ON THE ACCEPTED ELASTICITY OF ARTITHMETIC CONGRUENCE MONOIDS

1. Preliminaries

1.1. **ACMs.** An *Arithmetic Congruence Monoid* (ACM) is a monoid of the form

$$M(a,b) := \{1\} \cup (a + b\mathbb{N}_0) = \{1, a, a+b, a+2b, a+3b, ...\}$$

where a, b are integers with $0 < a \leqslant b$ and $a^2 \equiv a \pmod{b}$. This last condition ensures that $M(a,b)$ is closed under multiplication, and hence is a monoid.

Let $r \in M(a,b)$. We say that r is *irreducible* if, whenever there are elements $s, t \in M(a,b)$ such that $r = st$, either $s = 1$ or $t = 1$. All elements of $M(a,b)$, other than 1, can be factored into irreducibles, but this factorization is not necessarily unique.

Given a factorization of r into irreducibles, we call the number of irreducibles in this factorization the *length* of the factorization. We define the *length set* of r to be

$$\mathfrak{L}(r) := \{n \in \mathbb{N} \mid \exists \text{ irreducibles } a_1, ..., a_n \in M(a,b) \text{ such that } r = (a_1)\cdots(a_n)\},$$

and the *elasticity* of r to be

$$\rho(r) := \frac{\max\mathfrak{L}(r)}{\min\mathfrak{L}(r)}.$$

The elasticity of the monoid is defined as

$$\rho(M(a,b)) = \sup\{\rho(r) \mid r \in M(a,b)\},$$

and we say that the elasticity of the monoid is *accepted* if there is some $r \in M(a,b)$ such that $\rho(r) = \rho(M(a,b))$.

This paper attempts to classify which ACMs have accepted elasticity and which do not. There are three mutually exclusive types of ACMs: regular, global, and local. An ACM is *regular* if $\gcd(a,b) = 1$. Regular ACMs always have accepted elasticity, by theorem 3.4 of [1] for details. An ACM is *global* if $\gcd(a,b)$ is not a power of a prime. Global ACMs have infinite elasticity, hence they do not have accepted elasticity. An ACM is *local* if $\gcd(a,b)$ is a power of a prime, other than 1. Some local ACMs have accepted elasticities while others do not. We narrow our focus to only consider local ACMs.

For the remainder of this paper, let p be a prime number, $\alpha \in \mathbb{N}$, and $x, y \in \mathbb{N}$ with $0 < x \leqslant y$, $\gcd(x,y) = 1$, and $(p^\alpha x)^2 \equiv p^\alpha x \pmod{p^\alpha y}$. Define $M := M(p^\alpha x, p^\alpha y)$. We will also define β to be the least positive integer such that $p^\beta \in M$ through the rest of the paper. Given p, α, x, and y, we wish to determine whether or not M has accepted elasticity.

1.2. **Multisets.** This paper uses the notion of a *multiset*, which is essentially a set which may contain (finitely many) multiple copies of the same element. Formally, it is a pairing (A, μ) of a set A and a map $\mu : A \to \mathbb{N}$, where the multiplicity of each element of A in the multiset is its image under μ. We say that (A, μ) is finite if A is finite. If $A = \{a_1, a_2, ...\}$, we can denote (A, μ) by $\left\{\!\!\left\{ a_1^{\mu(a_1)}, a_2^{\mu(a_2)}, ... \right\}\!\!\right\}$, or by

$$\left\{\!\!\left\{ \underbrace{a_1, ..., a_1}_{\mu(a_1) \text{ times}}, \underbrace{a_2, ..., a_2}_{\mu(a_2) \text{ times}}, ... \right\}\!\!\right\}.$$

We say that (A_1, μ_1) is a *submultiset* of (A_2, μ_2), and write $(A_1, \mu_1) \subset (A_2, \mu_2)$ if $A_1 \subset A_2$ and, for all $a \in A_1$, $\mu_1(a) \leqslant \mu_2(a)$. The union $(A_1, \mu_1) \cup (A_2, \mu_2)$ is defined as $(A_1 \cup A_2, \tau)$, where $\tau(a) = \mu_1(a)$ if $a \in A_1 - A_2$, $\tau(a) = \mu_2(a)$ if $a \in A_2 - A_1$, and $\tau(a) = \mu_1(a) + \mu_2(a)$ if $a \in A_1 \cap A_2$.

Let $S = \{\!\{g_1^{m_1}, ..., g_n^{m_n}\}\!\}$ be a finite multiset of elements in an additive (resp. multiplicative) group G. We let $\sum S$ (resp. $\prod S$) denote the sum $\sum_{i=1}^n m_i \cdot g_i$ (resp. the product $\prod_{i=1}^n g_i^{m_i}$) in G.

Notice that

$$\sum (\mathcal{A} \cup \mathcal{B}) = \sum \mathcal{A} + \sum \mathcal{B}$$

Definition 1.2.1. *Let $S = \{\!\{g_1^{m_1}, ..., g_n^{m_n}\}\!\}$ be a multiset of elements from an additive (resp. multiplicative) group G, and let $h \in G$. We say that h is an* internal sum *(resp.* internal product*) of S if $\exists$ a submultiset $R \subset S$ such that $\sum R = h$ (resp. $\prod R = h$).*

1.3. **Machinery.**

Definition 1.3.1. *Let G be a finite abelian group, $g \in G$, and $k \in \mathbb{Z}_{>0}$. Define $\beta(G, g, k)$ to be the least multiple of $\mathrm{ord}_G(g)$ that is at least k.*

Lemma 1.3.1. *$\beta = \beta(\mathbb{Z}_y^\times, [p], \alpha)$.*

Proof. We must show that $p^{\beta(\mathbb{Z}_y^\times, [p], \alpha)}$ is the least positive power of p contained in M. To see this, we will use the fact, from lemma 4.1 of [1], that $M = M(p^\alpha, p^\alpha) \cap M(1, y)$. Notice that, if m is a positive integer, then $p^m \in M(p^\alpha, p^\alpha) \iff m \geqslant \alpha$, and $p^m \in M(1, y) \iff \mathrm{ord}_y(p) \mid m$. Hence $p^m \in M$ iff $m \geqslant \alpha$ and $\mathrm{ord}_y(p) \mid m$. Since $\beta(\mathbb{Z}_y^\times, [p], \alpha)$ is the least multiple of $\mathrm{ord}_y(p)$ that is at least α, $p^{\beta(\mathbb{Z}_y^\times, [p], \alpha)}$ is the least positive power of p contained in M. Thus $\beta = \beta(\mathbb{Z}_y^\times, [p], \alpha)$. □

Definition 1.3.2. *Let G be a finite abelian group, $g \in G$, and $k \in \mathbb{Z}_{>0}$. We say that the triple (G, g, k) is* accepted *if there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of G such that*

(1) $\bigcup_{i=1}^e \mathcal{A}_i = \bigcup_{i=1}^f \mathcal{B}_i$
(2) for $j = 1, ..., e$, $\mathcal{A}_j$ has no internal product in $\left\{g, g^2, ..., g^{\beta(G,g,k)-k}\right\}$
(3) for $j = 1, ..., e$, $\prod \mathcal{A}_j = g^{1-k}$
(4) for $j = 1, ..., f$, $\prod \mathcal{B}_j = g^{-k}$, and
(5) $\frac{f}{e} = \frac{k+\beta(G,g,k)-1}{k}$.

Otherwise, we say that (G,g,k) is not accepted.

From lemma 4.1 of [1], we know that $p \nmid y$. Therefore, using square brackets to denote equivalence classes modulo y, we have that $[p] \in \mathbb{Z}_y^\times$. We can now state the theorem that gives meaning to the above definition:

Theorem 1.3.1 (Equivalence Theorem)**.** *M has accepted elasticity iff $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted.*

Proof. Let r be an irreducible in M. We claim that $\alpha \leqslant v_p(r) \leqslant \alpha + \beta - 1$. Since $r \in M(p^\alpha, p^\alpha)$, $\alpha \leqslant v_p(r)$, proving the first inequality. To prove the second inequality, assume that $v_p(r) \geqslant \alpha + \beta$, and let $r = p^{\alpha+\beta}q$ for some integer q. Then $p^\beta \equiv p^{\alpha+\beta}q \equiv 1 \pmod{y}$ since $p^\beta, p^{\alpha+\beta}q \in M$. Hence $p^\alpha q \equiv 1 \pmod{y}$, and thus $p^\alpha q \in M$. But then $r = (p^\beta)(p^\alpha q)$, contradicting the irreducibility of r. Therefore, $\alpha \leqslant v_p(r) \leqslant \alpha + \beta - 1$. Define an *A-atom* to be an irreducible in M with a p-adic valuation of $\alpha + \beta - 1$, and define a *B-atom* to be an irreducible in M with a p-adic valuation of α.

Now, let s be an element of M. Since each irreducible factor of s has p-adic valuation of at least α, there are at most $\lfloor v_p(s)/\alpha \rfloor$ irreducibles in a factorization of s. And since each irreducible factor of s can have p-adic valuation of at most $\alpha + \beta - 1$, there are at least $\lceil v_p(s)/(\alpha + \beta - 1) \rceil$ irreducibles in a factorization of s. Thus

$$\mathfrak{L}(s) \subseteq \left\{ m \,\middle|\, \left\lceil \frac{v_p(s)}{\alpha + \beta - 1} \right\rceil \leqslant m \leqslant \left\lfloor \frac{v_p(s)}{\alpha} \right\rfloor \right\}.$$

and

$$\rho(s) \leqslant \frac{\left\lfloor \frac{v_p(s)}{\alpha} \right\rfloor}{\left\lceil \frac{v_p(s)}{\alpha+\beta-1} \right\rceil} \leqslant \frac{\frac{v_p(s)}{\alpha}}{\frac{v_p(s)}{\alpha+\beta-1}} = \frac{\alpha + \beta - 1}{\alpha}.$$

For the first inequality, equality holds iff there are factorizations of lengths $\lfloor v_p(s)/\alpha \rfloor$ and $\lceil v_p(s)/(\alpha + \beta - 1) \rceil$. For the second inequality, equality holds iff $v_p(s)/\alpha$ and $v_p(s)/(\alpha + \beta - 1)$ are integers. Thus overall equality holds if there are factorizations of lengths $v_p(s)/\alpha$ and $v_p(s)/(\alpha+\beta-1)$. The former occurs iff there is a factorization of s into all B-atoms and the latter iff there is a factorization of s into all A-atoms. Thus $\rho(s) = (\alpha+\beta-1)/\alpha$ iff s has a factorization into all A-atoms and a factorization into all B-atoms.

From Theorem 2.4 of [2], we know that $\rho(M) = (\alpha + \beta - 1)/\alpha$. Therefore, M has accepted elasticity iff there exists $s \in M$ such that s has a factorization into all A-atoms and all B-atoms.

Hence, the statement of this theorem is equivalent to the following: M contains an element which has a factorization into all A-atoms and a factorization into all B-atoms iff there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_y^\times$ such that

(1a) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2a) for $j = 1, ..., e$, $\mathcal{A}_j$ has no internal product in $\{[p], [p]^2, ..., [p]^{\beta-\alpha}\}$
(3a) for $j = 1, ..., e$, $\prod \mathcal{A}_j = [p]^{1-\alpha}$
(4a) for $j = 1, ..., f$, $\prod \mathcal{B}_j = [p]^{-\alpha}$, and
(5a) $f/e = (\alpha + \beta - 1)/\alpha$.

We will prove this equivalent statement:

($\Rightarrow$) Assume that $\exists s \in M$ such that s has a factorization $s = (A_1) \cdots (A_e)$ into A-atoms and $s = (B_1) \cdots (B_f)$ into B-atoms. For each i=1,...,e, let A_i have the prime factorization A_i=$p^{\alpha+\beta-1}(q_1^{(i)}) \cdots (q_{m_i}^{(i)})$ over the natural numbers. Since each A_i is a unit mod y, so is each $q_j^{(i)}$, so let $[a_j^{(i)}]$ denote the class of $q_j^{(i)}$ in $\mathbb{Z}_y^\times$ for all $i \in \{1, ..., e\}$ and $j \in \{1, ..., m_i\}$. Define the multisets $\mathcal{A}_i = \left\{\!\!\left\{ [a_1^{(i)}], ..., [a_{m_i}^{(i)}] \right\}\!\!\right\}$ for

$i = 1, ..., e$. Similarly, define the multisets $\mathcal{B}_i = \left\{\!\!\left\{ [b_1^{(i)}], ..., [b_{n_i}^{(i)}] \right\}\!\!\right\}$ where $[b_j^{(i)}]$ is the equivalence class of $r_j^{(i)}$ in $\mathbb{Z}_y^\times$ and $B_i = p^\alpha (r_1^{(i)}) \cdots (r_{n_i}^{(i)})$ is the prime factorization of B_i over the natural numbers. We will show that these integers and multisets satisfy conditions (1a)-(5a).

From the fundamental theorem of number theory, we know that s has a unique prime factorization over the natural numbers, hence the two prime factorizations

$$(A_1) \cdots (A_e) = p^{e(\alpha+\beta-1)} \prod_{i=1}^{e} \prod_{j=1}^{m_i} q_j^{(i)}$$

and

$$(B_1) \cdots (B_f) = p^{f\alpha} \prod_{i=1}^{f} \prod_{j=1}^{n_i} r_j^{(i)}$$

are the same. Each prime factorization has the same number of p's, hence $e(\alpha + \beta - 1) = f\alpha$, so condition (5a) holds. Furthermore, each prime factorization has the same primes when excluding p's, thus

$$\begin{aligned} \bigcup_{i=1}^{e} \bigcup_{j=1}^{m_i} \left\{\!\!\left\{ q_j^{(i)} \right\}\!\!\right\} &= \bigcup_{i=1}^{f} \bigcup_{j=1}^{n_i} \left\{\!\!\left\{ r_j^{(i)} \right\}\!\!\right\} \implies \\ \bigcup_{i=1}^{e} \bigcup_{j=1}^{m_i} \left\{\!\!\left\{ [a_j^{(i)}] \right\}\!\!\right\} &= \bigcup_{i=1}^{f} \bigcup_{j=1}^{n_i} \left\{\!\!\left\{ [b_j^{(i)}] \right\}\!\!\right\} \implies \\ \bigcup_{i=1}^{e} \mathcal{A}_i &= \bigcup_{i=1}^{f} \mathcal{B}_i, \end{aligned}$$

so condition (1a) holds.

Notice that, for $i = 1, ..., e$,

$$\begin{aligned} \prod \mathcal{A}_i &= \prod_{j=1}^{m_i} [a_j^{(i)}] \\ &= \left[\prod_{j=1}^{m_i} q_j^{(i)} \right] \\ &= [A_i]/[p^{\alpha+\beta-1}] \\ &= [p]^{1-\alpha} \end{aligned}$$

since $A_i \equiv p^\beta \equiv 1 \pmod{y}$. Therefore, condition (3a) holds. A similar argument proves condition (4a).

We will show that condition (2a) holds by contradiction. Assume that for some $j \in \{1, ..., e\}$, $\exists \mathcal{S} \subset \mathcal{A}_i$ such that $\prod \mathcal{S} \in \{[p], [p]^2, ..., [p]^{\beta-\alpha}\}$. Say $\mathcal{S} = \left\{\!\!\left\{ [a_{j_1}^{(i)}], ..., [a_{j_z}^{(i)}] \right\}\!\!\right\}$, and $\prod \mathcal{S} = [p]^\gamma$ for some $\gamma \in \{1, ..., \beta - \alpha\}$. Let $g = q_{j_1}^{(i)} \cdots q_{j_z}^{(i)}$ and $h = (q_1^{(i)} \cdots q_{m_i}^{(i)})/g$. Then $[g] = [p]^\gamma$. Furthermore, $A_i = p^{\alpha+\beta-1} gh = (p^{\beta-\gamma} g)(p^{\gamma+\alpha-1} h)$. Since $1 \leqslant \gamma \leqslant \beta - \alpha$, we know that $v_p(p^{\beta-\gamma} g) = \beta - \gamma \geqslant \alpha$ and $v_p(p^{\gamma+\alpha-1} h) = \gamma + \alpha - 1 \geqslant \alpha$. We also know that $[p^{\beta-\gamma} g] = [p]^{\beta-\gamma}[p]^\gamma = [p^\beta] = [1]$, and $[p^{\gamma+\alpha-1} h] = [A_i]/[p^{\beta-\gamma} g] = [1]$. Therefore, $A_i = (p^{\beta-\gamma} g)(p^{\gamma+\alpha-1} h)$ is a factorization in M, contradicting the irreducibility of A_i. Hence condition (2a) holds.

($\Leftarrow$) Now assume that there are integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_y^\times$ which satisfy conditions (1a)-(5a). Let

$$\mathcal{A}_i = \left\{\!\!\left\{ [a_1^{(i)}], ..., [a_{m_i}^{(i)}] \right\}\!\!\right\}$$

for i=1,...,e and

$$\mathcal{B}_i = \left\{\!\!\left\{ [b_1^{(i)}], ..., [b_{n_i}^{(i)}] \right\}\!\!\right\}$$

for i=1,...,f. Define $q_j^{(i)}, r_j^{(i)}$ to be the *least* prime natural number belonging to the equivalence classes $[a_j^{(i)}], [b_j^{(i)}]$, respectively. Notice that these primes necessarily exist by Dirichlet's theorem. Define $A_i = p^{\alpha+\beta-1} q_1^{(i)} \cdots q_{m_i}^{(i)}$ for $i = 1, ..., e$ and $B_i = p^\alpha r_1^{(i)} \cdots r_{n_i}^{(i)}$ for $i = 1, ..., f$.

Notice that, for $i = 1, ..., e$,

$$\begin{aligned} [A_i] &= [p^{\alpha+\beta-1} q_1^{(i)} \cdots q_{m_i}^{(i)}] \\ &= [p]^{\alpha-1} [a_1^{(i)}] \cdots [a_{m_i}^{(i)}] \\ &= [p]^{\alpha-1} \prod \mathcal{A}_i = [1], \end{aligned}$$

so $A_i \equiv 1 \pmod{y}$. By a similar argument, $B_i \equiv 1 \pmod{y}$ for $i = 1, ..., f$. Furthermore, since each A_i and each B_i has a p-adic valuation of at least α, they are elements of M. Furthermore, conditions (1a) and (5a) together ensure that $A_1 \cdots A_e = B_1 \cdots B_f$. Call this product s. It suffices to show that each A_i and each B_i is irreducible, for then $s \in M$ would have a factorization into all A-atoms and a factorization into all B-atoms.

Since any element of M with p-adic valuation less than 2α is irreducible, each B_i is irreducible. Assume that there is some $k \in \{1, ..., e\}$ such that A_k is reducible, and say that $A_k = (p^\gamma g)(p^{\alpha+\beta-\gamma-1} h)$ is a factorization in M. Pick a set of indices $\{i_1, ..., i_z\} \subset \{1, ..., m_k\}$ such that $g = q_{i_1}^{(k)} \cdots q_{i_z}^{(k)}$, and let $\mathcal{S} = \left\{\!\!\left\{ [a_{i_1}^{(k)}], ..., [a_{i_z}^{(k)}] \right\}\!\!\right\}$. Then $\prod \mathcal{S} = [a_{i_1}^{(k)}] \cdots [a_{i_z}^{(k)}] = [q_{i_1}^{(k)} \cdots q_{i_z}^{(k)}] = [p^{-\gamma}]$ since $[A_k] = [1]$. Because the two factors are in M, $\gamma \geqslant \alpha$ and $\alpha + \beta - \gamma - 1 \geqslant \alpha$, yielding $\alpha \leqslant \gamma \leqslant \beta - 1$. Therefore $\prod \mathcal{S} = [p^{-\gamma}] \in \{[p], [p]^2, ..., [p]^{\beta-\alpha}\}$, contradicting condition (2a). Therefore each A_i is irreducible. Hence $s \in M$ has a factorization into all A-atoms and a factorization into all B-atoms, completing the proof. □

Theorem 1.3.2 (Isomorphism Theorem)**.** *Suppose $\psi : G \to H$ is an isomorphism of finite abelian groups. Then (G, g, k) is accepted iff $(H, \psi(g), k)$ is accepted.*

Proof. Suppose (G, g, k) is accepted. Then there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements in G which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $\mathcal{A}_i'$ be the image of $\mathcal{A}_i$ under ψ for $i = 1, ..., e$ and $\mathcal{B}_i'$ the image of $\mathcal{B}_i$ under ψ for $i = 1, ..., f$. We wish to show that the integers e, f and multisets $\mathcal{A}_1', ..., \mathcal{A}_e', \mathcal{B}_1', ..., \mathcal{B}_f'$ satisfy

(1′) $\bigcup_{i=1}^e \mathcal{A}_i' = \bigcup_{i=1}^f \mathcal{B}_i'$
(2′) for $j = 1, ..., e$, $\mathcal{A}_j'$ has no internal product in $\left\{\psi(g), \psi(g)^2, ..., \psi(g)^{\beta(H,\psi(g),k)-k}\right\}$
(3′) for $j = 1, ..., e$, $\prod \mathcal{A}_j' = \psi(g)^{1-k}$
(4′) for $j = 1, ..., f$, $\prod \mathcal{B}_j' = \psi(g)^{-k}$, and
(5′) $f/e = (k + \beta(H, \psi(g), k) - 1)/k$.

Since $\text{ord}_H(\psi(g)) = \text{ord}_G(g)$, we have $\beta(H, \psi(g), k) = \beta(G, g, k)$. Hence condition $(5')$ holds. Conditions $(2')$, $(3')$, and $(4')$ also hold because isomorphisms preserve the group operation. Finally, because $\bigcup \mathcal{A}'_i$ and $\bigcup \mathcal{B}'_i$ are images of $\bigcup \mathcal{A}_i$ and $\bigcup \mathcal{B}_i$, respectively, under ψ (since we are looking at the union of multisets, not just sets), condition $(1')$ holds as well. Therefore, $(H, \psi(g), k)$ is accepted.

Now, suppose $(H, \psi(g), k)$ is accepted. Because $\psi^{-1} : H \to G$ is an isomorphism, we can apply the argument in the preceeding paragraph to see that if $(H, \psi(g), k)$ is accepted, then (G, g, k) is accepted. Thus (G, g, k) is accepted iff $(H, \psi(g), k)$ is accepted. □

Theorem 1.3.3 (Reduction Theorem). *Suppose G is a finite abelian group and H is a subgroup, with $h \in H$. If (H, h, k) is accepted, then (G, h, k) is accepted.*

Proof. Suppose (H, h, k) is accepted, and let positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e$, $\mathcal{B}_1, ..., \mathcal{B}_f$ of elements of H satisfy conditions (1)-(5). Because $\text{ord}_H(h)$ $= \text{ord}_G(h)$, it is clear that the integers e, f and the multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$, when viewed as multisets of elements of G, still satisfy conditions (1)-(5). Thus (G, h, k) is accepted. □

Definition 1.3.3. *Let G be a finite abelian group, $g \in G$, and $k \in \mathbb{N}$. We say that (G,g,k) is* overaccepted *if there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of G which satisfy conditions (1)-(4) from the definition of an accepted triple, but also satisfy*

$(\overline{5})$ $\frac{f}{e} \geqslant \frac{k+\beta(G,g,k)-1}{k}$

Theorem 1.3.4. *(G, g, k) is overaccepted if and only if (G, g, k) is accepted.*

Proof. The if statement is trivial, so we begin proving the only if statement. Suppose (G, g, k) is overaccepted. Then there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of G which satisfy conditions (1)-(4) and $(\overline{5})$.

