cdots p_k^{v_k} m$, $\gcd(m, \delta) = 1$. Suppose that $\sigma(x) = (w_1, \dots, w_k) + (u_1, \dots, u_k)$ a factorization in N. Since $w_i \geq e_i$ and $p_i \in H_{\Gamma_\zeta}$ for all i we have $y := p_1^{w_1} \cdots p_k^{w_k} \in H_{\Gamma_n}$. Now, $x \in H_{\Gamma_n}$ hence $x \equiv \gamma \pmod{\zeta}$ for some $\gamma \in \Gamma$ (noting that $\zeta \mid n$). H_{Γ_ζ} is regular and contains each p_i hence we may take inverses modulo ζ to deduce that $m \equiv (p_1^{v_1} \cdots p_k^{v_k})^{-1} x \pmod{\zeta}$ and so $m \in H_{\Gamma_\zeta}$. Noting also that $u_i \geq e_i$ for all i, it follows that $z := p_1^{u_1} \cdots p_k^{u_k} m \in H_{\Gamma_n}$. Finally note that $x = yz$ where $\sigma(y) = (w_1, \dots, w_k)$ and $\sigma(z) = (u_1, \dots, u_k)$. The only units in H_{Γ_n} and N are their respective identity elements hence we have shown that σ is indeed a transfer homomorphism. □

The factorization properties of N are well known. Indeed the above proof can be used to show that there is a transfer homomorphism from $M_{\delta,\delta}$ onto N hence with the hypotheses of Theorem 21, $M_{\delta,\delta}$ and H_{Γ_n} share the same arithmetic invariants. Using the known results on N which can be found in Proposition 2.2, 2.3 of [3] we have the corollary below. Note that parts of the following result may be deduced from previous theorems, we restate these parts for completeness.

Corollary 22. *Under the hypotheses of Theorem* 21 *we have the following:*

- *If δ is composite then:*
  1. *Given a reducible $x \in H_{\Gamma_n}$, write $x = \delta^k m$ with $\delta \nmid_{\mathbb{N}} m$ then $k \geq 2$ and*
  $$\mathcal{L}(x) = \{\ell \in \mathbb{N} \mid 2 \leq \ell \leq k\}$$

2. $\Delta(H_{\Gamma_n}) = \{1\}$.
3. $\rho(H_{\Gamma_n}) = \infty$.
4. H_{Γ_n} *is not fully elastic.*
5. H_{Γ_n} *has no prime elements.*

- *If* $\delta = p^\alpha$ *a prime power then:*
  1. *Given a nonunit* $x \in H_{\Gamma_n}$,
  $$\mathcal{L}(x) = \left\{ \ell \in \mathbb{N} : \left\lceil \frac{v_p(x)}{2\alpha - 1} \right\rceil \leq \ell \leq \left\lfloor \frac{v_p(x)}{\alpha} \right\rfloor \right\}$$
  2. $\Delta(H_{\Gamma_n}) = \{1\}$ *if* $r > 1$ *and* $\Delta(H_{\Gamma_n}) = \emptyset$ *if* $r = 0$.
  3. $\rho(H_{\Gamma_n}) = \frac{2\alpha-1}{\alpha}$ *and this elasticity is accepted.*
  4. H_{Γ_n} *is fully elastic if and only if* $r = 1$.
  5. H_{Γ_n} *is half-factorial if and only if* $r = 1$. *However it is never factorial.*
  6. H_{Γ_n} *has no prime elements.*

Examples:

- $H_{\Gamma_{62}}$ where $\Gamma = \{2, 4, 8, 16, 32\}$ satisfies the hypotheses of the above corollary.
- The above applies to ACMs of the form $M_{xd,yd}$ where $\gcd(x, y) = 1$ and each divisor of d is congruent to 1 modulo y. In particular it applies to local singular ACMs M_{xp^α, yp^α} where $p \equiv 1 \pmod{y}$.

We now consider a transfer homomorphism that does not require the condition on prime divisors of δ. By the structure theorem on finitely generated abelian groups, for all finite abelian groups A there exist a unique set of naturals $\{m_1, \ldots, m_r\}$ such that $m_i \mid m_{i+1}$ $\forall i$ and $A \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$. Let us call this the *canonical representation* of A.

Proposition 23. *Let* $\mathbb{Z}_\zeta^\times / \Gamma_\zeta = \{e, g_1\Gamma_\zeta, \ldots, g_m\Gamma_\zeta\}$ *and let* $\theta : \mathbb{Z}_\zeta^\times / \Gamma_\zeta \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ *be an isomorphism into its canonical representation. Then there is a transfer homomorphism*
$$\sigma : H_{\Gamma_n} \to N$$
where $N = \{z \in \mathbb{N}_0^{k+m} : z_i \geq e_i$ *for* $1 \leq i \leq k$ *and* $\sum_{i=1}^k z_i \theta(p_i\Gamma_\zeta) + \sum_{j=1}^m z_{k+j}\theta(g_j\Gamma_\zeta) = 0\}$.

Proof. Let $x \in H_{\Gamma_n}$ then we may write $x = p_1^{f_1} \cdots p_k^{f_k} q_{11} \cdots q_{1r_1} \cdots q_{m1} \cdots q_{mr_m} y$ where $q_{ij}\Gamma_\zeta \in g_i\Gamma_\zeta \ \forall i,j$ and $y \in H_{\Gamma_\zeta}$. Define $\sigma(x) = (f_1, \ldots, f_k, r_1, \ldots, r_m)$. Since $H_{\Gamma_n} = M_{\delta,\delta} \cap H_{\Gamma_\zeta}$ we must have that $f_i \geq e_i$ and $\theta(\Gamma_\zeta) = \theta(x\Gamma_\zeta) = \sum_{i=1}^k f_i\theta(p_i\Gamma_\zeta) + \sum_{j=1}^m r_j\theta(g_j\Gamma_\zeta) = 0$ so that σ is a map $H_{\Gamma_n} \to N$.

We see that σ is clearly a monoid homomorphism, let us show that it is surjective: Choose primes $q_1, \ldots, q_m$ such that $q_i\Gamma_\zeta = g_i\Gamma_\zeta$. Let $z = (z_1, \ldots, z_{k+m}) \in N$ and consider $x = p_1^{z_1} \cdots p_k^{z_k} q_1^{z_{k+1}} \cdots q_m^{z_{k+m}}$. We have $z_i \geq e_i$ for $1 \leq i \leq k$ hence $x \in M_{\delta,\delta}$ and by construction $\theta(x\Gamma_\zeta) = 0$ hence $x\Gamma_\zeta = \Gamma_\zeta$ (i.e. $x \in H_{\Gamma_\zeta}$) by injectivity of θ. It follows that $x \in H_{\Gamma_n}$ and $\sigma(x) = z$.

