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

Accepted Elasticity in Local Arithmetic Congruence Monoids

Lorin Crawford · Vadim Ponomarenko · Jason Steinberg · Marla Williams

Abstract For certain $a, b \in \mathbb{N}$, an *Arithmetic Congruence Monoid* $M(a, b)$ is a multiplicatively closed subset of $\mathbb{N}$ given by $\{x \in \mathbb{N} : x \equiv a \pmod{b}\} \cup \{1\}$. An *irreducible* in this monoid is any element that cannot be factored into two elements, each greater than 1. Each monoid element (apart from 1) may be factored into irreducibles in at least one way. The *elasticity of a monoid element* (apart from 1) is the longest length of a factorization into irreducibles, divided by the shortest length of a factorization into irreducibles. The *elasticity of the monoid* is the supremum of the elasticities of the monoid elements. A monoid has *accepted elasticity* if there is some monoid element that has the same elasticity as the monoid. An Arithmetic Congruence Monoid is *local* if $\gcd(a, b)$ is a prime power (apart from 1). It has already been determined whether Arithmetic Congruence Monoids have accepted elasticity in the non-local case; we make make significant progress in the local case, i.e. for many values of a, b.

Keywords non-unique factorization · arithmetical congruence monoid · accepted elasticity · elasticity of factorization

Mathematics Subject Classification (2000) 20M14 · 20D60 · 13F05

Lorin Crawford
Clark Atlanta University

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

Jason Steinberg
Princeton University

Marla Williams
Willamette University

1 Introduction

Factorization theory studies the arithmetic properties of domains or commutative, cancellative monoids where unique factorization fails to hold. For a reference see any of the recent works [2,5,12,15] or the upcoming survey [4]. The present work determines a standard arithmetic invariant for a particular type of monoid. Previous work in this direction left a significant gap, and we close much of this gap. Unfortunately, the problem becomes complex so it appears to be quite difficult to close the gap completely.

Let $\mathbb{N}$ denote the set of positive integers, and $\mathbb{N}_0$ denote the set of non-negative integers. Let $a, b \in \mathbb{N}$ with $a \leq b$ and $a^2 \equiv a \pmod b$. Set $M(a, b) = \{x \in \mathbb{N} : x \equiv a \pmod b\} \cup \{1\}$. This set is a monoid under multiplication. Such sets are called *arithmetic congruence monoids*, and their arithmetic has received considerable attention recently [6–11,14,16,19]. If $\gcd(a, b) = 1$, then the ACM is a Krull monoid, whose arithmetic is well-studied (see [13]). The accepted elasticity question was resolved in [8] for the case where $\gcd(a, b)$ is not a prime power, so we restrict our attention to the case wherein $\gcd(a, b)$ is a prime power, in which case $M(a, b)$ is called a *local* (singular) arithmetic congruence monoid. Specifically, we consider the local arithmetic congruence monoid, henceforth ACM, given as $M = M(p^\alpha \xi, p^\alpha n)$, for some $\xi, n, p, \alpha \in \mathbb{N}$ with p prime and $\gcd(\xi, n) = 1$. Note also that $\gcd(p, n) = 1$ is a consequence of $a^2 \equiv a \pmod b$.

For a monoid M, we say that a nonunit $x \in M$ is *irreducible* if there are no factorizations $x = y \cdot z$ where y, z are nonunits from M. ACM's are examples of C-monoids (for a reference see the monograph [15]); consequently each nonunit $x \in M = M(p^\alpha \xi, p^\alpha n)$ has at least one factorization into irreducibles. Set $\mathcal{L}(x) = \{n | x = x_1 x_2 \cdots x_n, \text{ with each } x_i \text{ irreducible in } M\}$; this set is known to be finite for all C-monoids (and easy to see for ACM's specifically, because $\mathbb{N}$ is well-ordered). We define the *elasticity* of x, denoted $\rho(x)$, as $\frac{\max \mathcal{L}(x)}{\min \mathcal{L}(x)}$. We define the *elasticity* of M as the supremum of $\rho(x)$ over all nonunits $x \in M$. If the supremum is actually a maximum, i.e. if there is some $x \in M$ where $\rho(x) = \rho(M)$, we say that M has *accepted elasticity*. This is an important semigroup invariant that is well-understood for certain semigroups but not for others. For example, in [15] it was shown that if the monoid is finitely generated then it has accepted elasticity; further, transfer homomorphisms preserve accepted elasticity. For a survey of elasticity (including accepted elasticity) in integral domains see [3].

It was shown in [8] that if $\gcd(a, b)$ is neither 1 nor a prime power, then M has infinite elasticity (and hence does not have accepted elasticity). Therein was also shown that if $\gcd(a, b) = 1$, then M is equivalent to a block monoid, with accepted elasticity, equal to half of the Davenport constant of $\mathbb{Z}_b^\times$. The question of accepted elasticity in local ACM's was considered in [9], where the question was answered completely in the special case of p generating $\mathbb{Z}_n^\times$. We reprove their result with our methods, as Theorem 3. We will be able to answer the question for most other cases. The answer depends on the (multiplicative) group structure of $\mathbb{Z}_n^\times$, and on the cyclic subgroup generated by the element $[p] \in \mathbb{Z}_n^\times$. Broadly, if this subgroup has "large" index, elasticity will be accepted for all or almost all α. Otherwise, the answer is more complicated, and depends on the residue class of α, modulo $\phi(n)$.

We now recall some standard notation from nonunique factorization theory. Let G be a finite abelian group. Although in our context we write G multiplicatively, our definitions will be compatible with the traditional ones in which groups are written additively. We use $\mathcal{F}(G)$ to denote the set of all finite length (unordered) sequences with terms from G, refer to the elements of $\mathcal{F}(G)$ as sequences, and write all sequences multiplicatively, so that a sequence $S \in \mathcal{F}(G)$ is written in the form

$$S = g_1 \cdot g_2 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{\cdot \nu_g(S)}, \text{ with } \nu_g(S) \in \mathbb{N}_0 \text{ for all } g \in G.$$

We call $\nu_g(S)$ the *multiplicity* of g in S. For $d \in \mathbb{N}$, we call

$$S^d = \prod_{g \in G} g^{\cdot d\nu_g(S)} \in \mathcal{F}(G) \text{ the } d-\textit{fold product} \text{ of } S.$$

The notation $S_1|S$ indicates that S_1 is a subsequence of S, that is $\nu_g(S_1) \leq \nu_g(S)$ for all $g \in G$. For $S_1, S_2, \ldots, S_m$, each a subsequence of S, if

$$\sum_{i=1}^m \nu_g(S_i) = \nu_g(S) \text{ for all } g \in G,$$

we write $S_1 S_2 \cdots S_m = S$ and call this a *partition* of S. If instead

$$\sum_{i=1}^m \nu_g(S_i) \leq \nu_g(S) \text{ for all } g \in G,$$

we write $S_1 S_2 \cdots S_m | S$ and call this a *subpartition* of S.

For a sequence $S = g_1 \cdot g_2 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{\cdot \nu_g(S)} \in \mathcal{F}(G)$, we call

$$|S| = l = \sum_{g \in G} \nu_g(S) \in \mathbb{N}_0 \text{ the } \textit{length} \text{ of } S,$$

$$\sigma(S) = \prod_{i=1}^l g_i = \prod_{g \in G} g^{\nu_g(S)} \in G \text{ the } \textit{sum} \text{ of } S,$$

$$\Sigma(S) = \Big\{ \prod_{i \in I} g_i : I \subseteq [1, l], 0 \neq |I| \Big\} \subseteq G \text{ the } \textit{set of subsequence sums} \text{ of } S,$$

$$\text{and } \Sigma'(S) = \Big\{ \prod_{i \in I} g_i : I \subseteq [1, l], 0 \neq |I| \neq l \Big\} \subseteq G$$

the *set of proper subsequence sums* of S.

Henceforth, let $M = M(p^\alpha \xi, p^\alpha n)$ be an ACM, and let $x \in \mathbb{Z}$ satisfy $\gcd(x, n) = 1$. We denote by $[x]$ the equivalence class in $\mathbb{Z}_n^\times$ containing x. We define the valuation $\nu_p(x)$ as the unique integer d such that $p^d|x$ and $p^{d+1} \nmid x$, as paralleling the above valuation for $p \in G$ and $x \in \mathcal{F}(G)$. The following are elementary results about ACM's that are either found in, or are easy to derive from, the previous ACM papers.

Lemma 1 *Let $M = M(p^\alpha \xi, p^\alpha n)$ be an ACM. Let β be the unique minimal integer satisfying $\beta \geq \alpha$ and $[p]^\beta = [1]$. Then*

1. *For any $u \in \mathbb{N}$, $u \in M \setminus \{1\}$ if and only if $[u] = 1$ and $\nu_p(u) \geq \alpha$.*
2. *If $u \in M$ is irreducible, then $\alpha \leq \nu_p(u) \leq \alpha + \beta - 1$.*
3. *$\rho(M) = \frac{\alpha+\beta-1}{\alpha}$.*
4. *For any $u \in M$, there are some $a, l \in \mathbb{N}_0$ such that $a \geq \alpha$ and $u = p^a q_1 q_2 \cdots q_l$, where each q_i is prime and satisfies $\gcd(q_i, pn) = 1$.*
5. *We may determine ξ as the unique integer in $[1, n-1]$ satisfying $[\xi] = [p]^{-\alpha}$.*
6. *We have $p^\beta \in M$ and $p^s \notin M$ for all $s \in [1, \beta)$.*

Consequently, an ACM $M(p^\alpha \xi, p^\alpha n)$ may be determined by p, α, n alone, and we will write $M(p, \alpha, n)$ for convenience, with ξ and β defined implicitly whenever needed. The main result for ACM's that our methods produce is the following theorem, whose proof will be presented in the final section.