Define ek multisets $\mathcal{A}_{i,j}$ for $i = 1, ..., e$ and $j = 1, ..., k$, so that $\mathcal{A}_{i,j}$=$\mathcal{A}_i$. Define fk multisets $\mathcal{B}_{i,j}$ for $i = 1, ..., f$ and $j = 1, ..., k$ so that $\mathcal{B}_{i,j} = \mathcal{B}_i$. Define fk multisets $\mathcal{S}_i$ for $i = 1, ..., fk$ so that $\mathcal{S}_{(j-1)k+k} = \mathcal{B}_{j,k}$ for $j = 1, ..., f$ and $k = 1, ..., k$ (that is, the multisets $\mathcal{S}_i$ are just a way of ordering the multisets $\mathcal{B}_{i,j}$ in one list). Since $f/e \geqslant (k + \beta(G, g, k) - 1)/k$, we have $fk \geqslant e(k + \beta(G, g, k) - 1)$. So we can define $e(k + \beta(G, g, k) - 1)$ multisets $\mathcal{B}'_1, ..., \mathcal{B}'_{e(k+\beta(G,g,k)-1)}$ so that $\mathcal{B}'_i = \mathcal{S}_i$ for $i = 1, ..., e(k + \beta(G, g, k) - 1) - 1$, and

$$\mathcal{B}'_{e(k+\beta(G,g,k)-1)} := \bigcup_{i=e(k+\beta(G,g,k)-1)}^{fk} \mathcal{S}_i.$$

We wish to show that conditions (1)-(5) hold for the positive integers ek and $e(k + \beta(G, g, k) - 1)$ and the multisets $\mathcal{A}_{i,j}$ and $\mathcal{B}'_i$.

Notice that

$$\begin{aligned}
\bigcup_{i=1}^{e(k+\beta(G,g,k)-1)} \mathcal{B}'_i &= \left(\bigcup_{i=1}^{e(k+\beta(G,g,k)-1)-1} \mathcal{B}'_i\right) \cup \mathcal{B}'_{e(k+\beta(G,g,k)-1)} \\
&= \left(\bigcup_{i=1}^{e(k+\beta(G,g,k)-1)-1} \mathcal{S}_i\right) \cup \left(\bigcup_{i=e(k+\beta(G,g,k)-1)}^{fk} \mathcal{S}_i\right) \\
&= \bigcup_{i=1}^{fk} \mathcal{S}_i = \bigcup_{j=1}^{k}\bigcup_{i=1}^{f} \mathcal{B}_{i,j} = \bigcup_{j=1}^{k}\bigcup_{i=1}^{e} \mathcal{A}_{i,j},
\end{aligned}$$

hence condition (1) holds.

Conditions (2) and (3) follow directly from the fact that $\mathcal{A}_{i,j} = \mathcal{A}_i$. For $i = 1, ..., e(k+\beta(G,g,k)-1)-1$, $\mathcal{B}'_i = \mathcal{S}_i$ is equal to $\mathcal{B}_k$ for some $k = 1, ..., f$, and hence $\prod \mathcal{B}'_i = g^{-k}$. Now we must consider $\mathcal{B}'_{e(k+\beta(G,g,k)-1)}$.

$$\begin{aligned}
\prod \mathcal{B}'_{e(k+\beta(G,g,k)-1)} &= \frac{\prod_{i=1}^{e(k+\beta(G,g,k)-1)} \left(\prod \mathcal{B}'_i\right)}{\prod_{i=1}^{e(k+\beta(G,g,k)-1)-1} \left(\prod \mathcal{B}'_i\right)} \\
&= \frac{\prod \left(\bigcup_{i=1}^{e(k+\beta(G,g,k)-1)} \mathcal{B}'_i\right)}{\left(g^{-k}\right)^{e(k+\beta(G,g,k)-1)-1}} \\
&= \frac{\prod \left(\bigcup_{j=1}^{k}\bigcup_{i=1}^{e} \mathcal{A}_{i,j}\right)}{g^{-ek^2+ek+k}} \text{ (recall } g^{\beta(G,g,k)} = 1 \text{)} \\
&= \frac{\prod_{j=1}^{k}\prod_{i=1}^{e} \left(\prod \mathcal{A}_{i,j}\right)}{g^{-ek^2+ek+k}} \\
&= \frac{\left(g^{1-k}\right)^{ek}}{g^{-ek^2+ek+k}} \\
&= g^{-k},
\end{aligned}$$

hence condition (4) holds. Condition (5) holds trivially, concluding the proof. □

Throughout the paper, we will also come across the following definition:

Definition 1.3.4. *Fix a finite abelian group G and an element $g \in G$. If there exists n such that for all $n' \geqslant n$, (G, g, n') is accepted, then define $\omega(G, g)$ to be the minimum such positive n. Otherwise, define $\omega(G, g) = \infty$. Given an ACM M, define $\omega(M) := \omega(\mathbb{Z}_y^\times, [p])$.*

2. General

2.1. Case $x = 1$.

Lemma 2.1.1. *If $ord_G(g) \mid k$ then (G, g, k) is accepted.*

Proof. Suppose $\mathrm{ord}_G(g) \mid k$. Then $g^k = 1_G$ and $\beta(G, g, k) = k$. So it suffices to find k multisets $\mathcal{A}_1, ..., \mathcal{A}_k$ and $2k-1$ multisets $\mathcal{B}_1, ..., \mathcal{B}_{2k-1}$ such that

(1b) $\bigcup_{i=1}^{k} \mathcal{A}_i = \bigcup_{i=1}^{2k-1} \mathcal{B}_i$
(2b) for $i = 1, ..., k, \prod \mathcal{A}_i = g$, and
(3b) for $i = 1, ..., 2k-1, \prod \mathcal{B}_i = 1_G$.

(Notice that condition (2) from the definition of an accepted triple vanishes because the set $\{g, g^2, ..., g^{\beta(G,g,k)-k}\}$ is empty when $\beta(G,g,k) = k$, and condition (5) is trivially true.)

Let $\mathcal{A}_1 = ... = \mathcal{A}_k = \{\!\{g\}\!\}$, let $\mathcal{B}_1 = \{\!\{g^k\}\!\}$, and let $\mathcal{B}_2 = ... = \mathcal{B}_{2k-1} = \varnothing$. Then one can easily see that these satisfy conditions (1b)-(3b), completing the proof. □

Theorem 2.1.1. *Let β be the least positive integer such that $p^\beta \in M$. The following are equivalent:*

(i) $x = 1$
(ii) $\alpha = \beta$
(iii) $p^\alpha \equiv 1 \pmod{y}$
(iv) $\rho(M) < 2$

Furthermore, if (i) - (iv) are true, then M has accepted elasticity.

Proof. (i $\Longrightarrow$ ii) If $x = 1$, then p^α is the least element of M other than 1. Hence $\beta = \alpha$.

(ii $\Longrightarrow$ iii) If $\alpha = \beta$, then $p^\alpha \in M$, hence $p^\alpha \equiv 1 \pmod{y}$.

(iii $\Longrightarrow$ i) Assume $p^\alpha \equiv 1 \pmod{y}$. We also know that $p^\alpha x \in M$, hence $p^\alpha x \equiv 1 \pmod{y}$. Since gcd($p^\alpha x, y$)=1, we have $x \equiv 1 \pmod{y}$. Since $0 < x \leqslant y$, we have $x = 1$.

(ii $\Longleftrightarrow$ iv) From theorem 2.4 of [2], we know that $\rho(M) = (\alpha + \beta - 1)/\alpha$. Since p^α divides all elements of M, $p^\alpha \mid p^\beta$, hence $\alpha \leqslant \beta$. Thus $\rho(M) < 2 \iff \alpha = \beta$.

Thus statements (i)-(iv) are equivalent.

Now, assume that (i)-(iv) are true. Then, from lemma 2.1.1 combined with the equivalence theorem, M has accepted elasticity. □

2.2. **Varying α.**

Theorem 2.2.1. *If (G, g, k) is accepted, then $(G, g, k + m\,ord_G(g))$ is accepted for any positive integer m.*

Proof. From lemma 2.1.1, the theorem holds if $k \mid \mathrm{ord}_G(g)$. So assume otherwise. Suppose (G, g, k) is accepted. Then there exists integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of G satisfying conditions (1)-(5) from the definition of an accepted triple.

We claim that $(G, g, k{+}m\ \mathrm{ord}_G(g))$ is overaccepted, and that the positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ satisfy the conditions for over acceptance:

(1″) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2″) for $j = 1, ..., e$, $\mathcal{A}_j$ has no internal product in $\left\{g, g^2, ..., g^{\beta(G,g,k+m\,\mathrm{ord}_G(g))-(k+m\,\mathrm{ord}_G(g))}\right\}$
(3″) for $j = 1, ..., e$, $\prod \mathcal{A}_j = g^{1-(k+m\,\mathrm{ord}_G(g))}$
(4″) for $j = 1, ..., f$, $\prod \mathcal{B}_j = g^{-(k+m\,\mathrm{ord}_G(g))}$, and
(5″) $\frac{f}{e} \geqslant \frac{(k+m\,\mathrm{ord}_G(g))+\beta(G,g,k+m\,\mathrm{ord}_G(g))-1}{(k+m\,\mathrm{ord}_G(g))}$.

Suppose that $\beta(G, g, k) = r\ \mathrm{ord}_G(g) \neq k$. Then $(r - 1)\ \mathrm{ord}_G(g) < k < r\ \mathrm{ord}_G(g) \Longrightarrow$

$$(r + m - 1)\,\mathrm{ord}_G(g) < k + m\,\mathrm{ord}_G(g) < (r + m)\,\mathrm{ord}_G(g),$$

so $\beta(G, g, k + m\ \mathrm{ord}_G(g)) = (r + m)\ \mathrm{ord}_G(g)$. Thus

$$\beta(G, g, k) - k = r\,\mathrm{ord}_G(g) - k = \beta(G, g, k + m\,\mathrm{ord}_G(g)) - (k + m\,\mathrm{ord}_G(g)).$$

Hence condition $(2'')$ follows immediately from the acceptance of (G, g, k).

It is also clear that $(1'')$,$(3'')$, and $(4'')$ also follow directly from the acceptance of (G, g, k). To see that $(5'')$ holds, notice that

$$\begin{aligned}
\frac{k+\beta(G,g,k)-1}{k} &\geqslant \frac{(k+m\operatorname{ord}_G(g))+\beta(G,g,k+m\operatorname{ord}_G(g))-1}{k+m\operatorname{ord}_G(g)} \iff \\
\frac{k+r\operatorname{ord}_G(g)-1}{k} &\geqslant \frac{(k+m\operatorname{ord}_G(g))+(r+m)\operatorname{ord}_G(g)-1}{k+m\operatorname{ord}_G(g)} \iff \\
\frac{r\operatorname{ord}_G(g)-1}{k} &\geqslant \frac{(r+m)\operatorname{ord}_G(g)-1}{k+m\operatorname{ord}_G(g)} \iff \\
(r\operatorname{ord}_G(g)-1)(k+m\operatorname{ord}_G(g)) &\geqslant ((r+m)\operatorname{ord}_G(g)-1)k \iff \\
(r\operatorname{ord}_G(g)-1)m\operatorname{ord}_G(g) &\geqslant m\operatorname{ord}_G(g)k \iff \\
r\operatorname{ord}_G(g)-1 &\geqslant k,
\end{aligned}$$

which is true because $r\operatorname{ord}_G(g) > k$ and both sides are integers. □

Theorem 2.2.2. *If $(G, g, 1)$ is accepted, then (G, g, k) is accepted for any positive integer k.*

Proof. Suppose $(G, g, 1)$ is accepted. Then, by definition, $\exists e, f \in \mathbb{N}$ and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of G such that

(1c) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2c) for $j = 1, ..., e$, $\mathcal{A}_j$ has no internal product in $\{g, g^2, ..., g^{\operatorname{ord}_G(g)-1}\}$
(3c) for $j = 1, ..., e$, $\prod \mathcal{A}_j = 1_G$ (the identity)
(4c) for $j = 1, ..., f$, $\prod \mathcal{B}_j = g^{-1}$, and
(5c) $f/e = \operatorname{ord}_G(g)$,

since $\beta(G, g, 1) = \operatorname{ord}_G(g)$.

By theorem 2.2.1, it suffices to only consider $1 \leqslant k \leqslant \operatorname{ord}_G(g)$. Then $\beta(G, g, k) = \operatorname{ord}_G(g)$. For $i = 1, ..., e$, $j = 1, ..., k$, define $\mathcal{A}_{i,j} = \mathcal{A}_i \cup \{\!\{(g^{-1})^{(k-1)}\}\!\}$ (that is, the single element g^{-1} with multiplicity $k-1$). For $i = 1, ..., f$, define $\mathcal{B}'_i = \bigcup_{j=1}^{k} \mathcal{B}_i$ (the union of k copies of $\mathcal{B}_i$), and for $i = f+1, ..., f+e(k-1)$, define $\mathcal{B}'_i = \{\!\{(g^{-1})^{(k)}\}\!\}$. Then it suffices to show that

(1d) $\bigcup_{i=1}^{e} \bigcup_{j=1}^{k} \mathcal{A}_{i,j} = \bigcup_{i=1}^{f+e(k-1)} \mathcal{B}'_i$
(2d) for $i = 1, ..., e$, $j = 1, ..., k$, $\mathcal{A}_{i,j}$ has no internal product in $\left\{g, g^2, ..., g^{\operatorname{ord}_G(g)-k}\right\}$
(3d) for $i = 1, ..., e$, $j = 1, ..., k$, $\prod \mathcal{A}_{i,j} = g^{1-k}$
(4d) for $i = 1, ..., f+e(k-1)$, $\prod \mathcal{B}'_i = g^{-k}$, and
(5d) $(f + e(k-1))/(ek) = (k + \operatorname{ord}_G(g) - 1)/k$.

Observe that

$$\begin{aligned}
\bigcup_{i=1}^{e}\bigcup_{j=1}^{k}\mathcal{A}_{i,j} &= \bigcup_{i=1}^{e}\bigcup_{j=1}^{k}\left(\mathcal{A}_i \cup \{\!\!\{(g^{-1})^{(k-1)}\}\!\!\}\right)\\
&= \left(\bigcup_{j=1}^{k}\bigcup_{i=1}^{e}\mathcal{A}_i\right)\cup\{\!\!\{(g^{-1})^{(ek(k-1))}\}\!\!\}\\
&= \left(\bigcup_{j=1}^{k}\bigcup_{i=1}^{f}\mathcal{B}_i\right)\cup\left(\bigcup_{k=1}^{e(k-1)}\{\!\!\{(g^{-1})^{(k)}\}\!\!\}\right) \text{ (by (1c))}\\
&= \left(\bigcup_{i=1}^{f}\mathcal{B}'_i\right)\cup\left(\bigcup_{i=f+1}^{f+e(k-1)}\mathcal{B}'_i\right)\\
&= \bigcup_{i=1}^{f+e(k-1)}\mathcal{B}'_i,
\end{aligned}$$

hence condition (1d) holds.

Next, we will show that (2d) holds by contradiction. Assume that (2d) does not hold. Then for some $i \in \{1, ..., e\}$ and $j \in \{1, ...k\}$, there exists $\mathcal{S} \subset \mathcal{A}_{i,j}$ such that $\prod \mathcal{S} \in \{g, g^2, ..., g^{\mathrm{ord}_G(g)-k}\}$. So let $\prod \mathcal{S} = g^{\delta}$ for $\delta \in \{1, ..., \mathrm{ord}_G(g) - k\}$. Since $\mathcal{A}_{i,j} = \mathcal{A}_i \cup \{\!\!\{(g^{-1})^{(k-1)}\}\!\!\}$, we can write $\mathcal{S} = \mathcal{S}' \cup \{\!\!\{(g^{-1})^{(\gamma)}\}\!\!\}$ for some $\mathcal{S}' \subset \mathcal{A}_i$ and some $\gamma \in \{0, ..., k-1\}$. Since $\prod \mathcal{S} = \prod \mathcal{S}' \prod \{\!\!\{(g^{-1})^{(\gamma)}\}\!\!\}$, we have

$$\begin{aligned}
\prod \mathcal{S}' &= \prod \mathcal{S}\left(\prod \{\!\!\{(g^{-1})^{(\gamma)}\}\!\!\}\right)^{-1}\\
&= \left(g^{\delta}\right)\left(g^{\gamma}\right)\\
&= g^{\gamma+\delta}.
\end{aligned}$$

However, since $1 \leqslant \gamma + \delta \leqslant \mathrm{ord}_G(g) - 1$, this contradicts condition (2c). Therefore condition (2d) holds.

To see that condition (3d) holds, notice that

$$\begin{aligned}
\prod \mathcal{A}_{i,j} &= \prod \left(\mathcal{A}_i \cup \{\!\!\{(g^{-1})^{(k-1)}\}\!\!\}\right)\\
&= \prod \mathcal{A}_i \prod \{\!\!\{(g^{-1})^{(k-1)}\}\!\!\}\\
&= g^{1-k}
\end{aligned}$$

by (3c).

To see that condition (4d) holds, notice that for $i = 1, ..., f$,

$$\begin{aligned}
\prod \mathcal{B}'_i &= \prod \left(\bigcup_{j=1}^{k}\mathcal{B}_i\right)\\
&= \prod_{j=1}^{k}\left(\prod \mathcal{B}_i\right)\\
&= \left(g^{-1}\right)^{k} = g^{-k}
\end{aligned}$$

by (4c), and, for $i = f+1, ..., f+e(k-1)$,

$$\prod \mathcal{B}'_i = \prod \left(\{\!\!\{(g^{-1})^{(k)}\}\!\!\}\right) = g^{-k}.$$

Finally, notice that $(f + e(k-1))/(ek) = (e \operatorname{ord}_G(g) + e(k-1))/(ek) = (k + \operatorname{ord}_G(g) - 1)/k$. Hence condition (5d) holds, completing the proof. □

3. Cyclic Unit Group

3.1. **Case $d < c$.** In this section, we will assume $\mathbb{Z}_y^\times$ is cyclic. Define $d := \operatorname{ord}_y(p)$ and $c := \phi(y)/d$. We will also define $\overline{\alpha}$ to be the residue of α modulo d contained in $\{1, 2, ..., d\}$.

Theorem 3.1.1. *M has accepted elasticity iff $(\mathbb{Z}_{cd}, \langle c \rangle, \alpha)$ is accepted.*

Proof. From the equivalence theorem, we know that M has accepted elasticity iff $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted. Then, from the isomorphism theorem, it suffices to show that there exists an isomorphism $\psi : \mathbb{Z}_y^\times \to \mathbb{Z}_{cd}$ such that $\psi([p]) = \langle c \rangle$.

Let $[g]$ be a generator of $\mathbb{Z}_y^\times$, and let $[p] = [g]^k$. The order of $[g]$ modulo y is $\phi(y) = cd$, and the order of $[p]$ modulo y is d. Then $[g]^{kd} = [p]^d = [1] \implies cd \mid kd \implies c \mid k$. So let $k = cm$. Let $b = \gcd(m, d)$. Then $[p]^{d/b} = [g]^{cdm/b} = [1] \implies d \mid d/b \implies b = \gcd(m, d) = 1$. Let the prime factorization of c be $p_1^{e_1} \cdots p_s^{e_s} q_1^{f_1} \cdots q_t^{f_t}$, where each p_i divides d and each q_i does not divide d. Let $c_1 = p_1^{e_1} \cdots p_s^{e_s}$ and let $c_2 = q_1^{f_1} \cdots q_t^{f_t}$. Then $c = c_1 c_2$ and $\gcd(c_1, m) = \gcd(c_2, d) = 1$. Choose n such that $nd \equiv 1 - m \pmod{c_2}$. Let $[h] = [g]^{m+nd}$. Then $\gcd(m+nd, d) = \gcd(m, d) = 1$. This also tells us that $\gcd(m+nd, c_1)=1$. Furthermore, $m+nd \equiv 1 \pmod{c_2}$, so $\gcd(m+nd, c_2) = 1$. Hence $\gcd(m+nd, cd)=1$. Therefore, if $[h]^r = [g]^{r(m+nd)} = [1]$, then $cd \mid r(m+nd) \implies cd \mid r$. Hence the order of $[h]$ must equal cd, and $[h]$ is a generator of $\mathbb{Z}_y^\times$. Furthermore, $[h]^c = [g]^{c(m+nd)} = [g]^{cm} = [p]$. Thus, if ψ takes $[h]$ to $\langle 1 \rangle$, then ψ is an isomorphism taking $[p]$ to $\langle c \rangle$. □

Theorem 3.1.2. *If $\operatorname{ord}_y(p) < \sqrt{\phi(y)}$ then M has accepted elasticity.*

Proof. The condition that $\operatorname{ord}_y(p) < \sqrt{\phi(y)}$ is equivalent to saying $d < c$. From theorem 3.1.1 and theorem 2.2.2, it suffices to show that $(\mathbb{Z}_{cd}, \langle c \rangle, 1)$ is accepted.