Finally let $x \in H_{\Gamma_n}$ be arbitrary and assume that $\sigma(x) = (v_1, \ldots, v_{k+m}) = u + w = (u_1, \ldots, u_{k+m}) + (w_1, \ldots, w_{k+m})$ is a factorization in N. As before, x must be of the form $x = p_1^{v_1} \cdots p_k^{v_k} q_{11} \cdots q_{1v_{k+1}} \cdots q_{m1} \cdots q_{mv_{k+m}} y$ where $q_{ij}\Gamma_\zeta \in g_i\Gamma_\zeta \ \forall i,j$ and $y \in H_{\Gamma_\zeta}$. Let $s = p_1^{u_1} \cdots p_k^{u_k} q_{11} \cdots q_{1u_{k+1}} \cdots q_{m1} \cdots q_{mu_{k+m}} y$, $t = p_1^{w_1} \cdots p_k^{w_k} q_{1(u_{k+1}+1)} \cdots q_{1v_{k+1}} \cdots q_{m(u_{k+m}+1)} \cdots q_{mv_{k+m}}$. Note that $x = st$, $\sigma(s) = u$ and $\sigma(t) = w$ and the fact that $u, w \in N$ ensures that $s, t \in H_{\Gamma_n}$. We have thus shown that σ is a transfer homomorphism. □

Corollary 24. *Let $\theta : \mathbb{Z}_\zeta^\times/\Gamma_\zeta \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ be an isomorphism into its canonical representation. Then all factorization properties of H_{Γ_n} are determined by the following parameters:*

- $(e_1, \ldots, e_k)$
- $(m_1, \ldots, m_r)$
- $(\theta(p_1\Gamma_\zeta), \ldots, \theta(p_k\Gamma_\zeta))$

Proof. Let N be as in Theorem 23. It suffices to show that the monoid N depends only on the listed parameters. To this end, it suffices to show that N is independent of the isomorphism $\theta : \mathbb{Z}_\zeta^\times/\Gamma_\zeta \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ chosen. Suppose then that $\psi : \mathbb{Z}_\zeta^\times/\Gamma_\zeta \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ is a group isomorphism. By the injectivity of θ and ψ we have:

$$\begin{aligned}
& \theta(p_1^{z_1} \cdots p_k^{z_k} g_1^{z_{k+1}} \cdots g_m^{z_{k+m}}\Gamma_\zeta) = \sum_{i=1}^k z_i\theta(p_i\Gamma_\zeta) + \sum_{j=1}^m z_{k+j}\theta(g_j\Gamma_\zeta) = 0 \\
\iff \quad & p_1^{z_1} \cdots p_k^{z_k} g_1^{z_{k+1}} \cdots g_m^{z_{k+m}}\Gamma_\zeta = \Gamma_\zeta \\
\iff \quad & \psi(p_1^{z_1} \cdots p_k^{z_k} g_1^{z_{k+1}} \cdots g_m^{z_{k+m}}\Gamma_\zeta) = \sum_{i=1}^k z_i\psi(p_i\Gamma_\zeta) + \sum_{j=1}^m z_{k+j}\psi(g_j\Gamma_\zeta) = 0
\end{aligned}$$

so that N is indeed independent of the choice of isomorphism θ. □

It follows that in the context of the above corollary we can associate to H_{Γ_n} a set of parameters $P(H_{\Gamma_n}) = \{(e_1, \ldots, e_k), (m_1, \ldots, m_r), \{(\theta(p_1\Gamma_\zeta), \ldots, \theta(p_k\Gamma_\zeta)) : \theta : \mathbb{Z}_\zeta^\times/\Gamma_\zeta \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \text{ is an isomorphism}\}\}$ which completely determines

the factorization properties of H_{Γ_n}. Let Θ denote the parameter space of all possible sets $P(H_{\Gamma_n})$ where H_{Γ_n} is a J-Monoid. The value of the above observation lies in the fact that distinct J-monoids can have the same parameter set in which case we conclude that they have the same factorization properties:

Example: Most results on ACMs can be restated in the form 'For all ACMs M such that $P(M) \in S \subseteq \Theta$, property Q holds' from which we can deduce the more general statement 'For all J-Monoids M such that $P(M) \in S \subseteq \Theta$, property Q holds'. The study of ACMs is therefore inadvertently the study of the more general J-monoid. Consider the following known result on ACMs:

Theorem. *Let $M_{a,n} = M_{p^k,p^k} \cap M_{1,f}$ where p is prime. If $\bar{p}$ generates $\mathbb{Z}_f^\times$ and $\bar{p}^k \neq 1$ then $\rho(M_{a,n})$ is accepted if and only if:*

- $\varphi = |\mathbb{Z}_f^\times| > 5$
- $\frac{k-1}{\varphi} - \left\lfloor \frac{k-1}{\varphi} \right\rfloor \geq \frac{1}{2}$

Using the above observations, one can lift this result to the more general context of J-monoids:

Theorem. *Let $(\Gamma_n, \cdot)$ be a group where $H_{\Gamma_n} = M_{p^k,p^k} \cap H_{\Gamma_\zeta}$ and p a prime. If $\bar{p}\Gamma_\zeta$ generates $\mathbb{Z}_\zeta^\times/\Gamma_\zeta$ and $\bar{p}^k\Gamma_\zeta \neq \Gamma_\zeta$ then $\rho(H_{\Gamma_n})$ is accepted if and only if:*

- $\varphi = |\mathbb{Z}_\zeta^\times/\Gamma_\zeta| > 5$
- $\frac{k-1}{\varphi} - \left\lfloor \frac{k-1}{\varphi} \right\rfloor \geq \frac{1}{2}$

4.1 Singular J-Monoids

In accordance with Theorem 2, we consider the case where we have equality throughout. We further assume that n is the minimum modulus for Γ_n, so equality throughout will occur exactly when Γ_n has a group structure, so H_{Γ_n} is a J-monoid. In this case, the theorem states that

$$H_{\Gamma_n} = M_{d,d} \cap H_{\Gamma_f}. \tag{2}$$

The following theorem specifies which elements of a J-monoid are irreducible regardless of any other properties of the monoid:

Theorem 25. *An element $x \in H_{\Gamma_n}$ is irreducible if and only if one of the following two conditions hold:*
(1): $x = dq$ and $d \nmid q$, or
(2): $x = d^2q$ and q has no subfactor in the coset $d^{-1}\Gamma_f$.

The term *subfactor* will be used to denote a factor of a factor. For instance, b is a subfactor of the factor (ab) in $(ab)(cd)$.

Proof. An element $x \in H_{\Gamma_n}$ is reducible if and only if there is some factorization of x into numbers that are themselves elements of both $M_{d,d}$ and H_{Γ_f}. A number is in $M_{d,d}$ if and only if it has d as a factor. Furthermore, an element of $M_{d,d}$ is reducible if and only if it has d^2 as a factor, and in that case each factor must have d as a subfactor. Therefore, if $x \in H_{\Gamma_n}$ is reducible, it must be of the form $x = d^2qr$, and it must factor as $x = (dq)(dr)$, for some $q, r \in \mathbb{N}$ (although dq and dr may not themselves be irreducible). In order for this to be a valid factorization in H_{Γ_n}, however, both dq and dr must be in H_{Γ_f} as well. Note that the elements of Γ_f must form a subgroup of $\mathbb{Z}_f^\times$. As a result, we can specify the conditions for dq and dr to be in H_{Γ_f}: we must have $q, r \in d^{-1}\Gamma_f$, the coset of Γ_f in $\mathbb{Z}_f^\times$. Therefore, given that some $x = d^2qr$ is in the monoid, it is reducible if and only if some subfactor of qr (wlog say it is q) is in the coset $d^{-1}\Gamma_f$. Because $qr \in d^{-2}\Gamma_f$ as a result of x being in the monoid, if $q \in d^{-1}\Gamma_f$, then $r \in d^{-1}\Gamma_f$ as well. Thus $x = d^2qr$ is reducible in the monoid if and only if qr has some subfactor in the coset $d^{-1}\Gamma_f$, and any element of the monoid not of this form (that is, if it does not have two factors of d) cannot be reducible. Therefore, $x \in H_{\Gamma_n}$ is irreducible if and only if either $d^2 \nmid x$ or x/d^2 is an integer which has no subfactors in $d^{-1}\Gamma_f$. □

This leads to the following corollary:

Corollary 26. *Let $x = d^kq$ be an element of H_{Γ_n}, where $k \geq 2$. If x is irreducible, then q has no subfactor in any coset $d^{-i}\Gamma_f$, where $1 \leq i \leq k-1$.*

Proof. Assume that x is an irreducible element of H_{Γ_n}. We can write x as $x = (d^2)(d^{k-2}q)$. Then by applying the previous theorem, we see that $d^{k-2}q$ can have no subfactor in $d^{-1}\Gamma_f$. If q has a subfactor z in $d^{-i}\Gamma_f$, then $d^{i-1}z \in d^{-1}\Gamma_f$, and $d^{i-1}z$ is a subfactor of $(d^{k-2}q)$ as long as $1 \leq i \leq k-1$. Thus no such subfactor of q can exist, so if x is irreducible, then q has no subfactor in any $d^{-i}\Gamma_f$ for $1 \leq i \leq k-1$.

