ON THE ACCEPTED ELASTICITY OF ARITHMETIC CONGRUENCE MONOIDS

1. Preliminaries

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

\[ M(a, b) := \{1\} \cup (a + b\mathbb{N}_0) = \{1, a, a + b, a + 2b, a + 3b, \ldots\} \]

where \(a, b\) are integers with \(0 < a \leq b\) 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

\[ \mathcal{L}(r) := \{n \in \mathbb{N} \mid \exists \text{ irreducibles } a_1, \ldots, a_n \in M(a, b) \text{ such that } r = (a_1) \cdots (a_n)\}, \]

and the elasticity of \(r\) to be

\[ \rho(r) := \frac{\max \mathcal{L}(r)}{\min \mathcal{L}(r)}. \]

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 \(0 < x \leq y\), \(\gcd(x, y) = 1\), 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 \(\beta\) to be the least positive integer such that \(p^\beta \in M\) through the rest of the paper. Given \(p, \alpha, x,\) 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 \((A, \mu)\) of a set \(A\) and a map \(\mu : A \rightarrow \mathbb{N}\), where the multiplicity of each element of \(A\) in the multiset is its image under \(\mu\). We say that \((A, \mu)\) is finite if \(A\) is finite. If \(A = \{a_1, a_2, \ldots\}\), we can denote \((A, \mu)\) by \(\left\{\left(a_1^{\mu(a_1)}, a_2^{\mu(a_2)}, \ldots\right)\right\}\), or by \(\left\{\frac{a_1}{\mu(a_1)} \times \frac{a_2}{\mu(a_2)} \times \ldots\right\}\).

We say that \((A_1, \mu_1)\) is a submultiset of \((A_2, \mu_2)\), and write \((A_1, \mu_1) \subset (A_2, \mu_2)\) if \(A_1 \subset A_2\) and, for all \(a \in A_1\), \(\mu_1(a) \leq \mu_2(a)\). 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 \(S = \{g_1^{m_1}, \ldots, g_n^{m_n}\}\) be a finite multiset of elements in an additive (resp. multiplicative) group \(G\). We let \(\sum S\) (resp. \(\prod S\)) denote the sum \(\sum_{i=1}^n m_i g_i\) (resp. the product \(\prod_{i=1}^n g_i^{m_i}\)) in \(G\).

Notice that \(\sum (A \cup B) = \sum A + \sum B\).

**Definition 1.2.1.** Let \(S = \{g_1^{m_1}, \ldots, g_n^{m_n}\}\) 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 \(h\) 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 \(\text{ord}_G(g)\) that is at least \(k\).

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

**Proof.** We must show that \(\beta(\mathbb{Z}^k_y, [p], \alpha)\) 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 \(p^m \in M(p^\alpha, p^\alpha) \iff m \geq \alpha\), and \(p^m \in M(1, y) \iff \text{ord}_G(p) | m\). Hence \(p^m \in M\) iff \(m \geq \alpha\) and \(\text{ord}_G(p) | m\). Since \(\beta(\mathbb{Z}^k_y, [p], \alpha)\) is the least multiple of \(\text{ord}_G(p)\) that is at least \(\alpha\), \(\beta(\mathbb{Z}^k_y, [p], \alpha)\) is the least positive power of \(p\) contained in \(M\). Thus \(\beta = \beta(\mathbb{Z}^k_y, [p], \alpha)\).

**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 \(A_1, \ldots, A_e, B_1, \ldots, B_f\) of elements of \(G\) such that

1. \(\bigcup_{i=1}^e A_i = \bigcup_{i=1}^f B_i\)
2. for \(j = 1, \ldots, e\), \(A_j\) has no internal product in \(\{g, g^2, \ldots, g^{\beta(G, g, k) - k}\}\)
3. for \(j = 1, \ldots, e\), \(\prod A_j = g^{1-k}\)
4. for \(j = 1, \ldots, f\), \(\prod B_j = g^{-k}\), and
5. \(\frac{e}{f} = \frac{k + \beta(G, g, k) - 1}{k}\)

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

From lemma 4.1 of [1], we know that \(p \not| y\). Therefore, using square brackets to denote equivalence classes modulo \(y\), we have that \([p] \in \mathbb{Z}^k_y\). 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 $\alpha \leq v_p(r) \leq \alpha + \beta - 1$. Since $r \in M(p^\alpha, p^\beta)$, $\alpha \leq v_p(r)$, proving the first inequality. To prove the second inequality, assume that $v_p(r) \geq \alpha + \beta$, 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, $\alpha \leq v_p(r) \leq \alpha + \beta - 1$. 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 $\alpha$.

Now, let $s$ be an element of $M$. Since each irreducible factor of $s$ has $p$-adic valuation of at least $\alpha$, there are at most $[v_p(s)/\alpha]$ 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 $[v_p(s)/(\alpha + \beta - 1)]$ irreducibles in a factorization of $s$. Thus

$$\Omega(s) \subseteq \left\{ m = \left\lfloor \frac{v_p(s)}{\alpha + \beta - 1} \right\rfloor \leq m \leq \left\lceil \frac{v_p(s)}{\alpha} \right\rceil \right\}.$$

and

$$\rho(s) \leq \frac{v_p(s)}{\alpha + \beta - 1} \leq \frac{v_p(s)}{\alpha} = \frac{\alpha + \beta - 1}{\alpha}.$$

For the first inequality, equality holds iff there are factorizations of lengths $[v_p(s)/\alpha]$ and $[v_p(s)/(\alpha + \beta - 1)]$. 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 $A_1, \ldots, A_e, B_1, \ldots, B_f$ of elements of $\mathbb{Z}_y^\times$ such that

1. $\bigcup_{i=1}^f A_i = \bigcup_{i=1}^f B_i$
2. for $j = 1, \ldots, e$, $A_j$ has no internal product in $\{[p], [p]^2, \ldots, [p]^{\beta-\alpha}\}$
3. for $j = 1, \ldots, e$, $B_j = [p]^{1-\alpha}$
4. for $j = 1, \ldots, f$, $B_j = [p]^{-\alpha}$, and
5. $f/e = (\alpha + \beta - 1)/\alpha$.

We will prove this equivalent statement:

$(\Rightarrow)$ Assume that $3s \in M$ 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 $i = 1, \ldots, e$, 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 $i \in \{1, \ldots, e\}$ and $j \in \{1, \ldots, m_i\}$. Define the multisets $A_i = \left\{ [a_1^{(i)}], \ldots, [a_{m_i}^{(i)}] \right\}$ for
Similarly, define the multisets $B_i = \begin{cases} [b_1^{(i)}], \ldots, [b_{m_i}^{(i)}] \end{cases}$ where $[b_j^{(i)}]$ is the equivalence class of $r_j^{(i)}$ in $\mathbb{Z}_p$ and $B_i = p^\alpha (r_1^{(i)}) \cdots (r_{m_i}^{(i)})$ 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 $(A_1) \cdots (A_e) = p^{(\alpha+\beta-1)} \prod_{i=1}^e \prod_{j=1}^{m_i} q_j^{(i)}$

and

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

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

$$\bigcup_{i=1}^e \bigcup_{j=1}^{m_i} [q_j^{(i)}] = \bigcup_{i=1}^f \bigcup_{j=1}^{n_i} [r_j^{(i)}] \implies$$

$$\bigcup_{i=1}^e \bigcup_{j=1}^{m_i} [a_j^{(i)}] = \bigcup_{i=1}^f \bigcup_{j=1}^{n_i} [b_j^{(i)}] \implies$$

$$\bigcup_{i=1}^e A_i = \bigcup_{i=1}^f B_i,$$

so condition (1a) holds.

Notice that, for $i = 1, \ldots, e$

$$\prod A_i = \prod [a_j^{(i)}] = \prod [q_j^{(i)}] = [A_i] / [p^{\alpha + \beta - 1}] = [p]^{-\alpha}$$

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

We will show that condition (2a) holds by contradiction. Assume that for some $j \in \{1, \ldots, e\}$, $|S| \subset A_i$ such that $\prod S \in \{[p], [p]^2, \ldots, [p]^\beta\}$. Say $S = \begin{cases} [a_j^{(i)}], \ldots, [b_{m_j}^{(i)}] \end{cases}$ and $\prod S = [p]^\gamma$ for some $\gamma \in \{1, \ldots, \beta-\alpha\}$. Let $g = q_j^{(i)} \cdots q_{m_j}^{(i)}$ and $h = (q_j^{(i)} \cdots q_{m_j}^{(i)}) / g$. Then $[g] = [p]^\gamma$. Furthermore, $A_i \equiv p^{\alpha + \beta - 1}gh = (p^{\beta+\gamma})(p^{\gamma+\alpha-1}h)$. Since $1 \leq \gamma \leq \beta - \alpha$, we know that $v_p(p^{\beta+\gamma}g) = \beta - \gamma \geq \alpha$ and $v_p(p^{\gamma+\alpha-1}h) = \gamma + \alpha - 1 \geq \alpha$. 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, $A_i \equiv (p^{\beta+\gamma}g)(p^{\gamma+\alpha-1}h)$ is a factorization in $M$, contradicting the irreducibility of $A_i$. Hence condition (2a) holds.
(⇐) Now assume that there are integers e, f and multisets \( A_1, ..., A_e, B_1, ..., B_f \) of elements of \( \mathbb{Z}_y^\times \) which satisfy conditions (1a)-(5a). Let

\[
A_i = \left\{ [a^{(i)}_1], ..., [a^{(i)}_m] \right\}
\]

for \( i = 1, ..., e \) and

\[
B_i = \left\{ [b^{(i)}_1], ..., [b^{(i)}_m] \right\}
\]

for \( i = 1, ..., f \). Define \( q^{(i)}_j, r^{(i)}_j \) to be the least prime natural number belonging to the equivalence classes \( [a^{(i)}_j],[b^{(i)}_j] \), respectively. Notice that these primes necessarily exist by Dirichlet’s theorem. Define \( A_i = p^{n+\beta-1}q^{(i)}_1 \cdots q^{(i)}_m \) for \( i = 1, ..., e \) and \( B_i = p^n r^{(i)}_1 \cdots r^{(i)}_m \) for \( i = 1, ..., f \).

Notice that, for \( i = 1, ..., e \),

\[
[A_i] = p^{n+\beta-1}q^{(i)}_1 \cdots q^{(i)}_m
\]

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 \( \alpha \), 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 \( 2\alpha \) is irreducible, each \( B_i \) is irreducible. Assume that there is some \( k \in \{1, ..., e\} \) such that \( A_k \) is reducible, and we that \( A_k = (p')^k g(p^{n+\beta-\gamma-1}h) \) is a factorization in \( M \). Pick a set of indices \( \{i_1, ..., i_z\} \subset \{1, ..., m_k\} \) such that \( g = q^{(k)}_{i_1} \cdots q^{(k)}_{i_z} \), and let \( S = \left\{ [a^{(k)}_{i_1}], ..., [a^{(k)}_{i_z}] \right\} \).

Then \( \prod S = [a^{(k)}_{i_1}] \cdots [a^{(k)}_{i_z}] = [q^{(k)}_{i_1} \cdots q^{(k)}_{i_z}] = [p^{n-\gamma}] \) since \( [A_k] = [1] \). Because the two factors are in \( M \), \( \gamma \geq \alpha \) and \( \alpha + \beta - \gamma - 1 \geq \alpha \), yielding \( \alpha \leq \gamma \leq \beta - 1 \). Therefore \( \prod S = [p^{n-\gamma}] \in \{ [p], [p]^2, ..., [p]^{\beta-1} \} \), 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.

\[\square\]

**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 \( A_1, ..., A_e, B_1, ..., B_f \) of elements in \( G \) which satisfy conditions (1)- (5) from the definition of an accepted triple. Let \( A'_i \) be the image of \( A_i \) under \( \psi \) for \( i = 1, ..., e \) and \( B'_i \) the image of \( B_i \) under \( \psi \) for \( i = 1, ..., f \). We wish to show that the integers \( e, f \) and multisets \( A'_1, ..., A'_e, B'_1, ..., B'_f \) satisfy

(1') \( \bigcup_{i=1}^e A'_i = \bigcup_{i=1}^f B'_i \)

(2') for \( j = 1, ..., e \), \( A'_j \) has no internal product in \{ \( \psi(g), \psi(g)^2, ..., \psi(g)^{\beta(H, \psi(g), k) - k} \) \}

(3') for \( j = 1, ..., e \), \( \prod A'_j = \psi(g)^{1-k} \)

(4') for \( j = 1, ..., f \), \( \prod B'_j = \psi(g)^{k-1} \), and

(5') \( f/e = (k + \beta(H, \psi(g), k) - 1)/k \).
Since \( \text{ord}_H(\psi(g)) = \text{ord}_C(g) \), 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 \( \bigcup A'_i \) and \( \bigcup B'_j \) are images of \( \bigcup A_i \) and \( \bigcup B_j \), respectively, under \( \psi \) (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 preceding 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. 

\[ \square \]

**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 \( A_1, \ldots, A_e, B_1, \ldots, B_f \) of elements of \( H \) satisfy conditions (1)-(5). Because \( \text{ord}_H(h) = \text{ord}_C(h) \), it is clear that the integers \( e, f \) and the multisets \( A_1, \ldots, A_e, B_1, \ldots, B_f \), when viewed as multisets of elements of \( G \), still satisfy conditions (1)-(5). Thus \((G, h, k)\) is accepted. 

\[ \square \]

**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 \( A_1, \ldots, A_e, B_1, \ldots, B_f \) of elements of \( G \) which satisfy conditions (1)-(4) from the definition of an accepted triple, but also satisfy

\[ (5) \quad \frac{e}{f} \geq \frac{k + \beta(G, g, k) - 1}{k} \]

**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 \( A_1, \ldots, A_e, B_1, \ldots, B_f \) of elements of \( G \) which satisfy conditions (1)-(4) and (5).