Theorem 1 *Fix $n \in \mathbb{N}$ and consider the arithmetic congruence monoid $M(p, \alpha, n)$ for various α and various primes p coprime to n. Then:*

1. *$M(p, \alpha, n)$ has accepted elasticity for all p and all sufficiently large α if for some distinct odd primes p_1, p_2, p_3 and positive integers a_1, a_2 we have:*
   (a) $n \in \{1, 2, 8, 12\}$; or
   (b) $p_1 p_2 p_3 | n$ or $4 p_1 p_2 | n$ or $8 p_1 | n$; or
   (c) $n \in \{p_1^{a_1} p_2^{a_2}, 2 p_1^{a_1} p_2^{a_2}\}$, and $\gcd(p_1 - 1, p_2 - 1) > 2$.
2. *For all other n, there are infinitely many primes p' for which $M(p', \alpha, n)$ has accepted elasticity for all sufficiently large α, and also infinitely many other primes p'' for which $M(p'', \alpha, n)$ does not have accepted elasticity for infinitely many α.*

The classification of p in (2) depends on its congruence class modulo $\phi(n)$.

Our results will also make more precise these broad statements, giving good bounds for "sufficiently large α" as well as classifying most (and for some n all) congruence classes modulo $\phi(n)$.

2 Configurations

Our primary tool in determining whether an ACM has accepted elasticity will be the study of configurations, as defined below.

Let G be a finite abelian group, and let $g \in G$. We denote the order of g in G by $|g|_G$, or $|g|$ when unambiguous.

Definition 1 Let G be a finite abelian group. Let $g \in G$. Let $\delta, \gamma \in \mathbb{N}$ satisfy $\delta \geq |g| > \gamma \geq 0$. Suppose that there is some sequence $S \in \mathcal{F}(G)$ and some $c, d \in \mathbb{N}$ with $\frac{c}{d} \geq 1 + \frac{\delta-1}{\delta-\gamma}$ satisfying

1. There is some partition $S_1 S_2 \cdots S_d = S$ such that for each $i \in [1, d]$,
   (a) $\sigma(S_i) = g^{\gamma+1}$, and
   (b) $\Sigma(S_i) \cap \{g, g^2, \ldots, g^\gamma\} = \emptyset$; and also
2. There is some subpartition $T_1 T_2 \cdots T_c | S$, satisfying $\sigma(T_i) = g^\gamma$ for each $i \in [1, c]$.

We call this sequence, partition, and subpartition a (G, g, δ, γ)-*configuration.*

Note that if (c, d) satisfy the conditions, then so do (kc, kd) for each $k \in \mathbb{N}$, by considering the subpartition $T_1^k T_2^k \cdots T_c^k | S^k = S_1^k S_2^k \cdots S_d^k$. Hence we will typically assume without loss of generality that $(\delta - \gamma)|d$.

The connection between (G, g, δ, γ)-configurations and accepted elasticity in ACMs, is given by the following. With this result we will be able to set aside p, α, β and instead focus on $G = \mathbb{Z}_n^\times, g = [p], \delta, \gamma$, such that $0 \leq \gamma < |g|$ and δ is a multiple of $|g|$.

Theorem 2 *Let $M = M(p, \alpha, n)$ be an ACM. Then M has accepted elasticity if and only if there exists a $(\mathbb{Z}_n^\times, [p], \beta, \beta - \alpha)$-configuration.*

Proof Suppose first that M has accepted elasticity. Then there is some pair of factorizations into irreducibles $u_1 u_2 \cdots u_s = v_1 v_2 \cdots v_t$ with $\frac{s}{t} = \frac{\alpha+\beta-1}{\alpha} = \rho(M)$. By Lemma 1, $s\alpha \leq \sum_{i=1}^s \nu_p(u_i) = \sum_{i=1}^t \nu_p(v_i) \leq t(\alpha + \beta - 1)$. All inequalities are therefore equalities, so $\nu_p(u_i) = \alpha, \nu_p(v_i) = \alpha + \beta - 1$ for all i.

Express each $v_i = p^{\alpha+\beta-1} q_1^{(i)} q_2^{(i)} \cdots q_{l_i}^{(i)}$ as in Lemma 1. For each $i \in [1, s]$, we define a sequence from $\mathbb{Z}_n^\times$ given by $S_i = [q_1^{(i)}][q_2^{(i)}] \cdots [q_{l_i}^{(i)}]$. We have $[1] = [v_i] = [p]^{\alpha+\beta-1}\sigma(S_i)$, so $\sigma(S_i) = [p]^{\beta-\alpha+1}$. Suppose there were a subsequence $T|S_i$ with $\sigma(T) = [p]^x$ for some $x \in [1, \beta - \alpha]$. Then we set $v_i' = p^{\beta-x} \prod q_j^{(i)}$, where the product is taken over all $[q_j^{(i)}] \in T$. We set $v_i'' = \frac{v_i}{v_i'}$. We have $\nu_p(v_i') \geq \alpha$ and $\nu_p(v_i'') = \alpha + x - 1 \geq \alpha$. Further $[v_i'] = [p]^{\beta-x}\sigma(T) = [p]^\beta = [1]$. Since $[1] = [v_i' v_i''] = [v_i'][v_i'']$, also $[v_i''] = 1$. Hence $v_i', v_i'' \in M$, which contradicts the irreducibility of v_i. Therefore, the S_i each satisfy the conditions of Definition 1.1. Set $S = S_1 S_2 \cdots S_t$.

Express each $u_i = p^\alpha r_1^{(i)} r_2^{(i)} \cdots r_{l_i}^{(i)}$ as in Lemma 1. For each $i \in [1, t]$, we define a sequence from $\mathbb{Z}_n^\times$ given by $T_i = [r_1^{(i)}][r_2^{(i)}] \cdots [r_{l_i}^{(i)}]$. We have $[1] = [u_i] = [p]^\alpha \sigma(T_i)$, so $\sigma(T_i) = [p]^{-\alpha} = [p]^{\beta-\alpha}$. By unique factorization in $\mathbb{N}$, in fact $T_1 T_2 \cdots T_s = S$. Thus, $T_1 \cdots T_s$ is a partition (and hence a subpartition) of S. It remains to observe that $\frac{s}{t} = \frac{\alpha+\beta-1}{\alpha} = 1 + \frac{\beta-1}{\beta-(\beta-\alpha)}$.

Suppose now that there exists a $(\mathbb{Z}_n^\times, [p], \beta, \beta-\alpha)$-configuration. We assume without loss that $\alpha|d$. Define $\phi : \mathbb{Z}_n^\times \to \mathbb{N}$ such that $\phi([x]) = q_x$ for some prime $q_x \neq p$ satisfying $[q_x] = [x]$. Such a ϕ exists by Dirichlet's theorem on primes. We now set $v_i = p^{\alpha+\beta-1} \prod_{[x]\in S_i} \phi([x])$ for $i \in [1, d]$. Note that $[v_i] = [p]^{\alpha+\beta-1}\sigma(S_i) = [p]^{\alpha+\beta-1}[p]^{\beta-\alpha+1} = [1]$, so $v_i \in M$. Suppose that v_i

were reducible with factors v_i', v_i''. We have $\alpha+\beta-1=\nu_p(v_i)=\nu_p(v_i')+\nu_p(v_i'')\geq \nu_p(v_i')+\alpha$, so $\nu_p(v_i')\leq \beta-1$. We have $v_i'=p^x\phi(T)$ for some x with $\alpha\leq x\leq \beta-1$ and some $T|S_i$. We have $[1]=[v_i']=[p]^x\sigma(T)$, so $\sigma(T)=[p]^{\beta-x}$, which is a contradiction. Hence each $v_i\in M$ is irreducible.

The second property gives us $\frac{c}{d}\geq 1+\frac{\beta-1}{\beta-(\beta-\alpha)}=\frac{\alpha+\beta-1}{\alpha}$. We set $c'=\lfloor d(\frac{\alpha+\beta-1}{\alpha})\rfloor=(\frac{d}{\alpha})(\alpha+\beta-1)$. For $i\in[1,c'-1]\subseteq[1,c]$, we take $u_i=p^\alpha\prod_{[x]\in T_i}\phi([x])$, and set $u_{c'}=\frac{\phi(S)}{u_1u_2\cdots u_{c'-1}}$. We have $[u_i]=[p]^\alpha\sigma(T_i)=[p]^\alpha[p]^{\beta-\alpha}=[1]$, so $u_i\in M$ for $i\in[1,c'-1]$. Set $u=v_1v_2\cdots v_d=u_1u_2\cdots u_{c'}$. We have $[1]=[u]=[u_1][u_2]\cdots[u_{c'-1}][u_{c'}]$, so $[u_{c'}]=[1]$. Further, since $\alpha c'=d(\alpha+\beta-1)=\nu_p(u)=(c'-1)\alpha+\nu_p(u_{c'})$ we have $\nu_p(u_{c'})=\alpha$. Hence $u_{c'}\in M$. Note that each u_i is irreducible since $\nu_p(u_i)=\alpha$.