□

In the case of J-monoids, $d = \delta > 1$, so $d^2 \nmid \delta$. Therefore, Theorem 15 applies to all J-monoids:

Theorem 27. *H_{Γ_n} has no primes.*

We will now separate our treatment of J-monoids into two cases, depending on whether d is a power of a prime. The case where $d = 1$ is the regular case, which has been solved in the previous section.

4.1.1 $d = p^\alpha$, p prime

Recall the following definition:

Definition 13. *Let β be the least positive integer such that $p^\beta \in H_{\Gamma_n}$.*

Such a β must exist because $d = p^\alpha$ and f are relatively prime, so some power of p^α must be congruent to 1 (mod f). As 1 must be an element of Γ_f, that power of p^α will be in the monoid. Furthermore, $\beta \geq \alpha$ because every element of the monoid has p^α as a factor. Then the elasticity of the monoid is known:

Theorem 28. $\rho(H_{\Gamma_n}) = \frac{\alpha+\beta-1}{\alpha}$

Proof. This is noted in the remarks following Theorem 16. □

A straightforward corollary follows:

Corollary 29. *A J-monoid H_{Γ_n} is half-factorial if and only if d is prime and in the monoid.*

Proof. Assume that $d = p^\alpha$ for some prime p. Then the elasticity of the J-monoid is $\frac{\alpha+\beta-1}{\alpha}$ by Theorem 28. The monoid will be half-factorial if and only if the elasticity of the monoid is 1, which occurs exactly when $\beta = 1$. However, $\beta \geq \alpha$ and $\alpha \geq 1$, so $\alpha = 1$ as well. Thus d is prime as $\alpha = 1$, and d itself is in the monoid because $\beta = 1$. We will later show that if d is not a power of a prime (or 1), the elasticity is infinite, so no other J-monoid can be half-factorial. □

We are also interested in determining when the elasticity of a J-monoid is accepted. This is a challenging problem, however, partially because it contains the problem of when an ACM has accepted elasticity, which itself has not been completely solved. Luckily, many of the results on ACMs can be generalized to CMs in light of Corollary 24. In addition to those generalizations, a few other results are given below.

Theorem 30. *If $d \in H_{\Gamma_n}$ (that is, if $\beta = \alpha$), then the elasticity is accepted.*

Proof. Consider $x = p^{\alpha(2\alpha-1)}r^\alpha$, where r is any prime in the coset $p\Gamma_f$ not equal to p. Such an integer r must exist because $\gcd(p, f) = 1$, so there are infinitely many primes in that coset by Dirichlet's Theorem. As x has d as a factor, and both $p^{\alpha(2\alpha-1)}$ and r^α are in the coset Γ_f, x is in both $M_{d,d}$ and H_{Γ_f}, so it must be in H_{Γ_n} as well. We can factor x in two key ways: $x = (p^\alpha)^{2\alpha-2}(p^\alpha r^\alpha) = (p^{2\alpha-1}r)^\alpha$. No element in either factorization has $d^2 = p^{2\alpha}$ as a factor, so all are irreducible. The first factorization must be the longest possible for x, because all factors have only α subfactors of p, the minimum number for a factor to be in the monoid. The second factorization must be the shortest, because all factors have $2\alpha - 1$ subfactors of p, the maximum number that an irreducible in the monoid can have (otherwise p^α can be factored out of the monoid element, leaving a factorization into two elements). Therefore the maximum length factorization of x has length $2\alpha - 1$, and the minimum length factorization has length α, so the elasticity of x is $\rho(x) = \frac{2\alpha-1}{\alpha}$. Because $\beta = \alpha$, however, the elasticity of the monoid is itself $\rho(H_{\Gamma_n}) = \frac{2\alpha-1}{\alpha}$, so the element x accepts the elasticity of the monoid. □

Theorem 31. *If d^2 is the smallest power of d in H_{Γ_n} and $\mathbb{Z}_f^\times/\Gamma_f$ is noncyclic, then the elasticity is accepted.*

Proof. Assume that d^2 is the smallest power of d in H_{Γ_n} and that $\mathbb{Z}_f^\times/\Gamma_f$ is noncyclic. Because $d^2 \in H_{\Gamma_f}$, $d\Gamma_f$ has order 2 in $\mathbb{Z}_f^\times/\Gamma_f$. But $\mathbb{Z}_f^\times/\Gamma_f$ must have at least one other component cycle of even order of which $d\Gamma_f$ is not a part (due to the Fundamental Theorem of Finitely Generated Abelian Groups). Let the element of order 2 in this other cycle be $g\Gamma_f$. Then $(\{\Gamma_f, d\Gamma_f, g\Gamma_f, dg\Gamma_f\}, \cdot) \cong C_2 \times C_2$. Let $q \in g\Gamma_f, r \in dg\Gamma_f, s \in p\Gamma_f, t \in p^{-1}\Gamma_f$ all be primes not equal to p. Note that since $d \notin \Gamma_f$ and $d^2 \in \Gamma_f$, $\alpha < \beta \leq 2\alpha$. There are two cases: $\beta = 2\alpha$ and $\beta \leq 2\alpha - 2$ (if $\beta = 2\alpha - 1$ then since $p^{2\alpha} \in \Gamma_f$, we must also have $p \in \Gamma_f$, but then $p^\alpha \in \Gamma_f$, a contradiction).
First assume $\beta \leq 2\alpha - 2$. Then let $x = p^{2\alpha(\alpha+\beta-1)}q^{4\alpha}r^{4\alpha}s^{2\alpha(\beta-\alpha+1)}$
$= (p^{\alpha+\beta-1}q^4s^{\beta-\alpha+1})^\alpha(p^{\alpha+\beta-1}r^4s^{\beta-\alpha+1})^\alpha$
$= (p^\alpha qr)^{4\alpha}(p^\alpha s^{\beta-\alpha})^{2(\beta-\alpha-1)-1}(p^\alpha s^{(\beta-\alpha)+(6\alpha\beta+2\beta-4\alpha^2-2\beta^2)})$. Each factor in the first factorization must be irreducible since neither $(p^{\beta-\alpha-1}q^4s^{\beta-\alpha+1})$ nor $(p^{\beta-\alpha-1}r^4s^{\beta-\alpha+1})$ has any subfactor in $d\Gamma_f$ (those are the "q" in condition (2) of Theorem 1), and each factor in the second factorization must be irreducible since d^2 does not divide any factor. Furthermore, to show that the final factor is in H_{Γ_n}, note that the power of s must be positive, and $s^{(\beta-\alpha)+(6\alpha\beta+2\beta-4\alpha^2-2\beta^2)}$ must be in $p^{\beta-\alpha}\Gamma_f$. To show that it is positive, note that $\beta > 2\alpha - \beta \Rightarrow \beta(2\alpha + 2 - \beta) > (2\alpha - \beta)^2$, which rearranges to $(6\alpha\beta + 2\beta - 4\alpha^2 - 2\beta^2) > 0$, and the power of s is that value added to $\beta - \alpha$. It also must be in $p^{\beta-\alpha}\Gamma_f$ because both s^β and $s^{2\alpha}$ are in Γ_f. The first factorization must be the shortest, as all factors have $\alpha + \beta - 1$ subfactors of p, the maximum possible number (as otherwise a p^β could be factored out), and the second factorization must be the longest, as all factors have only α subfactors of p, the minimum necessary for a number to be in the monoid. The first factorization has length 2α, and the second has length $2(\alpha + \beta - 1)$ so this element accepts the elasticity of $\frac{\alpha+\beta-1}{\alpha}$.
Now assume that $\beta = 2\alpha$. Then let $x = p^{2\alpha(\alpha+\beta-1)}q^{4\alpha}r^{4\alpha}t^{2\alpha(\beta-\alpha-1)}$
$= (p^{\alpha+\beta-1}q^4t^{\beta-\alpha-1})^\alpha(p^{\alpha+\beta-1}r^4t^{\beta-\alpha-1})^\alpha = (p^\alpha qr)^{4\alpha}(p^\alpha t^\alpha)^{2(\beta-\alpha-1)}$. Each factor in the first factorization must be irreducible since neither $(p^{\beta-\alpha-1}q^4t^{\beta-\alpha-1})$ nor $(p^{\beta-\alpha-1}r^4t^{\beta-\alpha-1})$ has any subfactor in $d\Gamma_f$, and each factor in the second factorization must be irreducible since d^2 does not divide any factor. The first factorization must be the shortest as all factors have $\alpha + \beta - 1$ subfactors of p, and the second factorization must be the longest as all factors have only α subfactors of p, the minimum necessary for a number to be in the monoid. The first factorization has length 2α, and the second has length $2(\alpha + \beta - 1)$ so this element accepts the elasticity of $\frac{\alpha+\beta-1}{\alpha}$. □