For $j = 1, ..., d$, let $\mathcal{A}_j = \{\!\!\{\langle 1 - jc \rangle^{(d)}, \langle jc - 1 \rangle^{(d)}\}\!\!\}$ containing d copies of $\langle 1 - jc \rangle$ and d copies of $\langle jc - 1 \rangle$. Also let

$$\begin{array}{rcl}
\mathcal{B}_1 = ... = \mathcal{B}_d & = & \{\!\!\{\langle -1 \rangle, \langle 1 - c \rangle\}\!\!\} \\
\mathcal{B}_{d+1} = ... = \mathcal{B}_{2d} & = & \{\!\!\{\langle -1 + c \rangle, \langle 1 - 2c \rangle\}\!\!\} \\
\mathcal{B}_{2d+1} = ... = \mathcal{B}_{3d} & = & \{\!\!\{\langle -1 + 2c \rangle, \langle 1 - 3c \rangle\}\!\!\} \\
\vdots & \vdots & \vdots \\
\mathcal{B}_{(d-1)d+1} = ... = \mathcal{B}_{d^2} & = & \{\!\!\{\langle -1 + (d-1)c \rangle, \langle 1 - dc \rangle\}\!\!\}
\end{array}$$

Then $\sum \mathcal{A}_j = \langle 0 \rangle$ for each $\mathcal{A}_j$ and $\sum \mathcal{B}_j = \langle -c \rangle$ for each $\mathcal{B}_j$. Also,

$$\bigcup_{i=1}^{d} \mathcal{A}_i = \bigcup_{j=1}^{d} \left\{\!\!\left\{\langle 1 - jc \rangle^{(d)}\right\}\!\!\right\} \cup \bigcup_{j=1}^{d} \left\{\!\!\left\{\langle jc - 1 \rangle^{(d)}\right\}\!\!\right\} = \bigcup_{i=1}^{d^2} \mathcal{B}_i.$$

Furthermore, $\beta(\mathbb{Z}_{cd}, \langle c \rangle, 1) = \operatorname{ord}(\langle c \rangle) = d$. Therefore, conditions (1), (3), (4), and (5) of the definition of an accepted triple are satisfied.

All that remains is to prove, for any $j = 1, ..., d$, that $\mathcal{A}_j$ has no internal sum in $\{\langle c\rangle, \langle 2c\rangle, ..., \langle (d{-}1)c\rangle\}$. Any submultiset of $\mathcal{A}_j$ is of the form $\{\!\{\langle 1 - jc\rangle^{(s)}, \langle jc - 1\rangle^{(t)}\}\!\}$, with $s, t \leqslant d < c$. This submultiset has a sum of $s\langle 1 - jc\rangle + t\langle jc - 1\rangle = \langle jc(t-s) + (s-t)\rangle$. Thus, if this internal sum were to be in $\{\langle c\rangle, \langle 2c\rangle, ..., \langle (d{-}1)c\rangle\}$, then we would have $c \mid s - t$. But since s, t are nonegative and less than c, we have $s - t = 0$, so $\{\!\{\langle 1 - jc\rangle^{(s)}, \langle jc - 1\rangle^{(t)}\}\!\}$ would have a sum of 0. Thus $\mathcal{A}_j$ has no internal sum in $\{\langle c\rangle, \langle 2c\rangle, ..., \langle (d-1)c\rangle\}$, and $(\mathbb{Z}_{cd}, \langle c\rangle, 1)$ is accepted, completing the proof. □

3.2. c and d Relatively Prime.

Theorem 3.2.1. *If c and d are relatively prime, then M has accepted elasticity iff $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0, 1\rangle, \alpha)$ is accepted.*

Proof. From 3.1.1 and the isomorphism theorem, it suffices to show that there is an isomorphism from $\mathbb{Z}_{cd}$ to $\mathbb{Z}_c \times \mathbb{Z}_d$ taking $\langle c\rangle$ to $\langle 0, 1\rangle$. The chinese remainder theorem tells us that the map $\psi : \mathbb{Z}_{cd} \to \mathbb{Z}_c \times \mathbb{Z}_d$ defined by $\langle n\rangle \mapsto \langle n, n\rangle$ is an isomorphism. Let c' be an integer such that $cc' \equiv 1 \pmod{d}$. Then the map $\pi : \mathbb{Z}_c \times \mathbb{Z}_d \to \mathbb{Z}_c \times \mathbb{Z}_d$ defined by $\langle s, t\rangle \mapsto \langle s, c't\rangle$ is an automorphism, since it has the inverse $\pi^{-1} : \langle s, t\rangle \mapsto \langle s, ct\rangle$. Thus the map $\pi \circ \psi : \mathbb{Z}_{cd} \to \mathbb{Z}_c \times \mathbb{Z}_d$ is an isomorphism taking $\langle c\rangle$ to $\langle c, cc'\rangle = \langle 0, 1\rangle$. □

Lemma 3.2.1. *If $gcd(c, d) = 1$, $\alpha \leqslant d$ and $d \leqslant \alpha c - \alpha$, then M has accepted elasticity.*

Proof.

$$\begin{aligned} d &\leqslant \alpha c - \alpha \\ d &< c\alpha - \alpha + 1 \\ \alpha + d - 2 &< c\alpha - 1 \\ \alpha d - \alpha + d^2 - 2d + 1 &< cd\alpha - d - \alpha + 1 \\ \frac{\alpha + d - 1}{\alpha} &< \frac{cd\alpha - d - \alpha + 1}{\alpha(d-1)}. \end{aligned}$$

We will show that $\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0, 1\rangle, \alpha$ is overaccepted by showing that there are positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ which satisfy conditions (1)-(4) and, additionally, f/e can be arbitrarily close to $\frac{cd\alpha - d - \alpha + 1}{\alpha(d-1)}$. This will ensure that condition $(\overline{5})$ will hold.

Let n be any nonnegative integer. Let k be a positive integer such that $kc - d + 1 \geqslant 0$. Define

$$\begin{aligned} \mathcal{A}_{1,1} = \cdots = \mathcal{A}_{1,\overline{\alpha}(d-1)n} &= \{\!\{\langle -1, -\overline{\alpha}\rangle^{(c-1)}, \langle 1, \overline{\alpha}\rangle^{(c-1)}, \langle 0, -1\rangle^{(\overline{\alpha}-1)}\}\!\} \\ \mathcal{A}_{2,1} = \cdots = \mathcal{A}_{2,\overline{\alpha}} &= \{\!\{\langle 1, 0\rangle^{(c(c-1)kn)}, \langle 0, -1\rangle^{(\overline{\alpha}-1)}\}\!\} \\ \mathcal{B}_{1,1} = \cdots = \mathcal{B}_{1,\overline{\alpha}(c-1)(d-1)n} &= \{\!\{\langle -1, -\overline{\alpha}\rangle, \langle 1, 0\rangle\}\!\} \\ \mathcal{B}_{2,1} = \cdots = \mathcal{B}_{2,\overline{\alpha}(c-1)n} &= \{\!\{\langle 1, \overline{\alpha}\rangle^{(d-1)}, \langle 1, 0\rangle^{(kc-d+1)}\}\!\} \\ \mathcal{B}_{3,1} = \cdots = \mathcal{B}_{3,(\overline{\alpha}-1)[1+(d-1)n]} &= \{\!\{\langle 0, -1\rangle^{(\overline{\alpha})}\}\!\}. \end{aligned}$$

Then we have

$$\bigcup \mathcal{A} = \bigcup \mathcal{B} =$$

$$\left\{\!\!\left\{\langle -1,-\overline{\alpha}\rangle^{(\overline{\alpha}(c-1)(d-1)n)}, \langle 1,\overline{\alpha}\rangle^{(\overline{\alpha}(c-1)(d-1)n)}, \langle 0,-1\rangle^{(\overline{\alpha}(\overline{\alpha}-1)[1+(d-1)n])}, \langle 1,0\rangle^{(\overline{\alpha}c(c-1)kn)}\right\}\!\!\right\},$$

so condition (1) holds.

We will show that condition (2) holds by contradiction. Assume that $\mathcal{A}_{1,i}$ has an internal sum in $\{\langle 0,1\rangle, ..., \langle 0, d-\alpha\rangle\}$. Then there is a submultiset $\mathcal{S} \subset \mathcal{A}_{1,i}$ such that $\sum \mathcal{S} = \langle 0,\gamma\rangle$ for some $\gamma \in \{1, ..., d-\alpha\}$. $\mathcal{S}$ must be of the form

$$\left\{\!\!\left\{\langle -1,-\alpha\rangle^{(m_1)}, \langle 1,\alpha\rangle^{(m_2)}, \langle 0,-1\rangle^{(m_3)}\right\}\!\!\right\}$$

where $m_1, m_2, m_3 \in \mathbb{Z}_{\geqslant 0}$, $m_1, m_2 \leqslant c-1$, and $m_3 \leqslant \alpha - 1$. Looking at the first coordinate of $\sum \mathcal{S}$ yields $m_2 - m_1 \equiv 0 \pmod c$, and the restrictions on m_1 and m_2 yield $m_1 = m_2$. Hence $\sum \mathcal{S} = \langle 0, -m_3\rangle \in \{\langle 0,1\rangle, ..., \langle 0, d-\alpha\rangle\}$, and therefore $m_3 \geqslant \alpha$, contradiction.

Now assume that $\mathcal{A}_{2,i}$ has an internal sum of $\langle 0,\gamma\rangle$ for some $\gamma \in \{1, ..., d-\alpha\}$. Then there is some submultiset $\mathcal{S} \in \mathcal{B}_{2,i}$ such that $\sum \mathcal{S} = \langle 0,\gamma\rangle$. $\mathcal{S}$ must be of the form

$$\left\{\!\!\left\{\langle 1,0\rangle^{(m_1)}, \langle 0,-1\rangle^{(m_2)}\right\}\!\!\right\}.$$

Here $m_2 \leqslant \alpha - 1$. But looking at the second coordinate of $\sum \mathcal{S}$ yields $m_2 \geqslant \alpha$, contradiction. Therefore, condition (2) holds.

It is straightforward to check that conditions (3) and (4) also hold. Finally, we will show that as n gets large, f/e approaches $\frac{cd\alpha - d - \alpha + 1}{\alpha(d-1)}$. We have

$$\begin{aligned}
\frac{f}{e} &= \frac{(\alpha(c-1)(d-1)n) + (\alpha(c-1)n) + ((\alpha-1)[1+(d-1)n])}{(\alpha(d-1)n) + (\alpha)} \\
&\to \frac{\alpha(c-1)(d-1) + \alpha(c-1) + (\alpha-1)(d-1)}{\alpha(d-1)} \\
&= \frac{cd\alpha - d - \alpha + 1}{\alpha(d-1)}
\end{aligned}$$

as n approaches infinity. This completes the proof. □

Theorem 3.2.2. *If* $\gcd(c,d) = 1$ *and* $\overline{\alpha} > \frac{d}{c}$*, then* M *has accepted elasticity.*

Proof. From theorem 2.2.1, it suffices to assume that $\frac{d}{c} \leqslant \alpha \leqslant d$. Then $\beta = d$. If $c = 1$, then $\alpha = d$ and we can apply theorem 2.1.1, so assume $c \geqslant 2$. From the above lemma, we know that the elasticity is accepted when $d \leqslant \alpha c - \alpha$, so assume $\alpha c - \alpha < d \leqslant \alpha c$. But since $c \geqslant 2$, and $\gcd(c,d) = 1$, $d \neq \alpha c$. Thus $d = \alpha c - w$ for some $w \in \{1, ..., \alpha - 1\}$. From theorem 3.2.1 and theorem 1.3.4, it suffices to show that $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is overaccepted in these cases.

Let's first examine the case where $d = \alpha c - (\alpha - 1)$. This means that $\frac{\alpha+\beta-1}{\alpha} = \frac{\alpha + \alpha c - (\alpha-1) - 1}{\alpha} = c$. Choose $n \in \mathbb{Z}_{>0}$ and define $e = \alpha n + (\alpha - 1) + 1$, $f = \alpha n(2c - 1) + n + (\alpha - 1)$, and

$$\begin{aligned}
\mathcal{A}_1 &= \left\{\!\!\left\{\langle 0,-1\rangle^{\alpha-1}, \langle -1,0\rangle^{2cn}\right\}\!\!\right\} \\
\mathcal{A}_{2,1} = \cdots = \mathcal{A}_{2,\alpha-1} &= \left\{\!\!\left\{\langle 0,1-\alpha\rangle, \langle -1,0\rangle^{2cn}\right\}\!\!\right\} \\
\mathcal{A}_3 = \cdots = \mathcal{A}_{3,\alpha n} &= \left\{\!\!\left\{\langle 1,-\alpha\rangle^{2c-1}, \langle 1,-1\rangle\right\}\!\!\right\} \\
\mathcal{B}_{1,1} = \cdots = \mathcal{B}_{1,\alpha-1} &= \{\!\{\langle 0,-1\rangle, \langle 0,1-\alpha\rangle\}\!\} \\
\mathcal{B}_{2,1} = \cdots = \mathcal{B}_{2,\alpha n(2c-1)} &= \{\!\{\langle 1,-\alpha\rangle, \langle -1,0\rangle\}\!\} \\
\mathcal{B}_{3,1} = \cdots = \mathcal{B}_{3,n} &= \{\!\{\langle 1,-1\rangle^{\alpha}, \langle -1,0\rangle^{\alpha}\}\!\}
\end{aligned}$$

To see that condition (1) holds, notice

$$\bigcup \mathcal{A} = \bigcup \mathcal{B}$$

$$= \left\{\!\!\left\{\langle 0,-1\rangle^{\alpha-1}, \langle 0,1-\alpha\rangle^{\alpha-1}, \langle -1,0\rangle^{2\alpha cn}, \langle 1,-\alpha\rangle^{\alpha n(2c-1)}, \langle 1,-1\rangle^{\alpha n}\right\}\!\!\right\}$$

Next we will show that condition (2) holds. Notice that for $\mathcal{A}_1$, the second component of any internal sum will always be between 0 and $-(\alpha-1)$, and hence can never be in $\{\langle 0,1\rangle,\ldots,\langle 0,d-\alpha\rangle\}$. The same is true for each $\mathcal{A}_{2,i}$.

We will use two cases of proof by contradiction to prove that condition (2) holds for each $\mathcal{A}_{3,i}$. Assume that $\exists\mathcal{S}\subset\mathcal{A}_{3,i}$ such that $\sum\mathcal{S}\in\{\langle 0,1\rangle,\ldots,\langle 0,d-\alpha\rangle\}$. For Case 1, say $\mathcal{S}=\{\!\{\langle 1,-\alpha\rangle^s\}\!\}$, and that $\sum\mathcal{S}=\langle 0,r\rangle$, where $1\leqslant r\leqslant d-\alpha$. This summation gives the relationship $s\langle 1,-\alpha\rangle=\langle 0,r\rangle$ meaning that $s\equiv 0 \pmod{c}$ and $-s\alpha\equiv r \pmod{d}$, where $0\leqslant s\leqslant 2c-1$. The first congruence yields $s=0$ or $s=c$. We know that $s\neq 0$ because then $0\equiv r \pmod{d}$ and that contradicts the bound of r. If $s=c$ then

$$\begin{aligned}\sum\mathcal{S} &= \langle c,-\alpha c\rangle\\ &= \langle c,-\alpha c+\alpha c-(\alpha-1)\rangle\\ &= \langle c,1-\alpha\rangle\end{aligned}$$

We now have the second component of the order pair as $1-\alpha$, which contradicts the bound of r. So therefore case 1 holds.

For case 2 say $\mathcal{S}=\{\!\{\langle 1,-\alpha\rangle^s,\langle 1,-1\rangle\}\!\}$, and that $\sum\mathcal{S}=\langle 0,r\rangle$, where $1\leqslant r\leqslant d-\alpha$. Here, the summation gives the relationship $s\langle 1,-\alpha\rangle+\langle 1,-1\rangle=\langle 0,r\rangle$ meaning

$$s+1\equiv 0 \pmod{c}\Rightarrow s\equiv -1 \pmod{c}$$

and

$$-s\alpha-1\equiv r \pmod{d}.$$

The first congruence yields $s=c-1$ or $s=2c-1$. By plugging in the values of s into the second congruence, we have

$$\begin{aligned}-\alpha c+\alpha-1\equiv r \pmod{d} &\Rightarrow -(\alpha-1)+\alpha-1\equiv r \pmod{d}\\ &\Rightarrow 0\equiv r \pmod{d}\end{aligned}$$

or

$$\begin{aligned}-2\alpha c+\alpha-1\equiv r \pmod{d} &\Rightarrow -2(\alpha-1)+\alpha-1\equiv r \pmod{d}\\ &\Rightarrow -2\alpha+2+\alpha-1\equiv r \pmod{d}\\ &\Rightarrow -\alpha+1\equiv r \pmod{d}.\end{aligned}$$

Here we use the fact that $\alpha c\equiv\alpha-1 \pmod{d}$ because $d\mid\alpha c-(\alpha-1)$. Furthermore, since $\alpha\geqslant 1$, both of these congruences are outside the range of $1\leqslant r\leqslant d-\alpha$. As a result, case 2 holds. We have thus proven that condition (2) is true.

To see that condition (3) holds as true, notice that

$$\begin{aligned}\sum\mathcal{A}_1 &= (\alpha-1)\langle 0,-1\rangle+(2cn)\langle -1,0\rangle\\ &= \langle -2cn,1-\alpha\rangle\\ &= \langle 0,1-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum\mathcal{A}_{2,i} &= \langle 0,1-\alpha\rangle+(2cn)\langle -1,0\rangle\\ &= \langle -2cn,1-\alpha\rangle\\ &= \langle 0,1-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{A}_{3,i} &= (2c-1)\langle 1,-\alpha\rangle + \langle 1,-1\rangle \\ &= \langle 2c, -2c\alpha + \alpha - 1\rangle \\ &= \langle 2c, -2(\alpha-1) + \alpha - 1)\rangle \\ &= \langle 0, 1-\alpha\rangle.\end{aligned}$$

Similarly, condition (4) holds true because

$$\begin{aligned}\sum \mathcal{B}_{1,i} &= \langle 0,-1\rangle + \langle 0, 1-\alpha\rangle \\ &= \langle 0, -\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{B}_{2,i} &= \langle 1,-\alpha\rangle + \langle -1, 0\rangle \\ &= \langle 0, -\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{B}_{3,i} &= (\alpha)\langle 1,-1\rangle + (\alpha)\langle -1, 0\rangle \\ &= \langle 0, -\alpha\rangle.\end{aligned}$$

Finally, to prove condition (5) we use $\lim_{n\to\infty} \frac{f}{e}$. Notice that by substituting in the values of e and f we have

$$\begin{aligned}\lim_{n\to\infty} \frac{\alpha n(2c-1) + n + (\alpha-1)}{\alpha n + (\alpha-1) + 1} &= \frac{\alpha(2c-1)+1}{\alpha} \\ &= 2c - 1 + \frac{1}{\alpha} \\ &> c\end{aligned}$$

Therefore, there exists an n large enough so that $\frac{f}{e} \geqslant c$. By showing that conditions (1)-(5) hold true, we have proven that $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is overaccepted for the $d = \alpha c - (\alpha - 1)$ case. Therefore, by theorem 1.3.4, the elasticity of M is accepted.

We now are left with the final case $d = \alpha c - w$, where $1 \leqslant w \leqslant \alpha - 2$. Again we will prove accepted elasticity by showing that $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is overaccepted. Observe that $\frac{\alpha+\beta-1}{\alpha} = \frac{\alpha+\alpha c-w-1}{\alpha} = c + 1 - \frac{w+1}{\alpha}$. Again choose some $n \in \mathbb{Z}_{>0}$. Next, define m such that $mw \geqslant \alpha$, but $(m-1)w < \alpha$. Define $e = (wm - \alpha + 1)n + 1 + (\alpha - 1) + (\alpha - 1)n$, $f = (mc-1)(\alpha-1)n + (\alpha-1)n + (\alpha-1)$, and

$$\begin{aligned}\mathcal{A}_{1,1} = \cdots = \mathcal{A}_{1,(wm-\alpha+1)n+1} &= \{\!\{\langle 0,-1\rangle^{\alpha-1}\}\!\} \\ \mathcal{A}_{2,1} = \cdots = \mathcal{A}_{2,\alpha-1} &= \{\!\{\langle 0, 1-\alpha\rangle, \langle -1, 0\rangle^{mcn}\}\!\} \\ \mathcal{A}_{3,1} = \cdots = \mathcal{A}_{3,\alpha n} &= \{\!\{\langle 1, -\alpha\rangle^{mc-1}, \langle 1, wm - 2\alpha + 1\rangle\}\!\} \\ \mathcal{B}_{1,1} = \cdots = \mathcal{B}_{1,\alpha-1} &= \{\!\{\langle 0,-1\rangle, \langle 0, 1-\alpha\rangle\}\!\} \\ \mathcal{B}_{2,1} = \cdots = \mathcal{B}_{2,(mc-1)(\alpha-1)n} &= \{\!\{\langle 1,-\alpha\rangle, \langle -1, 0\rangle\}\!\} \\ \mathcal{B}_{3,1} = \cdots = \mathcal{B}_{3,(\alpha-1)n} &= \{\!\{\langle -1, 0\rangle, \langle 1, wm - 2\alpha + 1\rangle, \langle 0, -1\rangle^{wm-\alpha+1}\}\!\}\end{aligned}$$

To see that condition (1) holds, notice that

$$\bigcup \mathcal{A} = \bigcup \mathcal{B} =$$

$$\left\{\!\!\left\{\langle 0,-1\rangle^{(\alpha-1)[(wm-\alpha+1)n+1]},\langle 0,1-\alpha\rangle^{\alpha-1},\langle -1,0\rangle^{mcn(\alpha-1)}\right\}\!\!\right\}\cup$$

$$\left\{\!\!\left\{\langle 1,-\alpha\rangle^{\alpha n(mc-1)},\langle 1,wm-2\alpha+1\rangle^{\alpha n}\right\}\!\!\right\}.$$

Next we will show that condition (2) holds. Notice that for each $\mathcal{A}_{1,i}$ and $\mathcal{A}_{2,i}$, the second coordinate of any internal sum will always be between $1-\alpha$ and 0, and hence there will be no internal sum in $\{\langle 0,1\rangle,...,\langle 0,d-\alpha\rangle\}$. Once again, we will use two cases of proof by contradiction to prove that condition (2) holds for each $\mathcal{A}_{3,i}$. Assume that $\exists\mathcal{S}\subset\mathcal{A}_{3,i}$ such that $\sum\mathcal{S}\in\{\langle 0,1\rangle,...,\langle 0,d-\alpha\rangle\}$. For case 1 say $\mathcal{S}=\{\!\!\{\langle 1,-\alpha\rangle^{s}\}\!\!\}$, and that $\sum\mathcal{S}=\langle 0,r\rangle$, where $1\leqslant r\leqslant d-\alpha$. This summation gives the relationship $s\langle 1,-\alpha\rangle=\langle 0,r\rangle$ meaning that $s\equiv 0 \pmod c$ and $-s\alpha\equiv r \pmod d$, where $0\leqslant s\leqslant mc-1$. Thus $s=tc$ for some $0\leqslant t\leqslant m-1$. Hence

$$\begin{aligned}\sum\mathcal{S} &= \langle c,-\alpha tc\rangle\\ &= \langle 0,-tw\rangle,\end{aligned}$$

since $\alpha c\equiv w \pmod d$. But we have $0\leqslant tw\leqslant(m-1)w<\alpha$, hence $\langle 0,-tw\rangle\notin\{\langle 0,1\rangle,...,\langle 0,d-\alpha\rangle\}$. Therefore, case 1 holds.