Finally, we have $\rho(u)\geq\frac{c'}{d}=\frac{\alpha+\beta-1}{\alpha}=\rho(M)$, so M has accepted elasticity. □

We now broadly outline the remainder of this paper. In the subsequent sections, we will find that if $G/\langle g\rangle$ is "large", then configurations will exist for all γ, provided that δ is sufficiently large. However, if $G/\langle g\rangle$ is "small", then configurations will exist for "small" gamma and will not exist for "large" gamma (keeping in mind that $\gamma\in[0,|g|-1]$).

In the ACM context, we fix p and n. As we vary α we get all γ,δ as $\gamma=(-\alpha \bmod |g|)$ and $\delta=\alpha+\gamma$, where $|g|$ denotes the order of $[p]$ in $\mathbb{Z}_n^\times$. Thus "large" δ corresponds to large α, while "large" γ corresponds to certain congruence classes of α modulo $|g|$, or more generally modulo $\phi(n)$, the Euler totient.

3 Finding Configurations

We first present some results that produce (G,g,δ,γ)-configurations in certain special cases. This section contains miscellaneous results, ending with a new proof of the case where $G=\langle g\rangle$, corresponding to ACM's where p is a primitive root modulo n.

Recall that by Theorem 2, we are only concerned with δ that are multiples of $|g|$. The following proposition, in the context of ACMs, states that $M(p,\alpha,n)$ has accepted elasticity, provided that $\alpha=\beta$. For other equivalent conditions, see Proposition 2.

Proposition 1 *Let G be any finite abelian group. Let $g\in G$, and let $\delta\in\mathbb{N}$ satisfy $\delta\geq|g|$. Then there is a $(G,g,\delta,0)$-configuration.*

Proof Set $d=1$, and set $S=S_1=(g)$. We have $\sigma(S_1)=g^{0+1}$, while $\{g,g^2,\ldots,g^\gamma\}=\emptyset$. For the second condition, we take $c=\lceil 1+\frac{\delta-1}{\delta}\rceil=2$ and set $T_1=T_2=\emptyset$, which gives $\sigma(T_i)=1=g^0$. □

Consequently, we will assume henceforth that $\gamma>0$ and $\beta>\alpha$. By the following proposition, we equally assume that $\xi>1$ and $\rho(M)\geq 2$. The following result is found as Theorem 2.4 in [7]; we include a brief proof for completeness.

Proposition 2 *Given ACM M, the following are equivalent: (1) $\xi = 1$; (2) $[p]^\alpha = [1]$; (3) $\beta = \alpha$; and (4) $\rho(M) < 2$.*

Proof If (1) holds, since $[\xi] = [p]^{-\alpha}$, in fact $[1] = [p]^\alpha$, so (2) holds. If (2) holds, since $\alpha \geq \alpha$ and $[p]^\alpha = [1]$, in fact $\beta = \alpha$, so (3) holds. If (3) holds, then $[\xi] = [p]^{-\alpha} = [p]^{-\beta} = [1]$. Because $1 \leq \xi \leq n-1$, in fact $\xi = 1$, so (1) holds. If (3) holds, then $\rho(M) = \frac{\beta+\alpha-1}{\alpha} = 2 - \frac{1}{\beta} < 2$, so (4) holds. Lastly, if (4) holds, then $\frac{\beta+\alpha-1}{\alpha} < 2$, so $\beta - 1 < \alpha \leq \beta$, so (3) holds. □

The following proposition, in the context of ACMs, states that if $M(p, \alpha, n)$ has accepted elasticity, then so does $M(p, \alpha + t, n)$ for all $t \in \mathbb{N}$ satisfying $[p]^t = [1]$.

Proposition 3 *Suppose that there is a (G, g, δ, γ)-configuration with $\gamma \geq 1$. Let $\delta' \in \mathbb{N}$ with $\delta' > \delta$. Then there is a (G, g, δ', γ)-configuration.*

Proof We will show that the same configuration works. Because δ only appears in relation to c and d, we only need to check that inequality. Because $\gamma \geq 1$, we have $\frac{\delta-1}{\delta-\gamma} \geq \frac{\delta'-\delta}{\delta'-\delta}$. Their mediant is $\frac{\delta'-1}{\delta'-\gamma}$, which must be between these fractions and thus no more than $\frac{\delta-1}{\delta-\gamma}$. Consequently, $\frac{c}{d} \geq 1 + \frac{\delta-1}{\delta-\gamma} \geq 1 + \frac{\delta'-1}{\delta'-\gamma}$. □

In the ACM context, the combination of the previous proposition with the following, states that if $M(p, 1, n)$ has accepted elasticity, then so does $M(p, \alpha, n)$ for all $\alpha \geq 1$.

Proposition 4 *Suppose that there is a $(G, g, |g|, |g| - 1)$-configuration. Let $\gamma \in \mathbb{N}_0$ with $\gamma < |g| - 1$. Then there is a $(G, g, |g|, \gamma)$-configuration.*

Proof Set $k = |g| - \gamma - 1$. Without loss, we may assume that $(k+1)|c$ and $(k+1)|d$. We set $S'_i = S_i(g^{-1})^{\cdot k}$ for $i \in [1, d]$. We have $S' = S'_1 S'_2 \cdots S'_d = SV$ for $V = (g^{-1})^{\cdot dk}$. We have $\sigma(S'_i) = g^{|g|-k} = g^{\gamma+1}$. Note that $\Sigma(g^{-1})^{\cdot k} = \{g^{-1}, \ldots, g^{-k}\} = \{g^{\gamma+1}, g^{\gamma+2}, \ldots, g^{|g|-1}\}$, and that $(\Sigma(S_i)) \cap \langle g \rangle = \{1\}$. Hence $(\Sigma(S'_i)) \cap \langle g \rangle = \{1, g^{\gamma+1}, g^{\gamma+2}, \ldots, g^{|g|-1}\}$, which is disjoint from $\{g, g^2, \ldots, g^\gamma\}$.

For each $i \in [1, \frac{c}{k+1}]$, we set $T'_i = T_{(i-1)(k+1)+1} T_{(i-1)(k+1)+2} \cdots T_{i(k+1)}$. We have $\sigma(T'_i) = [g]^{(k+1)(|g|-1)} = [g]^{-k-1} = [g]^\gamma$. For each $i \in [\frac{c}{k+1} + 1, \frac{c}{k+1} + \frac{kd}{k+1}]$, we set $T'_i = (g^{-1})^{\cdot k+1}$ and again $\sigma(T'_i) = g^\gamma$. By hypothesis $\frac{c}{d} \geq 1 + \frac{|g|-1}{|g|-(|g|-1)} = |g|$. Hence $\frac{c}{d} + k \geq |g| + k = (|g| - \gamma) + (|g| - 1) = (|g| - \gamma)(1 + \frac{|g|-1}{|g|-\gamma}) = (k+1)(1 + \frac{|g|-1}{|g|-\gamma})$. Consequently, $\frac{\frac{c}{k+1} + \frac{kd}{k+1}}{d} \geq 1 + \frac{|g|-1}{|g|-\gamma}$. □

The following proposition, in the context of ACMs, states that $M(p, \alpha, n)$ has accepted elasticity, provided that α is "large" and $|[p]|$ is composite. Specifically, if $|[p]| = rs$ in $\mathbb{Z}_n^\times$, then we need $\alpha \in (\beta - r, \beta)$. The remaining possibilities for α, namely $(\beta - rs, \beta - r]$, are not covered; however in some cases there are no configurations for these α, as will be shown in Proposition 6.

Proposition 5 *Let G be any finite abelian group. Let $g \in G$. Suppose that $|g| = rs$ with $r, s > 1$ and $rs > 4$. Let $\gamma \in \mathbb{N}$ satisfy $\gamma < r$. Then there is a (G, g, rs, γ)-configuration.*

Proof We first consider the special case $\{s = 2, \gamma = 1\}$; by hypothesis $r \geq 3$. We set $S_1 = (g^{-1})^{\cdot 2r-2}, S_2 = (g^2)^{\cdot 2r+1}, T = (g^{-1}) \cdot (g^2)$. We have $\sigma(S_1) = \sigma(S_2) = g^2 = g^{\gamma+1}$ and $\sigma(T) = g^\gamma$. Also, $\Sigma(S_1) = \langle g \rangle \setminus \{1, g\}$ and $\Sigma(S_2) = \langle g^2 \rangle$, which does not contain g since $|g|$ is even. We set $S = S_1 S_2$ and $d = 2$. We set $c = 2r - 2$ and see that $T^c | S$. Lastly we have $\frac{c}{d} = r - 1 \geq 2 = 1 + \frac{2r-1}{2r-1}$.

Henceforth we exclude the case $\{s = 2, \gamma = 1\}$. Set $S_1 = (g^{-1})^{\cdot rs-\gamma-1}$. We have $\sigma(S_1) = g^{\gamma+1-rs} = g^{\gamma+1}$, and $\Sigma(S_1) = \{g^{-1}, g^{-2}, \ldots, g^{-rs+\gamma+1}\} = \{g^{\gamma+1}, g^{\gamma+2}, \ldots, g^{rs-1}\}$, which has no intersection with $\{g^1, g^2, \ldots, g^\gamma\}$. Set $S_2 = (g^r)^{\cdot 2rs^2} \cdot (g^{\gamma+1})$. We have $\sigma(S_2) = g^{\gamma+1}$ and $\Sigma(S_2) = \langle g^r \rangle \cup g^{\gamma+1}\langle g^r \rangle$, which again has no intersection with $\{g^1, g^2, \ldots, g^\gamma\}$. We set $d = rs - \gamma$ and $S = S_1^{d-1} S_2$.