We also have some partial results concerning when the monoid has full elasticity. Again, many results from ACMs can be generalized, and only some results are given here.

Theorem 32. *If $\beta = \alpha$, then the monoid has full elasticity if and only if p^α is the minimum power of p in Γ_f.*

Proof. First assume that p^α is the smallest power of p that is in Γ_f, and consider any rational number $\frac{a}{b}$ with $1 \leq \frac{a}{b} < \frac{2\alpha-1}{\alpha}$, the elasticity of the monoid.

Let r be a prime in the coset $p\Gamma_f$ not equal to p, and consider the element $\mu(a,b) = (p^\alpha)^{b(2\alpha-1)-a\alpha}(p^{2\alpha-1}r)^{\alpha(a-b)} = (p^\alpha)^{a\alpha-a-1}(p^\alpha r^{\alpha(a-b)})$. Because no smaller power of p is in Γ_f, p^α is the only power of p in the monoid that is irreducible. Because p and r are in the same coset $p\Gamma_f$, and elements of that coset have order α by assumption, a product of powers of p and r is in the monoid if and only if the sum of their powers is a multiple of α (and the power of p is at least α). For any factorization of x, say we have i factors with no copies of r, and j with at least one copy of r. Each of the i factors has exactly α copies of p, and each of the j factors has at most $2\alpha-1$. Thus $\nu_p(\mu(a,b)) \le i\alpha+j(2\alpha-1) = (\ell(\mu(a,b))-j)\alpha+j(2\alpha-1) = \alpha\ell(\mu(a,b))+j(\alpha-1) \le \alpha\ell(\mu(a,b))+\alpha(a-b)(\alpha-1)$. However, $\alpha(a\alpha-a) = \nu_p(\mu(a,b))$, so $a\alpha-a \le \ell(\mu(a,b)) + (a-b)(\alpha-1)$, or $b\alpha - b \le \ell(\mu(a,b))$. The first factorization achieves this length so it is the shortest possible for x. We also have $\alpha \le \nu_p(x)$ for any x, so $\alpha L(\mu(a,b)) \le \nu(\mu(a,b)) = \alpha(a\alpha-a)$ and thus $L(\mu(a,b)) \le \nu(\mu(a,b)) = a\alpha - a$. This maximum length is achieved by the second factorization, so these are in fact the shortest and longest factorizations of $\mu(a,b)$. Therefore the elasticity of this element is $\rho(\mu(a,b)) = \frac{a}{b}$. Because a and b were chosen arbitrarily to represent any rational number in the interval $[1, \frac{2\alpha-1}{\alpha}]$, the monoid must have full elasticity.

Now assume that some smaller power than p^α is in Γ_f. Then for some s with $\alpha < s < 2\alpha$, $p^s \in H_{\Gamma_n}$, and is irreducible. The goal is to show that no element can have the elasticity $\frac{\alpha s^2+1}{\alpha s^2}$. Assume to the contrary that some element x has $\rho(x) = \frac{\alpha s^2+1}{\alpha s^2}$. Let $v_p(x)$ be the valuation of p at x, which gives the power of p in the prime factorization of x. Then by assumption, x has a factorization with a length of at least αs^2+1, and each factor must itself have a valuation of at least α, so $v_p(y) \ge \alpha^2 s^2+\alpha \ge \alpha^2 s+\alpha$. If j is the largest multiple of α less than or equal to $v_p(x)-\alpha$, we can write $x = (p^\alpha)^{j/\alpha}y$ for some $y \in H_{\Gamma_n}$, so x can be written as the product of at least $\frac{j}{\alpha}+1 \ge \frac{v_p(x)}{\alpha}-1$ factors. Also, if m is the largest multiple of s less than or equal to $v_p(x)-\alpha$, we can write $x = (p^s)^{m/s}z$ for some $z \in H_{\Gamma_n}$. The value of $v_p(z)$ must be in the interval $[\alpha, \alpha+s]$, so it can be written as the product of at most three irreducibles. Thus x can also be written as the product of $\frac{m}{s}+3$, or $\frac{v_p(x)}{s}+3$ irreducibles. As a result, the elasticity of x must be at least $\frac{v_p(x)/\alpha-1}{v_p(x)/s+3}$, or $\rho(x) \ge \frac{v_p(x)/\alpha-1}{v_p(x)/s+3} = \frac{s}{\alpha}\frac{v_p(x)-\alpha}{v_p(x)+3s}$. Since $v_p(x) \ge \alpha^2 s+\alpha$, and the function mapping t to $\frac{t-\alpha}{t+3s}$ is monotone increasing on $[\alpha^2 s+\alpha, \infty)$, $\rho(x) \ge \frac{s}{\alpha}\frac{v_p(x)-\alpha}{v_p(x)+3s} \ge \frac{s}{\alpha}\frac{\alpha^2 s+\alpha-\alpha}{\alpha^2 s+\alpha+3s} = \frac{s}{\alpha}\frac{\alpha^2 s}{\alpha^2 s+\alpha+3s} = \frac{\alpha s^2}{\alpha^2 s+\alpha+3s}$. At this point it suffices to show that $\frac{\alpha s^2}{\alpha^2 s+\alpha+3s} \ge \frac{\alpha s^2}{\alpha s^2-1} > \frac{\alpha s^2+1}{\alpha s^2}$. The second inequality is immediate for $\alpha \ge 2$ and $s \ge 3$ (these must hold as if $\alpha = 1$ the monoid is half-factorial, and $s > \alpha$ by assumption), so only the first inequality must be checked, and to show that, we only need to prove $\alpha^2 s+\alpha+3s \le \alpha s^2-1$, or equivalently, $\alpha s(s-\alpha) > \alpha+3s$.

First assume that $s-\alpha \ge 2$. Then $\alpha s(s-\alpha) \ge 2\alpha s = \frac{\alpha s}{2}+\frac{3\alpha s}{2} \ge \frac{3\alpha}{2}+3s > \alpha+3s$, so this case is fine. The other case is when $s-\alpha = 1$. Then we want to show that $\alpha s > \alpha+3s$, or $\alpha^2-3\alpha-3 > 0$. This is true as long as $\alpha \ge 4$. Thus the only cases we still have to check are for $(\alpha, s) = (2,3)$ and $(3,4)$. Since

$v_p(x) \geq \alpha^2 s^2 + \alpha$, $\rho(x) \geq \frac{(\alpha^2 s^2+\alpha)/\alpha - 1}{(\alpha^2 s^2+\alpha)/s+3}$. For $(2,3)$, $\rho(x) \geq \frac{18}{16} > \frac{19}{18} = \frac{ks^2+1}{ks^2}$, and for $(3,4)$, $\rho(x) \geq \frac{48}{40} > \frac{49}{48} = \frac{\alpha s^2+1}{\alpha s^2}$. Therefore no element x can possibly have the elasticity $\rho(x) = \frac{\alpha s^2+1}{\alpha s^2}$, so the monoid does not have full elasticity. □

The preceeding proof was adapted those in Section 3 of Ref. [7].