For case 2, say $\mathcal{S}=\{\!\!\{\langle 1,-\alpha\rangle^{s},\langle 1,wm-2\alpha+1\rangle\}\!\!\}$ and $\sum\mathcal{S}=\langle 0,r\rangle$, where $1\leqslant r\leqslant d-\alpha$. Here, the summation gives the relationship $s\langle 1,-\alpha\rangle+\langle 1,wm-2\alpha+1\rangle=\langle 0,r\rangle$, so

$$s+1\equiv 0 \pmod c\rightarrow s\equiv -1 \pmod c$$

and

$$-s\alpha+wm-2\alpha+1\equiv r \pmod d$$

where $0\leqslant s\leqslant mc-1$. Let $s=tc-1$, where $1\leqslant t\leqslant m$. By plugging in this value of s into the congruence of $r \pmod d$, we have

$$\Rightarrow\quad \alpha-tc\alpha+wm-2\alpha+1.$$

Since $\alpha c\equiv w \pmod d$ we have

$$\begin{aligned}&\Rightarrow\quad \alpha-tw+wm-2\alpha+1\\ &\Rightarrow\quad w(m-t)+1-\alpha\end{aligned}$$

This gives the inequality

$$0\leqslant w(m-t)<\alpha\Longleftrightarrow 1-\alpha\leqslant w(m-t)+1-\alpha<1$$

which is outside the bound of $1\leqslant r\leqslant d-\alpha$. As a result, case 2 holds and condition (2) is true.

To see that condition (3) holds, notice that

$$\begin{aligned}\sum\mathcal{A}_{1,i} &= (\alpha-1)\langle 0,-1\rangle\\ &= \langle 0,1-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum\mathcal{A}_{2,i} &= \langle 0,1-\alpha\rangle+(mcn)\langle -1,0\rangle\\ &= \langle -mcn,1-\alpha\rangle\\ &= \langle 0,1-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{A}_{3,i} &= (mc-1)\langle 1,-\alpha\rangle + \langle 1, wm-2\alpha+1\rangle \\ &= \langle mc, -mc\alpha+\alpha+wm-2\alpha+1\rangle \\ &= \langle mc, -mw+wm-\alpha+1\rangle \\ &= \langle mc, 1-\alpha\rangle \\ &= \langle 0, 1-\alpha\rangle.\end{aligned}$$

Similarly, condition (4) holds because

$$\begin{aligned}\sum \mathcal{B}_{1,i} &= \langle 0,-1\rangle + \langle 0,1-\alpha\rangle \\ &= \langle 0,-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{B}_{2,i} &= \langle 1,-\alpha\rangle + \langle -1,0\rangle \\ &= \langle 0,-\alpha\rangle\end{aligned}$$

and

$$\begin{aligned}\sum \mathcal{B}_{3,i} &= \langle -1,0\rangle + \langle 1, wm-2\alpha+1\rangle + (wm-\alpha+1)\langle 0,-1\rangle \\ &= \langle 0, wm-wm-2\alpha+\alpha+1-1\rangle \\ &= \langle 0,-\alpha\rangle.\end{aligned}$$

Finally, to prove condition $(\bar{5})$ we will use $\lim_{n\to\infty}\frac{f}{e}$. Notice that by substituting in the previously stated values of e and f we have

$$\begin{aligned}\lim_{n\to\infty}\frac{(mc-1)(\alpha-1)n+(\alpha-1)n+(\alpha-1)}{(wm-\alpha+1)n+1+(\alpha-1)+(\alpha-1)n} &= \frac{mc(\alpha-1)}{wm} \\ &= \frac{c(\alpha-1)}{w}\end{aligned}$$

Therefore, there exists an n large enough so that $\frac{f}{e} \geqslant c+1-\frac{w+1}{\alpha}$ because

$$\begin{aligned}\frac{c(\alpha-1)}{w} &> c+1-\frac{w+1}{\alpha} \iff \\ c+\frac{(\alpha-w-1)c}{w} &> c+\frac{(\alpha-w-1)}{\alpha} \iff \\ \frac{(\alpha-w-1)c}{w} &> \frac{(\alpha-w-1)}{\alpha}.\end{aligned}$$

The last inequality holds because $\alpha > w$, $c > 0$, and $\alpha - w - 1 > 0$, hence condition $(\bar{5})$ holds true. Thus $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is overaccepted for the $d = \alpha c - w$ case, completing the proof. □

3.3. **Fixing c.**

3.3.1. *The Case $c = 1$.* The condition that $c = 1$ is equivalent to p being a primitive root modulo y. The conditions for when these ACMs have accepted elasticity have already been proven in [3]. We restate the proof using our new notation and machinary.

Lemma 3.3.1. *For any integer $n \geqslant 3$, and any integer k such that $k \pmod{2n} \in \{n+1, ..., 2n\}$, $(\mathbb{Z}_{2n}, \langle 1\rangle, k)$ is accepted.*

Proof. From theorem 2.2.1, we may assume that $k \in \{n+1, ..., 2n\}$. Let

$$\begin{aligned}
\mathcal{A}_1 = \cdots = \mathcal{A}_{k-1} &= \left\{\!\!\left\{ \langle -1 \rangle^{(k-1)} \right\}\!\!\right\} \\
\mathcal{A}_k &= \left\{\!\!\left\{ \langle n \rangle^{(8n^2+1)}, \langle n+1-k \rangle \right\}\!\!\right\} \\
\mathcal{B}_1 = \cdots = \mathcal{B}_{k+2n-2} &= \left\{\!\!\left\{ \langle -1 \rangle^{(k-n)}, \langle n \rangle \right\}\!\!\right\} \\
\mathcal{B}_{k+2n-1} &= \left\{\!\!\left\{ \langle -1 \rangle^{(k-1)^2-(k-n)(k+2n-2)}, \langle n \rangle^{8n^2-k-2n+3}, \langle n+1-k \rangle \right\}\!\!\right\}.
\end{aligned}$$

It is clear that each $\mathcal{A}_i$ is well-defined. $\mathcal{B}_1, ..., \mathcal{B}_{k+2n-2}$ are each well-defined because $k > n$. To show that $\mathcal{B}_{k+2n-1}$ is well-defined, we must show that $(k-1)^2 - (k-n)(k+2n-2) \geqslant 0$ and $8n^2 - k - 2n + 3 > 0$. For the former, we have

$$\begin{aligned}
(k-1)^2 - (k-n)(k+2n-2) &= k^2 - 2k + 1 - [k^2 + 2nk - 2k - nk - 2n^2 + 2n] \\
&= 2n^2 - 2n + 1 - nk \\
&= n(2n-2-k) + 1 \\
&\geqslant n(n+1-k) + 1 > 0,
\end{aligned}$$

because $2n - 2 \geqslant n + 1$ when $n \geqslant 3$. For the latter, we have

$$\begin{aligned}
8n^2 - k - 2n + 3 &\geqslant 8n^2 - 3n + 3 \\
&= 8n(n - \frac{3}{8}) + 3 \\
&> 0,
\end{aligned}$$

again because $n \geqslant 3$. Thus each of these multisets is well defined. We claim that these multisets satisfy conditions (1)-(5) from the definition of an accepted triple.

$$\bigcup_{i=1}^{k} \mathcal{A}_i = \left\{\!\!\left\{ \langle -1 \rangle^{(k-1)^2}, \langle n \rangle^{(8n^2+1)}, \langle n+1-k \rangle \right\}\!\!\right\} = \bigcup_{i=1}^{k+2n-1} \mathcal{B}_i,$$

proving that condition (1) holds.

Notice that $\beta(\mathbb{Z}_{2n}, \langle 1 \rangle, k) = 2n$ because $k \leqslant 2n$. So condition (2) amounts to showing that no $\mathcal{A}_i$ has an internal sum in $\{\langle 1 \rangle, ..., \langle 2n-k \rangle\}$. For $i = 1, ..., k-1$, this is clear because the only internal sums are $\langle -1 \rangle, \langle -2 \rangle, ..., \langle -(k-1) \rangle$. For $\mathcal{A}_k$, the only internal sums are $\langle 1-k \rangle$ and $\langle n+1-k \rangle$. The former is clearly not in $\{\langle 1 \rangle, ..., \langle 2n-k \rangle\}$. To see that the same is true for $\langle n+1-k \rangle$, notice that $n+1 \leqslant k \leqslant 2n \implies 1-n \leqslant n+1-k \leqslant 0 \implies \langle n+1-k \rangle \in \{\langle n+1 \rangle, ..., \langle 2n \rangle\}$. Since $2n-k < n$, $\langle n+1-k \rangle \notin \{\langle 1 \rangle, ..., \langle 2n-k \rangle\}$. Hence condition (2) holds.

It is easy to see that condition (3) holds, and that condition (4) holds for $\mathcal{B}_1, ..., \mathcal{B}_{k+2n-2}$. We also have that

$$\sum \mathcal{B}_{k+2n-1} =$$

$$\begin{aligned}
& [(k-1)^2 - (k-n)(k+2n-2)]\langle -1 \rangle + (8n^2 - k - 2n + 3)\langle n \rangle + \langle n+1-k \rangle \\
= \; & \langle [(k-n)(k-2) - (k-1)^2] + [n(3-k)] + [n+1-k] \rangle \\
= \; & \langle k^2 - nk + 2k - nk - k^2 + 2k - 1 + 3n - nk + n + 1 - k \rangle \\
= \; & \langle -2nk + 2n - k \rangle \\
= \; & \langle -k \rangle,
\end{aligned}$$

hence condition (4) holds for all $\mathcal{B}_i$. Finally, since $\beta(\mathbb{Z}_{2n}, \langle 1 \rangle, k) = 2n$, condition (5) holds, and $(\mathbb{Z}_{2n}, \langle 1 \rangle, k)$ is accepted. □

Corollary 3.3.1. *For any M with $\mathbb{Z}_y^\times$ cyclic, if $d \geqslant 6$, d is even, and $\overline{\alpha} > \frac{d}{2}$, then M has accepted elasticity.*

Proof. We know that M has accepted elasticity if $(\mathbb{Z}_{cd}, \langle c\rangle, \alpha)$ is accepted, and we can apply the reduction and isomorphism theorems to the group generated by $\langle c\rangle$ to see that M has accepted elasticity if $(\mathbb{Z}_d, \langle 1\rangle, \alpha)$ has accepted elasticity. □

Theorem 3.3.1. *Assume $c = 1$ and $\overline{\alpha} \neq d$. Then M has accepted elasticity iff*

(I) $d \geqslant 6$ and
(II) $\overline{\alpha} > d/2$.

Proof. The if statement follows directly from the above corollary. We will prove the only if statement. From theorem 3.1.1, this amounts to showing that if either (I) or (II) is false, then $(\mathbb{Z}_d, \langle 1\rangle, \alpha)$ is not accepted.

First suppose that (II) is false. Let positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e$, $\mathcal{B}_1, ..., \mathcal{B}_f$ satisfy conditions (1)-(4) from the definition of an accepted triple. Then we will show that condition (5) will not be satisfied.

Define a function $v : \mathbb{Z}_d \to \mathbb{Z}$ by $v(\langle -n\rangle) = n$ for $n = 0, 1, ..., d-1$. For a multiset $\mathcal{S}$ of elements of $\mathbb{Z}_d$, let $v(\mathcal{S}) = \sum_{s\in\mathcal{S}} v(s)$. Notice that $v(\mathcal{S}) \equiv v(\sum \mathcal{S}) \pmod{d}$. Since no $\mathcal{A}_i$ has an internal sum in $\{\langle 1\rangle, ..., \langle \beta-\alpha\rangle\}$, there is no submultiset $\mathcal{S} \subset \mathcal{A}_i$ such that $v(\mathcal{S}) \equiv \overline{\alpha}, \overline{\alpha}+1, ..., d-1$. Furthermore, for any $a \in \mathcal{A}_i$, $v(a) \in \{0, 1, ..., \overline{\alpha}-1\}$. Since we are assuming $\overline{\alpha} \leqslant \frac{d}{2}$, we have $2(\overline{\alpha}-1) < d$, hence it is impossible for $v(\mathcal{A}_i)$ to be more than $\overline{\alpha}-1$. Since $v(\mathcal{A}_i) \equiv v(\langle 1-\alpha\rangle) = \overline{\alpha}-1 \pmod{d}$, we have $v(\mathcal{A}_i) = \overline{\alpha}-1$ for each $\mathcal{A}_i$. Furthermore, since $v(\mathcal{B}_i) \equiv v(\langle -\alpha\rangle) = \overline{\alpha} \pmod{d}$, we have $v(\mathcal{B}_i) \geqslant \overline{\alpha}$ for each $\mathcal{B}_i$. Thus we have

$$\begin{aligned} v\left(\bigcup_{i=1}^{e} \mathcal{A}_i\right) &= v\left(\bigcup_{i=1}^{f} \mathcal{B}_i\right) \\ \sum_{i=1}^{e} v(\mathcal{A}_i) &= \sum_{i=1}^{f} v(\mathcal{B}_i) \\ e(\overline{\alpha}-1) &\geqslant f\overline{\alpha} \implies \\ \frac{f}{e} &\leqslant \frac{\overline{\alpha}-1}{\overline{\alpha}} < 1 \leqslant 1 + \frac{\beta-1}{\alpha}, \end{aligned}$$

since $\alpha < \beta$ by theorem 2.1.1. Thus condition (5) cannot hold, and $(\mathbb{Z}_d, \langle 1\rangle, \alpha)$ is not accepted.

All that remains is to consider when (II) holds but (I) does not. From number theory, we know that $d = 1$ or d is even. Combined with the restrictions that $d < 6$ and $\frac{d}{2} < \overline{\alpha} < d$, the only remaining case to check is $d = 4$ and $\overline{\alpha} = 3$. Suppose that the integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ satisfy conditions (1)-(5) from the definition of an accepted triple. Then $f/e = 2$. Since $\sum \mathcal{B}_i = \langle 1\rangle$, each $\mathcal{B}_i$ contains an odd element. Since no $\mathcal{A}_i$ has an internal sum of $\langle 1\rangle$, each $\mathcal{B}_i$ contains a $\langle 3\rangle$. Since $3\langle 3\rangle = \langle 1\rangle$, each $\mathcal{A}_i$ contains at most 2 copies of $\langle 3\rangle$, and since each $f/e = 2$, each $\mathcal{A}_i$ contains exactly 2 copies of $\langle 3\rangle$. Then no $\mathcal{A}_i$ contains a $\langle 2\rangle$ because $\langle 3\rangle + \langle 2\rangle = \langle 1\rangle$. Hence each $\mathcal{B}_i$ contains exactly one $\langle 3\rangle$ and no $\langle 2\rangle$ or $\langle 1\rangle$, contradicting the fact that $\sum \mathcal{B}_i = \langle 1\rangle$. Thus $(\mathbb{Z}_d, \langle 1\rangle, \alpha)$ is not accepted, completing the proof. □

Corollary 3.3.2. *If $c = 1$ and $d > 1$, then $\omega(M) = \infty$.*

Proof. If $d > 1$, then $1 \leqslant \frac{d}{2}$, hence $(\mathbb{Z}_y^\times, [p], \alpha)$ is not accepted when $\overline{\alpha} = 1$. Thus, $\omega(\mathbb{Z}_y^\times, [p]) = \infty$. □

3.3.2. *The Case $c = 2$.*

Theorem 3.3.2. *If $c = 2$ and $\overline{\alpha} > d/2$ then M has accepted elasticity.*

Proof. If d is odd, then this follows directly from theorem 3.2.2. If d is even, and $d \geqslant 6$, then this follows from corollary 3.3.1. If $d = 2$, then $\overline{\alpha} = 2$, and acceptance follows from theorem 2.1.1. If $d = 4$, then we would have $\phi(y) = 8$, which is not true for any integer y, hence the proof is complete. □

Theorem 3.3.3. *If $c = 2$, d is even, and*

$$\alpha < \frac{1 + \sqrt{4d - 3}}{2}$$

then M does not have accepted elasticity.

Proof. First, observe that

$$\begin{array}{rcl} 0 & < & (d-1)^2 + 1 \\ 0 & < & d^2 - 2d + 2 \\ 4d - 3 & < & d^2 + 2d + 1 \\ \sqrt{4d-3} & < & d + 1 \\ \dfrac{1 + \sqrt{4d-3}}{2} & < & \dfrac{d+2}{2} \\ \dfrac{1 + \sqrt{4d-3}}{2} & \leqslant & \dfrac{d}{2}, \end{array}$$

so $\alpha \leqslant \frac{d}{2}$.

Claim: let $\mathcal{A}$ be a muliset of elements of $\mathbb{Z}_{2d} \backslash \{\langle 0 \rangle\}$ such that $\mathcal{A}$ has no internal sum in $\{\langle 2 \rangle, \langle 4 \rangle, ..., \langle 2(d - \alpha) \rangle\}$. Then $|\mathcal{A}| \leqslant 2\alpha$.

To prove this, we will use strong induction on α. For $\alpha = 1$, $\mathcal{A}$ contains no evens. If there are three distinct odds, say a_1, a_2, a_3, then either $a_1 + a_2$ or $a_1 + a_3$ is contained in $\{\langle 2 \rangle, \langle 4 \rangle, ..., \langle 2(d - \alpha) \rangle\}$, so $\mathcal{A}$ contains at most two distinct odds. If $\mathcal{A}$ contains two copies of the same element, say a, then $2a = \langle 0 \rangle$ which means $a = 0$ or d, and hence a is even, contradiction. Thus $|\mathcal{A}| \leqslant 2$, completing the base case.

Now, assume that the claim holds for $\alpha = 1, ..., k - 1$, with $k \leqslant \frac{d}{2}$. Assume that there is some multiset $\mathcal{A}$ of elements of $\mathbb{Z}_{2d} \backslash \{\langle 0 \rangle\}$ such that $\mathcal{A}$ has no internal sum in $\{\langle 2 \rangle, \langle 4 \rangle, ..., \langle 2(d - k) \rangle\}$ and $|A| \geqslant 2k + 1$.

Assume that $\mathcal{A}$ contains an even element. Then for some $m \in \{1, ..., k - 1\}$, $\langle -2m \rangle \in \mathcal{A}$. Let $\mathcal{A}' = \mathcal{A} \backslash \{\!\{\langle -2m \rangle\}\!\}$. If $\mathcal{A}'$ had an internal sum in

$$\{\langle 2[(d - k) + 1] \rangle, ..., \langle 2[(d - k) + m] \rangle\},$$

then $\mathcal{A}$ would have an internal sum in

$$\{\langle 2[(d - k) - m + 1] \rangle, ..., \langle 2(d - k) \rangle\}.$$

Since $m \leqslant k - 1$ and $k \leqslant \frac{d}{2}$, we have $m + k \leqslant 2k - 1 < d$, so $(d - k) - m + 1 > 1$. Thus $1 < (d - k) - m + 1 < d - k$. Hence $\mathcal{A}$ has no internal sum in $\{\langle 2[(d - k) - m + 1] \rangle, ..., \langle 2(d - k) \rangle\}$, so $\mathcal{A}'$ has no internal sum in $\{\langle 2[(d - k) + 1] \rangle, ..., \langle 2[(d - k) + m] \rangle\}$. Since $\mathcal{A}' \subset \mathcal{A}$, it also has no internal sums in $\{\langle 2 \rangle, ..., \langle 2(d - k) \rangle\}$. Thus $\mathcal{A}'$ has no internal sum in $\{\langle 2 \rangle, ..., \langle 2[(d - k) + m] \rangle\}$. Thus, by the inductive hypothesis,

$|\mathcal{A}'| \leqslant 2(k-m)$, and therefore $|\mathcal{A}| \leqslant 2k-2m+1 \leqslant 2k-1 < 2k+1$, contradiction. So $\mathcal{A}$ contains no even elements.

Suppose $\mathcal{A}$ contains three distinct odds, say a_1, a_2, a_3. Then a_1+a_2, a_1+a_3, and a_2+a_3 are three distinct elements of $\{\langle 0\rangle, \langle -2\rangle, ..., \langle -2(k-1)\rangle\}$, so we may assume that $k > 2$. Let $\mathcal{A}'' = \mathcal{A} \backslash \{\!\{a_1, a_2, a_3\}\!\}$. Since $\{\!\{a_1, a_2, a_3\}\!\}$ contains an internal sum of $\langle -2m\rangle$ for some $2 \leqslant m \leqslant k-1$. Thus, by the same argument as in the previous paragraph, $|\mathcal{A}''| \leqslant 2(k-m) \implies |\mathcal{A}| \leqslant 2k-2m+3 \leqslant 2k-1 < 2k+1$, contradiction. So $\mathcal{A}$ contains at most two distinct elements, both odd.

Let $\mathcal{A} = \left\{\!\!\left\{a_1^{(n_1)}, a_2^{(n_2)}\right\}\!\!\right\}$ where a_1, a_2 are odd and $n_1 + n_2 \geqslant 2k+1$. Let $\mathcal{S}_1 = \left\{\!\!\left\{a_1^{(n_1)}\right\}\!\!\right\}$ and $\mathcal{S}_2 = \left\{\!\!\left\{a_2^{(n_2)}\right\}\!\!\right\}$. Neither $\mathcal{S}_i$ can contain a nontrivial internal sum of $\langle 0\rangle$, for, if it did, let s be the minimal element of $\{1, ..., n_i\}$ such that $sa_i = \langle 0\rangle$. Then s must be even, and $\frac{s}{2}a_i = \langle d\rangle$. But since $k \leqslant \frac{d}{2}$, $\langle d\rangle \in \{\langle 2\rangle, ..., \langle 2(d-k)\rangle\}$, so $\mathcal{A}$ can't have an internal sum of $\langle d\rangle$, contradiction. Additionally, neither $\mathcal{S}_i$ can have two multisubsets with the same sum, for if $\exists 0 \leqslant s < t \leqslant n_i$ such that $a_i^s = a_i^t$, then $a_i^{t-s} = \langle 0\rangle$ is a nontrivial interal sum of $\mathcal{S}_i$, contradiction. Therefore, each $\mathcal{S}_i$ has n_i distinct nonzero internal sums, $\lfloor \frac{n_i}{2} \rfloor$ of them even. Thus, by the pigeonhole principle, one of these internal sums must lie in $\{\langle -2\lfloor \frac{n_i}{2} \rfloor\rangle, ..., \langle -2(k-1)\rangle\}$. Since $n_1 + n_2 = 2k+1$, we have $\lfloor \frac{n_1}{2} \rfloor + \lfloor \frac{n_2}{2} \rfloor \geqslant k$, so $\mathcal{A}$ has an internal sum in $\{\langle -2k\rangle, ..., \langle -2(2k-2)\rangle\} \subset \{\langle 2\rangle, ..., \langle 2(d-k)\rangle\}$, contradiction. This completes the proof of the claim.