We now set $c = s(rs - 2 + \gamma(s-2)) + 1$. We set $T_0 = (g^{-1}) \cdot (g^{\gamma+1})$ and $T_i = (g^{-1})^{\cdot r-\gamma} \cdot (g^r)$ for $i \in [1, c-1]$. Set $T = T_0 T_1 \cdots T_{c-1}$; we will prove that $T|S$. There are three group elements to consider. First, $(g^{\gamma+1})$ appears once in both T and S. Second, (g^r) appears $2rs^2$ times in S and $c - 1 \leq s(rs + rs) = 2rs^2$ times in T. Lastly, considering (g^{-1}), we need $(rs - \gamma - 1)^2 \geq 1 + (c-1)(r-\gamma)$. We chose c so that $(rs - \gamma - 1)^2 - (c-1)(r-\gamma) = (\gamma(s-1) - 1)^2$. This integer is zero only when $\gamma = 1$ and $s = 2$, a possibility which has been excluded.

We now prove that $\frac{c}{d} \geq 1 + \frac{rs-1}{rs-\gamma}$. This rearranges to $X \geq 0$, for $X = rs^2 + \gamma s^2 - 2\gamma s - 2s + 2 - 2rs + \gamma = (s-1)^2\gamma + s(r(s-2) - 2) + 2$. If $s \geq 3$ we have $X \geq 4\gamma + 3(r-2) + 2 \geq 0$; if $s = 2$ we have $X = \gamma - 2 \geq 0$ since $\gamma = 1$ has been excluded. □

Let G be a nontrivial finite abelian group. Suppose that $g \in G$ generates G, i.e. $G = \langle g \rangle$. It is a well-known result from group theory that if $G \cong \mathbb{Z}_n^\times$ for some n, then $|G| = |g|$ is even. In this situation the following proposition states that the bound of Proposition 5 is tight (provided $|g| > 4$). It also shows that although (G, g, δ, γ)-configurations may be plentiful, they are not omnipresent – not all ACMs have accepted elasticity.

Proposition 6 *Let G be a finite abelian group. Let $g \in G$ satisfy $G = \langle g \rangle$. Suppose that $|g| = 2r \geq 4$. Let $\gamma, \delta \in \mathbb{N}$ satisfy $\delta \geq 2r > \gamma \geq r$. Then there is no (G, g, δ, γ)-configuration.*

Proof We write $G = \{g^{-0}, g^{-1}, \ldots, g^{-(2r-1)}\}$, and define $\phi : G \to \mathbb{N}_0$ via $\phi(g^{-i}) = i$, for $i \in [0, 2r-1]$. Note that $\phi(ab) \equiv \phi(a) + \phi(b) \pmod{2r}$. We extend ϕ to sequences in the natural way, via $\phi(a \cdot b) = \phi(a) + \phi(b)$. For any sequence U, we have $\phi(U) \equiv \phi(\sigma(U)) \pmod{2r}$. If U satisfies $\Sigma(U) \cap \{g, g^2, \ldots, g^\gamma\} = \emptyset$; we will prove that in fact $\phi(U) = \phi(\sigma(U))$. We proceed by induction on $|U|$; if $|U| = 1$ the result is clear. Otherwise we write $U = U' \cdot (g^{-s})$. By the inductive hypothesis, $\phi(U') = \phi(\sigma(U'))$, so we have $\phi(U) = \phi(U') + s = \phi(\sigma(U')) + s$. Note that $s < 2r - \gamma$, because otherwise $g^{-s} \in$

$\{g, g^2, \ldots, g^\gamma\}$. Because $\gamma \geq r$ we have $s < r$. Similarly $\phi(\sigma(U')) < r$, but then $\phi(U) < 2r$. Combining with $\phi(U) \equiv \phi(\sigma(U))$ gives $\phi(U) = \phi(\sigma(U))$.

Suppose now there is a (G, g, δ, γ)-configuration. By the above, each S_i satisfies $\phi(S_i) = \phi(\sigma(S_i)) = 2r - \gamma - 1$. Now, $\phi(T_i) \geq \phi(\sigma(T_i)) = 2r - \gamma$. Hence we have $d(2r - \gamma - 1) = d\phi(S_i) = \phi(S) \geq \sum_{i=1}^{c} \phi(T_i) \geq c(2r - \gamma)$. We rearrange to get $\frac{c}{d} \leq \frac{2r-\gamma-1}{2r-\gamma} < 1 + \frac{\delta-1}{\delta-\gamma}$, a contradiction. □

We combine Propositions 5 and 6 into the following theorem, which was the main result of [9] (with different proof). It completely solves the special case where p is a primitive root modulo n. In particular, this requires $\mathbb{Z}_n^\times$ to be cyclic, which in the ACM context occurs only when $n = 2, 4, q^k$, or $2q^k$ for some odd prime q.

Theorem 3 ([9]) *Let G be a finite abelian group. Let $g \in G$ satisfy $G = \langle g \rangle$. Suppose that $|g|$ is even. Let $\delta, \gamma \in \mathbb{N}$ with $\delta \geq |g| > \gamma > 0$. Then there is a (G, g, δ, γ)-configuration if and only if*

1. *$|g| > 4$, and*
2. *$|g| > 2\gamma$.*

Proof The only cases not covered by Propositions 5 and 6 are the following. $\{|g| = 4, \gamma = 1\}$: Because $\nu_g(S) = 0$, for all i we have $\nu_{g^3}(T_i) \geq 1$, while $\nu_{g^3}(S_i) \leq 2$. Hence we have $2d \geq \nu_{g^3}(S) \geq c$, but also $\frac{c}{d} \geq 1 + \frac{\delta-1}{\delta-1} = 2$. Hence all inequalities are equalities and $\nu_{g^3}(S_i) = 2$ for all i. Then $\nu_{g^2}(S_i) = 0$ for all i, and thus $\nu_{g^2}(S) = 0$. But now $\sigma(T_i) \neq g$, so in fact there is no configuration. $\{|g| = 2, \gamma = 1\}$: Because $\nu_g(S_i) = 0$, we have $\sigma(T_i) \neq g$. □

4 $\langle g \rangle \oplus H$

With Theorem 3 we have resolved the case of $G = \langle g \rangle$, a cyclic group (provided $|G|$ is even, which holds for all nontrivial $G \cong \mathbb{Z}_n^\times$). Otherwise, $G/\langle g \rangle$ is nontrivial and in the remainder we explore its structure.

In this section we consider nontrivial subgroups $H \leq G$ such that $\langle g \rangle \oplus H \leq G$. Such subgroups H need not exist, e.g. for $(G, g) \cong (\mathbb{Z}_{25}, 5)$. However they do exist in two important cases, given by Propositions 7 and 8. In the ACM context, these cases will include all n except powers of 2.

We recall first a lemma from the classical theory of finite abelian groups.

Lemma 2 *Let G be a finite abelian group with $|G| = y$. Let $x \in \mathbb{N}$ satisfy $x | y$. Then there is some subgroup $H \leq G$ with $|H| = x$.*

Proof See, e.g., [18, p. 77]. □

The following proposition allows us to not only address noncyclic groups G, but also cyclic groups G provided that some prime divides $|G|$ but not $|g|$.

Proposition 7 *Let G be a finite abelian group with $g \in G$. Suppose that $|G| = xy$ and $\gcd(x, y) = \gcd(x, |g|) = 1$. Then there is some subgroup $H \leq G$ with $|H| = x$ and $\langle g \rangle \oplus H \leq G$.*

Proof By Lemma 2 there must be some $H \leq G$ with $|H| = x$. Let $z \in \langle g \rangle \cap H$. Then $|z|$ divides both $|g|$ and x, but then $|z| = 1$ so the conclusion follows. □

Proposition 8 is an elementary result concerning finite abelian groups that seems like it should be well-known, but we have no reference. For noncyclic groups G, it provides a "large" subgroup H such that $\langle g \rangle \oplus H \leq G$. This directly generalizes the well-known result that if $|g| = exp(G)$, then $\langle g \rangle \oplus (G/\langle g \rangle) \cong G$.

Proposition 8 *Let $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ be a finite abelian group, with $n_1|n_2|\cdots|n_k$. Let $g \in G$. Then there is some $H \leq G$ such that $\langle g \rangle \oplus H \leq G$ and $H \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_{k-1}}$.*

Proof We first assume that G is a p-group for some prime p, i.e. $G \cong \mathbb{Z}_{p^{a_1}} \oplus \mathbb{Z}_{p^{a_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{a_k}}$, for integers $a_k \geq a_{k-1} \geq \cdots \geq a_1 \geq 1$. We write G additively as k-tuples, and in particular $g = (g_1, g_2, \ldots, g_k)$. For each $i \in [1, k]$, let m_i be the order of g_i in $\mathbb{Z}_{p^{a_i}}$. Let M be chosen so that m_M is maximal among $\{m_1, \ldots, m_k\}$. By Lagrange's theorem on finite groups, each m_i is a power of p for all $i \in [1, k]$, so in particular $m_i|m_M$. Hence m_M is the order of g, and therefore each nonzero element of $\langle g \rangle$ has a nonzero element in the M^{th} coordinate. We now set $H = \{(b_1, \ldots, b_k) \in G : b_M = 0 \text{ and } p^{a_M} b_k = 0\}$, a subgroup of G. We have $\langle g \rangle \cap H = \{0\}$, so $\langle g \rangle \oplus H \leq G$. Further, by swapping the M^{th} and k^{th} coordinates, we see that $H \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_{k-1}} \oplus \{0\} \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_{k-1}}$.