Theorem 33. *If $d = p$ is prime, then the monoid has full elasticity.*

Proof. The elasticity of the monoid is β. Let $q \in p^{-1}\Gamma_f$ be a prime not equal to p. Consider the element $\mu(i,j) = p^{i\beta+ij+1}q^{i\beta+1} = (pq)^{i\beta+1}(p^\beta)^j = (pq^{i\beta+1})(p^\beta)^{i+j}$. Such an element can be created for any $i, j \in \mathbb{N}_0$. All factors are irreducible, as they all are either exactly p^β or have only one factor of p. The first factorization is the longest possible for $\mu(i,j)$, since there are as many factors with a single subfactor of p as possible. The second is the shortest possible because there are as few factors with a single subfactor of p as possible, and because no monoid element with both p^2 and q as divisors can be irreducible as a factor of (pq) could be factored out (so all factors with a q must have only one power of p). Therefore $\rho(\mu(i,j)) = \frac{i\beta+j+1}{i+j+1} = 1 + \frac{i(\beta-1)}{i+j+1}$. The fraction $\frac{i(\beta-1)}{i+j+1}$ can be exactly 0, and is bounded above by $\beta - 1$ but cannot reach it, and can take any rational value in $[0, \beta-1)$. Thus the elasticity of the elements $\mu(i,j)$ can take any rational value in $[1, \beta)$. To reach any rational value $\frac{a}{b}$ in that range, set $i = a$ and $j = (b(\beta-1) - a - 1$, which is a nonnegative integer because $\frac{a}{b} < \beta - 1$ implies $a < b(\beta-1)$. Then $\frac{i(\beta-1)}{i+j+1} = \frac{a(\beta-1)}{a+(b(\beta-1)-a-1)+1} = \frac{a(\beta-1)}{b(\beta-1)} = \frac{a}{b}$. Therefore $\rho(\mu(i,j))$ can reach any value in $[1,\beta)$, and the elasticity of the monoid is equal to β, so the monoid has full elasticity. □

4.1.2 $d = qr, \gcd(q,r) = 1, q$ **and** $r > 1$

The following definition will be useful in the proofs concerning J-monoids with a composite d.

Definition 14. *Let ℓ_1 and ℓ_2 be the least positive integers such that $q^{\ell_1} \in \Gamma_f$ and $r^{\ell_2} \in \Gamma_f$.*

Note that such integers must exist because $q\Gamma_f$ and $r\Gamma_f$ must have finite order in $\mathbb{Z}_f^\times/\Gamma_f$, and ℓ_1 and ℓ_2 are exactly those orders.

Theorem 34. *$\rho(H_{\Gamma_n}) = \infty$ and the elasticity is trivially not accepted.*

Proof. Consider the element $x = (qr)^{k\ell_1\ell_2+2}$ for any $k \in \mathbb{N}$. Its longest factorization is clearly of length $k\ell_1\ell_2 + 2$, and its shortest factorization must be $(qrq^{k\ell_1\ell_2})(qrr^{k\ell_1\ell_2})$, a factorization of length 2. Thus $\rho(x) = \frac{k\ell_1\ell_2+2}{2}$. By allowing k to approach infinity, this elasticity can itself approach infinity. Therefore the monoid has infinite elasticity. Each monoid element has finite elasticity, however, so the elasticity cannot be accepted. □

Theorem 35. *H_{Γ_n} does not have full elasticity.*

Proof. Let m be the least positive integer such that $d^m \in H_{\Gamma_n}$. Take some $x \in H_{\Gamma_n}$ and assume that the longest factorization of x into irreducibles is $x = (d^{k_1}s_1)(d^{k_2}s_2)\cdots(d^{k_j}s_j)$ where j is any number greater than $2m$. Then for every i, $1 \le k_i \le m$, $s_i \in d^{-k_i}\Gamma_f$, and no s_i has both q and r as a factor. We can write $s_1 s_2 \cdots s_j = (q^{m_1}u)(r^{m_2}v)$ where neither u nor v has a factor of either q or r. This can be done by grouping all the s_i with a subfactor of q into the first product, and all the rest into the second. Then $q^{m_1}u \in d^a\Gamma_f$ and $r^{m_2}v \in d^b\Gamma_f$ for some $0 \le a, b \le m-1$, so we can write $x = (d^{m-a}q^{m_1}u)(d^{m-b}r^{m_2}v)(d)^{j+a+b-2m}$ where each factor is in the monoid (although possibly reducible). Furthermore, if $j + a + b - 2m \ge \ell_1\ell_2$, then we can change this factorization to $x = (d^{m-a}q^{m_1+\ell_1\ell_2}u)(d^{m-b}r^{m_2+\ell_1\ell_2}v)(d)^{j+a+b-2m-\ell_1\ell_2}$, and this process can be repeated until the factor (d) is repeated fewer than $\ell_1\ell_2$ times. The first two factors need not be irreducible, but they can be factored into at most m irreducibles each as they both contain at most m factors of d. Therefore the shortest factorization of such an x cannot have more than $2m+\ell_1\ell_2-1$ factors, as some factorization of x has at most that many factors. We assumed that $j \ge 2m$, so we have shown that if the numerator of an element's elasticity is at least $2m$, its denominator cannot be greater than $2m + \ell_1\ell_2 - 1$. But since $2m \le 2m + \ell_1\ell_2 - 1$, and the elasticity of any element is always at least 1, no element can have an elasticity with a denominator greater than $2m + \ell_1\ell_2 - 1$. Therefore the monoid does not have full elasticity. □

Note that these two results apply to all J-monoids when d is not a power of a prime, regardless of any other properties of the monoid. This is unlike the case when d is a power of a prime, as in that case, other properties such as α, β and the structure of $\mathbb{Z}_f^\times/\Gamma_f$ are important.

4.2 Case when $n = p^r$ and $\Gamma = \langle p \rangle$

First we consider the case when $n = p^r$, and in the singular case the most natural question is to ask what happens when $\Gamma = \langle p \rangle$. The first step is to try to categorize the irreducibles in this monoid.

Definition 15. *Let $x \in H_\Gamma$. We call x of type I iff $x \equiv 0 \pmod{p^r}$, otherwise $x \in H_\Gamma$ is of type II. Moreover, for x of type II, we will write x in the following canonical form: $x = p^i + cp^r$, where $0 < i < r$.*

Let us characterize the irreducible elements in H_Γ.

Type I: Given that an element $x = cp^r$, it is obvious that if p divides c, then x is reducible as $x = cp^r = p(\frac{c}{p}p^r)$. Also, if $c \equiv 1 \pmod{p}$ then we can write $c = 1 + pk$ for some integer k. Then,

$$x = cp^r = (1 + pk)p^r = p(p^{r-1} + p^r k)$$

and we have that since $p, p^{r-1} + p^r k \in H_\Gamma$ we have that x is reducible. This are necessary conditions that turn out to be sufficient.