Now, we will show that $(\mathbb{Z}_{2d}, \langle 2\rangle, \alpha)$ is not accepted. Assume that this triple is accepted, and that the integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ satisfy conditions (1)-(5) from the definition of an accepted triple. By the claim, then, we know that each $\mathcal{A}_i$ contains at most 2α nonzero elements. Since $\sum \mathcal{B}_i = \langle -2\alpha\rangle$, but $\mathcal{A}_i$ can't have an internal sum of $\langle -2\alpha\rangle$, each $\mathcal{B}_i$ needs at least two nonzero elements. Thus, $f/e \leqslant \alpha \implies$

$$\begin{aligned} \alpha &\geqslant \frac{\alpha + d - 1}{\alpha} \\ \alpha^2 &\geqslant \alpha + d - 1 \\ \alpha^2 - \alpha + 1 - d &\geqslant 0 \\ \alpha &\geqslant \frac{1 + \sqrt{4d-3}}{2}, \end{aligned}$$

completing the proof. □

Theorem 3.3.4. *If $c = 2$, d is odd, and*

$$\alpha < \sqrt{d-1}$$

then M does not have accepted elasticity.

Proof. Let $\alpha < \sqrt{d-1}$, $c = 2$, d odd. Because the theorem is vacuously true if $d = 1$, we will assume $d \geqslant 3$. First observe that

$$\begin{aligned} (d-2)^2 &\geqslant 0 \\ d^2 - 4d + 4 &\geqslant 0 \\ \frac{d^2}{4} &\geqslant d - 1 \\ \frac{d}{2} &\geqslant \sqrt{d-1}. \end{aligned}$$

Thus $\alpha < \frac{d}{2}$.

We must show that $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is not accepted. Define $g : \mathbb{Z}_c \times \mathbb{Z}_d \to \mathbb{Z}$ by taking an element $\langle s,t\rangle$ to the element of $\{0,1,...,d-1\}$ that is congruent to t modulo d. Given a multiset $\mathcal{S}$ of elements of $\mathbb{Z}_c \times \mathbb{Z}_d$, define $g(\mathcal{S}) = \sum_{s\in\mathcal{S}} g(s)$. Notice that $g(\mathcal{S}) \equiv g(\sum \mathcal{S}) \pmod{d}$.

Claim: If $\mathcal{A}$ is a multiset of elements of $\mathbb{Z}_c \times \mathbb{Z}_d$ with no internal sum in $\{\langle 0,1\rangle, ..., \langle 0, \alpha - d\rangle\}$, then $g(\mathcal{A}) \leqslant (\alpha+1)(d-1)$.

We will prove this claim by induction on α. Suppose $\alpha = 1$. Call an element of $\mathbb{Z}_c \times \mathbb{Z}_d = \mathbb{Z}_2 \times \mathbb{Z}_d$ type 0 if its first coordinate is 0 and type 1 if its first coordinate is 1. If $\mathcal{A}$ has no restricted sums in $\{\langle 0,1\rangle, ..., \langle 0, d-1\rangle\}$, then its only type 0 element is $\langle 0,0\rangle$. Suppose $\mathcal{A}$ had three type 1 elements, a_1, a_2, and a_3. Then $a_1 + a_2 = a_1 + a_3 = \langle 0,0\rangle \implies a_2 = a_3$, and $a_2 + a_3 = \langle 0,0\rangle \implies 2a_2 = \langle 0,0\rangle \implies a_1 = a_2 = a_3 = \langle 1,0\rangle$. Thus if $\mathcal{A}$ has three type 1 elements, $g(\mathcal{A}) = 0$. Thus, $\mathcal{A}$ can have at most two elements with a nonzero g-value, and therefore $g(\mathcal{A}) \leqslant 2(d-1) = (\alpha+1)(d-1)$.

Suppose that the claim holds for $\alpha = 1, ..., k-1$, where $k \leqslant \frac{d}{2}$. For the sake of contradiction, suppose that there is some multiset $\mathcal{A}$ of elements of $\mathbb{Z}_c \times \mathbb{Z}_d$ such that $\mathcal{A}$ has no internal sums in $\{\langle 0,1\rangle, ..., \langle 0, d-k\rangle\}$ and $g(\mathcal{A}) > (k+1)(d-1)$.

Suppose $\mathcal{A}$ contains a nonzero type 0 element $\langle 0,-s\rangle$ for some $s \in \{1, ..., k-1\}$. Let $\mathcal{A}' = \mathcal{A} \backslash \{\!\{\langle 0,-s\rangle\}\!\}$. Then $\mathcal{A}'$ has no internal sum in $\{\langle 0,1\rangle, ..., \langle 0, d-k+s\rangle\}$. Thus by the inductive hypothesis applied to $\alpha = k-s$, we have $g(\mathcal{A}') \leqslant (k-s+1)(d-1) \implies g(A) \leqslant (k-s+2)(d-1) \leqslant (k+1)(d-1)$, contradiction. Thus all nonzero elements of $\mathcal{A}$ are type 1.

Suppose $\mathcal{A}$ contains three distinct type 1 elements, a_1, a_2, a_3. Then $a_1+a_2, a_1+a_3, a_2+a_3$ are three distinct elements of $\{\langle 0,0\rangle, \langle 0,-1\rangle, ..., \langle 0, -(k-1)\rangle\}$. Let $\mathcal{A}'' = \mathcal{A} \backslash \{\!\{a_1, a_2, a_3\}\!\}$. If $\langle 0,-s\rangle \in \{a_1+a_2, a_1+a_3, a_2+a_3\}$, then, by the argument in the above paragraph, $g(\mathcal{A}'') \leqslant (k-s+1)(d-1) \implies g(\mathcal{A}) \leqslant (k-s+4)(d-1)$. We also have $(k-s+4)(d-1) \leqslant (k+1)(d-1)$ if $s \geqslant 3$. Hence it must be that $\{a_1+a_2, a_1+a_3, a_2+a_3\} = \{\langle 0,0\rangle, \langle 0,-1\rangle, \langle 0,-2\rangle\}$. But then, solving, we get $\{a_1, a_2, a_3\} = \{\langle 0, \frac{d+1}{2}\rangle, \langle 0, \frac{d-1}{2}\rangle, \langle 0, \frac{d-3}{2}\rangle\}$. Then, since $g(\mathcal{A}'') \leqslant (k-1)(d-1)$, we have $g(\mathcal{A}) \leqslant (k-1)(d-1) + \frac{d+1}{2} + \frac{d-1}{2} + \frac{d-3}{2} = (k-1)(d-1) + \frac{3}{2}(d-1) < (k+1)(d-1)$, contradiction. Thus $\mathcal{A}$ contains at most two distinct type 1 elements.

Since we can ignore $\langle 0,0\rangle$ elements of $\mathcal{A}$, let $\mathcal{A} = \{\!\{\langle 1, a_1\rangle^{(n_1)}, \langle 1, a_2\rangle^{(n_2)}\}\!\}$. Since $g(\mathcal{A}) > (k+1)(d-1)$, it must be that $n_1 + n_2 \geqslant k+2$. WLOG, assume $n_1 \geqslant 2$. Let $2\langle 1, a_1\rangle = \langle 0, -s\rangle$, where $s \in 1, ..., k-1$. Let $\mathcal{A}''' = \mathcal{A} \backslash \{\!\{\langle 1, a_1\rangle^{(2)}\}\!\}$. Then, by the argument in the above paragraphs, $g(\mathcal{A}''') \leqslant (k-s+1)(d-1) \implies g(\mathcal{A}) \leqslant (k-s+3)(d-1)$. We also have $(k-s+3)(d-1) \leqslant (k+1)(d-1)$ when $s \geqslant 2$, so it must be that $s = 1$. But then $g(\mathcal{A}''') \leqslant k(d-1)$ and $a_1 = \frac{d-1}{2} \implies g(\{\!\{\langle 1, a_1\rangle^{(2)}\}\!\}) = d-1$, hence $g(\mathcal{A}) \leqslant (k+1)(d-1)$, contradiction. This completes the proof of the claim.

Now, we will show that $(\mathbb{Z}_c \times \mathbb{Z}_d, \langle 0,1\rangle, \alpha)$ is not accepted. For suppose it were. Then let the integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ satisfy conditions (1)-(5) from the definition of an accepted triple. Then, for each $\mathcal{A}_i$, we know $g(\mathcal{A}_i) \leqslant (\alpha+1)(d-1)$. Since $g(\mathcal{A}_i) \equiv 1-\alpha \pmod{d}$ and $d(1+\alpha)+1-\alpha-d < (\alpha+1)(d-1) < d(1+\alpha)+1-\alpha$, we have $g(\mathcal{A}_i) \leqslant d(1+\alpha)+1-\alpha-d = d\alpha - \alpha + 1$. Furthermore, for each $\mathcal{B}_i$ we have $g(\mathcal{B}_i) \equiv -\alpha \pmod{d}$, and thus $g(\mathcal{B}_i) \geqslant d - \alpha$.

Hence $e(d\alpha - \alpha + 1) \geqslant f(d - \alpha) \implies$

$$\begin{aligned} \frac{f}{e} &\leqslant \frac{d\alpha - \alpha + 1}{d - \alpha} \\ \frac{\alpha + d - 1}{\alpha} &\leqslant \frac{d\alpha - \alpha + 1}{d - \alpha} \\ d^2 - \alpha^2 - d + \alpha &\leqslant d\alpha^2 - \alpha^2 + \alpha \\ d - 1 &\leqslant \alpha^2 \\ \sqrt{d - 1} &\leqslant \alpha, \end{aligned}$$

which is a contradiction, completing the proof. □

Corollary 3.3.3. *Assume $c = 2$.*
If $d = 1$ then M has accepted elasticity for all α.
If $d = 2$ then M has accepted elasticity iff $\overline{\alpha} = 2$.
If $d = 3$ then M has accepted elasticity iff $\overline{\alpha} = 2$ or 3.
If $d = 4$ then M has accepted elasticity iff $\overline{\alpha} = 3$ or 4.

Proof. The above two proofs can be altered to show that M does not have accepted elasticity when
(a) d is even and $\frac{\alpha+\beta-1}{\alpha} > \alpha$, or
(b) d is odd and $\frac{\alpha+\beta-1}{\alpha} > \frac{\alpha d-\alpha+1}{d-\alpha}$.
Then algebra gives the result. □

Theorem 3.3.5. *If $c = 2$ and $d > 1$, then $\omega(M) = \infty$.*

Proof. Using the above results, it is clear that M does not have accepted elasticity when $c = 2$, $d > 1$, and $\overline{\alpha} = 1$, hence $\omega(M) = \infty$. □

3.3.3. *The Case $c = 3$.*

Lemma 3.3.2. *Let q be a prime and let S be a multiset of q-1 nonzero elements of $\mathbb{Z}_q$. Then S contains an internal sum of a for any $a \in \mathbb{Z}_q \backslash \{0\}$.*

Proof. Let $S = \{\!\{m_1, ..., m_{q-1}\}\!\}$ be a multiset, where $m_i \in \mathbb{Z}_q \backslash \{0\}$ for $i = 1, ..., q-1$. Define $n_1, ..., n_{q-1}$ as follows: let $n_1 = m_1$, and if $n_1, ..., n_{i-1}$ has been defined, define $n_i = km_i$, where k is the smallest natural number such that $km_i \notin \{n_1, ..., n_{i-1}\}$. Because q is prime, $m_i, 2m_i, ..., (q-1)m_i$ are all distinct in $\mathbb{Z}_q$, hence k exists and is less than q, since $i \leqslant q - 1$. Thus $n_1, ..., n_{q-1}$ are distinct nonzero elements of $\mathbb{Z}_q$. Therefore, every nonzero element of $\mathbb{Z}_q$, and specifically a, is contained in $\{n_1, ..., n_{p-1}\}$. Hence it suffices to show that n_i is an internal sum of S for each $i = 1, ..., p - 1$.

We will show that each n_r is an internal sum of the multiset $\{\!\{m_1, ..., m_r\}\!\}$ by induction. This is trivially true if $r = 1$. For $r > 1$, assume that n_i is an internal sum of $\{\!\{m_1, ..., m_i\}\!\}$ for each $i = 1, ..., r - 1$. Let $n_r = km_r$, where $0 < k < q$. If $k = 1$, then $n_r = m_r$, and n_r is an internal sum of $\{n_1, ..., n_r\}$. So assume that $1 < k < q$. Then $\exists s \in \{1, ..., r - 1\}$ such that $n_s = (k - 1)m_r$. From the inductive hypothesis, n_s is an internal sum of $\{\!\{m_1, ..., m_s\}\!\}$, hence $\exists \{i_1, ..., i_z\} \subset \{1, ..., s\}$ such that $m_{i_1} + \cdots + m_{i_z} = n_s$. Hence $m_{i_1} + \cdots + m_{i_z} + m_r = (k-1)m_r + m_r = km_r = n_r$, and thus n_r is an internal sum of $\{\!\{m_1, ..., m_r\}\!\}$, completing the induction.

Therefore, $n_1, ..., n_{q-1}$ are all internal sums of S, and hence a is an internal sum of S. □

Lemma 3.3.3. *Let q be a prime. Given an element $a \in \mathbb{Z}_{q^2}$, let $\overline{a}$ denote its residue class modulo q. Let $\{\!\{a_1, ..., a_{q+1}\}\!\}$ be a multiset of elements of $\mathbb{Z}_{q^2} \backslash \{0\}$ which has no internal sum in $\{q, 2q, ..., (q-1)q\}$. Then for any $i, j \in \{1, ..., q+1\}$ such that $\overline{a_i} = \overline{a_j}$, we have $a_i = a_j$.*

Proof. The internal sum condition implies that any internal sum with a residue of 0 modulo q must be 0 modulo q^2. Let $\overline{b} = \overline{a_i} = \overline{a_j}$. By lemma 3.3.2, since $\overline{b} \neq 0$, $\exists \{k_1, ..., k_n\} \subset \{1, ..., q+1\} \backslash \{i, j\}$ such that $\overline{a_{k_1}} + \cdots + \overline{a_{k_n}} = -\overline{b}$. Thus $\overline{a_i} + \overline{a_{k_1}} + \cdots + \overline{a_{k_n}} = 0 \implies a_i + a_{k_1} + \cdots + a_{k_n} = 0 \implies a_i = -(a_{k_1} + \cdots + a_{k_n})$. Similarly, $a_j = -(a_{k_1} + \cdots + a_{k_n})$, hence $a_i = a_j$. □

Lemma 3.3.4. *If a multiset A of elements of $\mathbb{Z}_{q^2} \backslash \{0\}$ have a size of at least $q+1$ and no internal sum in $q, 2q, ..., (q-1)q$. Then for any $b \in \{1, ..., q-1\}$, there are at most $q-1$ elements of A with a residue of b modulo q.*

Proof. For the sake of contradiction, suppose there are q elements $a_1, ..., a_q \in A$ such that $\overline{a_1} = \cdots = \overline{a_q}$ in $\mathbb{Z}_q$. Then from lemma 3.3.3, $a_1 = \cdots = a_q$. Hence $a_1 + \cdots + a_q = qa_1$ is an internal sum of A. Since qa_1 is a multiple of q and an internal sum of A, $qa_1 = 0$. Hence $a_1 \equiv 0 \pmod{q}$, contradiction. □

Theorem 3.3.6. *If $c = 3$ and $3 \mid d$, then $\omega(M) = \infty$.*

Proof. Suppose that the elasticity were accepted. Then, by the definition of an accepted triple and the equivalence theorem, there exist integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_{cd}$ such that

(1′) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2′) for $i = 1, ..., e$, $\mathcal{A}_i$ has no internal sum in $\{\langle c \rangle, \langle 2c \rangle, ..., \langle (d-1)c \rangle\}$
(3′) for $i = 1, ..., e$, $\sum \mathcal{A}_i = \langle 0 \rangle$
(4′) for $i = 1, ..., f$, $\sum \mathcal{B}_i = \langle -c \rangle$
(5′) $f/e = (\alpha + \beta - 1)/\alpha$.

Given an element $\langle n \rangle \in \mathbb{Z}_{cd}$, let $\overline{(n)}$ denote its residue class modulo c^2 (since $c^2 \mid cd$) and let $\overline{n}$ denote its residue class modulo c.

We claim that for $i = 1, ..., e$, $\mathcal{A}_i$ contains at most $2c-2$ nonzero elements. For assume that $\mathcal{A}_i$ did contain at least $2c-1$ nonzero elements. Since $\mathcal{A}_i$ has no internal sum in $\{\langle c \rangle, ..., \langle (d-1)c \rangle\}$, when the elements are viewed as elements of $\mathbb{Z}_{c^2}$, there is no internal sum in $\{\overline{(c)}, ..., \overline{((c-1)c)}\}$. Since when $c = 3$, we have $c + 1 < 2c - 1$, lemma 3.3.4 states that there are at most $c-1$ elements with the same nonzero residue modulo c. However, since there are $2c-1$ nonzero elements in $\mathcal{A}_i$ and $c-1$ nonzero residues modulo c, the pigeonhole principle tells us that there are three elements in $\mathcal{A}_i$ with the same nonzero residue modulo c. Since $c = 3$, this is a contradiction, proving the claim.

Now, for each $\mathcal{B}_i$, we have $\sum \mathcal{B}_i = \langle -c \rangle = \langle (d-1)c \rangle$ is not an internal sum of any $\mathcal{A}_i$, therefore each $\mathcal{B}_i$ contains at least two nonzero elements. Combining this with the above claim, we see that $f/e \leqslant c - 1 = 2$.

It now suffices to show that $(\alpha + \beta - 1)/\alpha > c - 1 = 2 \iff \beta - \alpha > 1$. Since $\overline{\alpha} = 1$, we have $\alpha = kd + 1$ for some nonnegative integer k, and so $\beta = (k+1)d$. Hence $\beta - \alpha = d - 1$. Since $3 \mid d$, we have $\beta - \alpha > 2$. Hence we always have $(\alpha + \beta - 1)/\alpha > c - 1$, completing the proof. □

Lemma 3.3.5. *Assume gcd(c, d)=1 and $d > 1$. For any $\epsilon > 0$ there exist integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_c \times \mathbb{Z}_d$ which satisfy conditions (1)-(4) of the definition of an accepted triple, and additionally satisfy*

$$(5a) \qquad \frac{f}{e} > \frac{cd\overline{\alpha} - d - \overline{\alpha} + 1}{\overline{\alpha}(d-1)} - \epsilon.$$

Proof. Using the isomorphism from theorem 3.2.1, conditions (1)-(4) become

(1a) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2a) for $i = 1, ..., e$, $\mathcal{A}_i$ has no internal sum in $\{\langle 0,1\rangle, \langle 0,2\rangle, ..., \langle 0, d-\overline{\alpha}\rangle\}$
(3a) for $i = 1, ..., e$, $\sum \mathcal{A}_i = \langle 0, 1-\overline{\alpha}\rangle$
(4a) for $i = 1, ..., f$, $\sum \mathcal{B}_i = \langle 0, -\overline{\alpha}\rangle$

Let n be any nonnegative integer. Let k be a positive integer such that $kc-d+1 \geqslant 0$. Define

$$\begin{aligned}
\mathcal{A}_{1,1} = \cdots = \mathcal{A}_{1,\overline{\alpha}(d-1)n} &= \left\{\!\!\left\{\langle -1, -\overline{\alpha}\rangle^{(c-1)}, \langle 1, \overline{\alpha}\rangle^{(c-1)}, \langle 0, -1\rangle^{(\overline{\alpha}-1)}\right\}\!\!\right\} \\
\mathcal{A}_{2,1} = \cdots = \mathcal{A}_{2,\overline{\alpha}} &= \left\{\!\!\left\{\langle 1, 0\rangle^{(c(c-1)kn)}, \langle 0, -1\rangle^{(\overline{\alpha}-1)}\right\}\!\!\right\} \\
\mathcal{B}_{1,1} = \cdots = \mathcal{B}_{1,\overline{\alpha}(c-1)(d-1)n} &= \{\!\!\{\langle -1, -\overline{\alpha}\rangle, \langle 1, 0\rangle\}\!\!\} \\
\mathcal{B}_{2,1} = \cdots = \mathcal{B}_{2,\overline{\alpha}(c-1)n} &= \left\{\!\!\left\{\langle 1, \overline{\alpha}\rangle^{(d-1)}, \langle 1, 0\rangle^{(kc-d+1)}\right\}\!\!\right\} \\
\mathcal{B}_{3,1} = \cdots = \mathcal{B}_{3,(\overline{\alpha}-1)[1+(d-1)n]} &= \left\{\!\!\left\{\langle 0, -1\rangle^{(\overline{\alpha})}\right\}\!\!\right\}
\end{aligned}$$

Then we have

$$\bigcup \mathcal{A} = \bigcup \mathcal{B} =$$

$$\left\{\!\!\left\{\langle -1, -\overline{\alpha}\rangle^{(\overline{\alpha}(c-1)(d-1)n)}, \langle 1, \overline{\alpha}\rangle^{(\overline{\alpha}(c-1)(d-1)n)}, \langle 0, -1\rangle^{(\overline{\alpha}(\overline{\alpha}-1)[1+(d-1)n])}, \langle 1, 0\rangle^{(\overline{\alpha}c(c-1)kn)}\right\}\!\!\right\},$$

so condition (1a) holds.

We will show that condition (2a) holds by contradiction. Assume that $\mathcal{A}_{1,i}$ has an internal sum in $\{\langle 0,1\rangle, ..., \langle 0, d-\overline{\alpha}\rangle\}$. Then there is a submultiset $\mathcal{S} \subset \mathcal{A}_{1,i}$ such that $\sum \mathcal{S} = \langle 0, \gamma\rangle$ for some $\gamma \in \{1, ..., d-\overline{\alpha}\}$. $\mathcal{S}$ must be of the form

$$\left\{\!\!\left\{\langle -1, -\overline{\alpha}\rangle^{(m_1)}, \langle 1, \overline{\alpha}\rangle^{(m_2)}, \langle 0, -1\rangle^{(m_3)}\right\}\!\!\right\}$$

where $m_1, m_2, m_3 \in \mathbb{Z}_{\geqslant 0}$, $m_1, m_2 \leqslant c-1$, and $m_3 \leqslant \overline{\alpha}-1$. Looking at the first coordinate of $\sum \mathcal{S}$ yields $m_2 - m_1 \equiv 0 \pmod{c}$, and the restrictions on m_1 and m_2 yield $m_1 = m_2$. Hence $\sum \mathcal{S} = \langle 0, -m_3\rangle \in \{\langle 0,1\rangle, ..., \langle 0, d-\overline{\alpha}\rangle\}$, and therefore $m_3 \geqslant \overline{\alpha}$, contradiction.