Suppose now that there are distinct primes $p_1, p_2 \ldots, p_s$ and corresponding p-groups $G_1, G_2, \ldots, G_s$, such that $G \cong G_1 \oplus G_2 \oplus \cdots \oplus G_s$. For each $i \in [1, s]$ we have $G_i \cong \mathbb{Z}_{p_i^{a(i,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{a(i,k_i)}}$, for integers $a(i, k_i) \geq \cdots \geq a(i, 1) \geq 1$. By the above, for each $i \in [1, s]$ we find $H_i \leq G_i$ such that $\langle g|_{G_i} \rangle \oplus H_i \leq G_i$ and $H_i \cong \mathbb{Z}_{p_i^{a(i,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{a(i,k_{i-1})}}$. Let ϕ_i denote the natural embedding of each p-group G_i into G, and set $H = \phi_1(H_1) + \phi_2(H_2) + \cdots + \phi_s(H_s)$. Because the primes are distinct, in fact $\phi_1(H_1) \oplus \phi_2(H_2) \oplus \cdots \oplus \phi_s(H_s) \leq G$, and also $\langle g \rangle \oplus H \leq G$. We now have $H \cong \prod H_i$, and the result follows since $n_k = \prod_i p_i^{a(i,k_i)}, n_{k-1} = \prod_i p_i^{a(i,k_{i-1})}, \ldots$. □

Proposition 8 admits an easy corollary, which will be useful in Section 6.

Corollary 1 *Let $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ be a finite abelian group, with $n_1|n_2|\cdots|n_k$. Let $g \in G$. Then $exp(G/\langle g \rangle) \geq n_{k-1}$.*

Theorem 4 is the main result of this section, which requires the following definition.

Definition 2 Let $H \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ be a finite abelian group, where $m_1|m_2|\cdots|m_k$. We define $d^\star(H) = (m_1 + m_2 + \cdots + m_k) - k = \sum_{i=1}^{k}(m_i - 1)$.

Theorem 4 *Let G be a finite abelian group and $g \in G$. Suppose that there is some $H \leq G$ with $\langle g \rangle \oplus H \leq G$. Let $\delta, \gamma \in \mathbb{N}$ that satisfy $\delta \geq |g| > \gamma > 0$.*

Then there is a (G, g, δ, γ)-configuration, provided that the following inequality holds:

$$d^\star(H) > \left(1 - \frac{1}{|g|}\right)\left(\frac{1}{|g| - \gamma} + \frac{\delta - 1}{\delta - \gamma}\right)$$

Proof We will construct the configuration explicitly. Let $\alpha \in \mathbb{N}$ be large. Let $h_1, \dots, h_k \in G$ with $\langle h_1 \rangle \oplus \cdots \langle h_k \rangle \oplus \langle g \rangle \le G$, $|h_i| = m_i$ for $i \in [1, k]$, and $m_1 | m_2 | \cdots | m_k$. Set $S_1 = (g^{-1})^{\cdot |g| - \gamma - 1} \cdot \prod_{i=1}^k (h_i g^\gamma)^{\cdot m_i - 1} \cdot (h_i^{-1} g^{-\gamma})^{\cdot m_i - 1}$, $S_2 = (g^{-1})^{\cdot |g| - \gamma - 1} \cdot \prod_{i=1}^k (h_i^{-1})^{\cdot |g|^2 m_i^2 \alpha}$. We set $T_0 = (g^{-1})^{\cdot |g| - \gamma}$, and for $i \in [1, k]$ set $T_i = (h_i g^\gamma) \cdot (h_i^{-1})$, $T_i' = (h_i^{-1} g^{-\gamma})^{\cdot |g| - 1} \cdot (h_i^{-1})^{\cdot |g|(m_i - 1) + 1}$. Note that $\sigma(S_1) = \sigma(S_2) = g^{\gamma + 1}$ and for all $i \in [1, k]$, $\sigma(T_i) = \sigma(T_i') = \sigma(T_0) = g^\gamma$. If $x \in \langle g \rangle \cap (\Sigma(S_1) \cup \Sigma(S_2))$ then in fact $x \in \Sigma((g^{-1})^{\cdot |g| - \gamma - 1})$ and consequently $x \notin \{g, g^2, \dots, g^\gamma\}$.

For convenience, set $a_1 = |g| - 1, a_\gamma = |g| - \gamma$. We set $d = a_1 a_\gamma \alpha + 1$ and $S = S_1^{a_1 a_\gamma \alpha} S_2$. We set $c = a_1(a_\gamma - 1)\alpha + d^\star(H)|g| a_\gamma \alpha$ and $T = T_0^{a_1(a_\gamma - 1)\alpha} \prod_{i=1}^k T_i^{(m_i - 1) a_1 a_\gamma \alpha} T_i'^{(m_i - 1) a_\gamma \alpha}$. We now verify that $T | S$. For g^{-1}, we have $\nu_{g^{-1}}(T) = a_\gamma a_1 (a_\gamma - 1)\alpha < (a_\gamma - 1) a_1 a_\gamma \alpha + (a_\gamma - 1) = \nu_{g^{-1}}(S)$. For any $i \in [1, k]$, we have $\nu_{h_i g^\gamma}(T) = (m_i - 1) a_1 a_\gamma \alpha = \nu_{h_i g^\gamma}(S)$. We also have $\nu_{h_i^{-1} g^{-\gamma}}(T) = (m_i - 1) a_1 a_\gamma \alpha = \nu_{h_i^{-1} g^{-\gamma}}(S)$. Lastly we have $\nu_{h_i^{-1}}(T) = (m_i - 1) a_1 a_\gamma \alpha + (m_i - 1) a_\gamma \alpha (|g|(m_i - 1) + 1) = (m_i - 1) m_i a_\gamma |g| \alpha \le m_i^2 |g|^2 \alpha = \nu_{h_i^{-1}}(S)$. We now calculate

$$\begin{aligned}
\frac{c}{d} &= \frac{a_1(a_\gamma - 1)\alpha + d^\star(H)|g| a_\gamma \alpha}{a_1 a_\gamma \alpha + 1} = \frac{a_1(a_\gamma - 1) + d^\star(H)|g| a_\gamma}{a_1 a_\gamma + \frac{1}{\alpha}} = \\
&= \frac{a_1(a_\gamma - 1) + d^\star(H)|g| a_\gamma}{a_1 a_\gamma} - \epsilon(\alpha) = 1 - \frac{1}{a_\gamma} + d^\star(H)\frac{|g|}{a_1} - \epsilon(\alpha) \\
&> 1 - \frac{1}{a_\gamma} + \frac{1}{|g| - \gamma} + \frac{\delta - 1}{\delta - \gamma} = 1 + \frac{\delta - 1}{\delta - \gamma}
\end{aligned}$$

Note that $\epsilon(\alpha) > 0$ satisfies $\lim_{\alpha \to \infty} \epsilon(\alpha) = 0$, so we may take $\epsilon(\alpha)$ small enough to satisfy the inequality in the third line above. □

Recall that in the ACM context we may assume that δ is a positive integer multiple of $|g|$. We will consider several cases separately in the following corollaries. For the smallest value of $\delta = |g|$, the following corollary shows that it suffices to have $d^\star(H) > \frac{|g|-1}{|g|-\gamma}$. If $d^\star(H) \ge |g|$ then this condition is met for all γ; otherwise it is met only for $\gamma < |g| - \frac{|g|-1}{d^\star(H)}$.

Corollary 2 *Let G be a finite abelian group and $g \in G$. Suppose that there is some $H \le G$ with $\langle g \rangle \oplus H \le G$. Let $\gamma \in \mathbb{N}$ such that $|g| > \gamma > 0$. Suppose that $d^\star(H) > \frac{|g|-1}{|g|-\gamma}$. Then there is a $(G, g, |g|, \gamma)$-configuration.*

Proof With $\delta = |g|$ we have $\left(1 - \frac{1}{|g|}\right)\left(\frac{1}{|g|-\gamma} + \frac{\delta-1}{\delta-\gamma}\right) = \frac{|g|-1}{|g|-\gamma}$. □

Corollary 3 *Let G be a finite abelian group, and let $exp(G)$ denote the exponent of G. Suppose that $d^\star(G) \geq 2\ exp(G) - 1$. Then there are (G, g, γ, δ)-configurations for all $g \in G$ and all $\gamma, \delta \in \mathbb{N}$ satisfying $\delta \geq |g| > \gamma > 0$.*

Proof Let $g \in G$. Apply Proposition 8 to get $H \leq G$ with $\langle g \rangle \oplus H \leq G$. We have $d^\star(H) + \ exp(G) - 1 = d^\star(G) \geq 2\ exp(G) - 1$, so $d^\star(H) \geq exp(G) \geq |g|$. We now apply Corollary 2 and Proposition 3. □

If we exclude the smallest value of δ, namely $|g|$, we only need the weak condition that $d^\star(H) \geq 3$ to get all possible γ.