Lemma 36. *Let $x = cp^r$. Then x is irreducible if and only if x is not congruent to 0 nor 1 modulo p*

Proof. By taking the contrapositive of the above remarks we already know that if x is irreducible then x is not congruent to 1 nor 0 modulo p. To prove the other direction, let c not be congruent to either 1 or 0 modulo p, and for sake of contradiction assume that x is reducible. Write $x = ab$. Then, $v_p(x) = r$, so $v_p(a) + v_p(b) = r$. Since every non-unit in our monoid is a multiple of p, we can let $v_p(a) = i$ where i must be greater than 0, and strictly less than r, so we have that the p-adic value of b is $r - i$. Then,

$$a = p^i + t_1 p^r \qquad b = p^{r-i} + t_2 p^r$$

Whence,

$$cp^r = x = ab = (p^i + t_1 p^r)(p^{r-i} + t_2 p^r)$$
$$\Rightarrow c = (1 + t_1 p^{r-i})(1 + t_2 p^i)$$

However we have that $c \equiv 1 \pmod{p}$ a contradiction. Thus, x was irreducible. □

Type II: Say $x \in H_\Gamma$ and $x = p^i + cp^r$ for $0 < i < r$. Then $v_p(x) = i$, so if x is reducible, and $x = yz$, then we must have that $i = v_p(y) + v_p(z)$, and so y and z must be of Type II. Furthermore, since y, z are multiples of p we must have that $i > 1$. Hence, there is an a with $0 < a < i$ such that

$$p^i + cp^r = x = yz = (p^{i-a} + t_1 p^r)(p^a + t_2 p^r)$$

$$\Rightarrow p^i + cp^r = p^i + p^r(t_1 t_2 p^r + t_1 p^a + t_2 p^{i-a})$$

Ergo, we have that c is a multiple of p. That is, if $x = p^i + cp^r$ is reducible then $i > 1$ and c is a multiple of p.

Lemma 37. *Let $x = p^i + cp^r$. If $i = 1$, then x is irreducible. If $i > 1$, then x is irreducible if and only if c is not a multiple of p.*

Proof. The fact that $i = 1$ implies that x is irreducible is immediate by looking at the p-adic value. Hence, assume $i > 1$. We want to show that x is irreducible if and only if c is not a multiple of p. Assume c is a multiple of p. Then we have that $p^i + cp^r = p(p^{i-1} + \frac{c}{p}p^r)$ is a valid factorization in our monoid. That is, if x is irreducible then c is not a multiple of p. Above we argued that if x is reducible, then c is a multiple of p, so we have that if c is not a multiple of p then x is irreducible. □

Lemma 38. *$\rho(H_\Gamma) \leq r$, and if $p = 2$ we can improve the bound to $\rho(H_\Gamma) \leq r - 1$.*

Proof. Note that due to the irreducibility criterion we have that if $x \in H_\Gamma$ is such that $v_p(x) > r$, then the element will be of Type I and it will be reducible. Also note that all the non-unit elements are multiples of p. Hence, $L(x) \leq v_p(x)$,

$\ell(x) \geq \frac{v_p(x)}{r}$, and so $\rho(x) \leq r$.

In the case when $p = 2$, we have that $v_2(x) \geq r$ implies that x is reducible, so $L(x) \leq v_2(x)$ and $\ell(x) \geq \frac{v_2(x)}{r-1}$, and hence $\rho(H_\Gamma) \leq r - 1$ □

Theorem 39. *If p is a prime such that $p > 2$, then $\rho(H_\Gamma) = r$. Furthermore, if $p = 2$, then we have that $\rho(H_\Gamma) = r - 1$.*

Proof. Assume first that $p = 2$. If $r = 1, 2$, then $\rho\left(H_{\Gamma_n}\right) = 2$, and we have half-factoriality. Hence assume that $r > 2$. Pick t such that $1 + 2^{r-1}t$ is a multiple of 3. Then, $1 + 2^{r-1}t = 3k$ for some k. Note that k will be congruent to 3 modulo 4 because $1 + 2^{r-1} \equiv 1 \pmod 4$. Then, let m be such that

$$m = \frac{k(3k)^{2r-3} - 1}{2}$$

Note that we will have that m is an odd integer. Hence,

$$(1 + 2)(1 + 2m) = (3)(k(3k)^{2r-3}) = (3k)^{2r-2} = (1 + 2^{r-1}t)^{2r-2}$$

$$\Rightarrow (2^{r-1} + 2^r)(2^{r-1} + m2^r) = (2 + 2^r t)^{2r-2}$$

By the irreducibility criterion we see that both above factorizations are into irreducibles, one of length $2r - 2$ and another of length 2. By our above lemma we have that $\rho(H_\Gamma) = r - 1$.

Now assume that $p > 2$. Consider $(p + (p^{r-1} - 2)p^r)^{2r}$, this element is the product of $2r$ irreducibles by the criterion given in the last paper, so this is a factorization of length $2r$. Also,

$$(p + (p^{r-1} - 2)p^r)^{2r} = p^{2r}(1 + (p^{r-1} - 2)(p^{r-1}))^{2r} = p^{2r}[(p^{r-1} - 1)^2]^{2r}$$

$$= [p^r(p^{r-1} - 1)][p^r(p^{r-1} - 1)^{4r-1}]$$

This last expression is a factorization of length 2 since the elements are irreducible by the irreducibility criterion of elements of Type I. □

4.3 Γ of size 2

Another natural question is to see what happens when Γ has size 2, since the case when it has size 1 (an ACM) has already been studied in depth. Say $\Gamma = \{a, b\}$ has modulo n. There are different possibilites for what the multiplication table for Γ might look like.

4.3.1 Type F monoids

Definition 16. *We call a monoid **Type F** if it satisfies $\Gamma = \{a, b\}$ and $a^2 \equiv a \equiv ab$ and $b^2 \equiv b$ modulo n. From now on define $\alpha = \gcd(a, n)$ and $\beta = \gcd(b, n)$.*

Let us first try to characterize when a Type F monoid will have finite elasticity. By Theorem 8 result, we see that there are only two options: Both α and β are both powers of primes, or one is a power of a prime dividing the other (which is a composite number). The following theorem shows that the fomer can never happen (which is somewhat interesting).

Theorem 40. *If H_{Γ_n} is a Type F monoid with finite elasticity, then the* gcd *set contains a composite number.*

Proof. Assume for sake of a contradiction that there is a monoid H_{Γ_n} such that both α and β are prime powers. Then $\alpha = p^{c_1}$ and $\beta = q^{c_2}$. Since $a^2 \equiv a \equiv ab$ and $b^2 \equiv b$ we have:

$$n \mid a(a-1)$$

$$n \mid b(b-1)$$

$$n \mid a(b-1)$$

Define $n' = n/(p^{v_p(n)})$. Hence, $n' \mid n$ implies $n' \mid a(b-1)$. If $p \neq q$ then n' is coprime with a, so we would have $n' \mid b-1$. We have that $q \mid n'$ so $q \mid b-1$, but this is a contradiction with the fact that $q \mid b$. Hence, p ought to be equal to q.

Hence, say that $\alpha = p^{c_1}$ and $\beta = p^{c_2}$. Since $n \mid a(a-1)$, then we have that $n' \mid a-1$. Hence, $n' \cdot \delta_1 + 1$ is a multiple of $p^{v_p(n)}$, and in a similar manner $n' \cdot \delta_2 + 1$ is a multiple of $p^{v_p(n)}$. Hence, $n'(\delta_1 - \delta_2)$ is a multiple of $p^{v_p(n)}$, but since n' is coprime with p we have that $\delta_1 - \delta_2$ is a multiple of $p^{v_p(n)}$. That is, $\delta_1 = \delta_2 + zp^{v_p(n)}$. If $z = 0$, then $a = b$ (a contradiction), and if $z > 0$, then $a > n$ (another contradiction). □

By virtue of the above theorem we have that if H_{Γ_n} is a Type F monoid with finite elasticity, then the gcd-set is of the form $\{p^t, x\}$ with $p \mid x$. The next natural question is to check if p^t is the gcd given by a or the one given by b.