Define \( e k \) multisets \( A_{i,j} \) for \( i = 1, \ldots, e \) and \( j = 1, \ldots, k \), so that \( A_{i,j} = A_i \). Define \( f k \) multisets \( B_{i,j} \) for \( i = 1, \ldots, f \) and \( j = 1, \ldots, k \) so that \( B_{i,j} = B_i \). Define \( f k \) multisets \( S_i \) for \( i = 1, \ldots, f k \) so that \( S_{i-1} + k = B_{i,k} \) for \( j = 1, \ldots, f k \) and \( k = 1, \ldots, k \) (that is, the multisets \( S_i \) are just a way of ordering the multisets \( B_{i,j} \) in one list). Since \( f/e \geq (k + \beta(G, g, k) - 1)/k \), we have \( f k \geq e(k + \beta(G, g, k) - 1) \). So we can define \( e(k + \beta(G, g, k) - 1) \) multisets \( B'_{1}, \ldots, B'_{e(k + \beta(G, g, k) - 1)} \) so that \( B'_i = S_i \) for \( i = 1, \ldots, e(k + \beta(G, g, k) - 1) - 1 \), and

\[ B'_{e(k + \beta(G, g, k) - 1)} := \bigcup_{i = e(k + \beta(G, g, k) - 1)}^{f k} S_i \]

We wish to show that conditions (1)-(5) hold for the positive integers \( e k \) and \( e(k + \beta(G, g, k) - 1) \) and the multisets \( A_{i,j} \) and \( B'_{i} \).
Notice that
\[ e^{(k+\beta(G,g,k)-1)} \bigcup_{i=1}^{e} \mathcal{B}'_i = \left( \bigcup_{i=1}^{e} \mathcal{B}'_i e^{(k+\beta(G,g,k)-1)} \right) \cup \mathcal{B}'_{e^{(k+\beta(G,g,k)-1)}-1} \]
\[ = \left( \bigcup_{i=1}^{e} \mathcal{S}_i \right) \cup \left( \bigcup_{i=e^{(k+\beta(G,g,k)-1)}-1}^{f} \mathcal{S}_i \right) \]
\[ = \bigcup_{i=1}^{f} \mathcal{S}_i = \bigcup_{j=1}^{k} \mathcal{B}_{i,j} = \bigcup_{j=1}^{k} \mathcal{A}_{i,j}, \]

hence condition (1) holds.

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

\[ \prod \mathcal{B}'_{e^{(k+\beta(G,g,k)-1)}} = \frac{\prod_{i=1}^{e^{(k+\beta(G,g,k)-1)}} (\prod \mathcal{B}'_i)}{\prod_{i=1}^{e^{(k+\beta(G,g,k)-1)}} (\mathcal{B}'_i)} \]
\[ = \frac{\prod_{i=1}^{e^{(k+\beta(G,g,k)-1)}} (\prod \mathcal{A}_{i,j})}{g^{-ek^2+ek+k}} \text{ (recall } g^{\beta(G,g,k)} = 1 \text{ )} \]
\[ = \frac{\prod_{i=1}^{k} \prod_{j=1}^{e} (\prod \mathcal{A}_{i,j})}{g^{-ek^2+ek+k}} \]
\[ = \frac{(g^{-k})^{ek}}{g^{-ek^2+ek+k}} \]
\[ = g^{-k}, \]

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

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 \( n' \geq n \), \( (G,g,n') \) 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 \( \omega(M) := \omega(\mathbb{Z}_g^n, [p]) \).

2. **General**

2.1. **Case** \( x = 1 \).

**Lemma 2.1.1.** If \( \text{ord}_G(g) \mid k \) then \( (G,g,k) \) is accepted.

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

(1b) \[ \bigcup_{i=1}^{k} \mathcal{A}_i = \bigcup_{i=1}^{2k-1} \mathcal{B}_i \]
(2b) for \( i = 1, \ldots, k \), \( \prod \mathcal{A}_i = g \), and
(3b) for \( i = 1, \ldots, 2k-1 \), \( \prod \mathcal{B}_i = 1_G \).
(Notice that condition (2) from the definition of an accepted triple vanishes because the set \( \{g, g^2, \ldots, g^{\beta(G, g, k) - k}\} \) is empty when \( \beta(G, g, k) = k \), and condition (5) is trivially true.)

Let \( A_1 = \ldots = A_k = \{g\} \), let \( B_1 = \{g^k\} \), and let \( B_2 = \ldots = B_{2k-1} = \emptyset \). Then one can easily see that these satisfy conditions (1b)-(3b), completing the proof. □

**Theorem 2.1.1.** Let \( \beta \) 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 \( \implies \) ii) If \( x = 1 \), then \( p^\alpha \) is the least element of \( M \) other than 1. Hence \( \beta = \alpha \).

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

(iii \( \implies \) 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 \( 0 < x \leq y \), we have \( x = 1 \).

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

**Theorem 2.2.1.** If \( (G, g, k) \) is accepted, then \( (G, g, k + m \text{ord}_G(g)) \) is accepted for any positive integer \( m \).

**Proof.** From lemma 2.1.1, the theorem holds if \( k \mid \text{ord}_G(g) \). So assume otherwise. Suppose \( (G, g, k) \) is accepted. Then there exists integers \( e, f \) and multisets \( A_1, \ldots, A_e, B_1, \ldots, B_f \) of elements of \( G \) satisfying conditions (1)-(5) from the definition of an accepted triple.

We claim that \( (G, g, k + m \text{ord}_G(g)) \) is overaccepted, and that the positive integers \( e, f \) and multisets \( A_1, \ldots, A_e, B_1, \ldots, B_f \) satisfy the conditions for over acceptance:

(1’’) \( \bigcup_{i=1}^{e} A_i = \bigcup_{j=1}^{f} B_j \)
(2’’) for \( j = 1, \ldots, e, A_j \) has no internal product in
\( \{g, g^2, \ldots, g^{\beta(G, g, k + m \text{ord}_G(g)) - 1 - k - m \text{ord}_G(g)}\} \)
(3’’) for \( j = 1, \ldots, e, \prod A_j = g^{\beta(G, g, k + m \text{ord}_G(g)) - 1} \)
(4’’) for \( j = 1, \ldots, f, \prod B_j = g^{-\beta(G, g, k + m \text{ord}_G(g))} \), and
(5’’) \( \frac{e}{p} \geq \frac{(k + m \text{ord}_G(g)) + \beta(G, g, k + m \text{ord}_G(g)) - 1}{(k + m \text{ord}_G(g))} \)

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

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

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

\( \beta(G, g, k) - k = r \text{ ord}_G(g) - k = \beta(G, g, k + m \text{ ord}_G(g)) - (k + m \text{ ord}_G(g)) \).
Hence condition (2") follows immediately from the acceptance of \((G, g, k, 1)\).

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

\[
\frac{k + \beta(G, g, k) - 1}{k} \geq \frac{(k + m \, \text{ord}_G(g)) + \beta(G, g, k + m \, \text{ord}_G(g)) - 1}{k + m \, \text{ord}_G(g)} \iff
\]

\[
\frac{k + r \, \text{ord}_G(g) - 1}{k} \geq \frac{(k + m \, \text{ord}_G(g)) + (r + m) \, \text{ord}_G(g) - 1}{k + m \, \text{ord}_G(g)} \iff
\]

\[
\frac{r \, \text{ord}_G(g) - 1}{k} \geq \frac{(r + m) \, \text{ord}_G(g) - 1}{k + m \, \text{ord}_G(g)} \iff
\]

\[
(r \, \text{ord}_G(g) - 1)(k + m \, \text{ord}_G(g)) \geq ((r + m) \, \text{ord}_G(g) - 1)k \iff
\]

\[
(r \, \text{ord}_G(g) - 1)m \, \text{ord}_G(g) \geq m \, \text{ord}_G(g)k \iff
\]

\[
r \, \text{ord}_G(g) - 1 \geq k,
\]

which is true because \(r \, \text{ord}_G(g) > k\) and both sides are integers. \(\square\)

**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 \(A_1, \ldots, A_e, B_1, \ldots, B_f\) of elements of \(G\) such that

1. \(\bigcup_{j=1}^e A_j = \bigcup_{i=1}^f B_i\)
2. For \(j = 1, \ldots, e\), \(A_j\) has no internal product in \(\{g, g^2, \ldots, g^{\text{ord}_G(g) - 1}\}\)
3. For \(j = 1, \ldots, e\), \(\prod A_j = 1_G\) (the identity)
4. For \(j = 1, \ldots, f\), \(\prod B_j = g^{-1}\), and
5. \(f/e = \text{ord}_G(g)\),

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

By theorem 2.2.1, it suffices to only consider \(1 \leq k \leq \text{ord}_G(g)\). Then \(\beta(G, g, k) = \text{ord}_G(g)\). For \(i = 1, \ldots, e, j = 1, \ldots, k\), define \(A_{i,j} = A_i \cup \{(g^{-1})^{(j-1)}\}\) (that is, the single element \(g^{-1}\) with multiplicity \(k-1\)). For \(i = 1, \ldots, f\), define \(B_i' = \bigcup_{j=1}^k B_i\) (the union of \(k\) copies of \(B_i\)), and for \(i = f + 1, \ldots, f + e(k-1)\), define \(B_i' = \{(g^{-1})^{(j-1)}\}\). Then it suffices to show that

1. \(\bigcup_{i=1}^e \bigcup_{j=1}^k A_{i,j} = \bigcup_{i=1}^{f+e(k-1)} B_i'\)
2. For \(i = 1, \ldots, e, j = 1, \ldots, k, A_{i,j}\) has no internal product in \(\{g, g^2, \ldots, g^{\text{ord}_G(g) - k}\}\)
3. For \(i = 1, \ldots, f, e(k-1), \prod A_{i,j} = g^{1-k}\)
4. For \(i = 1, \ldots, f + e(k-1), \prod B_i' = g^{-k},\) and
5. \((f + e(k-1))/(ek) = (k + \text{ord}_G(g) - 1)/k).
Observe that
\[
\bigcup_{i=1}^{e} \bigcup_{j=1}^{k} A_{i,j} = \bigcup_{i=1}^{e} \bigcup_{j=1}^{k} \left( A_i \cup \{ (g-1)^{(k-1)} \} \right)
\]
\[
= \left( \bigcup_{j=1}^{k} A_i \right) \cup \left\{ (g-1)^{(e(k-1))} \right\}
\]
\[
= \left( \bigcup_{j=1}^{f} B_i \right) \cup \left( \bigcup_{k=1}^{f+e(k-1)} B_i \right) \quad \text{(by (1c))}
\]
\[
= \bigcup_{i=1}^{f+e(k-1)} B_i,
\]
hence condition (1d) holds.

Next, we will show that (2d) holds by contradiction. Assume that (2d) does not hold. Then for some \( i \in \{1, \ldots, e\} \) and \( j \in \{1, \ldots, k\} \), there exists \( S \subset A_{i,j} \) such that \( \prod S \in \{g, g^2, \ldots, g^{\text{ord}_G(g)-k}\} \). So let \( \prod S = g^\delta \) for \( \delta \in \{1, \ldots, \text{ord}_G(g)-k\} \). Since \( A_{i,j} = A_i \cup \{ (g-1)^{(k-1)} \} \), we can write \( S = S' \cup \{ (g-1)^{(\gamma)} \} \) for some \( S' \subset A_i \) and some \( \gamma \in \{0, \ldots, k-1\} \). Since \( \prod S = \prod S' \prod \{ (g-1)^{(\gamma)} \} \), we have
\[
\prod S' = \prod S \left( \prod \{ (g-1)^{(\gamma)} \} \right)^{-1}
\]
\[
= (g^\delta)(g^\gamma)
\]
\[
= g^{\gamma+\delta}.
\]
However, since \( 1 \leq \gamma + \delta \leq \text{ord}_G(g) - 1 \), this contradicts condition (2c). Therefore condition (2d) holds.

To see that condition (3d) holds, notice that
\[
\prod A_{i,j} = \prod \left( A_i \cup \{ (g-1)^{(k-1)} \} \right)
\]
\[
= \prod A_i \prod \{ (g-1)^{(k-1)} \}
\]
\[
= g^{1-k}
\]
by (3c).