Corollary 4 *Let G be a finite abelian group and $g \in G$. Suppose that there is some $H \leq G$ with $\langle g \rangle \oplus H \leq G$. Let $\delta, \gamma \in \mathbb{N}$ satisfy $\delta \geq 2|g|$ and $|g| > \gamma > 0$. Suppose that $d^\star(H) \geq 3$. Then there is a (G, g, δ, γ)-configuration.*

Proof Since $\delta - \gamma > |g| > \gamma - 1$, we have $1 > \frac{\gamma-1}{\delta-\gamma}$. Therefore, $d^\star(H) \geq 3 > 2 + \frac{\gamma-1}{\delta-\gamma} = 1 + \frac{\delta-1}{\delta-\gamma} > \left(1 - \frac{1}{|g|}\right)\left(\frac{1}{|g|-\gamma} + \frac{\delta-1}{\delta-\gamma}\right)$. □

Corollary 4 gives configurations for all γ, provided that $d^\star(H) \geq 3$ and δ is sufficiently large. If $d^\star(H) = 2$ (i.e. $H \cong \mathbb{Z}_3$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$), then Corollary 5 shows that again we get configurations for all γ provided that δ is sufficiently large. If $d^\star(H) = 1$ (i.e. $H \cong \mathbb{Z}_2$), then we do not get configurations for all γ, no matter the size of δ, as will be shown later in Proposition 10.

Corollary 5 *Let G be a finite abelian group and $g \in G$. Suppose that there is some $H \leq G$ with $\langle g \rangle \oplus H \leq G$ and $d^\star(H) = 2$. Let $\delta, \gamma \in \mathbb{N}$ satisfy $\delta > |g|\frac{|g|-1}{2}$ and $|g| > \gamma > 0$. Then there is a (G, g, δ, γ)-configuration.*

Proof It suffices to prove that $2 > \left(1 - \frac{1}{|g|}\right)\left(\frac{1}{|g|-\gamma} + \frac{\delta-1}{\delta-\gamma}\right)$ for $\gamma = |g| - 1$. This is a rearrangement of $\delta > |g|\frac{|g|-1}{2}$. □

In the special case of $H = \langle h \rangle$ with $|h| = |g|$, e.g. $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$, we have $d^\star(H) = |g| - 1$. Here Theorem 4 does not apply for $\{\delta = |g|, \gamma = |g| - 1\}$, although it would for larger δ or smaller γ. In fact there is a configuration for this case as well, and hence for all δ, γ by Proposition 4.

Proposition 9 *Let G be a finite abelian group. Let $g, h \in G$ with $\langle g \rangle \oplus \langle h \rangle \leq G$ and $|g| = |h|$. Let $\delta, \gamma \in \mathbb{N}_0$ satisfy $\delta \geq |g| > \gamma \geq 0$. Then there is a (G, g, δ, γ)-configuration.*

Proof By Propositions 3 and 4, it suffices to consider the case $\delta = |g|$ and $\gamma = |g| - 1$. Set $k = |g|$ for convenience. Set $d = 2$, $S_1 = (hg^{-1})^{\cdot 2k}, S_2 = (h^{-1})^{\cdot 2k}$, and $S = S_1 S_2$. We have $\sigma(S_1) = (h^k)^2 (g^{-k})^2 = 1 = (h^{-k})^2 = \sigma(S_2)$. We have $\Sigma(S_1) = \{h^i g^{-i} : i \in [1, 2k]\}$. Suppose that for some $i, j \in \mathbb{N}$ we had $h^i g^{-i} = g^j$. Then we have $h^i = g^{j+i}$ so by hypothesis $h^i = 1$ and hence $k|i$ so $h^i g^{-i} = ((hg^{-1})^k)^{i/k} = 1$. We also have $\Sigma(S_2) = \langle h \rangle$ so $\Sigma(S_2) \cap \langle g \rangle = \{1\}$. We set $c = 2k$ and set $T = (hg^{-1}) \cdot (h^{-1})$. We have $\sigma(T) = g^{-1} = g^\gamma$, and $T^c = S$, in fact a partition of S. Lastly, we compute $\frac{c}{d} = |g| = 1 + \frac{\delta-1}{\delta-(\delta-1)} = 1 + \frac{\delta-1}{\delta-\gamma}$, as desired. □

5 $exp(G/\langle g\rangle)$

We now continue the study of $G/\langle g\rangle$, but drop the $\langle g\rangle \oplus H \leq G$ restriction which is too strong in some cases. Instead we consider its exponent of $G/\langle g\rangle$, where we can find configurations if this exponent is at least 3. On the other hand, in certain cases where this exponent is 2 or 3, we prove the nonexistence of configurations for $\gamma = |g| - 1$.

In the ACM context this approach is fruitful for almost all n, p where Theorem 3 does not apply, and complements the results of the previous section.

The following result uses a construction similar to that in Theorem 4.

Theorem 5 *Let G be a finite abelian group and $g \in G$. Set $K = \langle g\rangle$, $m = exp(G/K)$. Let $\delta, \gamma \in \mathbb{N}$ that satisfy $\delta \geq |g| > \gamma > 0$. Then there is a (G, g, δ, γ)-configuration, provided that the following inequality holds:*

$$m \geq 1 + \frac{1}{|g| - \gamma} + \frac{\delta - 1}{\delta - \gamma}$$

Proof We will construct the configuration explicitly. Let $hK \in G/K$ satisfy $|hK| = exp(G/K) = m$. Note that $h^s \notin K$ for $s \in [-(m-1), (m-1)] \setminus \{0\}$. For each $i \in [1, |g|]$, we set $S_i = (g^{-1})^{\cdot|g|-\gamma-1} \cdot (hg^i)^{\cdot m-1} \cdot (h^{-1}g^{-i})^{\cdot m-1}$. We set $T_0 = (g^{-1})^{\cdot|g|-\gamma}$, and for $i \in [1, |g|]$ set $T_i = (hg^{\gamma+i}) \cdot (h^{-1}g^{-i})$. Note that for all $i \in [1, |g|]$, we have $\sigma(S_i) = g^{\gamma+1}$ and $\sigma(T_i) = g^{\gamma} = \sigma(T_0)$. If $x \in K \cap \Sigma(S_i)$ then in fact $x \in \Sigma((g^{-1})^{|g|-\gamma-1})$ and consequently $x \notin \{g, g^2, \ldots, g^{\gamma}\}$.

For convenience, set $a_\gamma = |g| - \gamma$. We set $d = |g|a_\gamma$ and $S = \prod_{i=1}^{|g|} S_i^{a_\gamma}$. We set $c = (a_\gamma - 1)|g| + (m-1)a_\gamma|g| = ma_\gamma|g| - |g|$ and $T = T_0^{(a_\gamma-1)|g|} \prod_{i=1}^{|g|} T_i^{(m-1)a_\gamma}$. We now verify that $T|S$ (in fact $T = S$). For g^{-1}, we have $\nu_{g^{-1}}(T) = a_\gamma(a_\gamma - 1)|g| = \nu_{g^{-1}}(S)$. For any $i \in [1, k]$, we have $\nu_{hg^i}(T) = (m-1)a_\gamma = \nu_{hg^i}(S)$ and equally $\nu_{h^{-1}g^i}(T) = (m-1)a_\gamma = \nu_{h^{-1}g^i}(S)$. Lastly, we calculate $\frac{c}{d} = \frac{ma_\gamma|g|-|g|}{|g|a_\gamma} = m - \frac{1}{a_\gamma} \geq 1 + \frac{\delta-1}{\delta-\gamma}$ by hypothesis. □

As before, the theorem leads to several corollaries. Corollary 6 gives configurations for all but one γ, and all sufficiently large δ.

Corollary 6 *Let G be a finite abelian group. Let $g \in G$. Set $K = \langle g\rangle$. Suppose that $exp(G/K) \geq 3$. Let $\delta, \gamma \in \mathbb{N}$ with $\delta \geq 3|g|$ and $|g| - 1 > \gamma > 0$. Then there is a (G, g, δ, γ)-configuration.*

Proof Suppose by way of contradiction that Theorem 5 fails to hold, i.e. $3 < 1 + \frac{1}{|g|-\gamma} + \frac{\delta-1}{\delta-\gamma} \leq 1 + \frac{1}{2} + \frac{3|g|-1}{2|g|+2}$, where we used the hypotheses regarding δ and γ. This rearranges to $3|g| + 3 < 3|g| + 1$, a contradiction. □

Corollary 7 *Let G be a finite abelian group. Let $g \in G$. Set $K = \langle g\rangle$. Suppose that $exp(G/K) = m$, for some $m \geq 4$. Let $\delta, \gamma \in \mathbb{N}$ with either*

1. *$\delta \geq 2|g|$ and $|g| > \gamma > 0$; or*
2. *$\delta = |g|$ and $\frac{m-2}{m-1}|g| \geq \gamma > 0$.*

Then there is a (G, g, δ, γ)-configuration.