Now assume that $\mathcal{A}_{2,i}$ has an internal sum of $\langle 0, \gamma\rangle$ for some $\gamma \in \{1, ..., d-\overline{\alpha}\}$. Then there is some submultiset $\mathcal{S} \in \mathcal{B}_{2,i}$ such that $\sum \mathcal{S} = \langle 0, \gamma\rangle$. $\mathcal{S}$ must be of the form

$$\left\{\!\!\left\{\langle 1, 0\rangle^{(m_1)}, \langle 0, -1\rangle^{(m_2)}\right\}\!\!\right\}.$$

Here $m_2 \leqslant \overline{\alpha} - 1$. But looking at the second coordinate of $\sum \mathcal{S}$ yields $m_2 \geqslant \overline{\alpha}$, contradiction. Therefore, condition (2a) holds.

It is straightforward to check that conditions (3a) and (4a) also hold.

Finally, we will show that some value of n yields condition (5a). We have

$$\begin{aligned}
\frac{f}{e} &= \frac{(\overline{\alpha}(c-1)(d-1)n) + (\overline{\alpha}(c-1)n) + ((\overline{\alpha}-1)[1+(d-1)n])}{(\overline{\alpha}(d-1)n) + (\overline{\alpha})} \\
&\to \frac{\overline{\alpha}(c-1)(d-1) + \overline{\alpha}(c-1) + (\overline{\alpha}-1)(d-1)}{\overline{\alpha}(d-1)} \\
&= \frac{cd\overline{\alpha} - d - \overline{\alpha} + 1}{\overline{\alpha}(d-1)}
\end{aligned}$$

as n approaches infinity. Therefore, for some sufficiently large n, condition (5a) holds. □

Theorem 3.3.7. *If $c = 3$ and $3 \nmid d$, then $\omega(M)$ is finite. If $d \geqslant 4$, then*

$$\omega(M) \leqslant \left\lfloor \frac{d-3}{2} \right\rfloor d + 2.$$

If $d = 1$ or 2, then $\omega(M) = 1$.

Proof. From theorem 3.3.6, we know that if $3 \mid d$ then $\omega(M) = \infty$.

If $d = 1$ or 2, then theorem 3.1.2 combined with theorem 2.2.2 yields $\omega(M) = 1$. So assume $d \geqslant 4$.

From lemma 3.3.5 and theorem 1.3.4, we know that M has accepted elasticity if

$$\frac{cd\overline{\alpha} - d - \overline{\alpha} + 1}{\overline{\alpha}(d-1)} > \frac{\alpha + \beta - 1}{\alpha}.$$

Let $\alpha = kd + \overline{\alpha}$, so that $\beta = (k+1)d$. Then, plugging in $c = 3$ and rearranging terms, we get

$$\begin{aligned}
\frac{3d\overline{\alpha} - d - \overline{\alpha} + 1}{\overline{\alpha}(d-1)} &> \frac{(kd + \overline{\alpha}) + ((k+1)d) - 1}{(kd + \overline{\alpha})} \\
kd[3d\overline{\alpha} - d - \overline{\alpha} + 1] + \overline{\alpha}[3d\overline{\alpha} - d - \overline{\alpha} + 1] &> \overline{\alpha}(d-1)[2kd + \overline{\alpha} + d - 1] \\
kd[(3d\overline{\alpha} - d - \overline{\alpha} + 1) - 2\overline{\alpha}(d-1)] &> \overline{\alpha}[(d-1)(\overline{\alpha} + d - 1) - (3d\overline{\alpha} - d - \overline{\alpha} + 1)] \\
kd[d\overline{\alpha} - d + \overline{\alpha} + 1] &> \overline{\alpha}[d^2 - d - 2d\overline{\alpha}] \\
k &> \frac{\overline{\alpha}(d - 2\overline{\alpha} - 1)}{(\overline{\alpha} - 1)d + \overline{\alpha} + 1},
\end{aligned}$$

hence M has accepted elasticity when $k > \frac{\overline{\alpha}(d-2\overline{\alpha}-1)}{(\overline{\alpha}-1)d+\overline{\alpha}+1}$.

If $\overline{\alpha} > 1$, notice that

$$\begin{aligned}
\frac{\overline{\alpha}}{\overline{\alpha}-1} - \frac{\overline{\alpha}(d - 2\overline{\alpha} - 1)}{(\overline{\alpha}-1)d + \overline{\alpha} + 1} &= \frac{\frac{\overline{\alpha}}{\overline{\alpha}-1}[(\overline{\alpha}-1)d + (\overline{\alpha}-1) + 2] - \overline{\alpha}(d - 2\overline{\alpha} - 1)}{(\overline{\alpha}-1)d + \overline{\alpha} + 1} \\
&= \frac{\overline{\alpha}[(d + 1 + \frac{2}{\overline{\alpha}-1}) - (d - 2\overline{\alpha} - 1)]}{(\overline{\alpha}-1)d + \overline{\alpha} + 1} \\
&= \frac{2\overline{\alpha}(\overline{\alpha} + 1 + \frac{1}{\overline{\alpha}-1})}{(\overline{\alpha}-1)d + \overline{\alpha} + 1} \\
&> 0.
\end{aligned}$$

Hence $\frac{\overline{\alpha}}{\overline{\alpha}-1} > \frac{\overline{\alpha}(d-2\overline{\alpha}-1)}{(\overline{\alpha}-1)d+\overline{\alpha}+1}$, and, since $2 \geqslant \frac{\overline{\alpha}}{\overline{\alpha}-1}$, we conclude that M has accepted elasticity when $\overline{\alpha} \geqslant 2$ and $k \geqslant 2$.

We also know that when $\overline{\alpha} = 1$ and $k > \frac{d-3}{2}$, then M has accepted elasticity. Hence, if $\frac{d-3}{2} \geqslant 2$, then M has accepted elasticity for all $\alpha \geqslant \left\lfloor \frac{d-3}{2} \right\rfloor d + 2$. Therefore, if $d \geqslant 7$ and $3 \nmid d$, then $\omega(M) \leqslant \left\lfloor \frac{d-3}{2} \right\rfloor d + 2$.

It can be shown in the specific cases of $d = 4$ and $d = 5$ that $\omega(M) = 2$, so the desired bound is still correct. □

3.3.4. *The Case $c \geqslant 4$.*

Lemma 3.3.6. *There exist integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ which satisfy conditions (1)-(4) from the definition of an accepted triple, and additionally satisfy*

$$(5') \qquad f/e = c - 1.$$

Proof. We will let $e = d$ and $f = (c-1)d$. Let

$$\mathcal{A}_i = \left\{\!\!\left\{ \langle 1+ic\rangle^{(c-1)}, \langle -1-ic\rangle^{(c-1)}, \langle (1-\alpha)c\rangle \right\}\!\!\right\}$$

for $i = 1, ..., d$, let

$$\mathcal{B}_{i,1} = \{\!\{ \langle 1+ic\rangle, \langle -1-(i+1)c\rangle, \langle (1-\alpha)c\rangle \}\!\}$$

for $i = 1, ..., d$, and let

$$\mathcal{B}_{i,j} = \{\!\{ \langle 1+ic\rangle, \langle -1-(i+\alpha)c\rangle \}\!\}$$

for $i = 1, ..., d$ and $j = 2, ..., c-1$. Then we claim that $\mathcal{A}_i$ for $i = 1, ..., d$ and $\mathcal{B}_{i,j}$ for $i = 1, ..., d$ and $j = 1, ..., c-1$ satisfy conditions (1)-(4) and (5′).

To see that (1) holds, notice that

$$\begin{aligned}
\bigcup_{i=1}^{d} \mathcal{A}_i &= \bigcup_{i=1}^{d} \left\{\!\!\left\{ \langle 1+ic\rangle^{(c-1)}, \langle -1-ic\rangle^{(c-1)}, \langle (1-\alpha)c\rangle \right\}\!\!\right\} \\
&= \left(\bigcup_{i=1}^{d} \left\{\!\!\left\{ \langle 1+ic\rangle^{(c-1)} \right\}\!\!\right\} \right) \cup \left(\bigcup_{i=1}^{d} \left\{\!\!\left\{ \langle -1-ic\rangle^{(c-1)} \right\}\!\!\right\} \right) \cup \left(\bigcup_{i=1}^{d} \{\!\{ \langle (1-\alpha)c\rangle \}\!\} \right) \\
&= \left(\bigcup_{i=1}^{d} \{\!\{ \langle 1+ic\rangle \}\!\} \right) \cup \left(\bigcup_{i=1}^{d} \{\!\{ \langle -1-(i+1)c\rangle \}\!\} \right) \cup \left(\bigcup_{i=1}^{d} \{\!\{ \langle (1-\alpha)c\rangle \}\!\} \right) \\
&\quad \cup \left(\bigcup_{j=2}^{c-1} \bigcup_{i=1}^{d} \{\!\{ \langle 1+ic\rangle \}\!\} \right) \cup \left(\bigcup_{j=2}^{c-1} \bigcup_{i=1}^{d} \{\!\{ \langle -1-(i+\alpha)c\rangle \}\!\} \right) \\
&= \bigcup_{i=1}^{d} \bigcup_{j=1}^{c-1} \mathcal{B}_{i,j}.
\end{aligned}$$

We will show that (2) holds by contradiction. Assume (2) does not hold. Then there is some $k \in \{1, ..., d\}$ and some $m \in \{1, ..., \beta-\alpha\}$ such that $\mathcal{A}_k$ has an internal sum of $\langle mc\rangle$. Suppose $\mathcal{S} \subset \mathcal{A}_k$ is such that $\sum \mathcal{S} = \langle mc\rangle$. Then $\mathcal{S}$ is either of the form $\left\{\!\!\left\{ \langle 1+kc\rangle^{(r)}, \langle -1-kc\rangle^{(s)} \right\}\!\!\right\}$ or the form $\left\{\!\!\left\{ \langle 1+kc\rangle^{(r)}, \langle -1-kc\rangle^{(s)}, \langle (1-\alpha)c\rangle \right\}\!\!\right\}$. First suppose $\mathcal{S}$ is of the first form. Then $r\langle 1+kc\rangle + s\langle -1-kc\rangle = \langle mc\rangle$, so $(r-s) + (r-s)kc \equiv mc \pmod{cd}$. Then $c \mid r-s$. But since $r, s \in \{0, ..., c-1\}$, it must be that $r = s$. Thus $mc \equiv 0 \pmod{cd}$, and hence $m \equiv 0 \pmod{d}$, which is a contradiction since $\beta - \alpha < d$. If $\mathcal{S}$ is of the second form, we can similarly conclude that $r = s$. Then we get $(1-\alpha)c \equiv mc \pmod{cd} \implies m \equiv 1-\alpha \pmod{d}$. Since no element of $\{1, ..., \beta-\alpha\}$ has residue $1-\alpha$ modulo d, this is again a contradiction. Therefore, condition (2) holds.

Checking that conditions (3), (4), and (5') hold is routine, completing the proof. □

Theorem 3.3.8. *If $c \geqslant 4$, then $\omega(M) \leqslant \left\lceil \frac{d-1}{c-2} \right\rceil$. In particular, $\omega(M) \leqslant d-1$..*

Proof. By theorem 1.3.4 combined with lemma 3.3.6, it suffices to show that $\rho \leqslant c-1$ whenever $\alpha \geqslant (d-1)/(c-2)$. Let $\alpha = kd + \overline{\alpha}$. Since β is the least multiple of d such that $\beta \geqslant \alpha$, we have $\beta = (k+1)d$, and hence

$$\rho = \frac{\alpha + \beta - 1}{\alpha} = \frac{(2k+1)d + \overline{\alpha} - 1}{kd + \overline{\alpha}}.$$

Thus, if $k \geqslant 1$, then

$$\rho < \frac{(2k+1)d + \overline{\alpha}}{kd + \overline{\alpha}} \leqslant \frac{(2k+1)d}{kd} = \frac{2k+1}{k} \leqslant 3 \leqslant c-1.$$

Therefore, for $k \geqslant 1$, $\rho < c-1$.

Now, we will consider the case where $k = 0$, so that $\alpha = \overline{\alpha}$ and $\beta = d$. Then

$$\begin{aligned} \rho &\leqslant c-1 \\ \frac{\overline{\alpha}+d-1}{\overline{\alpha}} &\leqslant c-1 \\ d-1 &\leqslant \overline{\alpha}(c-2) \\ \frac{d-1}{c-2} &\leqslant \overline{\alpha} \end{aligned}$$

Thus for any $\alpha \geqslant (d-1)/(c-2)$, $\rho \leqslant c-1$, as desired. □

4. Noncyclic Unit Group

Assume $\mathbb{Z}_y^\times$ is noncyclic.

4.1. **General Noncyclic Case.**

Theorem 4.1.1. *$\mathbb{Z}_y^\times$ is canonically isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $n_i \mid n_{i+1}$ for $i = 1, ..., k-1$. If $ord_y(p) \mid n_{k-1}$, then M has accepted elasticity.*

Proof. Let $d = \operatorname{ord}_p(y)$, let $[p] \in \mathbb{Z}_y^\times$ represent the residue class of p modulo y, and let $\psi([p]) = \langle a_1, ..., a_k \rangle$, where $a_i \in \mathbb{Z}_{n_i}$ for $i = 1, ..., k$. Define

$$\begin{aligned} g_1 &:= \frac{n_{k-1}}{d} \\ g_2 &:= \frac{n_k}{d} \\ h_1 &:= \frac{a_{k-1}}{g_1} \\ h_2 &:= \frac{a_k}{g_2} \\ m &:= \gcd(h_1, h_2) \\ b_1 &:= \frac{h_1}{m} \\ b_2 &:= \frac{h_2}{m} \end{aligned}$$

By assumption, $d \mid n_{k-1}$, and thus $d \mid n_k$, hence $g_1, g_2 \in \mathbb{Z}$. Since $d\langle a_1, ..., a_k \rangle = \langle 0, ..., 0 \rangle$, we have $da_{k-1} \equiv 0 \pmod{n_{k-1}} \implies g_1 d \mid a_{k-1} d \implies g_1 \mid a_{k-1}$, so $h_1 \in \mathbb{Z}$. Similarly $h_2 \in \mathbb{Z}$. Hence m is well defined, and clearly $b_1, b_2 \in \mathbb{Z}$ with $\gcd(b_1, b_2)$=1. Let u, v be integers such that $ub_2 - vb_1 = 1$, and observe that $\gcd(u, v) = 1$.

From theorem 2.2.2, it suffices to assume that $\alpha = 1$. Then $\beta = d$. From theorem 1.3.1, it suffices to find positive integers e and f, along with multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ such that

(1′) $\bigcup_{i=1}^{e} \mathcal{A}_i = \bigcup_{i=1}^{f} \mathcal{B}_i$
(2′) for $j = 1, ..., e$, $\mathcal{A}_j$ has no internal product in $\{r\langle a_1, ..., a_k \rangle \mid 1 \leqslant r \leqslant d-1\}$
(3′) for $j = 1, ..., e$, $\sum \mathcal{A}_j = \langle 0, ..., 0 \rangle$
(4′) for $j = 1, ..., f$, $\sum \mathcal{B}_j = \langle -a_1, ..., -a_k \rangle$, and

$(5')$ $f/e = d$.

Define $e = 2$, $f = 2d$, and

$$\begin{aligned}
\mathcal{A}_1 &= \left\{\!\!\left\{ \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2\rangle^{(2d)} \right\}\!\!\right\} \\
\mathcal{A}_2 &= \left\{\!\!\left\{ \langle 0, ..., 0, (u-h_1)g_1, (v-h_2)g_2\rangle^{(2d)} \right\}\!\!\right\} \\
\mathcal{B}_1 = \cdots = \mathcal{B}_{2d} &= \{\!\!\{ \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2\rangle, \langle 0, ..., 0, (u-h_1)g_1, (v-h_2)g_2\rangle \}\!\!\}\,.
\end{aligned}$$

Conditions $(1')$ and $(5')$ hold trivially, hence it suffices to show that these multisets satisfy conditions $(2')$,$(3')$, and $(4')$.

Since $\mathrm{ord}_y(p) = d$, $da_i \equiv 0 \pmod{n_i}$ for $i = 1, ..., k$, we have

$$\begin{aligned}
\sum \mathcal{A}_1 &= 2d\langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2\rangle \\
&= \langle 0, ..., 0, -2ud\frac{n_{k-1}}{d}, -2vd\frac{n_k}{d}\rangle \\
&= \langle 0, ..., 0\rangle. \\
\sum \mathcal{A}_2 &= 2d\langle 0, ..., 0, (u-h_1)g_1, (v-h_2)g_2\rangle \\
&= \langle 0, ..., 0, 2(u-h_1)d\frac{n_{k-1}}{d}, 2(v-h_2)d\frac{n_k}{d}\rangle \\
&= \langle 0, ..., 0\rangle. \\
\sum \mathcal{B}_1 = \cdots = \sum \mathcal{B}_{2d} &= \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2\rangle + \\
&\quad\ \langle 0, ..., 0, (u-h_1)g_1, (v-h_2)g_2\rangle \\
&= \langle -a_1, ..., -a_{k-2}, -g_1h_1, -g_2h_2\rangle \\
&= \langle -a_1, ..., -a_k\rangle.
\end{aligned}$$

Therefore, conditions $(3')$ and $(4')$ hold.

Now, for the sake of contradiction, suppose that $\mathcal{A}_1$ had an internal sum contained in $\{r\langle a_1, ..., a_k\rangle \mid 1 \leqslant r \leqslant d-1\}$. Then there exist positive integers r, s, with $1 \leqslant r \leqslant d-1$ such that

$$r\langle a_1, ..., a_k\rangle = s\langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2\rangle.$$

Looking at the last two coordinates gives us the congruences

$$\begin{aligned}
ra_{k-1} \equiv -sug_1 \pmod{n_{k-1}} &\implies rh_1 \equiv -su \pmod{d} \\
ra_k \equiv -svg_2 \pmod{n_k} &\implies rh_2 \equiv -sv \pmod{d}
\end{aligned}$$

which gives us

$$\begin{aligned}
rh_2u &\equiv -suv \\
&\equiv rh_1v \\
rmub_2 &\equiv rmvb_1 \\
rmvb_1 + rm &\equiv rmvb_1 \\
rm &\equiv 0 \pmod{d}.
\end{aligned}$$

Therefore, $rh_1 = rmb_1 \equiv 0 \pmod{d} \implies su \equiv 0 \pmod{d}$. Similarly, $sv \equiv 0 \pmod{d}$. Then $d \mid s$, for, if it didn't, then there would be some factor of d, greater than 1, which divides both u and v, and this is impossible since $\gcd(u, v) = 1$. And since $d\langle -a_1, ..., -a_{k-2}, -ug_1, -ug_2\rangle = 0$, we have $s\langle -a_1, ..., -a_{k-2}, -ug_1, -ug_2\rangle = 0 \implies r\langle a_1, ..., a_k\rangle = 0$. Since the order of $\langle a_1, ..., a_k\rangle$ is d, this implies that $d \mid r$, which contradicts $1 \leqslant r \leqslant d-1$. Therefore, $\mathcal{A}_1$ has no internal sums contained in $\{r\langle a_1,...,a_k\rangle \mid 1 \leqslant r \leqslant d-1\}$.

If we let $u' = u - h_1$ and $v' = v - h_2$, then

$$\begin{aligned} u'b_2 - v'b_1 &= (u-h_1)b_2 - (v-h_2)b_1 \\ &= ub_2 - mb_1b_2 - vb_1 + mb_1b_2 \\ &= ub_2 - vb_1 \\ &= 1, \end{aligned}$$

and so the argument for why $\mathcal{A}_2 = \{\!\{\langle 0,...,0,u'g_1,v'g_2\rangle^{(2d)}\}\!\}$ has no internal sums contained in $\{r\langle a_1,...,a_k\rangle \mid 1 \leqslant r \leqslant d-1\}$ is nearly identical to the arument for $\mathcal{A}_1 = \{\!\{\langle -a_1,...,-a_{k-2},-ug_1,-ug_2\rangle^{(2d)}\}\!\}$. Therefore, condition $(2')$ holds, completing the proof. □

Corollary 4.1.1. *If* $y = 8, 12, 24, 63, 80, 126, 240, 252, 504, 513, 544, 1026, 1632,$ *or* 2107*, then* M *has accepted elasticity.*

Proof. For each of these values of y, when $\mathbb{Z}_y^\times$ is canonically written as $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, it happens that $n_{k-1} = n_k$, hence it is always true that $\text{ord}_y(p) \mid n_{k-1}$. □

4.2. Case Study: $\mathbb{Z}_y^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Theorem 4.2.1. *Assume* $\mathbb{Z}_y^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$*. Then the elasticity of* M *is not accepted iff* $(\mathbb{Z}_y^\times, [p], \alpha)$ *is not accepted iff*

(1) $\text{ord}_y(p) = 3$ *and* $\overline{\alpha} = 1$*, or*
(2) $\text{ord}_y(p) = 6$ *and* $\overline{\alpha} = 1$ *or* 2.

The following lemmas and corollaries are necessary before proceeding to the proof of theorem 4.2.1.

Let $y \in \mathbb{N}$ such that $\mathbb{Z}_y^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, with ψ an isomorphism mapping $\mathbb{Z}_y^\times \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, and for multisets $\mathcal{S}$ of elements of $\mathbb{Z}_y^\times$, let $\mathcal{S}'$ be the image of $\mathcal{S}$ under ψ.