To see that condition (4d) holds, notice that for \( i = 1, \ldots, f \),
\[
\prod B'_i = \prod \left( \bigcup_{j=1}^{k} B_i \right)
\]
\[
= \prod \left( \prod B_i \right)
\]
\[
= (g^{-1})^k = g^{-k}
\]
by (4c), and, for \( i = f + 1, \ldots, f + e(k - 1), \)
\[
\prod B'_i = \prod \left( \{ (g^{-1})^{(k)} \} \right) = g^{-k}.
\]

Finally, notice that \((f + e(k - 1))/(ek) = (ek + e(k - 1))/ek = (k + ord_C(g) - 1)/k.\) Hence condition (5d) holds, completing the proof. \( \square \)

3. Cyclic Unit Group

3.1. Case \( d < c. \) In this section, we will assume \( \mathbb{Z}_q^x \) is cyclic. Define \( d := \text{ord}_q(p) \) and \( c := \phi(y)/d. \) We will also define \( \alpha \) to be the residue of \( \alpha \) modulo \( c \) contained in \{1, 2, \ldots, 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 \((\mathbb{Z}_q^x, [p], \alpha)\) is accepted. Then, from the isomorphism theorem, it suffices to show that there exists an isomorphism \( \psi : \mathbb{Z}_q^x \to \mathbb{Z}_{cd} \) such that \( \psi([p]) = \langle c \rangle. \)

Let \([g]\) be a generator of \( \mathbb{Z}_q^x \), and let \([p] = [g]^k. \) The order of \([g]\) modulo \( y \) is \( \phi(y) = cd, \) and the order of \([g]\) modulo \( y \) is \( d. \) Then \([g]^{kd} = [p]^d = [1] \implies cd | kd \implies c | k. \) So let \( k = cm. \) Let \( b = \text{gcd}(m, d). \) Then \([p]^{d/b} = [g]^{cdm/b} = [1] \implies d | d/b \implies b = \text{gcd}(m, d) = 1. \) Let the prime factorization of \( c \) be \( p_{1}^{u_1} \cdots p_{s}^{u_s} q_{1}^{v_1} \cdots q_{t}^{v_t}, \) where each \( p_i \) divides \( d \) and each \( q_i \) does not divide \( d. \) Let \( c = c_1 c_2 \) and \( \text{gcd}(c_1, m) = \text{gcd}(c_2, d) = 1. \) Choose \( n \) such that \( nd \equiv 1 \pmod{c_2}. \) Let \([h] = [g]^{m+nd}. \) Then \( \text{gcd}(m+nd, d) = \text{gcd}(m, d) = 1. \) This also tells us that \( \text{gcd}(m+nd, c_1) = 1. \) Furthermore, \( m+nd \equiv 1 \pmod{c_2}, \) so \( \text{gcd}(m+nd, c_2) = 1. \) Hence \( \text{gcd}(m+nd, cd) = 1. \) Therefore, if \([h]^r = [g]^{r(m+nd)} = [1], \) then \( cd | r(m+nd) \implies cd | r. \) Hence the order of \([h]\) must equal \( cd, \) and \([h]\) is a generator of \( \mathbb{Z}_q^x. \) Furthermore, \([h]^c = [g]^{cm} = [p]. \)

Thus, if \( \psi \) takes \([h]\) to \( \langle 1 \rangle, \) then \( \psi \) is an isomorphism taking \([p]\) to \( \langle c \rangle. \) \( \square \)

Theorem 3.1.2. If \( \text{ord}_p(p) < \sqrt{\phi(y)} \) then \( M \) has accepted elasticity.

Proof. The condition that \( \text{ord}_p(p) < \sqrt{\phi(y)} \) 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 \( j = 1, \ldots, d, \) let \( A_j = \{ \langle 1-jc \rangle, \langle jc-1 \rangle \} \) containing \( d \) copies of \( \langle 1-jc \rangle \) and \( d \) copies of \( \langle jc-1 \rangle. \) Also let
\[
A_1 = \ldots = A_d = \{ \langle -1 \rangle, \langle 1-c \rangle \}
\]
\[
B_{d+1} = \ldots = B_{2d} = \{ \langle -1 + c \rangle, \langle 1 - 2c \rangle \}
\]
\[
B_{2d+1} = \ldots = B_{3d} = \{ \langle -1 + 2c \rangle, \langle 1 - 3c \rangle \}
\]
\[
\vdots \quad \vdots \quad \vdots
\]
\[
B_{(d-1)d+1} = \ldots = B_{d^2} = \{ \langle -1 + (d-1)c \rangle, \langle 1 - dc \rangle \}
\]

Then \( \sum A_j = \langle 0 \rangle \) for each \( A_j \) and \( \sum B_j = \langle -c \rangle \) for each \( B_j. \) Also,
\[
\bigcup_{i=1}^{d} A_i = \bigcup_{j=1}^{d} \{ \langle 1-jc \rangle \} \cup \bigcup_{j=1}^{d} \{ \langle jc-1 \rangle \} = \bigcup_{i=1}^{d} B_i.
\]

Furthermore, \( \beta(\mathbb{Z}_{cd}, \langle c \rangle, 1) = \text{ord}(\langle c \rangle) = d. \) Therefore, conditions (1), (3), (4), and (5) of the definition of an accepted triple are satisfied.
All that remains is to prove, for any \( j = 1, \ldots, d \), that \( A_j \) has no internal sum in \( \{ (c), (2c), \ldots, (d-1)c \} \). Any submultiset of \( A_j \) is of the form \( \{ (1 - jc)^s, (jc - 1)^t \} \), with \( s, t \leq d < c \). This submultiset has a sum of \( s(1 - jc) + t(jc - 1) = (jc)(t-s) + (s-t) \). Thus, if this internal sum were to be in \( \{ (c), (2c), \ldots, (d-1)c \} \), then we would have \( c \mid s - t \). But since \( s, t \) are nonnegative and less than \( c \), we have \( s - t = 0 \), so \( \{ (1 - jc)^s, (jc - 1)^t \} \) would have a sum of 0. Thus \( A_j \) has no internal sum in \( \{ (c), (2c), \ldots, (d-1)c \} \), and \( (\mathbb{Z}_{cd}, \langle c \rangle, 1) \) is accepted, completing the proof. \( \square \)

### 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 \( c' \equiv 1 \pmod{d} \). Then the map \( \pi : \mathbb{Z}_c \times \mathbb{Z}_d \to \mathbb{Z}_c \times \mathbb{Z}_d \) defined by \( \langle s, t \rangle \mapsto \langle s, ct \rangle \) 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 \( \langle c, c' \rangle = \langle 0, 1 \rangle \). \( \square \)

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

**Proof.**

\[
\begin{align*}
\frac{d}{\alpha} & \leq \alpha c - \alpha \\
\frac{d}{\alpha} & < \alpha c - \alpha + 1 \\
\frac{\alpha + d - 2}{\alpha} & < \frac{\alpha}{\alpha - 1} \quad \text{for } \alpha > 1.
\end{align*}
\]

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 \( A_1, \ldots, A_c, B_1, \ldots, B_f \) which satisfy conditions (1)-(4) and, additionally, \( f/e \) can be arbitrarily close to \( \frac{\alpha d - c d + 1}{\alpha (d - 1)} \). This will ensure that condition (5) will hold.

Let \( n \) be any nonnegative integer. Let \( k \) be a positive integer such that \( k c - d + 1 \geq 0 \). Define

\[
\begin{align*}
A_{1,1} \cdots A_{1,\alpha(d-1)n} & = \left\{ \langle -1, -\alpha \rangle, \langle 1, \alpha \rangle, \langle 0, -1 \rangle \right\} \\
A_{2,1} \cdots A_{2,\alpha} & = \left\{ \langle 1, 0 \rangle, \langle -\alpha(kn) \rangle \right\} \\
B_{1,1} \cdots B_{1,\alpha(-1)(d-1)n} & = \left\{ \langle -1, -\alpha \rangle, \langle 1, 0 \rangle \right\} \\
B_{2,1} \cdots B_{2,\alpha(e-1)n} & = \left\{ \langle 1, \alpha \rangle, \langle 0, -1 \rangle \right\} \\
B_{3,1} \cdots B_{3,(\alpha-1)(d-1)n} & = \left\{ \langle 0, -1 \rangle \right\}.
\end{align*}
\]

Then we have

\[
\bigcup A = \bigcup B.
\]
so condition (1) holds.

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

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

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

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

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

Here $m_2 \leq \alpha - 1$. But looking at the second coordinate of $\sum S$ yields $m_2 \geq \alpha$, 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 $\frac{c d a + d - \alpha + 1}{a (d - 1)}$. We have

$$\frac{f}{e} = \frac{(\alpha(c - 1)(d - 1)n + (\alpha(c - 1)n + ((\alpha - 1)(1 + (d - 1)n)]}{(\alpha + 1)(d - 1)n + (\alpha)}$$

$$\to \frac{\alpha(c - 1)(d - 1) + \alpha(c - 1) + (\alpha - 1)(d - 1)}{\alpha(d - 1)} - \frac{c d a + d - \alpha + 1}{a (d - 1)}$$

as $n$ approaches infinity. This completes the proof. \qed

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

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

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

$$A_1 = \left\langle \langle 0, -1 \rangle^{\alpha - 1}, \langle -1, 0 \rangle^{2\alpha n} \right\rangle$$

$$A_2 = \cdots = A_{2, \alpha - 1} = \left\langle \langle 0, 1 - \alpha \rangle, \langle -1, 0 \rangle^{2\alpha n} \right\rangle$$

$$A_3 = \cdots = A_{3, \alpha n} = \left\langle \langle 1 - \alpha \rangle^{2\alpha - 1}, \langle -1, 1 \rangle \right\rangle$$

$$B_{1, 1} = \cdots = B_{1, \alpha - 1} = \left\langle \langle 0, -1 \rangle, \langle 0, 1 - \alpha \rangle \right\rangle$$

$$B_{2, 1} = \cdots = B_{2, \alpha n(2c - 1)} = \left\langle \langle 1, -\alpha \rangle, \langle -1, 0 \rangle \right\rangle$$

$$B_{3, 1} = \cdots = B_{3, \alpha n} = \left\langle \langle 1, -1 \rangle^{\alpha}, \langle -1, 0 \rangle^{\alpha} \right\rangle$$

To see that condition (1) holds, notice

$$\bigcup A = \bigcup B$$

$$\bigcup \left\langle \langle 0, -1 \rangle^{\alpha - 1}, \langle 0, 1 - \alpha \rangle^{\alpha - 1}, \langle -1, 0 \rangle^{2\alpha n}, \langle 1 - \alpha \rangle^{\alpha n(2c - 1)}, \langle 1, -1 \rangle^{\alpha n} \right\rangle$$
Next we will show that condition (2) holds. Notice that for \( A_1 \), the second component of any internal sum will always be between 0 and \(- (\alpha - 1)\), and hence can never be in \( \{0, 1, \ldots, \langle 0, d - \alpha \rangle \} \). The same is true for each \( A_{2,i} \).

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

\[
\sum \mathcal{S} = \langle c, -\alpha c \rangle = \langle c, -\alpha c + \alpha c - (\alpha - 1) \rangle = \langle c, 1 - \alpha \rangle
\]

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 \( \mathcal{S} = \{\langle 1, -\alpha \rangle, \langle 1, -1 \rangle\} \), and that \( \sum \mathcal{S} = \langle 0, r \rangle \), where \( 1 \leq r \leq d - \alpha \). Here, the summation gives the relationship \( s\langle 1, -\alpha \rangle + \langle 1, -1 \rangle = \langle 0, r \rangle \) meaning

\[ s + 1 \equiv 0 \quad (\text{mod} \ c) \Rightarrow s \equiv -1 \quad (\text{mod} \ c) \]

and

\[-\alpha s - 1 \equiv r \quad (\text{mod} \ d).\]

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

\[-\alpha c + \alpha - 1 \equiv r \quad (\text{mod} \ d) \Rightarrow - (\alpha - 1) + \alpha - 1 \equiv r \quad (\text{mod} \ d) \]

\[0 \equiv r \quad (\text{mod} \ d)\]

or

\[-2\alpha c + \alpha - 1 \equiv r \quad (\text{mod} \ d) \Rightarrow -2(\alpha - 1) + \alpha - 1 \equiv r \quad (\text{mod} \ d) \]

\[-2\alpha + 2 + \alpha - 1 \equiv r \quad (\text{mod} \ d) \]

\[-\alpha + 1 \equiv r \quad (\text{mod} \ d).\]

Here we use the fact that \( \alpha c \equiv - (\alpha - 1) \ (\text{mod} \ d) \) because \( d \mid \alpha c - (\alpha - 1) \). Furthermore, since \( \alpha \geq 1 \), both of these congruences are outside the range of \( 1 \leq r \leq d - \alpha \). 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

\[
\sum A_1 = \langle \alpha - 1, 0 \rangle + \langle 2cn, -1 \rangle = \langle -2cn, 1 - \alpha \rangle = \langle 0, 1 - \alpha \rangle
\]

and

\[
\sum A_{2,i} = \langle 0, 1 - \alpha \rangle + \langle 2cn, -1 \rangle = \langle -2cn, 1 - \alpha \rangle = \langle 0, 1 - \alpha \rangle
\]
Observe that (1) will prove accepted elasticity by showing that $p \equiv q \pmod{d}$.

Therefore, there exists an $n$ such that $\alpha \equiv 0 \pmod{\alpha}$.

Next, define $m$ such that $m \alpha \equiv 0 \pmod{\beta}$.

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

$$\lim_{n \to \infty} \frac{\beta(n - 1)}{\alpha} = \frac{\beta}{\alpha}.$$ 

Therefore, there exists an $n$ large enough so that $\frac{\beta}{\alpha} \geq c$. 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 $1 \leq w \leq \alpha - 2$. 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 $\alpha = \frac{\alpha - w + 1}{\alpha} = c + 1 - \frac{w + 1}{\alpha}$. Again choose some $n \in \mathbb{Z}_{\geq 0}$. Next, define $m$ such that $mw \equiv 0 \pmod{\beta}$.

Next, define $m$ such that $mw \equiv 0 \pmod{\beta}$.

Next, define $m$ such that $mw \equiv 0 \pmod{\beta}$.

To see that condition (1) holds, notice that

$$\bigcup A = \bigcup B =$$
A use two cases of proof by contradiction to prove that condition (2) holds for each $tx$, hence there will be no internal sum in the second coordinate of any internal sum will always be between 1

Next we will show that condition (2) holds. Notice that for each $tx, S$ such that $0 of $S$ where $0 = \alpha c$ and $0 = \alpha x$

and $d = \alpha d$, so $y = \alpha y$. Therefore, case 1 holds.