Proof Suppose by way of contradiction that Theorem 5 fails to hold, i.e. $m < 1 + \frac{1}{|g|-\gamma} + \frac{\delta-1}{\delta-\gamma}$.
(1) Then $m < 1 + 1 + \frac{2|g|-1}{|g|+1}$, which rearranges to $(m-4)|g| < 1-m$, a contradiction.
(2) Then $m < 1 + \frac{|g|}{|g|-\gamma}$, which rearranges to $\gamma > \frac{m-2}{m-1}|g|$, a contradiction. $\square$

These corollaries show that there are configurations for all γ (for δ sufficiently large) if $exp(G/K) \geq 4$, and all but one γ for $exp(G/K) = 3$. The case of that missing γ is addressed in Proposition 11, while the case of $exp(G/K) = 2$ is addressed in Proposition 10.

Proposition 10 *Let G be a finite abelian group. Suppose that $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2w}$ or $G \cong \mathbb{Z}_{2w}$, with $w \geq 2$. Let $g \in G$, and set $K = \langle g \rangle$. Suppose that $G/K \cong \mathbb{Z}_2$. Let $\delta \in \mathbb{N}$ with $\delta \geq |g|$. Then there is no $(G, g, \delta, |g|-1)$-configuration.*

Proof We first consider the special case of $G \cong \mathbb{Z}_4, \gamma = 1$. By considering possible S_i it is easy to see that $\frac{c}{d} > 1$ is impossible. Suppose now that $|g| > 2$, and we have such a configuration. Set $\gamma = |g|-1$ for convenience. Choose coset representative $h \in G \setminus K$. We have $G = K \cup (hK)$. For $X \in \mathcal{F}(G)$, we define X^+, X^- such that $X^+ \in \mathcal{F}(1K)$, $X^- \in \mathcal{F}(hK)$, and $X = X^+ \cdot X^-$. We define $Q = \{k \in G : |k| > 2\} \subseteq G$ and $\phi : \mathcal{F}(G) \to \mathbb{N}_0$ via $\phi(S) = \sum_{k \in Q} \nu_k(S)$. For each $i \in [1, c]$, we claim that $\phi(T_i) \geq 1$ because otherwise T_i would consist of elements of order at most 2, hence $\sigma(T_i)$ would be of order at most 2, but $\sigma(T_i) = g^{-1}$ which is of order $|g|$. We now claim that $\phi(S_i) \leq 2$ for each $i \in [1, d]$. Suppose to the contrary for some i we have $\phi(S_i) \geq 3$. We have $\phi(S_i^+) = 0$ so in fact $\phi(S_i^-) \geq 3$. Hence there are some $(hg^x), (hg^y), (hg^z) \in Q$ with $(hg^x) \cdot (hg^y) \cdot (hg^z) | S_i^-$. Taking these pairwise, we get $h^2 g^{x+z} = h^2 g^{y+z} = 1$, since $\Sigma(S_i) \cap \{g, g^2, \ldots, g^\gamma\} = \emptyset$. Modulo $|g|$, we have $x + z \equiv y + z \equiv 0$ and hence $x \equiv y$. But then $(hg^x)^2 = (hg^x)(hg^y) = 1$, so in fact $(hg^x) \notin Q$. Combining the above, we get $2d \geq \phi(S) \geq c$ hence $2 \geq \frac{c}{d} \geq 1 + \frac{\delta-1}{\delta-\gamma}$. This rearranges to $1 \geq \gamma = |g|-1$, so $2 \geq |g|$, which is a contradiction. $\square$

Note that the conditions of Proposition 10 exclude the case $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, where configurations exist for all γ by Proposition 9.

Proposition 11 *Let G be a finite abelian group. Suppose that $G \cong \mathbb{Z}_{9w}$. Let $g \in G$, and set $K = \langle g \rangle$. Suppose that $G/K \cong \mathbb{Z}_3$. Let $\delta \in \mathbb{N}$ with $\delta \geq |g|$. Then there is no $(G, g, \delta, |g|-1)$-configuration.*

Proof Suppose we had such a configuration. Set $\gamma = |g|-1$ for convenience. Choose coset representative $h \in G \setminus K$. We have $G = K \cup (hK) \cup (h^2K)$, with $h^3 \in K$. If there were some $s \in [1, |g|-1]$ such that $h^3 = g^{3s}$, then we have $(hg^{-s})^3 = 1$ and hence $G \cong K \oplus \mathbb{Z}_3$, which violates the hypothesis. Similarly, there is no such s with $(h^2)^3 = g^{3s}$.

Let S_i be in our configuration; we claim that S_i contains at most 4 nontrivial elements. First, S_i can contain no nontrivial elements from K. Suppose that S_i contains four elements from hK, say $hg^{x_1}, hg^{x_2}, hg^{x_3}, hg^{x_4}$. Multiplying these three at a time, we get $h^3 g^{x_1+x_2+x_3}, h^3 g^{x_1+x_2+x_4} \in \Sigma S_i \cap K = \{1\}$.

Hence $x_3 \equiv x_4 \pmod{|g|}$ and by symmetry $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \pmod{|g|}$. But now $(hg^{x_1})^3 \in \Sigma S_i \cap K = \{1\}$, so $h^3 = (g^{-x_1})^3$, which contradicts our hypothesis. Hence S_i contains at most three nontrivial elements from hK and by symmetry at most three nontrivial elements from h^2K. Suppose now S_i contained at least 5 nontrivial elements. At least three must be from the same coset, so without loss S_i contains $hg^{x_1}, hg^{x_2}, hg^{x_3}, h^2g^{x_4}$. But now $h^3g^{x_1+x_4} = h^3g^{x_2+x_4} = h^3g^{x_3+x_4} = 1$, so $x_1 \equiv x_2 \equiv x_3 \pmod{|g|}$ and again $(hg^{x_1})^{\cdot 3}|S_i$, a contradiction.

Since $\nu_{g^{-1}}(S) = 0$ and $\sigma(T_i) = g^{-1}$, each T_i in our configuration must have at least two nonunit elements. Combining the above, we get $4d \geq 2c$, and hence $2 \geq \frac{c}{d} > 1 + \frac{\delta-1}{\delta-\gamma}$. This rearranges to $1 \geq \gamma = |g| - 1$, so $2 \geq |g|$. But then $G \cong \mathbb{Z}_6$, a contradiction. □

Compare Proposition 11 with Corollary 5, which gives us the opposite conclusion for large δ, if $G \cong K \oplus \mathbb{Z}_3$. Note that by Corollary 6, Proposition 11 is tight for $\delta \geq 3|g|$. That is, $\gamma = |g| - 1$ is the only value of γ that does not have a configuration.

6 Applications to ACM's and Open Problems

We are now ready to apply our results on configurations to prove results about ACM's. We write $n = 2^s p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. By the Chinese Remainder Theorem, we have $\mathbb{Z}_n^\times \cong \mathbb{Z}_{2^s}^\times \times \mathbb{Z}_{p_1^{a_1}}^\times \times \cdots \mathbb{Z}_{p_k^{a_k}}^\times$. The structure here is well known (see, e.g. [20]): $\mathbb{Z}_2^\times \cong \mathbb{Z}_1$, $\mathbb{Z}_4^\times \cong \mathbb{Z}_2$, $\mathbb{Z}_{2^s}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{s-2}}$ (for $s \geq 3$), and $\mathbb{Z}_{p^a}^\times \cong \mathbb{Z}_{\phi(p^a)} = \mathbb{Z}_{p^{a-1}(p-1)}$. Apart from the special case of $\mathbb{Z}_1$, each of these additive groups has even rank. We may therefore canonically write $\mathbb{Z}_n^\times \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_t}$, where $2|n_1|n_2| \cdots |n_t$.

Theorem 1 *Fix $n \in \mathbb{N}$ and consider the arithmetic congruence monoid $M(p, \alpha, n)$ for various α and various primes p coprime to n. Then:*

1. *$M(p, \alpha, n)$ has accepted elasticity for all p and all sufficiently large α if for some distinct odd primes p_1, p_2, p_3 and positive integers a_1, a_2 we have:*
   (a) $n \in \{1, 2, 8, 12\}$; or
   (b) $p_1p_2p_3|n$ or $4p_1p_2|n$ or $8p_1|n$; or
   (c) $n \in \{p_1^{a_1}p_2^{a_2}, 2p_1^{a_1}p_2^{a_2}\}$, and $\gcd(p_1 - 1, p_2 - 1) > 2$.
2. *For all other n, there are infinitely many primes p' for which $M(p', \alpha, n)$ has accepted elasticity for all sufficiently large α, and also infinitely many other primes p'' for which $M(p'', \alpha, n)$ does not have accepted elasticity for infinitely many α.*

The classification of p in (2) depends on its congruence class modulo $\phi(n)$.

Proof If $n \in \{1, 2\}$ then $\mathbb{Z}_n^\times \cong \mathbb{Z}_1$ so $\gamma = 0$ regardless of p, α, and we apply Proposition 1. If $n \in \{8, 12\}$, then $\mathbb{Z}_n^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and we apply Proposition 9.

If n is of one of the forms in 1b, then $\mathbb{Z}_n^\times$ has 2-rank at least 3 and hence $t \geq 3$. We apply Proposition 8 to get some $H \leq G$ with $\langle g \rangle \oplus H \leq G$. Because

H has rank at least 2, $d^\star(H) \geq 2$. We may therefore apply Corollary 5 to get configurations for all γ and all $\delta > \binom{|g|}{2}$.

If n is of one of the forms in 1c, then set $w = \gcd(p_1 - 1, p_2 - 1)$. We have $t = 2$ and $n_1 = w$, and $w \geq 4$ since w is even. We apply Proposition 8 to get some $H \leq G$ with $\langle g \rangle \oplus H \leq G$. Because $n_1 \geq 4$, $d^\star(H) \geq 3$. We may therefore apply Corollary 4 to get configurations for all γ and all $\delta > 2|g|$.