Lemma 41. *Let $\Gamma = \{a, b\}$ be a Type F monoid with modulo n. Then, if $H_\Gamma < \infty$ we have that* $\gcd(b, n) = p^t$ *and* $\gcd(a, n) = x$ *with $p \mid x$.*

Proof. We have proven above that given that the monoid has finite elasticity then the gcd set is $\{p^t, x\}$, so all we need to show is that $\gcd(b, n)$ correspond to p^t. Assume not for a sake of a contradiction. Then we have that $\gcd(b, n) = x$, and $\gcd(a, n) = p^t$. Let $q \mid x$ be different from p (this can be done since x is composite), so we have $n \mid ab - a$, then $q \mid ab - a$, but since $q \mid b$ we have that $q \mid a$, a contradiction since $\gcd(a, n) = p^t$. Ergo, it must be the case that $\gcd(a, n) = x$ and $\gcd(b, n) = p^t$. □

Theorem 42. *Given that $\Gamma = \{a, b\}$ is a Type F monoid with* $\gcd(a, n) = x$ *and* $\gcd(b, n) = p$ *with $p \mid x$, then $\rho(H_\Gamma) = k$ where k is the smallest integer such that $p^k \in H_\Gamma$. Assume further $v_p(a) = 1$.*

Proof. Say k is minimal such that $p^k \in H_\Gamma$. It is easy to see that we must have $p^k \equiv b \pmod{n}$. Then with this in mind say $y \in H_\Gamma$ is such that $v_p(y) \geq k+1$.

If $y = a + nt$, then we have that

$$\frac{a}{p} + \frac{n}{p}t \equiv 0 \pmod{p^k}$$

Note that the solution for the above equation is given by $t = \alpha + cp^k$ where α will be given by $\alpha = (ap^k - a)/n$. Clearly, such an α satisfies the above equation, so all we need to do is to check that α is indeed an integer. Note that since $p^k \equiv b \pmod{n}$ we have that $ap^k \equiv a \pmod{n}$. Thus,

$$y = a + n(\alpha + cp^k)$$

$$= p^k(a + nc)$$

is a factorization within the monoid. If $y = b + nt$, the construction is similar. Hence if y is irreducible then $v_p(y) \leq k$. Ergo,

$$\rho(H_\Gamma) \leq k$$

.
Now consider the element

$$a(p^k)^\ell(a(\frac{a}{p})^{k\ell}) = a^{kl+2}$$

. Note that $a(a/p)^{k\ell}$ is going to be in the monoid since the lcm of the *Delta*-set=$\gcd(a, n) = x$, then $x \mid a$ so

$$x \mid a(\frac{a}{p})^{k\ell}$$

. As $a^{k\ell+1}$ and $p^{k\ell}$ are in H_Γ, we have that by Corollary 14, $a(\frac{a}{p})^{k\ell} \in H_\Gamma$. This element has elasticity of at least

$$\frac{k\ell + 2}{\ell + 2}$$

, as its longest factorization is of length $k\ell+2$ and it has a factorization of length $\ell + 2$. Letting $\ell \to \infty$ we witness a sequence of elements that show $\rho(H_\Gamma) \geq k$. By the upper bound above, we see that $\rho(H_\Gamma) = k$. □

Remark: In general, when $v_p(a)$ is arbitrary, a similar sequence will instead bound the elasticity below by $\frac{k}{v_p(a)}$, showing that $\frac{k}{v_p(a)} \leq \rho(H_{\Gamma_n}) \leq k$.

5 Semi-Regular Congruence Monoids

Recall that a monoid is considered *semi-regular* if the gamma set contains both units and non-units. As expected, semi-regular congruence monoids display factorization properties similar to both singular and regular arithmetic congruence monoids. In fact, some of the factorization properties of specific elements of semi-regular monoids remain unchanged from their ACM counterparts.

Proposition 1. *Let H_{Γ_n} be a semi-regular congruence monoid, then Γ_n contains 1.*

Proof. Suppose that H_{Γ_n} is a semiregular congruence monoid, such that $\Gamma_n = \Gamma_n^\times \cup \Gamma_n^\bullet$ with both non-empty. Because $\Gamma_n^\times$ is non-empty, there exists at least one element $x \in \Gamma_n^\times$. If $x = 1$, then clearly Γ_n contains 1. If $x \neq 1$, then take powers of x. Since Γ_n must be multiplicatively closed, all powers of x must be in $\Gamma_n^\times$, and since x is a unit, some power of x must equal 1. Therefore if Γ_n contains a unit, Γ_n contains 1. □

Lemma 43. *Let $\Gamma_n = \Gamma_n^\times \cup a$ with a nonunit $a^2 \equiv a \pmod n$ for a fixed modulus n. If $x \in M_{1,n}$ is irreducible in $M_{1,n}$, then x is also reducible in H_{Γ_n}.*

Proof. Let x be an irreducible element in $M_{1,n}$ and assume that x is reducible in H_{Γ_n}. Then $x = yz$ where either $y, z \in M_{a,n}$ or $y \in M_{1,n}$ and $z \in M_{a,n}$. First suppose $y, z \in M_{a,n}$, then $yz \equiv a \pmod n$, but because $a \not\equiv 1 \pmod n$ there is a contradiction. Next suppose that $y \in M_{1,n}$ and $z \in M_{a,n}$. Then $yz \equiv a \pmod n$ and again there is a contradiction because $a \not\equiv 1 \pmod n$. Hence x is irreducible in H_{Γ_n}. □

Our research focused on two subcases of semi-regular congruence monoids discussed in the following subsections.

5.1 The Case When $\Gamma_n = \{1, n\}$, and $n = p^k$

Although some properties directly generalize from the ACM case, it is not always the case that a CM is made up of arithmetic congruence monoids. An important distinction to be made is given by the following definition.

Definition 17. *Let a monoid H_{Γ_n} be a* **harmonious** *monoid if it can be written as the union of Arithmetic Congruence Monoids, such that for multiplicatively closed $\Gamma_n = \{\gamma_1, \gamma_2, \gamma_3 \ldots \gamma_m\}$, $\overline{\gamma_i} \equiv \overline{\gamma_i}^2 \pmod n$ for all i.*

Theorem 44. *Let H_{Γ_n} be a semi-regular, harmonious monoid such that $\Gamma_n = \{1, n\}$ for a modulus n, where $n = p^k$. Then $\frac{\varphi(p^k)+3}{2} - \frac{1}{k} \leq \rho(H_{\Gamma_n}) \leq \varphi(p^k)+2k$.*

Proof. Let $\Gamma = \{1, n\}$ be multiplicatively closed, and let $n = p^k$, such that $\overline{p^k} \equiv \overline{p^{2k}} \pmod n$. Construct an element $x \in H_{\Gamma_n}$, such that

$$x = (p^{2k-1} \cdot r^{\phi(p^k)-1})^k \cdot (p^{2k-1} \cdot s^{\phi(p^k)-1})^k$$

where φ is Euler's totient function, r is a rational prime with $\bar{r}$ congruent to a primitive root modulo n, and s is a rational prime with $\bar{s} \equiv \bar{r}^{-1} \pmod{n}$. Because H_{Γ_n} contains all multiples of p^k, x is clearly an element on the monoid. Because $p^k \nmid r^{\phi(p^k)-1}$ and $p^k \nmid s^{\phi(p^k-1}$, it follows that $(p^{2k-1} \cdot r^{\varphi(p^k)-1})$ and $(p^{2k-1} \cdot s^{\phi(p^k)-1})$ are both irreducible in M_{p^k,p^k}. Since neither $r^{\varphi(p^k)-1}$ nor $s^{\varphi(p^k)-1}$ has a subproduct that is congruent to 1 modulo p^k, both $(p^{2k-1} \cdot r^{\phi(p^k)-1})$ and $(p^{2k-1} \cdot s^{\varphi(p^k)-1})$ are irreducible in H_{Γ_n} as well.
The smallest power of p that is reducible in H_{Γ_n} is p^{2k}, hence the largest power of p that remains irreducible is p^{2k-1}. Furthermore, the smallest power of p that is an element of the monoid is p^k. Therefore, the shortest factorization of x will contain the maximum power of p^{2k-1} found in the element, and the longest factorization will contain the maximum power of p^k found in the element. Hence:

$$x = (p^{2k-1} \cdot r^{\phi(p^k)-1})^k \cdot (p^{2k-1} \cdot r^{\phi(p^k)-1})^k = (p^k)^{4k-2} \cdot (r \cdot s)^{(\phi(p^k)-1)k}.$$