For case 2, say $S = \{\langle 1, -\alpha \rangle \}$, and that $\sum S = \langle 0, r \rangle$, where $1 \leq r \leq d - \alpha$. This summation gives the relationship $s(\langle 1, -\alpha \rangle) = \langle 0, r \rangle$ meaning that $s = 0 (mod c)$ and $-\alpha = r (mod d)$, where $0 \leq s \leq mc - 1$. Thus $s = tc$ for some $0 \leq t \leq m - 1$. Hence

$$\sum S = \langle c, -\alpha t \rangle = \langle 0, -tw \rangle,$$

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

For case 2, $S = \{\langle 1, -\alpha \rangle \}$ and $\sum S = \langle 0, r \rangle$, where $1 \leq r \leq d - \alpha$. Here, the summation gives the relationship $s(\langle 1, -\alpha \rangle) + \langle 1, w - 2\alpha + 1 \rangle = \langle 0, r \rangle$, so

$$s + 1 \equiv 0 (mod c) \rightarrow s \equiv -1 (mod c)$$

and

$$-s\alpha + wm - 2\alpha + 1 \equiv r (mod d)$$

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

$$\Rightarrow \alpha - t\alpha + wm - 2\alpha + 1.$$

Since $\alpha c \equiv w (mod d)$ we have

$$\Rightarrow \alpha - tw + w - 2\alpha + 1$$

$$\Rightarrow w(m - t) + 1 - \alpha$$

This gives the inequality

$$0 \leq w(m - t) < \alpha \iff 1 - \alpha \leq w(m - t) + 1 - \alpha < 1$$

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

To see that condition (3) holds, notice that

$$\sum A_{1,i} = \langle \alpha - 1, -1 \rangle$$

$$= \langle 0, 1 - \alpha \rangle$$

and

$$\sum A_{2,i} = \langle 0, 1 - \alpha \rangle + \langle mc, -1, 0 \rangle$$

$$= \langle -mc, 1 - \alpha \rangle$$

$$= \langle 0, 1 - \alpha \rangle$$
and
\[ \sum A_{3,i} = (mc - 1)(1, -\alpha) + (1, wm - 2\alpha + 1) = (mc, -mc\alpha + \alpha + wm - 2\alpha + 1) = (mc, -mw + wm - \alpha + 1) = (mc, 1 - \alpha) = (0, 1 - \alpha). \]

Similarly, condition (4) holds because
\[ \sum B_{1,i} = (0, -1) + (0, 1 - \alpha) = (0, -\alpha) \]
and
\[ \sum B_{2,i} = (1, -\alpha) + (-1, 0) = (0, -\alpha) \]
and
\[ \sum B_{3,i} = (-1, 0) + (1, wm - 2\alpha + 1) + (wm - \alpha + 1)(0, -1) = (0, wm - wm - 2\alpha + \alpha + 1 - 1) = (0, -\alpha). \]

Finally, to prove condition (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
\[ \lim_{n \to \infty} \frac{(mc - 1)(\alpha - 1)n + (\alpha - 1)n + (\alpha - 1)}{(wm - \alpha + 1)n + 1 + (\alpha - 1) + (\alpha - 1)n} = \frac{mc(\alpha - 1)}{wm} = \frac{c(\alpha - 1)}{w} \]

Therefore, there exists an \( n \) large enough so that \( \frac{f}{e} \geq c + 1 - \frac{w + 1}{\alpha} \) because
\[ \frac{c(\alpha - 1)}{w} > c + 1 - \frac{w + 1}{\alpha} \Leftrightarrow \frac{c + (\alpha - w - 1)c}{w} > \frac{c + (\alpha - w - 1)}{\alpha} \Leftrightarrow \frac{(\alpha - w - 1)c}{w} > \frac{(\alpha - w - 1)}{\alpha}. \]

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

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 machinery.

**Lemma 3.3.1.** For any integer \( n \geq 3 \), and any integer \( k \) such that \( k \mod 2n \in \{n + 1, ..., 2n\} \), \( (\mathbb{Z}_{2n}, \langle 1 \rangle, k) \) is accepted.
From theorem 2.2.1, we may assume that \( k \in \{n + 1, \ldots, 2n\} \). Let

\[
\begin{align*}
A_1 = \cdots = A_{k-1} &= \left\{ \langle -1 \rangle^{(k-1)} \right\} \\
A_k &= \left\{ \langle n \rangle^{8n^2+1}, \langle n + 1 - k \rangle \right\} \\
B_1 = \cdots = B_{k+2n-2} &= \left\{ \langle -1 \rangle^{(k-n)}, \langle n \rangle \right\} \\
B_{k+2n-1} &= \left\{ \langle -1 \rangle^{(k-1)^2-(k-n)(k+2n-2)}, \langle n \rangle^{8n^2-2n^2+3}, \langle n + 1 - k \rangle \right\}.
\end{align*}
\]

It is clear that each \( A_i \) is well-defined. \( B_1, \ldots, B_{k+2n-2} \) are each well-defined because \( k > n \). To show that \( B_{k+2n-1} \) is well-defined, we must show that \((k-1)^2 - (k-n)(k+2n-2) \geq 0 \) and \( 8n^2 - k - 2n + 3 > 0 \). For the former, we have

\[
\begin{align*}
(k-1)^2 - (k-n)(k+2n-2) &= k^2 - 2k + 1 - (k^2 + 2nk - 2k - nk - 2n^2 + 2n) \\
&= 2n^2 - 2n + 1 - nk \\
&= n(2n - 2 - k) + 1 \\
&\geq n(n + 1 - k) + 1 > 0,
\end{align*}
\]

because \( 2n - 2 \geq n + 1 \) when \( n \geq 3 \). For the latter, we have

\[
8n^2 - k - 2n + 3 \geq 8n^2 - 3n + 3 = 8n(n - 3/8) + 3 > 0,
\]

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

\[
\bigcup_{i=1}^{k} A_i = \left\{ \langle -1 \rangle^{(k-1)^2}, \langle n \rangle^{8n^2+1}, \langle n + 1 - k \rangle \right\} = \bigcup_{i=1}^{k+2n-1} B_i,
\]

proving that condition (1) holds.

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

It is easy to see that condition (3) holds, and that condition (4) holds for \( B_1, \ldots, B_{k+2n-2} \). We also have that

\[
\sum_{i=1}^{k+2n-1} B_{k+2n-1} =
\]

\[
\frac{(k-1)^2 - (k-n)(k+2n-2)}{(1)} + \langle 8n^2 - k - 2n + 3 \rangle + \langle n + 1 - k \rangle
\]

\[
= \langle k^2 - nk + 2k - nk - k^2 + 2k - 1 + 3n - nk + n + 1 - k \rangle
\]

\[
= \langle -2nk + 2n - k \rangle
\]

\[
= \langle -k \rangle,
\]

hence condition (4) holds for all \( B_i \). Finally, since \( \beta(\mathbb{Z}_{2n}, \langle 1 \rangle, k) = 2n \), condition (5) holds, and \( (\mathbb{Z}_{2n}, \langle 1 \rangle, k) \) is accepted. \( \square \)
Corollary 3.3.1. For any $M$ with $\mathbb{Z}_d^*$ cyclic, if $d \geq 6$, $d$ is even, and $\bar{\alpha} > \frac{d}{2}$, then $M$ has accepted elasticity.

Proof. We know that $M$ has accepted elasticity if $(\mathbb{Z}_{ed}, \langle c \rangle, \alpha)$ 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. \hfill \square

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

(I) $d \geq 6$ and

(II) $\bar{\alpha} > d/2$.

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 $A_1, \ldots, A_e, B_1, \ldots, B_f$ 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 $v : \mathbb{Z}_d \rightarrow \mathbb{Z}$ by $v(\langle -n \rangle) = n$ for $n = 0, 1, \ldots, d-1$. For a multiset $S$ of elements of $\mathbb{Z}_d$, let $v(S) = \sum_{s \in S} v(s)$. Notice that $v(S) \equiv v(\sum S) \pmod{d}$.

Since no $A_i$ has an internal sum in $\langle 1 \rangle, \ldots, \langle \beta - \alpha \rangle$, there is no submultiset $S \subseteq A_i$ such that $v(S) = \bar{\alpha}, \bar{\alpha} + 1, \ldots, d-1$. Furthermore, for any $a \in A_i$, $v(a) \in \{0, 1, \ldots, \bar{\alpha} - 1\}$. Since we are assuming $\bar{\alpha} \leq \frac{d}{2}$, we have $2(\bar{\alpha} - 1) < d$, hence it is impossible for $v(A_i)$ to be more than $\bar{\alpha} - 1$. Since $v(A_i) \equiv v(\langle 1 - \alpha \rangle) = \bar{\alpha} - 1 \pmod{d}$, we have $v(A_i) = \bar{\alpha} - 1$ for each $A_i$. Furthermore, since $v(B_i) \equiv v(\langle -\alpha \rangle) = \bar{\alpha} \pmod{d}$, we have $v(B_i) \geq \bar{\alpha}$ for each $B_i$. Thus we have

$$v\left(\bigcup_{i=1}^e A_i\right) = v\left(\bigcup_{i=1}^f B_i\right)$$

$$\sum_{i=1}^e v(A_i) = \sum_{i=1}^f v(B_i)$$

$$\varepsilon(\bar{\alpha} - 1) \geq \frac{f \bar{\alpha}}{\varepsilon} \implies \frac{f}{\varepsilon} \leq \frac{\bar{\alpha} - 1}{\bar{\alpha}} < 1 + \frac{\beta - 1}{\alpha},$$

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 $\frac{d}{2} < \bar{\alpha} < d$, the only remaining case to check is $d = 4$ and $\bar{\alpha} = 3$.

Suppose that the integers $e, f$ and multisets $A_1, \ldots, A_e, B_1, \ldots, B_f$ satisfy conditions (1)-(5) from the definition of an accepted triple. Then $f/e = 2$. Since $\sum B_i = \langle 1 \rangle$, each $B_i$ contains an odd element. Since no $A_i$ has an internal sum of $\langle 1 \rangle$, each $A_i$ contains a $\langle 3 \rangle$. Since $3 \langle 3 \rangle = \langle 1 \rangle$, each $A_i$ contains at most 2 copies of $\langle 3 \rangle$, and since each $f/e = 2$, each $A_i$ contains exactly 2 copies of $\langle 3 \rangle$. Then no $A_i$ contains a $\langle 2 \rangle$ because $\langle 3 \rangle + \langle 2 \rangle = \langle 1 \rangle$. Hence each $B_i$ contains exactly one $\langle 3 \rangle$ and no $\langle 2 \rangle$ or $\langle 1 \rangle$, contradicting the fact that $\sum B_i = \langle 1 \rangle$. Thus $(\mathbb{Z}_d, \langle 1 \rangle, \alpha)$ is not accepted, completing the proof. \hfill \square

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

Proof. If \( d > 1 \), then \( 1 \leq \frac{d}{2} \), hence \((\mathbb{Z}_p^*, [p], \alpha)\) is not accepted when \( \overline{p} = 1 \). Thus, 
\( \omega(\mathbb{Z}_p^*, [p]) = \infty \). \( \square \)

3.3.2. The Case \( m = 2 \).

**Theorem 3.3.2.** If \( m = 2 \) and \( \overline{p} > \frac{d}{2} \) then \( M \) has accepted elasticity.

Proof. If \( d \) is odd, then this follows directly from theorem 3.2.2. If \( d \) is even, and \( d \geq 6 \), then this follows from corollary 3.3.1. If \( d = 2 \), then \( \overline{p} = 2 \), 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. \( \square \)

**Theorem 3.3.3.** If \( m = 2 \), \( d \) is even, and  
\[ \alpha < \frac{1 + \sqrt{4d - 3}}{2} \]

then \( M \) does not have accepted elasticity.

Proof. First, observe that  
\[
\begin{align*}
0 &< (d-1)^2 + 1 \\
0 &< d^2 - 2d + 2 \\
4d - 3 &< d^2 + 2d + 1 \\
\sqrt{4d - 3} &< d + 1 \\
\frac{1 + \sqrt{4d - 3}}{2} &< \frac{d + 2}{2} \\
\frac{1 + \sqrt{4d - 3}}{2} &< \frac{d}{2},
\end{align*}
\]

so \( \alpha \leq \frac{d}{2} \).

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

To prove this, we will use strong induction on \( \alpha \). For \( \alpha = 1 \), \( A \) 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 \( A \) contains at most two distinct odds. If \( A \) contains two copies of the same element, say \( a \), then \( 2a = \langle 0 \rangle \) which means \( a = 0 \) or \( d \), and hence \( \alpha \) is even, contradiction. Thus \( |A| \leq 2 \), completing the base case.

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

Assume that \( A \) contains an even element. Then for some \( m \in \{1, ..., k - 1\}, \langle -2m \rangle \in A \). Let \( A' = A \setminus \langle -2m \rangle \}. If \( A' \) had an internal sum in 
\[ \langle 2 \{ (d - k) + 1 \}, ..., \langle 2 \{ (d - k) + m \} \rangle \}, \]

then \( A \) would have an internal sum in 
\[ \{ \langle 2 \{ (d - k) - m + 1 \}, ..., \langle 2 \{ (d - k) \} \}. \]

Since \( m \leq k - 1 \) and \( k \leq \frac{d}{2} \), we have \( m + k \leq 2k - 1 < d \), so \( (d - k) - m + 1 > 1 \). Thus \( 1 < (d - k) - m + 1 < d - k \). Hence \( A \) has no internal sum in \( \langle 2 \{ (d - k) - m + 1 \}, ..., \langle 2 \{ (d - k) \} \rangle \}, so \( A' \) has no internal sum in \( \{ \langle 2 \{ (d - k) + 1 \}, ..., \langle 2 \{ (d - k) + m \} \rangle \}. Since \( A' \subset A \), it also has no internal sums in \( \{ \langle 2 \rangle, ..., \langle 2 \{ (d - k) \} \}\}. Thus \( A' \) has no internal sum in \( \{ \langle 2 \rangle, ..., \langle 2 \{ (d - k) + m \} \rangle \}. Thus, by the inductive hypothesis,
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 $d \geq 3$. First observe that

$$(d-2)^2 \geq 0$$

$$d^2 - 4d + 4 \geq 0$$

$$\frac{d^2}{4} \geq \frac{d-1}{2} \geq \sqrt{d-1}.$$
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 \( \{0, 1, \ldots, d-1\} \) that is congruent to \( t \) modulo \( d \). Given a multiset \( S \) of elements of \( \mathbb{Z}_c \times \mathbb{Z}_d \), define \( g(S) = \sum_{s \in S} g(s) \).