For all n, if $p \equiv 1 \pmod{\phi(n)}$ then $\gamma = 0$ regardless of α, and we apply Proposition 1. This demonstrates a prime with accepted elasticity for sufficiently large α.

Suppose now that n has none of the forms from 1; we need to find primes where elasticity is not accepted. If $n > 2$ admits a primitive root then we take such a p and apply Theorem 3 with $\gamma = |g| - 1$. Suppose now that $n = 4p_1^{a_1}$. Then $\mathbb{Z}_n^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2n_2}$ and we may choose g with $|g| = 2n_2$ and apply Proposition 10. This equally works if $n = p_1^{a_1}p_2^{a_2}$ (or $n = 2p_1^{a_1}p_2^{a_2}$) and $\gcd(p_1 - 1, p_2 - 1) = 2$. It also works if $n = 2^s$ with $s \geq 4$.

Finally, note that each $[p]$ contains infinitely many primes by Dirichlet's theorem on primes in arithmetic progression. □

The conclusions of Theorem 1 may be sharpened with more careful use of our configuration results. We continue to write $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_t}$, with $2|n_1|n_2|\cdots|n_t$. We divide such groups into four types, with groups corresponding to $n \in \{1, 2, 4\}$ excluded for convenience.

Type I:	$t \geq 2$ and $n_{t-1} \geq 4$
Type II:	$t \geq 3$ and $n_{t-1} = 2$
Type III:	$t = 2$ and $n_{t-1} = 2$
Type IV:	$t = 1$

Type I corresponds to Theorem 1.1c and Type II to Theorem 1.1b. Asymptotically, "almost all" n are of these two types, because "almost all n have about $\log\log n$ prime factors" (see, e.g. [17]). We have strong results for these two types, while Types III and IV require more care. Type III corresponds to $\{2^s, 4p_1^{a_1}, p_1^{a_1}p_2^{a_2}, 2p_1^{a_1}p_2^{a_2} : s \geq 4, p_1, p_2 \text{ odd primes}, \gcd(p_1 - 1, p_2 - 1) = 2\}$. Type IV corresponds to $\{p_1^{a_1}, 2p_1^{a_1} : p_1 \text{ odd prime}\}$.

Suppose that G is of Type I. Combining Corollary 1 with Corollary 7 gives configurations for all g and γ, for $\delta \geq 2|g|$. The same method gives configurations for the missing $\delta = |g|$, for all g, provided that $\gamma \leq \frac{n_{t-1}-2}{n_{t-1}-1}|g| \leq \frac{2}{3}|g|$. If $|g| \leq n_{t-1}$ (in particular if $n_{t-1} = n_t$) then combining Propositions 8 and 9 gives configurations for all δ, γ.

Next, suppose that G is of Type II, i.e. $G \cong \mathbb{Z}_2^{t-1} \times \mathbb{Z}_{n_t}$. For $t \geq 4$, we combine Proposition 8 with Corollary 4 to get configurations for all g and γ, provided $\delta \geq 2|g|$. Corollary 2 gives configurations for the missing $\delta = |g|$, for all g, provided that $\gamma < \frac{|g|(t-2)+1}{t-1}$. For $t = 3$, we apply Corollary 5, which gives configurations for all g, γ, provided that $\delta > |g|\frac{|g|-1}{2}$.

Suppose now that G is of Type III, i.e. $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{n_t}$. Here, we must consider various g separately. We first consider $|g| = n_t$. If $n_t = 2$, then by Proposition 9 there are configurations for all δ, γ. Assuming that $n_t \geq 4$, then by Proposition 10, there is no configuration for $\gamma = n_t - 1$, for any δ. By Propositions 5 and 3, there are configurations for all $\gamma < n_t$ and all δ, provided $n_t \geq 6$. In between, for $\gamma \in [\frac{n_t}{2}, n_t - 2]$, we have no results. Suppose now that $|g| = \frac{n_t}{2}$. If $\frac{n_t}{2}$ is odd, then by Proposition 7 and Corollary 5 there are configurations for all γ, provided $\delta > \binom{n_t/2}{2}$. If $\frac{n_t}{2}$ is even, we have only the result of Propositions 5 and 3, which give configurations for $\gamma < \frac{n_t}{4}$, provided $n_t \geq 12$. Lastly, we consider $|g| < \frac{n_t}{2}$. If $exp(G/\langle g\rangle) = 3$, then we apply Corollary 6 to get configurations for all $\delta \geq 3|g| = n_t$ and all $\gamma \neq |g| - 1$. Otherwise, $exp(G/\langle g\rangle) > 3$, and we apply Corollary 7 to get configurations for all $\delta \geq 2|g|$ and all γ, as well as for $\delta = |g|$ and certain γ.

Lastly, suppose that G is of Type IV, i.e. $G \cong \mathbb{Z}_{n_t}$. If $|g| = n_t$, then by Theorem 3, irrespective of δ, configurations exist when $n_t > 4$ and $\gamma < \frac{n_t}{2}$, and do not exist otherwise. If $|g| = \frac{n_t}{2}$ and $n_t \geq 4$, then by Proposition 10, there is no configuration for $\gamma = n_t - 1$, for any δ. If $|g| = \frac{n_t}{2}$ and $n_t = 2$, then by Proposition 1, configurations exist for all δ. Suppose now that $|g| = \frac{n_t}{3}$. If $9|n_t$, then by Proposition 11, there is no configuration for any δ, for $\gamma = |g| - 1$; however by Corollary 6, there are configurations for all other γ. If instead $9 \nmid n_t$, then by Proposition 7 and Corollary 5, there are configurations for all γ, provided $\delta > |g|\frac{|g|-1}{2}$. Lastly, we consider $|g| < \frac{n_t}{3}$; by Corollary 7 there are configurations for all $\delta \geq 2|g|$ and all γ, as well as for $\delta = |g|$ and certain γ.

Although we have made substantial progress on the elasticity question for ACM's, there are still several gaps in our work. Most notable is the case of Type III and Type IV groups with g satisfying $|g| = \frac{|G|}{2}$, where little is known for most γ, δ. Preliminary work in the Type IV case suggests that there is a cutoff $\tau \approx \sqrt{|g|}$, such that if $\gamma < \tau$ configurations exist for δ sufficiently large and if $\gamma > \tau$ configurations do not exist. This and other computational work leads us to the following conjecture, for general G, g.

Conjecture 1 Suppose that there is a (G, g, δ, γ)-configuration, and $\gamma > 0$. Then there is a $(G, g, \delta, \gamma - 1)$-configuration.

Another gap is for Type III groups with g satisfying $|g| = \frac{|G|}{4}$, where very few γ are understood. Lastly, many of our results produce configurations for all sufficiently large α (e.g. Corollaries 5, 7), leaving open the question of whether configurations exist for smaller α.

Acknowledgements This research was supported in part by NSF REU grant 1061366. The authors would like to gratefully acknowledge the assistance of an anonymous referee whose very helpful comments substantially improved this paper.

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. D. D. Anderson and Jonathan Preisser. Factorization in integral domains without identity. *Results Math.*, 55(3-4):249–264, 2009.
3. David F. Anderson. Elasticity of factorizations in integral domains: a survey. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 1–29. Dekker, New York, 1997.
4. Paul Baginski and Scott T. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory: Contributions from CANT 2011*. Springer, forthcoming.
5. 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.
6. 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.
7. 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.
8. M. Banister, J. Chaika, S. T. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math.*, 108(1):105–118, 2007.
9. 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.
10. M. Banister, J. Chaika, and W. Meyerson. Technical report, Trinity University REU, 2003.
11. S. T. Chapman and David Steinberg. On the elasticity of generalized arithmetical congruence monoids. *Results Math.*, 58(3-4):221–231, 2010.
12. Marco Fontana, Evan Houston, and Thomas Lucas. *Factoring ideals in integral domains*, volume 14 of *Lecture Notes of the Unione Matematica Italiana*. Springer, Heidelberg, 2013.
13. Alfred Geroldinger. Additive group theory and non-unique factorizations. In *Combinatorial number theory and additive group theory*, Adv. Courses Math. CRM Barcelona, pages 1–86. Birkhäuser Verlag, Basel, 2009.
14. Alfred Geroldinger and Franz Halter-Koch. Congruence monoids. *Acta Arith.*, 112(3):263–296, 2004.
15. 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.
16. Franz Halter-Koch. C-monoids and congruence monoids in Krull domains. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 71–98. Chapman & Hall/CRC, Boca Raton, FL, 2005.
17. G. H. Hardy. *Ramanujan: twelve lectures on subjects suggested by his life and work.* Chelsea Publishing Company, New York, 1959.
18. Thomas W. Hungerford. *Algebra.* Holt, Rinehart and Winston, Inc., New York, 1974.
19. Matthew Jenssen, Daniel Montealegre, and Vadim Ponomarenko. Irreducible Factorization Lengths and the Elasticity Problem within $\mathbb{N}$. *Amer. Math. Monthly*, 120(4):322–328, 2013.
20. Ivan Niven and Herbert S. Zuckerman. *An introduction to the theory of numbers.* John Wiley & Sons, New York-Chichester-Brisbane, fourth edition, 1980.