It follows, then that the elasticity of this element is

$$\rho(x) = \frac{4k-2+(\phi(p^k)-1)k}{2k} = \frac{(\phi(p^k)+3)k-2}{2k} = \frac{\phi(p^k)+3}{2} - \frac{1}{k}.$$

From Theorem 6, we obtain an upper bound of $\varphi(p^k) + 2k$ for the elasticity. Hence $\frac{\varphi(p^k)+3}{2} - \frac{1}{k} \leq \rho\left(H_{\Gamma_n}\right) \leq \varphi(p^k) + 2k$. □

5.2 Γ_n Contains Units and a Composite Divisor of n

An immediate difference worth noting between this case and the one prior, is that the amount of units included in the gamma set is irrelevant here. Our results apply to the case when Γ_n contains a composite divisor of n (including when Γ_n contains n) regardless of the number of units found in Γ_n. In the previous case, the inclusion of additional units drastically changed the factorization properites.

Theorem 45. *Let n be a fixed modulus, $\Gamma^\times$ be non-empty, $d \mid n$, $\overline{d^2} \equiv \overline{d} \pmod{n}$, d be composite, and $\Gamma = \Gamma^\times \cup \{d\}$. Then H_{Γ_n} has infinite and full elasticity.*

Proof. First note that:

$$\begin{aligned} H_{\Gamma_n} &= H_{\Gamma_n^\times} \cup M_{d,n} \\ &= H_{\Gamma_n^\times} \cup (M_{d,d} \cap M_{1,f}) \end{aligned}$$

where $f = \frac{n}{d}$. Let $x \in M_{d,n}$, $x = d^{\phi(f)m+2}$, where ϕ is Euler's totient function. Since d is composite, $d = ab$ where $\gcd(a, b) = 1$. Hence we can rewrite x as:

$$x = d^{\phi(f)m+2} = \left(d \cdot a^{\phi(f)m}\right)\left(d \cdot b^{\phi(f)m}\right).$$

Since $d \in M_{d,d} \cap M_{1,f}$, we have:

$$d \equiv 1 \pmod{f} \implies ab \equiv 1 \pmod{f}$$

$$\implies \gcd(a, f) = \gcd(b, f) = 1$$

$$\implies a^{\phi(f)} \equiv b^{\phi(f)} \equiv 1 \pmod{f}.$$

Therefore $d \cdot (a^{\phi(f)})^m$, $d \cdot (b^{\phi(f)})^m \in M_{d,d} \cap M_{1,f}$. We need to show that $d \cdot a^{\phi(f)m}$and $d \cdot b^{\phi(f)m}$ are both irreducible in H_{Γ_n}. Since $d^2 \nmid d \cdot a^{\phi(f)m}$ and $d^2 \nmid d \cdot b^{\phi(f)m}$, it follows that both $d \cdot a^{\phi(f)m}$ and $d \cdot b^{\phi(f)m}$ are both irreducible in $M_{d,n}$. Assume that $d \cdot a^{\phi(f)m}$ is reducible in H_{Γ_n}. Then $d \cdot a^{\phi(f)m} = xy$ where $x \in H_{\Gamma_n^\times}$ and $y \in M_{d,n}$. Since $y \in M_{d,n}$, $y = dk$ where $k \equiv 1 \pmod{f}$, but $k \not\equiv 1 \pmod{n}$. Hence:

$$d \cdot a^{\phi(f)m} = xy \implies d \cdot a^{\phi(f)m} = x(dk) \implies a^{\phi(f)m} = xk.$$

Because every rational prime that divides x must also divide a, and $a \mid n$, the $\gcd(x, n) \neq 1$, which contradicts $x \in H_{\Gamma_n^\times}$. Therefore $d \cdot a^{\phi(f)m}$ and $d \cdot b^{\phi(f)m}$ are both irreducible in H_{Γ_n}. Recall that $L(x)$ represents the number of irreducible factors in the longest factorization of x. Here, it is clear that $L(x) \geq \phi(f)m + 2$. Because x cannot contain a factor found in $H_{\Gamma_n^\times}$, the longest factorization is dependent on how many factors of d are in x. Hence $L(x) = \phi(f)m + 2$. Now looking at the elasticity of x we obtain:

$$\rho(x) = \frac{\phi(f)m + 2}{2}.$$

Since m is arbitrary, we conclude that $\rho(H_{\Gamma_n}) = \infty$. Because Γ contains a unit, by 3, H_{Γ_n} contains a prime element q. Hence for any integers r and s, with $r \geq s \geq 1$, and $\phi(f) > 1$ we can construct an element $y \in H_{\Gamma_n}$:

$$y = d^{\phi(f)(r-s)+2} \cdot q^{\phi(f)s-2} = \left(d \cdot a^{\phi(f)(r-s)}\right) \cdot \left(d \cdot b^{\phi(f)(r-s)}\right) q^{\phi(f)s-2}.$$

Since $L\left(d^{\phi(f)(r-s)+2)}\right) = \phi(f)(r-s) + 2$, $l\left(d^{\phi(f)(r-s)+2}\right) = 2$, $L\left(q^{\phi(f)s-2}\right) = l\left(q^{\phi(f)s-2}\right) = \phi(f)s - 2$, and $d^{\phi(f)(r-s)+2}$ has no factors in $H_{\Gamma^\times}$, it follows that:

$$\rho(y) = \frac{\phi(f)(r-s) + 2 + \phi(f)s - 2}{2 + \phi(f)s - 2}$$

$$= \frac{\phi(f)r}{\phi(f)s}$$

$$= \frac{r}{s}.$$

If $\phi(f) = 1$, then without loss of generality replace r and s with $2r$ and $2s$ respectively. Therefore H_{Γ_n} is fully elastic. □

This case is significant because it is the first time in the research of both CMs and ACMs alike to find a monoid with infinite elasticty that is also fully elastic.

References

[1] D. D. Anderson, David F. Anderson, Scott T. Chapman, and William W. Smith. Rational elasticity of factorizations in Krull domains. *Proc. Amer. Math. Soc.*, 117(1):37–43, 1993.

[2] David F. Anderson and Scott T. Chapman. On the elasticities of Krull domains with finite cyclic divisor class group. *Comm. Algebra*, 28(5):2543–2553, 2000.

[3] Paul Baginski and Scott T. Chapman. Arithmetic congruence monoids: A survey.

[4] 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.

[5] 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.

[6] 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.

[7] M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math.*, 108(1):105–118, 2007.

[8] 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.

[9] S. T. Chapman and David Steinberg. On the elasticity of generalized arithmetical congruence monoids. *Results Math.*, 58(3-4):221–231, 2010.

[10] Alfred Geroldinger and Franz Halter-Koch. Congruence monoids. *Acta Arith.*, 112(3):263–296, 2004.

[11] 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.

[12] Alfred Geroldinger, Franz Halter-Koch, Wolfgang Hassler, and Florian Kainrath. Finitary monoids. *Semigroup Forum*, 67(1):1–21, 2003.

[13] Franz Halter-Koch. Arithmetical semigroups defined by congruences. *Semigroup Forum*, 42(1):59–62, 1991.