Notice that \( g(S) \equiv g(\sum S) \pmod{d} \).

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

We will prove this claim by induction on \( \alpha \). 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 \( A \) has no restricted sums in \( \{\langle 0, 1 \rangle, \ldots, \langle 0, d-1 \rangle\} \), then its only type 0 element is \( \langle 0, 0 \rangle \). Suppose \( A \) 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 \( A \) has three type 1 elements, \( g(A) = 0 \). Thus, \( A \) can have at most two elements with a nonzero \( g \)-value, and therefore \( g(A) \leq 2(d-1) = (\alpha + 1)(d-1) \).

Suppose that the claim holds for \( \alpha = 1, \ldots, k-1 \), where \( k \leq \frac{d}{2} \). For the sake of contradiction, suppose that there is some multiset \( A \) of elements of \( \mathbb{Z}_c \times \mathbb{Z}_d \) such that \( g(A) \leq (k-1)(d-1) \) and \( g(A) > (k + 1)(d-1) \).

Suppose \( A \) contains a nonzero type 0 element \( \langle 0, -s \rangle \) for some \( s \in \{1, \ldots, k-1\} \). Let \( A' = A \setminus \{\langle 0, -s \rangle\} \). Then \( A' \) has no internal sum in \( \{\langle 0, 1 \rangle, \ldots, \langle 0, d-k \rangle\} \). Hence it must be that \( g(A') \leq (k-1)(d-1) \). But then, solving, we get \( g(A') \leq (k-1)(d-1) \).

Since we can ignore \( \langle 0, 0 \rangle \) elements of \( A \), let \( A = \langle 1, a_1 \rangle^{(n_1)} \langle 1, a_2 \rangle^{(n_2)} \). Since \( g(A) > (k + 1)(d-1) \), it must be that \( n_1 + n_2 \geq k + 2 \). WLOG, assume \( n_1 \geq 2 \). Let \( 2(1, a_1) = \langle 0, -s \rangle \), where \( s \in 1, \ldots, k-1 \). Let \( A'' = A \setminus \langle 1, a_1 \rangle^{(2)} \). Then, by the argument in the above paragraphs, \( g(A'') \leq (k-1)(d-1) \). Hence, \( g(A) \leq (k + 1)(d-1) \), contradiction.

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 \( c, f \) and multisets \( A_1, \ldots, A_n, B_1, \ldots, B_f \) satisfy conditions (1)-(5) from the definition of an accepted triple. Then, for each \( A_i \), we know \( g(A_i) \leq (\alpha + 1)(d-1) \). Since \( g(A_i) \equiv 1 - \alpha \pmod{d} \), we have \( g(A_i) \leq d(1 + \alpha) + 1 - \alpha - d \leq d(1 + \alpha) + 1 - \alpha - d = da - \alpha + 1 \). Furthermore, for each \( B_i \) we have \( g(B_i) \equiv -\alpha \pmod{d} \), and thus \( g(B_i) \geq d - \alpha \).
Hence \( c(d\alpha - \alpha + 1) \geq f(d - \alpha) \Rightarrow \)

\[
\frac{f}{c} \leq \frac{d\alpha - \alpha + 1}{d - \alpha} \\
\frac{\alpha + d - 1}{\alpha} \leq \frac{d\alpha - \alpha + 1}{d - \alpha} \\
d^2 - \alpha^2 - d + \alpha \leq d\alpha^2 - \alpha^2 + \alpha \\
d - 1 \leq \alpha^2 \\
\sqrt{d - 1} \leq \alpha,
\]

which is a contradiction, completing the proof.

\[\square\]

**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 \( \omega(M) = \infty \). \[\square\]

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 \( a \in \mathbb{Z}_q \setminus \{0\} \).

**Proof.** Let \( S = \{m_1, \ldots, m_{q-1}\} \) be a multiset, where \( m_i \in \mathbb{Z}_q \setminus \{0\} \) for \( i = 1, \ldots, q-1 \). Define \( n_1, \ldots, n_{q-1} \) as follows: let \( n_1 = m_1 \), and if \( n_1, \ldots, n_{s-1} \) has been defined, define \( n_s = km_s \), where \( k \) is the smallest natural number such that \( km_s \notin \{n_1, \ldots, n_{s-1}\} \).

If \( q \) is prime, \( m_i, 2m_i, \ldots, (q-1)m_i \) are all distinct in \( \mathbb{Z}_q \), hence \( k \) exists and is less than \( q \), since \( 1 \leq q \leq q-1 \). Thus \( n_1, \ldots, n_{q-1} \) are distinct nonzero elements of \( \mathbb{Z}_q \). Therefore, every nonzero element of \( \mathbb{Z}_q \), and specifically \( a \), is contained in \( \{n_1, \ldots, n_{q-1}\} \). Hence it suffices to show that \( n_i \) is an internal sum of \( S \) for each \( i = 1, \ldots, p-1 \).

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

Therefore, \( n_1, \ldots, n_{q-1} \) are all internal sums of \( S \), and hence \( a \) is an internal sum of \( S \). \[\square\]
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 $\mathbb{Z}_q \setminus \{0\}$ 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 $\overline{b} \neq 0$, $\exists \{k_1, ..., k_n\} \subset \{1, ..., q + 1\}\setminus\{i, j\}$ 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, $a_j = -(a_{k_1} + 3 \cdots + a_{k_n})$, hence $a_i = a_j$.

Lemma 3.3.4. If a multiset $A$ of elements of $\mathbb{Z}_q \setminus \{0\}$ 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 $\overline{a_i} = \cdots = \overline{a_q}$ 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 $a_1 = 0$ (mod $q$), 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 $A_1, ..., A_e, B_1, ..., B_f$ of elements of $\mathbb{Z}_{cd}$ such that

\begin{itemize}
  \item[(1')] $\bigcup_{i=1}^{e} A_i = \bigcup_{j=1}^{f} B_j$
  \item[(2')] for $i = 1, ..., e$, $A_i$ has no internal sum in $\{\langle c \rangle, \langle 2c \rangle, ..., \langle (d - 1)c \rangle\}$
  \item[(3')] for $i = 1, ..., e$, $\sum A_i = \langle 0 \rangle$
  \item[(4')] for $i = 1, ..., f$, $\sum B_i = \langle -c \rangle$
  \item[(5')] $f/e = (\alpha + \beta - 1)/\alpha$.
\end{itemize}

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 $\overline{a}$ denote its residue class modulo $c$.

We claim that for $i = 1, ..., e$, $A_i$ contains at most $2c - 2$ nonzero elements. For assume that $A_i$ did contain at least $2c - 1$ nonzero elements. Since $A_i$ has no internal sum in $\{\langle c \rangle, ..., \langle (d - 1)c \rangle\}$, when the elements are viewed as elements of $\mathbb{Z}_c$, 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 $A_i$ and $c - 1$ nonzero residues modulo $c$, the pigeonhole principle tells us that there are three elements in $A_i$ with the same nonzero residue modulo $c$. Since $c = 3$, this is a contradiction, proving the claim.

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

It now suffices to show that $\frac{(\alpha + \beta - 1)/\alpha}{c - 1} = 2 \iff \beta - \alpha > 1$. Since $\overline{a} = 1$, 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 $\frac{(\alpha + \beta - 1)/\alpha}{c - 1} = 2$, 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 \( A_1, \ldots, A_e, B_1, \ldots, B_f \) 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
\[
(5a) \quad \frac{e}{f} > \frac{c\pi - d - \pi + 1}{\pi(d - 1)} - \epsilon.
\]

Proof. Using the isomorphism from theorem 3.2.1, conditions (1)-(4) become
\[(1a) \quad \bigcup_{i=1}^{f} A_i = \bigcup_{i=1}^{f} B_i
\]
(2a) for \( i = 1, \ldots, e \), \( A_i \) has no internal sum in \( \{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \ldots, \langle 0, d - \pi \rangle\} \)
(3a) for \( i = 1, \ldots, e \), \( \sum A_i = \langle 0, 1 - \pi \rangle 
(4a) for \( i = 1, \ldots, f \), \( \sum B_i = \langle 0, -\pi \rangle 

Let \( n \) be any nonnegative integer. Let \( k \) be a positive integer such that \( kc - d + 1 \geq 0 \). Define
\[
A_{1,1} = \cdots = A_{1,\pi(d-1)n} = \left\{ \langle -1, -\pi \rangle^{(e-1)}, \langle 1, \pi \rangle^{(e-1)}, \langle 0, -1 \rangle^{(\pi-1)} \right\}
\]
\[
A_{2,1} = \cdots = A_{2,\pi} = \left\{ \langle 1, 0 \rangle^{(e-1)(kn)}, \langle 0, -1 \rangle^{(\pi-1)} \right\}
\]
\[
B_{1,1} = \cdots = B_{1,\pi(d-1)n} = \left\{ \langle -1, -\pi \rangle, \langle 0, 0 \rangle \right\}
\]
\[
B_{2,1} = \cdots = B_{2,\pi(c-1)n} = \left\{ \langle 1, \pi \rangle^{(d-1)}, \langle 1, 0 \rangle^{(kc-d+1)} \right\}
\]
\[
B_{3,1} = \cdots = B_{3,\pi-1}[1+(d-1)n] = \left\{ \langle 0, -1 \rangle^{(\pi-1)} \right\}
\]

Then we have
\[
\bigcup A = \bigcup B = \left\{ \langle -1, -\pi \rangle^{(d-1)n}, \langle 1, \pi \rangle^{(\pi-1)(d-1)n}, \langle 0, -1 \rangle^{(\pi-1)[1+(d-1)n]}, \langle 0, 0 \rangle^{(\pi-1)(kn)} \right\},
\]
so condition (1a) holds.

We will show that condition (2a) holds by contradiction. Assume that \( A_{1,i} \) has an internal sum in \( \{\langle 0, 1 \rangle, \ldots, \langle 0, d - \pi \rangle\} \). Then there is a submultiset \( S \subset A_{1,i} \) such that \( \sum S = \langle 0, \gamma \rangle \) for some \( \gamma \in \{1, \ldots, d - \pi\} \). \( S \) must be of the form
\[
\left\{ \langle -1, -\pi \rangle^{m_1}, \langle 1, \pi \rangle^{m_2}, \langle 0, -1 \rangle^{m_3} \right\}
\]
where \( m_1, m_2, m_3 \in \mathbb{Z}_{\geq 0}, m_1 \leq c - 1, \) and \( m_3 \leq \pi - 1 \). Looking at the first coordinate of \( \sum S \) yields \( m_2 - m_1 \equiv 0 \pmod{c} \), and the restrictions on \( m_1 \) and \( m_2 \) yield \( m_1 = m_2 \). Hence \( \sum S = \langle 0, -m_3 \rangle \in \{\langle 0, 1 \rangle, \ldots, \langle 0, d - \pi \rangle\} \), and therefore \( m_3 \geq \pi \), contradiction.

Now assume that \( A_{2,1} \) has an internal sum of \( \langle 0, \gamma \rangle \) for some \( \gamma \in \{1, \ldots, d - \pi\} \). Then there is some submultiset \( S \subset B_{2,i} \) such that \( \sum S = \langle 0, \gamma \rangle \). \( S \) must be of the form
\[
\left\{ \langle 1, 0 \rangle^{m_1}, \langle 0, -1 \rangle^{m_2} \right\}
\]
Here \( m_2 \leq \pi - 1 \). But looking at the second coordinate of \( \sum S \) yields \( m_2 \geq \pi \), 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
\[
\frac{e}{f} = \frac{(\pi(c - 1)(d - 1)n + (\pi(c - 1)n) + ((\pi - 1)(1 + (d - 1)n))}{(\pi(d - 1)n) + (\pi)}
\]
\[
\rightarrow \frac{\pi(c - 1)(d - 1) + \pi(c - 1) + (\pi - 1)(d - 1)}{\pi(d - 1)}
\]
\[
\rightarrow \frac{c \pi - d - \pi + 1}{\pi(d - 1)}
\]
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 \( d \geq 4 \), then
\[
\omega(M) \leq \left\lfloor \frac{d-3}{2} \right\rfloor d + 2.
\]
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 \( d \geq 4 \).