Let $\bar{0} = \langle 0,0\rangle \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Then if $c \in \mathbb{Z}_3$, then $\langle \bar{0}, c\rangle, \langle a, c\rangle, \langle b, c\rangle, \langle a+b, c\rangle \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, where a and b are distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Lemma 4.2.1. *If* $(\mathbb{Z}_y^\times, [p], \alpha)$ *is accepted,* $\text{ord}_y(p) = 3$*, and* $\alpha \equiv 1 \pmod 3$*, then* $\psi([p]) = \langle \bar{0}, x\rangle$ *with* $x = 1$ *or* -1*, and* $\mathcal{A}_i'$ *takes one of the following forms:*

(1) $\{\!\{\langle a,x\rangle, \langle b,x\rangle, \langle a+b,x\rangle, \langle \bar{0},0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$
(2) $\{\!\{\langle a,-x\rangle, \langle b,-x\rangle, \langle a+b,-x\rangle, \langle \bar{0},0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$
(3) $\{\!\{\langle a,x\rangle, \langle a,-x\rangle, \langle b,x\rangle, \langle b,-x\rangle, \langle \bar{0},0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$
(4) $\{\!\{\langle a,x\rangle, \langle a,-x\rangle, \langle b,0\rangle^{2m}, \langle \bar{0},0\rangle^n\}\!\}$, $m,n \in \mathbb{N}_o$
(5) $\{\!\{\langle a,x\rangle, \langle b,-x\rangle, \langle a+b,0\rangle^{2m+1}, \langle \bar{0},0\rangle^n\}\!\}$, $m,n \in \mathbb{N}_o$*, or*
(6) $\{\!\{\langle a,0\rangle^j, \langle b,0\rangle^k, \langle a+b,0\rangle^l, \langle \bar{0},0\rangle^n\}\!\}$, $j \equiv k \equiv l \pmod 2$, $n \in \mathbb{N}_o$,

where a *and* b *are distinct nonzero elements of* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Suppose $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, $\text{ord}_y(p) = 3$, and $\alpha \equiv 1 \pmod 3$. Then there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_y^\times$ which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $i \in \{1, ..., e\}$. Since $\alpha \equiv 1 \pmod 3$, and $\beta(\mathbb{Z}_y^\times, [p], \alpha) = m\text{ord}_y(p)$ for some positive integer m such that $m\text{ord}_y(p) \geqslant \alpha > (m-1)\text{ord}_y(p)$, then $\beta(\mathbb{Z}_y^\times, [p], \alpha) = \alpha + 2$. By condition $(2')$ of theorem 1.3.2, we have for $j = 1, ..., e$, $\mathcal{A}_j'$ has no internal sum in $\{\psi([p]), \psi([p]^2)\}$. Further, by conditions (3′) and (4′) of theorem 1.3.2, we have $\sum \mathcal{A}'_j = \psi([p]^{1-\alpha}) = \psi([1]) = \langle \bar{0}, 0\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}'_i = \psi([p]^{-\alpha}) = \psi([p]^{-1}) = \psi([p]^2)$ for $i = 1, ..., f$. Note that if $\psi([p]) = \langle a, 0\rangle$ for some $a \neq \bar{0}$, then $\psi([p]^2) = \langle \bar{0}, 0\rangle$, and $\mathrm{ord}_y(p) = 2$. If $\psi([p]) = \langle a, x\rangle$ with $a \neq \bar{0}, x \neq 0$, then $\psi([p]^3) = \langle a, 0\rangle$, and $\mathrm{ord}_y(p) = 6$. If $\psi([p]) = \langle \bar{0}, x\rangle$ with $x \neq 0$, then $\psi([p]^3) = \langle \bar{0}, 0\rangle$ and $\mathrm{ord}_y(p) = 3$. So fix $\psi([p]) = \langle \bar{0}, x\rangle$. Note that for all $n \in \mathbb{N}_o$, inserting $\langle \bar{0}, 0\rangle^n$ into any of the following arguments does not change any internal sums of the $\mathcal{A}'_i$, nor does it change $\sum \mathcal{A}'_i$ as a whole. So $\langle \bar{0}, 0\rangle^{n_i} \in \mathcal{A}'_i$ for $i = 1, ..., e$, $n_i \geqslant 0$.

(1) Suppose $\mathcal{A}'_i$ contains more than two elements with a $\mathbb{Z}_3$ component of x. Since $\langle a, x\rangle^2 = \langle \bar{0}, -x\rangle = \psi([p]^2)$ for all $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, then no $\langle a, x\rangle$ occurs twice in $\mathcal{A}'_i$ by (2′) of theorem 1.3.2. But $\mathcal{A}'_i$ contains more than two elements with x as the $\mathbb{Z}_3$ component by assumption, so $\langle a, x\rangle, \langle b, x\rangle, \langle a + b, x\rangle \in \mathcal{A}'_i$. And $\langle a, -x\rangle\langle b, x\rangle\langle a + b, x\rangle = \langle a, 0\rangle\langle a, x\rangle = \langle \bar{0}, x\rangle = \psi([p])$, so $\langle a, -x\rangle, \langle a, 0\rangle \notin \mathcal{A}'_i$ for all $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, and hence $\mathcal{A}'_i = \{\!\{\langle a, x\rangle, \langle b, x\rangle,$
$\langle a + b, x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$, with a and b distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) Similarly, $\langle a, -x\rangle^2 = \langle \bar{0}, x\rangle = \psi([p])$ and $\langle a, x\rangle\langle b, -x\rangle\langle a + b, -x\rangle = \langle a, 0\rangle$
$\langle a, -x\rangle = \langle \bar{0}, -x\rangle = \psi([p]^2)$ for all $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, so by (2′) of theorem 1.3.2, if $\mathcal{A}'_i$ contains more than two elements having $\mathbb{Z}_3$ component equal to $-x$, then $\langle a, -x\rangle^2, \langle a, x\rangle, \langle a, 0\rangle \notin \mathcal{A}'_i$ for all $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, and therefore $\mathcal{A}'_i = \{\!\{\langle a, -x\rangle, \langle b, -x\rangle,$
$\langle a + b, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$, with a and b distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(3) If $\mathcal{A}'_i$ contains exactly two elements with $\mathbb{Z}_3$ component equal to x, then $\mathcal{A}'_i$ must also contain two elements with a $\mathbb{Z}_3$ component of $-x$ to obtain $\sum \mathcal{A}'_i = \langle \bar{0}, 0\rangle$. Say $\langle a, x\rangle, \langle b, x\rangle \in \mathcal{A}'_i$ for a and b distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$, then $\langle a + b, -x\rangle \notin \mathcal{A}'_i$ as shown in part (1). So $\langle a, -x\rangle, \langle b, -x\rangle \in \mathcal{A}'_i$. Further, $\langle a, 0\rangle, \langle b, 0\rangle, \langle a + b, 0\rangle \notin \mathcal{A}'_i$ by (2′) of theorem 1.3.2 since $\langle a, 0\rangle\langle a, x\rangle = \langle b, 0\rangle\langle b, x\rangle = \langle a + b, 0\rangle\langle a, -x\rangle\langle b, -x\rangle = \langle \bar{0}, x\rangle = \psi([p])$.

(4) Now suppose $\mathcal{A}'_i$ contains exactly one element having a $\mathbb{Z}_3$ component equal to x. Then since $\sum \mathcal{A}'_i = \langle \bar{0}, 0\rangle$ by (3′) of theorem 1.3.2, $\mathcal{A}'_i$ contains $3n + 1$ elements with $-x$ as their $\mathbb{Z}_3$ component for some $n \in \mathbb{N}_o$. But $\mathcal{A}'_i$ may contain at most three elements of this form, so $\mathcal{A}'_i$ contains exactly one such element. If $\langle a, x\rangle, \langle a, -x\rangle \in \mathcal{A}'_i$ for some $a \neq \bar{0}$, then $\langle a, 0\rangle \notin \mathcal{A}'_i$ since $\langle a, 0\rangle\langle a, x\rangle = \langle \bar{0}, x\rangle = \psi([p])$. If $\langle b, 0\rangle \in \mathcal{A}'_i$ for some $b \neq \bar{0}, a$, then $\langle a + b, 0\rangle \notin \mathcal{A}'_i$ since $\langle a, x\rangle\langle b, 0\rangle\langle a + b, 0\rangle = \langle \bar{0}, x\rangle = \psi([p])$. And $\sum \mathcal{A}'_i = \langle \bar{0}, 0\rangle = \sum \{\!\{\langle a, x\rangle, \langle a, -x\rangle, \langle b, 0\rangle^{2m}\}\!\}$ for $m \in \mathbb{N}_o$, with a and b distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(5) If still $\mathcal{A}'_i$ contains exactly one element having x as its $\mathbb{Z}_3$, but now $\langle a, x\rangle \in \mathcal{A}'_i$ and $\langle a, -x\rangle \notin \mathcal{A}'_i$ for some $a \neq \bar{0}$, then let $\langle b, -x\rangle \in \mathcal{A}'_i$ with $b \neq \bar{0}, a$. Then $\langle a, 0\rangle, \langle b, 0\rangle \notin \mathcal{A}'_i$ by (2′) of theorem 1.3.2, but $\langle a + b, 0\rangle \in \mathcal{A}'_i$ since $\langle a, x\rangle\langle b, x\rangle \neq \langle \bar{0}, 0\rangle$ and $\langle a+b, 0\rangle$ is the only element which can yet be a part of this $\mathcal{A}'_i$ under these conditions. To maintain $\sum \mathcal{A}'_i = \langle \bar{0}, 0\rangle$, we can have $\langle a + b, 0\rangle^{2m+1} \in \mathcal{A}'_i$ for $m \in \mathbb{N}_o$, so $\mathcal{A}'_i = \{\!\{\langle a, x\rangle, \langle b, -x\rangle, \langle a + b, 0\rangle^{2m+1},$
$\langle \bar{0}, 0\rangle^n\}\!\}$.

(6) Suppose now each element of $\mathcal{A}'_i$ has $\mathbb{Z}_3$ component equal to 0. So $\mathcal{A}'_i = \{\!\{\langle a, 0\rangle^j, \langle b, 0\rangle^k, \langle a + b, 0\rangle^l\}\!\}$ for some $j, k, l \in \mathbb{N}_o$ and a and b distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathcal{A}'_i$ has no internal sums equal to $\psi([p])$ or $\psi([p]^2)$. Without loss of generality, suppose $j \equiv 1 \pmod 2$, so $\langle a, 0\rangle^j = \langle a, 0\rangle$. If

$k \equiv l \equiv 0 \pmod 2$, then $\langle b, 0\rangle^k = \langle a+b, 0\rangle^l = \langle \bar{0}, 0\rangle$, and $\sum \mathcal{A}_i' = \langle a, 0\rangle$. So let $k \equiv 1 \pmod 2$. Then $\langle a, 0\rangle^j \langle b, 0\rangle^k = \langle a+b, 0\rangle$, and we must also have $l \equiv 1 \pmod 2$ to have $\sum \mathcal{A}_i' = \langle a, 0\rangle^j \langle b, 0\rangle^k \langle a+b, 0\rangle^l = \langle \bar{0}, 0\rangle$. Conversely, if $j \equiv 0 \pmod 2$, then $\langle a, 0\rangle^j = \langle \bar{0}, 0\rangle$, and we must have $\langle b, 0\rangle^k \langle a+b, 0\rangle^l = \langle \bar{0}, 0\rangle$, and hence $k \equiv l \equiv 0 \pmod 2$. In either case, $j \equiv k \equiv l \pmod 2$.

□

Lemma 4.2.2. *If* $(\mathbb{Z}_y^\times, [p], \alpha)$ *is accepted,* $ord_y(p) = 6$*, and* $\alpha \equiv 1 \pmod 6$*, then* $\psi([p]) = \langle a, x\rangle$ *with* $x = 1$ *or* -1*, and* $\mathcal{A}_i'$ *takes one of the following forms:*

(1) $\{\!\{\langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$*, or*

(2) $\{\!\{\langle b, 0\rangle^{2m}, \langle \bar{0}, 0\rangle^n\}\!\}$, $m, n \in \mathbb{N}_o$,

where a *and* b *are distinct nonzero elements of* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Suppose $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, $\mathrm{ord}_y(p) = 6$, and $\alpha \equiv 1 \pmod 6$. Then there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of $\mathbb{Z}_y^\times$ which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $i \in \{1, ..., e\}$. Since $\alpha \equiv 1 \pmod 6$, and $\beta(\mathbb{Z}_y^\times, [p], \alpha) = m\mathrm{ord}_y(p)$ for some positive integer m such that $m\mathrm{ord}_y(p) \geqslant \alpha > (m-1)\mathrm{ord}_y(p)$, then $\beta(\mathbb{Z}_y^\times, [p], \alpha) = \alpha + 5$. By ($2'$) of theorem 1.3.2, $\mathcal{A}_i'$ has no internal sum in $\{\psi([p]), \psi([p]^2), ..., \psi([p]^5)\} = \{\langle a, x\rangle, \langle \bar{0}, -x\rangle, \langle a, 0\rangle, \langle \bar{0}, x\rangle, \langle a, -x\rangle\}$. Further, by conditions ($3'$) and ($4'$) of theorem 1.3.2, we have $\sum \mathcal{A}_j' = \psi([p]^{1-\alpha}) = \psi([1]) = \langle \bar{0}, 0\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}_i' = \psi([p]^{-\alpha}) = \psi([p]^5) = \langle a, -x\rangle$ for $i = 1, ..., f$. It can be seen then that the only elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ which can be in $\mathcal{A}_i'$ are of the form $\langle b, 0\rangle, \langle b, x\rangle, \langle b, -x\rangle$, or $\langle \bar{0}, 0\rangle$ for some $b \neq \bar{0}, a$. Note that of these, only $\langle b, 0\rangle, \langle \bar{0}, 0\rangle$ may be repeated within the same $\mathcal{A}_i'$ since $\langle b, x\rangle^2 = \langle \bar{0}, -x\rangle = \psi([p]^2)$, $\langle b, -x\rangle^2 = \langle \bar{0}, x\rangle = \psi([p]^4)$. Further, for all $n \in \mathbb{N}_o$, inserting $\langle \bar{0}, 0\rangle^n$ into any of the following arguments does not change any internal sums of $\mathcal{A}_i'$, nor does it change $\sum \mathcal{A}_i'$. So $\langle \bar{0}, 0\rangle^{n_i} \in \mathcal{A}_i'$ for $i = 1, ..., e$, $n_i \geqslant 0$.

(1) If $\langle b, x\rangle \in \mathcal{A}_i'$ then: $\langle b, 0\rangle \notin \mathcal{A}_i'$ since $\langle b, 0\rangle\langle b, x\rangle = \langle \bar{0}, x\rangle$, and $\langle a+b, c\rangle \notin \mathcal{A}_i'$ for any $c \in \{0, 1, 2\}$ since $\langle a+b, c\rangle\langle b, x\rangle = \langle a, c+x\rangle \in \{\langle a, 0\rangle, \langle a, x\rangle, \langle a, -x\rangle\} \subseteq \{\psi([p]), \psi([p]^2), ..., \psi([p]^5)\}$. We must have $\langle b, -x\rangle \in \mathcal{A}_i'$ to have $\sum \mathcal{A}_i' = \langle \bar{0}, 0\rangle$. So $\langle b, x\rangle \in \mathcal{A}_i'$ iff $\langle b, -x\rangle \in \mathcal{A}_i'$ iff $\mathcal{A}_i' = \{\!\{\langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$ for $b \neq \bar{0}, a \in \mathbb{Z}_2 \times \mathbb{Z}_2$, $n \in \mathbb{N}_o$.

(2) If $\langle b, 0\rangle \in \mathcal{A}_i'$ for some $b \neq \bar{0}, a$ then $\langle a+b, 0\rangle \notin \mathcal{A}_i'$ since $\langle a+b, 0\rangle\langle b, 0\rangle = \langle a, 0\rangle$. Then $\mathcal{A}_i' = \{\!\{\langle b, 0\rangle^t, \langle \bar{0}, 0\rangle^n\}\!\}$ for some $t, n \in \mathbb{N}_0$, and since $\sum \mathcal{A}_i' = \langle \bar{0}, 0\rangle$, then $t = 2m$ for some m.

□

Lemma 4.2.3. *If* $(\mathbb{Z}_y^\times, [p], \alpha)$ *is accepted,* $ord_y(p) = 6$*, and* $\alpha \equiv 2 \pmod 6$*, then* $\psi([p]) = \langle a, x\rangle$ *with* $x = 1$ *or* -1*, and* $\mathcal{A}_i'$ *takes one of the following forms:*

(1) $\{\!\{\langle a, -x\rangle, \langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$

(2) $\{\!\{\langle a, -x\rangle, \langle b, 0\rangle^{2m}, \langle \bar{0}, 0\rangle^n\}\!\}$, $m, n \in \mathbb{N}_o$

(3) $\{\!\{\langle b, x\rangle, \langle a+b, x\rangle, \langle \bar{0}, 0\rangle^n\}\!\}$, $n \in \mathbb{N}_o$*, or*

(4) $\{\!\{\langle b, -x\rangle, \langle a+b, 0\rangle^{2m+1}, \langle \bar{0}, 0\rangle^n\}\!\}$, $m, n \in \mathbb{N}_o$,

where a *and* b *are distinct nonzero elements of* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Suppose $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, $\mathrm{ord}_y(p) = 6$, and $\alpha \equiv 2 \pmod 6$. Then there exist positive integers e, f and multisets $\mathcal{A}_1, ..., \mathcal{A}_e, \mathcal{B}_1, ..., \mathcal{B}_f$ of elements of

$\mathbb{Z}_y^\times$ which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $i \in \{1, ..., e\}$. Since $\alpha \equiv 2 \pmod 6$, and $\beta(\mathbb{Z}_y^\times, [p], \alpha) = m\text{ord}_y(p)$ for some positive integer m such that $m\text{ord}_y(p) \geqslant \alpha > (m-1)\text{ord}_y(p)$, then $\beta(\mathbb{Z}_y^\times, [p], \alpha) = \alpha+4$. By ($2'$) of theorem 1.3.2, $\mathcal{A}_i'$ has no internal sum in $\{\psi([p]), \psi([p]^2), \psi([p]^3), \psi([p]^4)\} = \{\langle a, x\rangle, \langle \bar{0}, -x\rangle, \langle a, 0\rangle, \langle \bar{0}, x\rangle\}$. Further, by ($3'$) and ($4'$) of theorem 1.3.2, we have $\sum \mathcal{A}_j' = \psi([p]^5) = \langle a, -x\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}_i' = \psi([p]^4) = \langle \bar{0}, x\rangle$ for $i = 1, ..., f$. It can be seen then that the only elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ which can be in $\mathcal{A}_i'$ are of the form $\langle a, -x\rangle, \langle b, 0\rangle, \langle b, x\rangle, \langle b, -x\rangle$, or $\langle \bar{0}, 0\rangle$ for $b \neq \bar{0}, a$. As before, only $\langle b, 0\rangle, \langle \bar{0}, 0\rangle$ may be repeated within the same $\mathcal{A}_i'$, and $\langle \bar{0}, 0\rangle^{n_i} \in \mathcal{A}_i'$ for $i = 1, ..., e$, $n_i \geqslant 0$.

1. Suppose $\langle a, -x\rangle, \langle b, x\rangle \in \mathcal{A}_i'$ for some $b \neq \bar{0}, a$. Then $\langle b, 0\rangle, \langle a+b, x\rangle, \langle a+b, 0\rangle, \langle a+b, -x\rangle \notin \mathcal{A}_i'$ since $\langle b, x\rangle\langle b, 0\rangle = \langle a, -x\rangle\langle b, x\rangle\langle a+b, x\rangle = \langle \bar{0}, x\rangle$, $\langle b, x\rangle\langle a+b, 0\rangle = \langle a, x\rangle$, $\langle b, x\rangle\langle a+b, -x\rangle = \langle a, 0\rangle$. And $\langle a, -x\rangle^2, \langle b, x\rangle^2 \notin \mathcal{A}_i'$ but $\langle a, -x\rangle\langle b, x\rangle \neq \langle a, -x\rangle$, so $\langle b, -x\rangle \in \mathcal{A}_i'$, and $\mathcal{A}_i' = \{\!\!\{\langle a, -x\rangle, \langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\!\}$ with $n \in \mathbb{N}_o$, and $\sum \mathcal{A}_i' = \langle a, -x\rangle$.
2. Suppose now $\langle a, -x\rangle \in \mathcal{A}_i'$ and $\langle b, x\rangle \notin \mathcal{A}_i'$ for $b \neq \bar{0}, a$. If $\langle b, -x\rangle \in \mathcal{A}_i'$ then $\langle a+b, x\rangle, \langle a+b, 0\rangle, \langle a+b, -x\rangle, \langle b, 0\rangle \notin \mathcal{A}_i'$ since $\langle a+b, x\rangle\langle b, -x\rangle = \langle a, 0\rangle$, $\langle a+b, 0\rangle\langle b, -x\rangle\langle a, -x\rangle = \langle \bar{0}, x\rangle$, $\langle b, -x\rangle\langle b, 0\rangle = \langle \bar{0}, -x\rangle$, $\langle b, -x\rangle\langle a+b, -x\rangle = \langle a, x\rangle$. Then $\langle b, x\rangle \in \mathcal{A}_i'$ for $\sum \mathcal{A}_i' = \langle a, -x\rangle$, but we assumed differently so $\langle b, x\rangle, \langle b, -x\rangle \notin \mathcal{A}_i'$ for $b \neq a, \bar{0}$. If $\mathcal{A}_i' = \{\!\!\{\langle a, -x\rangle, \langle \bar{0}, 0\rangle^n\}\!\!\}$, then $\sum \mathcal{A}_i' = \langle a, -x\rangle$. Also, if $\langle b, 0\rangle^{2m} \in \mathcal{A}_i'$ for some m, then $\langle a+b, 0\rangle \notin \mathcal{A}_i'$ since $\langle b, 0\rangle\langle a+b, 0\rangle = \langle a, 0\rangle$, and $\mathcal{A}_i' = \big\{\!\!\big\{\langle a, -x\rangle, \langle b, 0\rangle^{2m}, \langle \bar{0}, 0\rangle^n\big\}\!\!\big\}$ with $\sum \mathcal{A}_i' = \langle a, -x\rangle$ still.
3. If $\langle a, -x\rangle \in \mathcal{A}_i'$ then $\mathcal{A}_i'$ is as in (1) or (2) above. So let $\langle a, -x\rangle \notin \mathcal{A}_i'$, and $\langle b, x\rangle \in \mathcal{A}_i'$. If $\langle b, -x\rangle \in \mathcal{A}_i'$ then we must also have $\langle a, -x\rangle \in \mathcal{A}_i'$, so $\langle b, -x\rangle \notin \mathcal{A}_i'$. So the only remaining option is to have $\langle a+b, x\rangle \in \mathcal{A}_i'$ by the argument in (1) above. And $\langle b, x\rangle\langle a+b, x\rangle = \langle a, -x\rangle$, so this is sufficient and $\mathcal{A}_i' = \{\!\!\{\langle b, x\rangle, \langle a+b, x\rangle, \langle \bar{0}, 0\rangle^n\}\!\!\}$ for some $n \in \mathbb{N}_o$.
4. Now let $\langle b, -x\rangle \in \mathcal{A}_i'$, $\langle a, -x\rangle \notin \mathcal{A}_i'$ for some $b \neq \bar{0}, a$. So $\langle b, x\rangle \notin \mathcal{A}_i'$, and as shown in (2) above, the only other element which may be in $\mathcal{A}_i'$ is $\langle a+b, 0\rangle$. Note $\langle b, -x\rangle\langle a+b, 0\rangle = \langle a, -x\rangle$, and $\langle a+b, 0\rangle^{2m} = \langle \bar{0}, 0\rangle$, so $\mathcal{A}_i' = \big\{\!\!\big\{\langle b, -x\rangle, \langle a+b, 0\rangle^{2m+1}, \langle \bar{0}, 0\rangle^n\big\}\!\!\big\}$ for some $m, n \in \mathbb{N}_o$.