From lemma 3.3.5 and theorem 1.3.4, we know that \( M \) has accepted elasticity if
\[
\frac{cd\bar{\alpha} - d - \bar{\alpha} + 1}{\bar{\alpha}(d-1)} > \frac{(k d + \bar{\alpha}) + \{(k+1)d - 1\}}{\bar{\alpha}(d-1)}.
\]
Let \( \alpha = kd + \bar{\alpha} \), so that \( \beta = (k+1)d \). Then, plugging in \( c = 3 \) and rearranging terms, we get
\[
\frac{3d\bar{\alpha} - d - \bar{\alpha} + 1}{\bar{\alpha}(d-1)} > \frac{(k d + \bar{\alpha}) + \{(k+1)d - 1\}}{\bar{\alpha}(d-1)}.
\]

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

If \( \bar{\alpha} > 1 \), notice that
\[
\frac{\bar{\alpha}}{\bar{\alpha} - 1} - \frac{\bar{\alpha}(d - 2\bar{\alpha} - 1)}{(\bar{\alpha} - 1)d + \bar{\alpha} + 1} = \frac{\bar{\alpha}(\bar{\alpha} - 1)[(\bar{\alpha} - 1)d + (\bar{\alpha} - 1) + 2] - \bar{\alpha}(d - 2\bar{\alpha} - 1)}{(\bar{\alpha} - 1)d + \bar{\alpha} + 1}
\]
\[
= \frac{\bar{\alpha}[(d + 1 + \frac{1}{\bar{\alpha} - 1}) - (d - 2\bar{\alpha} - 1)]}{(\bar{\alpha} - 1)d + \bar{\alpha} + 1}
\]
\[
= \frac{2\bar{\alpha}(\bar{\alpha} + 1 + \frac{1}{\bar{\alpha} - 1})}{(\bar{\alpha} - 1)d + \bar{\alpha} + 1}
\]
\[
> 0.
\]
Hence \( \frac{\bar{\alpha}}{\bar{\alpha} - 1} > \frac{\bar{\alpha}(d-2\bar{\alpha} - 1)}{(\bar{\alpha} - 1)d + \bar{\alpha} + 1} \), and, since \( 2 \geq \frac{\bar{\alpha}}{\bar{\alpha} - 1} \), we conclude that \( M \) has accepted elasticity when \( \bar{\alpha} \geq 2 \) and \( k \geq 2 \).

We also know that when \( \bar{\alpha} = 1 \) and \( k > \frac{d-3}{2} \), then \( M \) has accepted elasticity.

Hence, if \( \frac{d-3}{2} \geq 2 \), then \( M \) has accepted elasticity for all \( \alpha \geq \left\lfloor \frac{d-3}{2} \right\rfloor d + 2 \). Therefore, if \( d \geq 7 \) and \( 3 \nmid d \), then \( \omega(M) \leq \left\lfloor \frac{d-3}{2} \right\rfloor d + 2 \).

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. \( \square \)

3.3.4. The Case \( c \geq 4 \).

Lemma 3.3.6. There exist integers \( e, f \) and multisets \( A_1, \ldots, A_e, B_1, \ldots, B_f \) which satisfy conditions (1)-(4) from the definition of an accepted triple, and additionally satisfy
\[
(5') \quad f/e = c - 1.
\]
Proof. We will let $e = d$ and $f = (c - 1)d$. Let

$$A_i = \left\{ \langle 1 + i\alpha \rangle^{(c-1)}, \langle -1 - i\alpha \rangle^{(c-1)}, \langle (1 - \alpha)\psi \rangle \right\}$$

for $i = 1, \ldots, d$, let

$$B_{i,1} = \left\{ \langle 1 + i\alpha \rangle, \langle -1 - (i + 1)\alpha \rangle, \langle (1 - \alpha)\psi \rangle \right\}$$

for $i = 1, \ldots, d$, and let

$$B_{i,j} = \left\{ \langle 1 + i\alpha \rangle, \langle -1 - (i + \alpha)\psi \rangle \right\}$$

for $i = 1, \ldots, d$ and $j = 2, \ldots, c - 1$. Then we claim that $A_i$ for $i = 1, \ldots, d$ and $B_{i,j}$ for $i = 1, \ldots, d$ and $j = 1, \ldots, c - 1$ satisfy conditions (1)-(4) and (5').

To see that (1) holds, notice that

$$\bigcup_{i=1}^{d} A_i = \bigcup_{i=1}^{d} \left\{ \langle 1 + i\alpha \rangle^{(c-1)}, \langle -1 - i\alpha \rangle^{(c-1)}, \langle (1 - \alpha)\psi \rangle \right\}$$

and

$$\bigcup_{j=2}^{c-1} B_{i,j} = \bigcup_{j=2}^{c-1} \left\{ \langle 1 + i\alpha \rangle, \langle -1 - (i + \alpha)\psi \rangle \right\}$$

where $\psi$ is a primitive root modulo $d$. The proof is completed by showing that conditions (1)-(4) and (5') hold.

We will show that (2) holds by contradiction. Assume (2) does not hold. Then there is some $k \in \{1, \ldots, d\}$ and some $m \in \{1, \ldots, \beta - \alpha\}$ such that $A_k$ has an internal sum of $\langle mc \rangle$. Suppose $S \subseteq A_k$ is such that $\sum S = \langle mc \rangle$. Then $S$ is either of the form $\left\{ \langle 1 + kc \rangle^{(r)}, \langle -1 - kc \rangle^{(s)} \right\}$ or the form $\left\{ \langle 1 + \alpha \rangle^{(r)}, \langle -1 - \alpha \rangle^{(s)} \right\}$. First suppose $S$ is of the first form. Then $r(1 + kc) + s(-1 - kc) = \langle mc \rangle$, so $(r - s)kc \equiv mc \pmod{cd}$. But since $r, s \in \{0, \ldots, c - 1\}$, 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 $S$ is of the second form, we can similarly conclude that $r = s$.

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

Theorem 3.3.8. If $c \geq 4$, then $\omega(M) \leq \left\lfloor \frac{d-1}{c-2} \right\rfloor$. In particular, $\omega(M) \leq d - 1$.

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

\[
\rho < \frac{(2k + 1)d + \pi}{kd + \alpha} \leq \frac{(2k + 1)d}{kd} = \frac{2k + 1}{k} \leq 3 \leq c - 1.
\]

Therefore, for \( k \geq 1 \), \( \rho < c - 1 \).

Now, we will consider the case where \( k = 0 \), so that \( \alpha = \pi \) and \( \beta = d \). Then

\[
\begin{align*}
\frac{\alpha + d - 1}{\alpha} & \leq c - 1 \quad (c - 1) \\
\frac{d - 1}{\alpha} & \leq c - 1 \quad (c - 2) \\
\frac{d - 1}{c - 2} & \leq \pi
\end{align*}
\]

Thus for any \( \alpha \geq (d - 1)/(c - 2) \), \( \rho \leq c - 1 \), as desired. \( \square \)

4. Noncyclic Unit Group

4.1. General Noncyclic Case.

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

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

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

By assumption, \( d \mid n_{k-1} \), and thus \( d \mid n_k \), hence \( g_1, g_2 \in \mathbb{Z} \). Since \( d \langle a_1, \ldots, a_k \rangle = \langle 0, \ldots, 0 \rangle \), 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 \( A_1, \ldots, A_e, B_1, \ldots, B_f \) of elements of \( \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \) such that

\begin{enumerate}
  \item [(1')] \( \bigcup_{i=1}^e A_i = \bigcup_{i=1}^f B_i \)
  \item [(2')] for \( j = 1, \ldots, e \), \( A_j \) has no internal product in \( \{r\langle a_1, \ldots, a_k \rangle \mid 1 \leq r \leq d - 1 \} \)
  \item [(3')] for \( j = 1, \ldots, e \), \( \sum A_j = \langle 0, \ldots, 0 \rangle \)
  \item [(4')] for \( j = 1, \ldots, f \), \( \sum B_j = \langle -a_1, \ldots, -a_k \rangle \), and
\end{enumerate}
(5') \( f/e = d \).
Define \( e = 2, f = 2d \), and
\[
\mathcal{A}_1 = \langle \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2 \rangle \rangle^{2d} \\
\mathcal{A}_2 = \langle \langle 0, ..., 0, (u - h_1)g_1, (v - h_2)g_2 \rangle \rangle^{2d}
\]
\[
\mathcal{B}_1 = \cdots = \mathcal{B}_{2d} = \langle \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2 \rangle, \langle 0, ..., 0, (u - h_1)g_1, (v - h_2)g_2 \rangle \rangle.
\]
Conditions (1') and (5') hold trivially, hence it suffices to show that these multisets satisfy conditions (2'), (3'), and (4').

Since \( \text{ord}_p(p) = d, da_i \equiv 0 \pmod{n_i} \) for \( i = 1, ..., k \), we have
\[
\sum \mathcal{A}_1 = 2d\langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2 \rangle
\]
\[
= \langle 0, ..., 0, -2ud^{n_k-1}, -2vd^{n_k}/d \rangle
\]
\[
= \langle 0, ..., 0 \rangle.
\]
\[
\sum \mathcal{A}_2 = 2d\langle 0, ..., 0, (u - h_1)g_1, (v - h_2)g_2 \rangle
\]
\[
= \langle 0, ..., 0, 2(u - h_1)d^{n_k-1}, 2(v - h_2)d^{n_k}/d \rangle
\]
\[
= \langle 0, ..., 0 \rangle.
\]
\[
\sum \mathcal{B}_1 = \cdots = \sum \mathcal{B}_{2d} = \langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2 \rangle + \langle 0, ..., 0, (u - h_1)g_1, (v - h_2)g_2 \rangle
\]
\[
= \langle -a_1, ..., -a_{k-2}, -g_1h_1, -g_2h_2 \rangle
\]
\[
= \langle -a_1, ..., -a_k \rangle.
\]
Therefore, conditions (3') and (4') hold.

Now, for the sake of contradiction, suppose that \( \mathcal{A}_1 \) had an internal sum contained in \( \{r\langle a_1, ..., a_k \rangle \mid 1 \leq r \leq d - 1 \} \). Then there exist positive integers \( r, s \), with \( 1 \leq r \leq d - 1 \) 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
\[
r a_{k-1} \equiv -sug_1 \pmod{n_{k-1}} \implies rh_1 \equiv -su \pmod{d}
\]
\[
r a_k \equiv -svg_2 \pmod{n_k} \implies rh_2 \equiv -sv \pmod{d}
\]
which gives us
\[
rh_2u \equiv -svu
\]
\[
eq rh_1v
\]
\[
rmb_2 \equiv rmb_1
\]
\[
rmb_1 + rm \equiv rmb_1
\]
\[
rm \equiv 0 \pmod{d}.
\]
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 \( d\langle -a_1, ..., -a_{k-2}, -ug_1, -vg_2 \rangle = 0 \), 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 $1 \leq r \leq d - 1$. Therefore, $A_1$ has no internal sums contained in $(r^{a_1, \ldots, a_k})_{1 \leq r \leq d - 1}$.

If we let $u' = u - h_1$ and $v' = v - h_2$, then
\[
\begin{align*}
\frac{u'b_2 - v'b_1}{v} &= (u - h_1)b_2 - (v - h_2)b_1 \\
&= ub_2 - mb_1b_2 - vb_1 + mb_1b_2 \\
&= ub_2 - vb_1 \\
&= 1,
\end{align*}
\]
and so the argument for why $A_2 = \{ (u', v') \mid 1 \leq r \leq d - 1 \}$ has no internal sums contained in $(r^{a_1, \ldots, a_k})_{1 \leq r \leq d - 1}$ is nearly identical to the argument for $A_1 = \{ (u, v) \mid 1 \leq r \leq d - 1 \}$. Therefore, condition $(2')$ holds, completing the proof. \hfill \Box

**Corollary 4.1.1.** If $y = 8, 12, 24, 63, 80, 126, 240, 252, 504, 513, 544, 1026, 1682, \text{ or } 2107$, then $M$ has accepted elasticity.

**Proof.** For each of these values of $y$, when $Z_y^x$ 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 $\text{ord}_y(p) \mid n_{k-1}$. \hfill \Box

### 4.2. Case Study: $Z_y^x \cong Z_2 \times Z_6 \cong Z_2 \times Z_2 \times Z_3$.

**Theorem 4.2.1.** Assume $Z_y^x \cong Z_2 \times Z_2 \times Z_3$. Then the elasticity of $M$ is not accepted iff $(Z_y^x, [p], \alpha)$ 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 $Z_y^x \cong Z_2 \times Z_2 \times Z_3$, with $\psi$ an isomorphism mapping $Z_y^x \to Z_2 \times Z_2 \times Z_3$, and for multisets $S$ of elements of $Z_y^x$, let $S'$ be the image of $S$ under $\psi$.

Let $\emptyset = \langle 0, 0 \rangle \in Z_2 \times Z_2$. Then if $c \in Z_3$, then $\langle 0, c \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle a + b, c \rangle \in Z_2 \times Z_2 \times Z_3$, where $a$ and $b$ are distinct nonzero elements of $Z_2 \times Z_2$.

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

1. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle a + b, x \rangle, \langle 0, 0 \rangle \}$, $n \in \mathbb{N}_0$
2. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle 0, 0 \rangle \}$, $n \in \mathbb{N}_0$
3. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle 0, 0 \rangle \}$, $n \in \mathbb{N}_0$
4. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle 0, 0 \rangle \}$, $m, n \in \mathbb{N}_0$
5. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle 0, 0 \rangle \}$, $m, n \in \mathbb{N}_0$, or
6. $\{ \langle a, x \rangle, \langle b, x \rangle, \langle 0, 0 \rangle \}$, $j = k \equiv l \pmod{2}$, $n \in \mathbb{N}_0$.

where $a$ and $b$ are distinct nonzero elements of $Z_2 \times Z_2$.

**Proof.** Suppose $(Z_y^x, [p], \alpha)$ is accepted, $\text{ord}_y(p) = 3$, and $\alpha \equiv 1 \pmod{3}$. Then there exist positive integers $e, f$ and multisets $A_1, \ldots, A_e, B_1, \ldots, B_f$ of elements of $Z_y^x$ which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $i \in \{1, \ldots, e\}$. Since $\alpha \equiv 1 \pmod{3}$, and $\beta(Z_y^x, [p], \alpha) = \text{ord}_y(p)$ for some positive integer $m$ such that $m \text{ord}_y(p) \geq \alpha > (m - 1)\text{ord}_y(p)$, then $\beta(Z_y^x, [p], \alpha) = \alpha + 2$. By condition $(2')$ of theorem 1.3.2, we have for $j = 1, \ldots, e$, $A'_i$ has no internal
sum in \( \{ \psi([p]), \psi([p]^2) \} \). Further, by conditions (3') and (4') of theorem 1.3.2, we have \( \sum \mathcal{A}'_i = \psi([p]^{1-\alpha}) = \psi([1]) = \langle 0, 0 \rangle \) for \( j = 1, \ldots, e \), and \( \sum \mathcal{B}'_j = \psi([p]^{-\alpha}) = \psi([p]^{-1}) = \psi([p]^2) \) for \( i = 1, \ldots, f \). Note that if \( \psi([p]) = \langle a, 0 \rangle \) for some \( a \neq 0 \), then \( \psi([p]^2) = \langle 0, 0 \rangle \), and \( \text{ord}_p(p) = 2 \). If \( \psi([p]) = \langle a, x \rangle \) with \( a \neq 0, x \neq 0 \), then \( \psi([p]^3) = \langle a, 0 \rangle \), and \( \text{ord}_p(p) = 6 \). If \( \psi([p]) = \langle 0, x \rangle \) with \( x \neq 0 \), then \( \psi([p]^3) = \langle 0, 0 \rangle \) and \( \text{ord}_p(p) = 3 \). So fix \( \psi([p]) = \langle 0, x \rangle \). Note that for all \( n \in \mathbb{N}_n \), inserting \( \langle 0, 0 \rangle^n \) 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 \( \langle 0, 0 \rangle^n \in \mathcal{A}'_i \) for \( i = 1, \ldots, e \), \( n_i \geq 0 \).

1. Suppose \( \mathcal{A}'_i \) contains more than two elements with a \( \mathbb{Z}_3 \) component of \( x \). Since \( \langle a, x \rangle^2 = \langle 0, -x \rangle = \psi([p]^2) \) for all \( a \in \mathbb{Z}_3 \times \mathbb{Z}_2 \), 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 \( \langle a, -x \rangle \langle b, x \rangle \langle a + b, x \rangle = \langle a, 0 \rangle \langle a, x \rangle = \langle 0, 0 \rangle = \psi([p]) \), 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 \( \mathcal{A}'_i = \{ \langle a, x \rangle, \langle b, x \rangle, \langle a + b, x \rangle, 0, 0 \} \), with \( a \) and \( b \) distinct nonzero elements of \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

2. Similarly, \( \langle a, -x \rangle^2 = \langle 0, -x \rangle = \psi([p]^2) \) and \( \langle a, x \rangle \langle b, -x \rangle \langle a + b, -x \rangle = \langle a, 0 \rangle \langle a, -x \rangle = \langle 0, -x \rangle = \psi([p]^2) \) 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 \( \mathcal{A}'_i = \{ \langle a, -x \rangle, \langle b, -x \rangle, \langle a + b, -x \rangle, 0, 0 \} \), 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 \( \sum \mathcal{A}'_i = \langle 0, 0 \rangle \). 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 \( \langle a, 0 \rangle \langle a, x \rangle = \langle b, 0 \rangle \langle b, x \rangle = \langle a + b, 0 \rangle \langle a, -x \rangle \langle b, -x \rangle = \langle 0, 0 \rangle = \psi([p]) \).

4. Now suppose \( \mathcal{A}'_i \) contains exactly one element having a \( \mathbb{Z}_3 \) component equal to \( x \). Then since \( \sum \mathcal{A}'_i = \langle 0, 0 \rangle \) by (3') of theorem 1.3.2, \( \mathcal{A}'_i \) contains \( 3n + 1 \) elements with \( -x \) as their \( \mathbb{Z}_3 \) component for some \( n \in \mathbb{N}_n \). 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 \( a \neq 0 \), then \( \langle a, 0 \rangle \notin \mathcal{A}'_i \) since \( \langle a, 0 \rangle \langle a, x \rangle = \langle 0, x \rangle = \psi([p]) \). If \( \langle b, 0 \rangle \in \mathcal{A}'_i \) for some \( b \neq 0, a \), then \( \langle a + b, 0 \rangle \notin \mathcal{A}'_i \) since \( \langle a, x \rangle \langle b, 0 \rangle \langle a + b, 0 \rangle = \langle 0, x \rangle = \psi([p]) \). And \( \sum \mathcal{A}'_i = \langle 0, 0 \rangle = \sum \{ \langle a, x \rangle, \langle a, -x \rangle, \langle b, 0 \rangle \} \) for all \( m \in \mathbb{N}_m \), 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 \( \mathbb{Z}_3 \) component, but now \( \langle a, x \rangle \in \mathcal{A}'_i \) and \( \langle a, -x \rangle \notin \mathcal{A}'_i \) for some \( a \neq 0 \), then let \( \langle b, -x \rangle \in \mathcal{A}'_i \) with \( b \neq 0, a \). 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 \( \langle a, x \rangle \langle b, x \rangle \neq \langle 0, 0 \rangle \) 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 \( \sum \mathcal{A}'_i = \langle 0, 0 \rangle \), we can have \( \langle a + b, 0 \rangle \langle a + b, 0 \rangle \in \mathcal{A}'_i \) for all \( m \in \mathbb{N}_m \), so \( \mathcal{A}'_i = \{ \langle a, x \rangle, \langle b, -x \rangle, \langle a + b, 0 \rangle \} \) for all \( m \in \mathbb{N}_m \), with \( a \) and \( b \) distinct nonzero elements of \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

6. Suppose now each element of \( \mathcal{A}'_i \) has \( \mathbb{Z}_3 \) component equal to \( 0 \). So \( \mathcal{A}'_i = \{ \langle a, 0 \rangle \langle a, 0 \rangle \} \) for some \( j, k, l \in \mathbb{N}_m \) 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 \( j \equiv 1 \) (mod 2), so \( \langle a, 0 \rangle^j = \langle a, 0 \rangle^2 \). If
Lemma 4.2.2. If \((Z_y^x, [p], \alpha)\) is accepted, \(\text{ord}_y(p) = 6\), and \(\alpha \equiv 1 \pmod{6}\), then
\[
\psi([p]) = \langle a, x \rangle \quad \text{with} \quad x = 1 \text{ or } -1,
\]
and \(A_i'\) takes one of the following forms:

1. \(\{\langle b, x \rangle, \langle b, -x \rangle, \langle 0, 0 \rangle^n \}, n \in \mathbb{N}_0\), or
2. \(\{\langle b, 0 \rangle^{2m}, \langle 0, 0 \rangle^n \}, m, n \in \mathbb{N}_0\),

where \(a\) and \(b\) are distinct nonzero elements of \(Z_y \times Z_y\).

Proof. Suppose \((Z_y^x, [p], \alpha)\) is accepted, \(\text{ord}_y(p) = 6\), and \(\alpha \equiv 1 \pmod{6}\). Then there exist positive integers \(e, f\) and multisets \(A_1, ..., A_e, B_1, ..., B_f\) of elements of \(Z_y^x\) which satisfy conditions (1)-(5) from the definition of an accepted triple. Let \(i \in \{1, ..., e\}\). Since \(\alpha \equiv 1 \pmod{6}\), and \(\beta(Z_y^x, [p], \alpha) = \text{ord}_y(p)\) for some positive integer \(m\) such that \(\text{ord}_y(p) \geq \alpha > (m - 1)\text{ord}_y(p)\), then \(\beta(Z_y^x, [p], \alpha) = \alpha + 5\).

By (2') of theorem 1.3.2, \(A_i'\) has no internal sum in \(\{\psi([p]), \psi([p]^2), ..., \psi([p]^5)\} = \{(a, x), \langle 0, -x \rangle, \langle 0, 0 \rangle, \langle 0, x \rangle, \langle a, -x \rangle\}\). Further, by conditions (3') and (4') of theorem 1.3.2, we have \(\sum A_i' = \psi([p]^{1-\alpha}) = \psi([1]) = \langle 0, 0 \rangle\) for \(j = 1, ..., e\), and
\[
\sum B_i' = \psi([p]^{-\alpha}) = \psi([p]^5) = \langle a, -x \rangle \quad \text{for} \quad i = 1, ..., f.
\]
It can be seen that the only elements of \(Z_y \times Z_y \times Z_y\) which can be in \(A_i'\) are of the form \(\langle b, 0 \rangle, \langle b, x \rangle, \langle b, -x \rangle\), or \(\langle 0, 0 \rangle\) for some \(b \neq 0, a\). Note that of these, only \(\langle b, 0 \rangle, \langle 0, 0 \rangle\) may be repeated within the same \(A_i'\) since \(\langle b, x \rangle^2 = \langle 0, -x \rangle = \psi([p]^2)\), \(\langle b, -x \rangle^2 = \langle 0, x \rangle = \psi([p]^4)\). Further, for all \(n \in \mathbb{N}_0\), inserting \(\langle 0, 0 \rangle^n\) into any of the following arguments does not change any internal sums of \(A_i'\), nor does it change \(\sum A_i'\). So \(\langle 0, 0 \rangle^n, i \in A_i'\) for \(i = 1, ..., e, n_i \geq 0\).

1. If \(\langle b, x \rangle \in A_i'\) then \(\langle b, 0 \rangle \notin A_i'\) since \(\langle b, 0 \rangle, \langle b, x \rangle = \langle 0, x \rangle\), and \(\langle a + b, c \rangle \notin A_i'\) for any \(c \in \{0, 1, 2\}\) since \(\langle a + b, c \rangle, \langle b, x \rangle = \langle a, c + x \rangle \notin \{\psi([p]), \psi([p]^2), ..., \psi([p]^5)\}\). We must have \(\langle b, -x \rangle \in A_i'\) to have \(\sum A_i' = \langle 0, 0 \rangle\). So \(\langle b, x \rangle \in A_i'\) iff \(\langle b, -x \rangle \in A_i'\) iff \(A_i' = \{\langle b, x \rangle, \langle b, -x \rangle, \langle 0, 0 \rangle^n\}\) for \(b \neq 0, a \in Z_y \times Z_y, n \in \mathbb{N}_0\).
2. If \(\langle b, 0 \rangle \in A_i'\) for some \(b \neq 0, a\) then \(\langle a + b, 0 \rangle \notin A_i'\) since \(\langle a + b, 0 \rangle, \langle b, 0 \rangle = \langle a, 0 \rangle\). Then \(A_i' = \{\langle b, 0 \rangle^t, \langle 0, 0 \rangle^n\}\) for some \(t, n \in \mathbb{N}_0\), and since \(\sum A_i' = \langle 0, 0 \rangle\), then \(t = 2m\) for some \(m\).

Lemma 4.2.3. If \((Z_y^x, [p], \alpha)\) is accepted, \(\text{ord}_y(p) = 6\), and \(\alpha \equiv 2 \pmod{6}\), then
\[
\psi([p]) = \langle a, x \rangle \quad \text{with} \quad x = 1 \text{ or } -1,
\]
and \(A_i'\) takes one of the following forms:

1. \(\{\langle a, -x \rangle, \langle b, x \rangle, \langle b, -x \rangle, \langle 0, 0 \rangle^n \}, n \in \mathbb{N}_0\)
2. \(\{\langle a, -x \rangle, \langle b, 0 \rangle^{2m}, \langle 0, 0 \rangle^n \}, m, n \in \mathbb{N}_0\)
3. \(\{\langle b, x \rangle, \langle a + b, x \rangle, \langle 0, 0 \rangle^n \}, n \in \mathbb{N}_0\), or
4. \(\{\langle b, -x \rangle, \langle a + b, 0 \rangle^{2m+1}, \langle 0, 0 \rangle^n \}, m, n \in \mathbb{N}_0\),

where \(a\) and \(b\) are distinct nonzero elements of \(Z_y \times Z_y\).

Proof. Suppose \((Z_y^x, [p], \alpha)\) is accepted, \(\text{ord}_y(p) = 6\), and \(\alpha \equiv 2 \pmod{6}\). Then there exist positive integers \(e, f\) and multisets \(A_1, ..., A_e, B_1, ..., B_f\) of elements of
$\mathbb{Z}^*_y$ which satisfy conditions (1)-(5) from the definition of an accepted triple. Let $i \in \{1, \ldots, e\}$. Since $\alpha \equiv 2 \pmod{6}$, and $\beta(\mathbb{Z}^*_y, [p], \alpha) = \text{mord}_y(p)$ for some positive integer $m$ such that $\text{mord}_y(p) \geq \alpha > (m-1)\text{ord}_y(p)$, then $\beta(\mathbb{Z}^*_y, [p], \alpha) = \alpha + 4$. By $(2')$ of theorem 1.3.2, $\mathcal{A}'_i$ has no internal sum in $\{\psi([p]), \psi([p]^2), \psi([p]^3), \psi([p]^4)\} = \{\langle x, x \rangle, \langle 0, -x \rangle, \langle a, 0 \rangle, \langle 0, x \rangle\}$. Further, by $(3')$ and $(4')$ of theorem 1.3.2, we have $\sum A'_j = \psi([p]^j) = \langle a, -x \rangle$ for $j = 1, \ldots, e$, and $\sum A'_i = \psi([p]^1) = \langle 0, x \rangle$ for $i = 1, \ldots, f$. 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 $\langle 0, 0 \rangle$ for $b \neq 0, a$. As before, only $\langle b, 0 \rangle, \langle 0, 0 \rangle$ may be repeated within the same $\mathcal{A}'_i$, and $\langle 0, 0 \rangle^m \in \mathcal{A}'_i$ for $i = 1, \ldots, e, n_i \geq 0$.

1. Suppose $\langle a, -x \rangle, \langle b, x \rangle \in \mathcal{A}'_i$ for some $b \neq 0, a$. 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 $\langle b, x \rangle \langle b, 0 \rangle = \langle a, -x \rangle \langle b, x \rangle \langle a + b, x \rangle = \langle 0, x \rangle$, $\langle b, x \rangle \langle a + b, 0 \rangle = \langle a, x \rangle$, $\langle b, x \rangle \langle a + b, -x \rangle = \langle a, 0 \rangle$. 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 $\mathcal{A}'_i = \{\langle a, -x \rangle, \langle b, x \rangle, \langle b, -x \rangle, \langle 0, b \rangle^m\}$ with $n \in \mathbb{N}_0$, and $\sum A'_i = \langle a, -x \rangle$.