Note that if $\langle a, -x\rangle, \langle b, x\rangle, \langle b, -x\rangle \notin \mathcal{A}_i'$ for $b \neq a, \bar{0}, i \in \{1, ..., e\}$ then $\sum \mathcal{A}_i' \neq \langle a, -x\rangle$, so there are no other cases. □

Definition 4.2.1. *Given p, α from $(\mathbb{Z}_y^\times, [p], \alpha)$, and $\langle x, y, z\rangle \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, if $ord_y(p) > 2$, $\alpha \equiv \pm 1 \pmod 3$, and $\psi([p]) = \langle p_1, p_2, p_3\rangle$ so $\psi([p]^{-\alpha}) = (-\alpha)\psi([p]) = \langle -\alpha p_1, -\alpha p_2, -\alpha p_3\rangle$, then define a function $W : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{R}$ and let the* weight *of $\langle x, y, z\rangle$ be given by*

$$W(\langle x, y, z\rangle) = \begin{cases} 0 & \textit{if} \quad z = 0 \\ \frac{1}{2} & \textit{if} \quad z \equiv \alpha p_3 \pmod 3 \\ 1 & \textit{if} \quad z \equiv -\alpha p_3 \pmod 3 \end{cases}$$

Since $ord_y(p) > 2$, then $p_3 \equiv \pm 1 \pmod 3$; with $\alpha \equiv \pm 1 \pmod 3$ also, then $\alpha p_3 \not\equiv -\alpha p_3 \pmod 3$, and this function is well-defined.

If $A = \{\!\{\langle x_1, y_1, z_1\rangle, ..., \langle x_n, y_n, z_n\rangle\}\!\}$ is a multiset in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, then let the weight *of A, denoted $W(A)$, be given by*

$$W(A) = \sum_{i=1}^{n} W(\langle x_i, y_i, z_i\rangle).$$

Note that for multisets $S_1, ..., S_n$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $W(\cup_{i=1}^{n} S_n) = \sum_{i=1}^{n} W(S_n)$. Also, if $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted then $W(\mathcal{B}_i') \geqslant 1$ for $i = 1, ..., f$.

Corollary 4.2.1. *If $ord_y(p) = 3$, $\alpha \equiv 1 \pmod 3$, $\psi([p])$ is given to be $\langle \bar{0}, x\rangle$ with $x = \pm 1$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted then $W(\mathcal{A}_i') \leqslant 3$ for $i = 1, ..., e$, and $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant 3e$.*

Proof. If $\mathrm{ord}_y(p) = 3$, $\alpha \equiv 1 \pmod 3$, $\psi([p]) = \langle \bar{0}, x\rangle$ with $x = \pm 1$ and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then lemma 4.2.1 holds, and $\mathcal{A}_i'$ is restricted to one of six forms:

(1) $W(\{\!\{\langle a, x\rangle, \langle b, x\rangle, \langle a+b, x\rangle\}\!\}) = 1.5$,
(2) $W(\{\!\{\langle a, -x\rangle, \langle b, -x\rangle, \langle a+b, -x\rangle\}\!\}) = 3$,
(3) $W(\{\!\{\langle a, x\rangle, \langle a, -x\rangle, \langle b, x\rangle, \langle b, -x\rangle\}\!\}) = 3$,
(4) $W(\{\!\{\langle a, x\rangle, \langle a, -x\rangle, \langle b, 0\rangle^{2m}\}\!\}) = 1.5$,
(5) $W(\{\!\{\langle a, x\rangle, \langle b, -x\rangle, \langle a+b, 0\rangle^{2m+1}\}\!\}) = 1.5$,
(6) $W(\{\!\{\langle a, 0\rangle^{j}, \langle b, 0\rangle^{k}, \langle a+b, 0\rangle^{l}\}\!\}) = 0$.

So $W(\mathcal{A}_i') \leqslant 3$, hence $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant \sum_{i=1}^{e} 3 = 3e$. □

Corollary 4.2.2. *If $ord_y(p) = 6$, $\alpha \equiv 1 \pmod 6$, $\psi([p])$ is given to be $\langle a, x\rangle$ with $a \neq \bar{0}, x = \pm 1$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted then $W(\mathcal{A}_i') \leqslant 1.5$ for $i = 1, ..., e$, and $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant 1.5e$.*

Proof. If $\mathrm{ord}_y(p) = 6$, $\alpha \equiv 1 \pmod 6$, $\psi([p]) = \langle a, x\rangle$ with $a \neq \bar{0}, x = \pm 1$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then lemma 4.2.2 holds, and $\mathcal{A}_i'$ is restricted to one of two forms:

(1) $W(\{\!\{\langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^{n}\}\!\}) = 1.5$,
(2) $W(\{\!\{\langle b, 0\rangle^{2m}, \langle \bar{0}, 0\rangle^{n}\}\!\}) = 0$.

So $W(\mathcal{A}_i') \leqslant 1.5$, hence $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant \sum_{i=1}^{e} 1.5 = 1.5e$. □

Corollary 4.2.3. *If $ord_y(p) = 6$, $\alpha \equiv 2 \pmod 6$, $\psi([p])$ is given to be $\langle a, x\rangle$ with $a \neq \bar{0}, x = \pm 1$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted then $W(\mathcal{A}_i') \leqslant 2$ for $i = 1, ..., e$, and $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant 2e$.*

Proof. If $\mathrm{ord}_y(p) = 6$, $\alpha \equiv 2 \pmod 6$, $\psi([p]) = \langle a, x\rangle$ with $a \neq \bar{0}, x = \pm 1$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then lemma 4.2.3 holds, and $\mathcal{A}_i'$ is restricted to one of four forms:

(1) $W(\{\!\{\langle a, -x\rangle, \langle b, x\rangle, \langle b, -x\rangle, \langle \bar{0}, 0\rangle^{n}\}\!\}) = 2$,
(2) $W(\{\!\{\langle a, -x\rangle, \langle b, 0\rangle^{2m}, \langle \bar{0}, 0\rangle^{n}\}\!\}) = .5$,
(3) $W(\{\!\{\langle b, x\rangle, \langle a+b, x\rangle, \langle \bar{0}, 0\rangle^{n}\}\!\}) = 2$,
(4) $W(\{\!\{\langle b, -x\rangle, \langle a+b, 0\rangle^{2m+1}, \langle \bar{0}, 0\rangle^{n}\}\!\}) = .5$.

So $W(\mathcal{A}_i') \leqslant 2e$, hence $\sum_{i=1}^{e} W(\mathcal{A}_i') \leqslant \sum_{i=1}^{e} 2 = 2e$. □

Lemma 4.2.4. *If $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then $\sum_{i=1}^{e} |A_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}| \geqslant 2\rho e$, where $\rho = \frac{\alpha+\beta-1}{\alpha}$ is the elasticity of $M(p^\alpha x, p^\alpha y)$.*

Proof. If $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then by condition (5) from the definition of an accepted triple, $f/e = (\alpha + \beta - 1)/\alpha = \rho$. By condition (1) from the definiton of an accepted triple, $\bigcup_{i=1}^e \mathcal{A}_i = \bigcup_{j=1}^f \mathcal{B}_j$, so $\bigcup_{i=1}^e (\mathcal{A}_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}) = \bigcup_{j=1}^f (\mathcal{B}_j - \{\!\{\langle \bar{0}, 0\rangle^{n_j}\}\!\})$. Then $\sum_{i=1}^e |\mathcal{A}_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}\,| = \sum_{j=1}^f |\mathcal{B}_j - \{\!\{\langle \bar{0}, 0\rangle^{n_j}\}\!\}\,| \geqslant 2f$ since $|\mathcal{B}_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}\,| \geqslant 2$ for all $i = 1, ..., f$. So $\sum_{i=1}^e |\mathcal{A}_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}\,| \geqslant 2f = 2\rho e$. □

Lemma 4.2.5. *If $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, $ord_y(p) > 2$ and $\alpha \equiv \pm 1 \pmod 3$, then $\sum_{i=1}^e W(\mathcal{A}'_i) \geqslant \rho e$, where $\rho = \frac{\alpha+\beta-1}{\alpha}$ is the elasticity of $M(p^\alpha x, p^\alpha y)$.*

Proof. If $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then by $(5')$ of theorem 1.3.2, $f/e = \rho$, so $\rho e = f$. And since $1 \leqslant W(\mathcal{B}'_i)$, then $\rho e = f = \sum_{i=1}^f 1 \leqslant \sum_{i=1}^f W(\mathcal{B}'_i) = W(\bigcup_{i=1}^f \mathcal{B}'_i) = W(\bigcup_{i=1}^e \mathcal{A}'_i) = \sum_{i=1}^e W(\mathcal{A}'_i)$ by $(1')$ of theorem 1.3.2. □

Corollary 4.2.4. *$(\mathbb{Z}_y^\times, [p], \alpha)$ is not accepted if one of the following is true:*

(1) $ord_y(p) = 3$, $\overline{\alpha} = 1$,
(2) $ord_y(p) = 6$, $\overline{\alpha} = 1$, or
(3) $ord_y(p) = 6$, $\overline{\alpha} = 2$.

Proof. By way of contradiction, suppose $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted.

(1) Let $\mathrm{ord}_y(p) = 3$, $\alpha \equiv 1 \pmod 3$. By corollary 4.2.1, since $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted, then $\sum_{i=1}^e W(\mathcal{A}'_i) \leqslant 3e$. If this is true, then by lemma 4.2.1 we have $|A_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}\,| \leqslant 4$ for $i = 1, ..., e$, and we get $2\rho e \leqslant \sum_{i=1}^e |A_i - \{\!\{\langle \bar{0}, 0\rangle^{n_i}\}\!\}\,| \leqslant 4e$ by lemma 4.2.4, so $2\rho \leqslant 4$ and $\rho \leqslant 2$. But $\beta = \alpha + 2$ by lemma 4.2.1, so $\rho = (\alpha + \beta - 1)/\alpha = (2\alpha + 1)/\alpha > 2$, and this is a contradiction, so $(\mathbb{Z}_y^\times, [p], \alpha)$ is not accepted.

(2) Let $\mathrm{ord}_y(p) = 6$, $\alpha \equiv 1 \pmod 6$. So $\beta = \alpha + 5$ by lemma 4.2.2, and $\rho = (\alpha+\beta-1)/\alpha = (2\alpha+4)/\alpha > 2$. Then we have $2e < \rho e \leqslant \sum_{i=1}^e W(\mathcal{A}'_i) \leqslant 1.5e$ by lemma 4.2.5 and corollary 4.2.2, and this is a contradiction so $(\mathbb{Z}_y^\times, [p], \alpha)$ is not accepted.

(3) Let $\mathrm{ord}_y(p) = 6$, $\alpha \equiv 2 \pmod 6$. So $\beta = \alpha + 4$ by lemma 4.2.3, and $\rho = (\alpha+\beta-1)/\alpha = (2\alpha+3)/\alpha > 2$. Then we have $2e < \rho e \leqslant \sum_{i=1}^e W(\mathcal{A}'_i) \leqslant 2e$ by lemma 4.2.5 and corollary 4.2.3, and this is a contradiction so $(\mathbb{Z}_y^\times, [p], \alpha)$ is not accepted.

□

We are now able to prove theorem 4.2.1.

Proof of Theorem 4.2.1. The if statement is done by corollary 4.2.4, so we begin proving the only if statement by contradiction.

(1) If $\mathrm{ord}_y(p) = 1$, then $p^\alpha \equiv 1 \pmod y$ for all α, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted by theorem 2.1.1.

(2) If $\mathrm{ord}_y(p) = 2$, then $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted by theorem **??**.

(3) Let $\mathrm{ord}_y(p) = 3$, and fix $\psi([p]) = \langle \bar{0}, x\rangle$ with $x \neq 0$.

If $\alpha \equiv 0 \pmod 3$, then $p^\alpha \equiv 1 \pmod y$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted by theorem 2.1.1.

If $\alpha \equiv 2 \pmod 3$, then $\beta = \alpha + 1$, so $\rho = (\alpha + \beta - 1)/\alpha = 2\alpha/\alpha = 2$. By $(3')$ of theorem 1.3.2, $\sum \mathcal{A}'_j = \psi([p]^{1-\alpha}) = \psi([p]^2) = \langle \bar{0}, -x\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}'_j = \psi([p]^{-\alpha}) = \psi([p]) = \langle \bar{0}, x\rangle$ for $j = 1, ..., f$. Finally, by $(2')$ of theorem 1.3.2, for $j = 1, ..., e$, $\mathcal{A}'_j$ has no internal sum in $\{\psi([p])\} = \{\langle \bar{0}, x\rangle\}$.

So let $\mathcal{A}'_1 = \{\!\!\{\langle a,0\rangle, \langle b,x\rangle^2, \langle b,-x\rangle, \langle a+b,x\rangle\}\!\!\}$, $\mathcal{A}'_2 = \{\!\!\{\langle a,x\rangle, \langle a,-x\rangle, \langle b,0\rangle, \langle b,-x\rangle\}\!\!\}$. And let $\mathcal{B}'_1 = \{\!\!\{\langle b,0\rangle, \langle b,x\rangle\}\!\!\}$, $\mathcal{B}'_2 = \{\!\!\{\langle a,0\rangle, \langle a,x\rangle\}\!\!\}$, $\mathcal{B}'_3 = \{\!\!\{\langle a,-x\rangle, \langle b,x\rangle, \langle a+b,x\rangle\}\!\!\}$, and $\mathcal{B}'_4 = \{\!\!\{\langle b,-x\rangle^2\}\!\!\}$, where a and b are distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Then $e = 2, f = 4$, so $f/e = 2$, and $\bigcup_{i=1}^{2} \mathcal{A}'_i = \{\!\!\{\langle a,0\rangle, \langle a,x\rangle, \langle a,-x\rangle, \langle b,0\rangle, \langle b,x\rangle^2, \langle b,-x\rangle^2, \langle a+b,x\rangle\}\!\!\} = \bigcup_{i=1}^{4} \mathcal{B}'_i$, and conditions $(1')$, $(5')$ of theorem 1.3.2 are met.

Both $\mathcal{A}'_1, \mathcal{A}'_2$ have no internal sum of $\psi([p]) = \langle \bar{0}, x\rangle$, so condition $(2')$ of theorem 1.3.2 is met.

Meeting conditions $(3')$ and $(4')$ of theorem 1.3.2, we have $\sum \mathcal{A}'_1 = \sum \mathcal{A}'_2 = \langle \bar{0}, -x\rangle = \psi([p]^{1-\alpha})$, and $\sum \mathcal{B}'_1 = \sum \mathcal{B}'_2 = \sum \mathcal{B}'_3 = \sum \mathcal{B}'_4 = \langle \bar{0}, x\rangle = \psi([p]^{-\alpha})$.

So $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $ord_y(p) = 3$, $\alpha \equiv 2 \pmod 3$.

(4) Let $\mathrm{ord}_y(p) = 6$, and fix $\psi([p]) = \langle a, x\rangle$ with $a \neq \bar{0}, x \neq 0$.

If $\alpha \equiv 0 \pmod 6$, then $p^\alpha \equiv 1 \pmod y$, and $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted by theorem 2.1.1.

If $\alpha = 3$, then $\beta = \alpha + 3 = 6$ since $\mathrm{ord}_y(p) = 6$, and $\rho = (\alpha + \beta - 1)/\alpha = 8/3$. By theorem 1.3.2, $\sum \mathcal{A}'_j = \psi([p]^{1-\alpha}) = \psi([p]^4) = \langle \bar{0}, x\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}'_j = \psi([p]^{-\alpha}) = \psi([p]^3) = \langle a, 0\rangle$ for $j = 1, ..., f$. Further, by $(2')$ of theorem 1.3.2, for $j = 1, ..., e$, $\mathcal{A}'_j$ has no internal sum in $\{\psi([p]), \psi([p]^2), \psi([p]^3)\} = \{\langle a,x\rangle, \langle \bar{0}, -x\rangle, \langle a, 0\rangle\}$.

So let $\mathcal{A}'_1 = \{\!\!\{\langle b,-x\rangle^2, \langle a+b,0\rangle^8\}\!\!\}$, $\mathcal{A}'_2 = \{\!\!\{\langle a,-x\rangle, \langle b,0\rangle^7, \langle a+b,-x\rangle\}\!\!\}$, and $\mathcal{A}'_3 = \{\!\!\{\langle \bar{0},x\rangle\}\!\!\}$. And let $\mathcal{B}'_1 = \mathcal{B}'_2 = ... = \mathcal{B}'_7 = \{\!\!\{\langle b,0\rangle, \langle a+b,0\rangle\}\!\!\}$, and $\mathcal{B}'_8 = \{\!\!\{\langle \bar{0},x\rangle, \langle a,-x\rangle, \langle b,-x\rangle^2, \langle a+b,0\rangle, \langle a+b,-x\rangle\}\!\!\}$, where a and b are distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Then $e = 3, f = 8$, so $f/e = 8/3$ and $\bigcup_{i=1}^{3} \mathcal{A}'_i = \{\!\!\{\langle \bar{0},x\rangle, \langle a,-x\rangle, \langle b,0\rangle^7, \langle b,-x\rangle^2, \langle a+b,0\rangle^7, \langle a+b,-x\rangle\}\!\!\} = \bigcup_{i=1}^{8} \mathcal{B}'_i$, and conditions $(1')$, $(5')$ of theorem 1.3.2 are met.

None of $\mathcal{A}'_1, \mathcal{A}'_2, \mathcal{A}'_3$ have internal sums in $\{\langle a,x\rangle, \langle \bar{0},-x\rangle, \langle a,0\rangle$, so condition $(2')$ of theorem 1.3.2 is met.

Meeting conditions $(3')$ and $(4')$ of theorem 1.3.2, we have $\sum \mathcal{A}'_1 = \sum \mathcal{A}'_2 = \sum \mathcal{A}'_3 = \langle \bar{0}, x\rangle$, and $\sum \mathcal{B}'_1 = ... = \sum \mathcal{B}'_8 = \langle \bar{0}, x\rangle$.

So $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\alpha = 3$, and by theorem 2.2.1 and the equivalence theorem, it follows that $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\mathrm{ord}_y(p) = 6$ and $\alpha \equiv 3 \pmod 6$.

If $\alpha = 4$, we have $\beta = 6$ and $\rho = 9/4$. By theorem 1.3.2, $\sum \mathcal{A}'_j = \psi([p]^3) = \langle a, 0\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}'_j = \psi([p]^2) = \langle \bar{0}, -x\rangle$ for $j = 1, ..., f$. Further, by $(2')$ of theorem 1.3.2, for $j = 1, ..., e$, $\mathcal{A}'_j$ has no internal sum in $\{\langle a,x\rangle, \langle \bar{0},-x\rangle\}$.

So let $\mathcal{A}'_1 = \mathcal{A}'_2 = \{\!\!\{\langle a,-x\rangle^3, \langle b,0\rangle^4\}\!\!\}$, $\mathcal{A}'_3 = \mathcal{A}'_4 = \{\!\!\{\langle a,-x\rangle^3, \langle a+b,0\rangle^4\}\!\!\}$. And let $\mathcal{B}'_1 = ... = \mathcal{B}'_8 = \{\!\!\{\langle a,-x\rangle, \langle b,0\rangle, \langle a+b,0\rangle\}\!\!\}$, $\mathcal{B}'_9 = \{\!\!\{\langle a,-x\rangle^4\}\!\!\}$, where a and b are distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Then $e = 4, f = 9$, so $f/e = 9/4$ and $\bigcup_{i=1}^{4} \mathcal{A}'_i = \{\!\!\{\langle a,-x\rangle^{12}, \langle b,0\rangle^8, \langle a+b,0\rangle^8\}\!\!\} = \bigcup_{i=1}^{9} \mathcal{B}'_i$, and conditions $(1')$, $(5')$ of theorem 1.3.2 are met.

None of $\mathcal{A}'_1, ..., \mathcal{A}'_4$ have internal sums in $\{\langle a,x\rangle, \langle \bar{0},-x\rangle\}$, so condition $(2')$ of theorem 1.3.2 is met.

Meeting conditions $(3')$ and $(4')$ of theorem 1.3.2, we have $\sum \mathcal{A}_1' = ... = \sum \mathcal{A}_4' = \langle a, 0\rangle$, and $\sum \mathcal{B}_1' = ... = \sum \mathcal{B}_9' = \langle \bar{0}, -x\rangle$.

So $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\alpha = 4$, and by theorem 2.2.1 and the equivalence theorem, it follows that $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\text{ord}_y(p) = 6$ and $\alpha \equiv 4 \pmod 6$.

If $\alpha = 5$, we have $\beta = 6$ and $\rho = 2$. By theorem 1.3.2, $\sum \mathcal{A}_j' = \psi([p]^2) = \langle \bar{0}, -x\rangle$ for $j = 1, ..., e$, and $\sum \mathcal{B}_j' = \psi([p]) = \langle a, x\rangle$ for $j = 1, ..., f$. Further, by $(2')$ of theorem 1.3.2, for $j = 1, ..., e$, $\mathcal{A}_j'$ has no internal sum of $\langle a, x\rangle$.

So let $\mathcal{A}_1' = \{\!\!\{\langle \bar{0}, x\rangle^4, \langle \bar{0}, -x\rangle^2\}\!\!\}$, $\mathcal{A}_2' = \{\!\!\{\langle a, 0\rangle^4, \langle \bar{0}, -x\rangle\}\!\!\}$. And let $\mathcal{B}_1' = ... = \mathcal{B}_3' = \{\!\!\{\langle a, 0\rangle, \langle \bar{0}, x\rangle\}\!\!\}$, $\mathcal{B}_4' = \{\!\!\{\langle a, 0\rangle, \langle \bar{0}, x\rangle, \langle \bar{0}, -x\rangle^3\}\!\!\}$, where a and b are distinct nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Then $e = 2, f = 4$, so $f/e = 2$ and $\bigcup_{i=1}^{2} \mathcal{A}_i' = \{\!\!\{\langle \bar{0}, x\rangle^4, \langle \bar{0}, -x\rangle^3, \langle a, 0\rangle^4\}\!\!\} = \bigcup_{i=1}^{4} \mathcal{B}_i'$, and conditions $(1')$, $(5')$ of theorem 1.3.2 are met.

Neither $\mathcal{A}_1'$ nor $\mathcal{A}_2'$ contain an internal sum of $\langle a, x\rangle$, so condition $(2')$ of theorem 1.3.2 is met.

Meeting conditions $(3')$ and $(4')$ of theorem 1.3.2, we have $\sum \mathcal{A}_1' = \sum \mathcal{A}_2' = \langle \bar{0}, -x\rangle$, and $\sum \mathcal{B}_1' = ... = \sum \mathcal{B}_4' = \langle a, x\rangle$.

So $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\alpha = 5$, and by theorem 2.2.1 and the equivalence theorem, it follows that $(\mathbb{Z}_y^\times, [p], \alpha)$ is accepted when $\text{ord}_y(p) = 6$ and $\alpha \equiv 5 \pmod 6$.

□

References

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

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

[3] 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.