2. Suppose now $\langle a, -x \rangle \in \mathcal{A}'_i$ and $\langle b, x \rangle \notin \mathcal{A}'_i$ for $b \neq 0, a$. If $\langle b, -x \rangle \in \mathcal{A}'_i$ then $\langle a + b, x \rangle, \langle a + b, 0 \rangle, \langle a + b, -x \rangle \notin \mathcal{A}'_i$ since $\langle a + b, x \rangle \langle b, -x \rangle = \langle a, 0 \rangle, \langle a + b, 0 \rangle \langle b, -x \rangle \langle a, -x \rangle = \langle 0, x \rangle, \langle b, -x \rangle \langle a, 0 \rangle = \langle 0, -x \rangle, \langle b, -x \rangle \langle a + b, x \rangle = \langle a, x \rangle$. Then $\langle b, x \rangle \in \mathcal{A}'_i$ for $\sum A'_i = \langle a, -x \rangle$, but we assumed differently so $\langle b, x \rangle \notin \mathcal{A}'_i$ for $b \neq 0, a$. If $\mathcal{A}'_i = \{\langle a, -x \rangle, \langle 0, b \rangle^m\}$, then $\sum A'_i = \langle a, -x \rangle$. Also, if $\langle b, 0 \rangle^m \in \mathcal{A}'_i$ for some $n$, 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 $\mathcal{A}'_i = \{\langle a, -x \rangle, \langle b, 0 \rangle^m, \langle 0, b \rangle^m\}$ with $\sum A'_i = \langle a, -x \rangle$ 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 $\langle a + b, x \rangle \notin \mathcal{A}'_i$, 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 $\mathcal{A}'_i = \{\langle b, x \rangle, \langle a + b, x \rangle, \langle 0, b \rangle^m\}$ for some $n \in \mathbb{N}_0$.

4. Now let $\langle b, -x \rangle \in \mathcal{A}'_i$, $\langle a, -x \rangle \notin \mathcal{A}'_i$ for some $b \neq 0, a$. 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 $\langle a + b, 0 \rangle^m = \langle 0, 0 \rangle$, so $\mathcal{A}'_i = \{\langle b, -x \rangle, \langle a + b, 0 \rangle^m, \langle 0, 0 \rangle^m\}$ for some $m, n \in \mathbb{N}_0$.

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

**Definition 4.2.1.** Given $p, \alpha$ from $(\mathbb{Z}^*_y, [p], \alpha)$, and $\langle x, y, z \rangle \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, if $\text{ord}_y(p) > 2$, $\alpha \equiv \pm 1 \pmod{3}$, and $\psi([p]) = \psi([p]^{-\alpha}) = (-\alpha)\psi([p]) = \langle -\alpha p_1, -\alpha p_2, -\alpha p_3 \rangle$, then define a function $W : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \rightarrow \mathbb{R}$ and let the weight of $\langle x, y, z \rangle$ be given by

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

Since $\text{ord}_y(p) > 2$, then $p_3 \equiv \pm 1 \pmod{3}$; with $\alpha \equiv \pm 1 \pmod{3}$ also, then $\alpha p_3 \neq -\alpha p_3 \pmod{3}$, and this function is well-defined.
If $A = \{ \langle x_1, y_1, z_1 \rangle, \ldots, \langle x_n, y_n, z_n \rangle \}$ is a multiset in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, 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 $S_1, \ldots, S_n$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $W(\bigcup_{i=1}^{n} S_i) = \sum_{i=1}^{n} W(S_i)$. Also, if $(\mathbb{Z}_p^x, [p], \alpha)$ is accepted then $W(B'_i) \geq 1$ for $i = 1, \ldots, f$.

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

**Proof.** If $\text{ord}_p(p) = 3$, $\alpha \equiv 1 \pmod{3}$, $\psi([p]) = \langle 0, x \rangle$ with $x = \pm 1$ and $(\mathbb{Z}_p^x, [p], \alpha)$ is accepted, then the lemma 4.2.1 holds, and $\mathcal{A}_i^0$ 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. $W(\{\langle a, x \rangle, \langle a, -x \rangle, \langle b, 0 \rangle, \langle b, 0 \rangle\}) = 1.5,$
5. $W(\{\langle a, x \rangle, \langle b, -x \rangle, \langle a + b, 0 \rangle, \langle 0, 0 \rangle\}) = 1.5,$
6. $W(\{\langle a, 0 \rangle, \langle b, 0 \rangle, \langle a + b, 0 \rangle, \langle b, 0 \rangle\}) = 0.$

So $W(\mathcal{A}_i^0) \leq 3$, hence $\sum_{i=1}^{\alpha} W(\mathcal{A}_i^0) \leq \sum_{i=1}^{\alpha} 3 = 3e$. \hfill \Box

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

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

1. $W(\{\langle b, x \rangle, \langle b, -x \rangle, \langle 0, 0 \rangle\}) = 1.5,$
2. $W(\{\langle b, 0 \rangle, \langle 0, 0 \rangle\}) = 0.$

So $W(\mathcal{A}_i^0) \leq 1.5$, hence $\sum_{i=1}^{\alpha} W(\mathcal{A}_i^0) \leq \sum_{i=1}^{\alpha} 1.5 = 1.5e$. \hfill \Box

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

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

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

So $W(\mathcal{A}_i^0) \leq 2e$, hence $\sum_{i=1}^{\alpha} W(\mathcal{A}_i^0) \leq \sum_{i=1}^{\alpha} 2 = 2e$. \hfill \Box

**Lemma 4.2.4.** If $(\mathbb{Z}_p^x, [p], \alpha)$ is accepted, then $\sum_{i=1}^{\alpha} |A_i - \langle 0, 0 \rangle^n \rangle| \geq 2pe$, where $\rho = \frac{\alpha + 1}{\alpha}$ 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 definition of an accepted triple, \(\bigcup_{i=1}^f \mathcal{A}_i = \bigcup_{i=1}^f \mathcal{B}_j\), so \(\bigcup_{i=1}^f (\mathcal{A}_i - \{0,0\}) = \bigcup_{i=1}^f (\mathcal{B}_j - \{0,0\})\). Then \(\sum_{i=1}^f |\mathcal{A}_i - \{0,0\}| = \sum_{j=1}^f |\mathcal{B}_j - \{0,0\}| \geq 2f\) since \(|\mathcal{B}_j - \{0,0\}| \geq 2\) for all \(i = 1, \ldots, f\). So \(\sum_{i=1}^f |\mathcal{A}_i - \{0,0\}| \geq 2f = 2\rho e\). □

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

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 \(1 \leq W(\mathcal{B}_j)\), then \(\rho e = f = \sum_{i=1}^f 1 \leq \sum_{i=1}^f W(\mathcal{B}_j) = W(\bigcup_{i=1}^f \mathcal{B}_j) = W(\bigcup_{i=1}^f \mathcal{A}_i) = \sum_{i=1}^e W(\mathcal{A}_i)\) 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. \(\text{ord}_p(p) = 3\), \(\overline{\alpha} = 1\),
2. \(\text{ord}_p(p) = 6\), \(\overline{\alpha} = 1\), or
3. \(\text{ord}_p(p) = 6\), \(\overline{\alpha} = 2\).

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

1. Let \(\text{ord}_p(p) = 3\), \(\alpha \equiv 1 \pmod{3}\). By corollary 4.2.1, since \((\mathbb{Z}_y^\times, [p], \alpha)\) is accepted, then \(\sum_{i=1}^e W(\mathcal{A}_i) \leq 3e\). If this is true, then by lemma 4.2.1 we have \(|\mathcal{A}_i - \{0,0\}| \leq 4\) for \(i = 1, \ldots, e\), and we get \(2\rho e \leq \sum_{i=1}^e |\mathcal{A}_i - \{0,0\}| \leq 4e\) by lemma 4.2.4, so \(2\rho \leq 4\) and \(\rho \leq 2\). 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 \(\text{ord}_p(p) = 6\), \(\alpha \equiv 1 \pmod{6}\). So \(\beta = \alpha + 5\) by lemma 4.2.2, and \(\rho = (\alpha + \beta - 1)/\alpha = (2\alpha + 4)/\alpha > 2\). Then we have \(2e < \rho e \leq \sum_{i=1}^e W(\mathcal{A}_i) \leq 1.5e\) 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 \(\text{ord}_p(p) = 6\), \(\alpha \equiv 2 \pmod{6}\). So \(\beta = \alpha + 4\) by lemma 4.2.3, and \(\rho = (\alpha + \beta - 1)/\alpha = (2\alpha + 3)/\alpha > 2\). Then we have \(2e < \rho e \leq \sum_{i=1}^e W(\mathcal{A}_i) \leq 2e\) 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 \(\text{ord}_p(p) = 1\), then \(p^\alpha \equiv 1 \pmod{y}\) for all \(\alpha\), and \((\mathbb{Z}_y^\times, [p], \alpha)\) is accepted by theorem 2.1.1.
2. If \(\text{ord}_p(p) = 2\), then \((\mathbb{Z}_y^\times, [p], \alpha)\) is accepted by theorem ??.
3. Let \(\text{ord}_p(p) = 3\), and fix \(\psi([p]) = \langle 0, x \rangle\) 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, \(\sum_{i=1}^e \mathcal{A}_i = \sum_{i=1}^e \mathcal{B}_j = \langle 0, x \rangle\) for \(j = 1, \ldots, e\), and \(\psi([p]) = \langle 0, x \rangle\) for \(j = 1, \ldots, f\). Finally, by (2') of theorem 1.3.2, for \(j = 1, \ldots, e\), \(\mathcal{A}_j\) has no internal sum in \(\{\psi([p])\} = \langle 0, x \rangle\).
So let $A'_1 = \{\langle a,0 \rangle , \langle b,x \rangle , \langle a+b,x \rangle \}$, $A'_2 = \{\langle a,x \rangle , \langle a,-x \rangle , \langle b,0 \rangle , \langle b,-x \rangle \}$. And let $B'_1 = \{\langle b,0 \rangle , \langle b,x \rangle \}$, $B'_2 = \{\langle a,0 \rangle , \langle a,x \rangle \}$, $B'_3 = \{\langle a,-x \rangle , \langle b,x \rangle , \langle a+b,x \rangle \}$, and $B'_4 = \{\langle b,-x \rangle \}$, 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 $\bigcup_{i=1}^{3} A'_i = \{\langle a,0 \rangle , \langle a,x \rangle , \langle a,-x \rangle , \langle b,0 \rangle , \langle b,-x \rangle , \langle a+b,x \rangle \}$ is accepted by theorem 1.3.2.

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

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

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

(4) Let $ord_y(p) = 6$, and fix $\psi([p]) = \langle a,x \rangle$ with $a \neq 0, x \neq 0$.

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

If $\alpha = 3$, then $\beta = \alpha + 3 = 6$ since $ord_y(p) = 6$, and $\rho = (\alpha + \beta - 1)/\alpha = 8/3$. By theorem 1.3.2, $\sum A'_1 = \psi([p]^{1-\alpha}) = \psi([p]^3) = \langle 0,x \rangle$ for $j = 1, \ldots, e$, and $\sum B'_j = \psi([p]^{1-\alpha}) = \psi([p]^3) = \langle a,0 \rangle$ for $j = 1, \ldots, f$.

Further, by (2') of theorem 1.3.2, for $j = 1, \ldots, e$, $A'_j$ has no internal sum in $\{\psi([p]^2), \psi([p]^3)\} = \{\langle a,x \rangle, \langle 0,-x \rangle, \langle a,0 \rangle \}$.

So let $A'_1 = \{\langle b,-x \rangle, \langle a+b,0 \rangle, \langle a+b,-x \rangle \}$, $A'_2 = \{\langle a,-x \rangle, \langle b,0 \rangle, \langle a+b,-x \rangle \}$, and $A'_3 = \{\langle 0,x \rangle \}$. And let $B'_1 = B'_2 = \ldots = B'_5 = \{\langle 0,0 \rangle, \langle a+b,0 \rangle \}$, and $B'_6 = \{\langle 0,x \rangle, \langle a,-x \rangle, \langle b,-x \rangle, \langle a+b,0 \rangle, \langle a+b,-x \rangle \}$, 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 $\bigcup_{i=1}^{3} A'_i = \{\langle 0,x \rangle, \langle a,-x \rangle, \langle b,0 \rangle \}$, $\langle b,-x \rangle, \langle a+b,0 \rangle \}$, $\langle a+b,-x \rangle \}$ is accepted by theorem 1.3.2.

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

Meeting conditions (3') and (4') of theorem 1.3.2, we have $\sum A'_1 = \sum A'_2 = \sum A'_3 = \langle 0,x \rangle$, and $\sum B'_1 = \ldots = \sum B'_6 = \langle 0,x \rangle$.

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

If $\alpha = 4$, we have $\beta = 6$ and $\rho = 9/4$. By theorem 1.3.2, $\sum A'_1 = \psi([p]^3) = \langle a,0 \rangle$ for $j = 1, \ldots, e$, and $\sum B'_j = \psi([p]^2) = \langle 0,-x \rangle$ for $j = 1, \ldots, f$.

Further, by (2') of theorem 1.3.2, for $j = 1, \ldots, e$, $A'_j$ has no internal sum in $\{\langle a,x \rangle, \langle 0,-x \rangle \}$.

So let $A'_1 = A'_2 = \{\langle a,-x \rangle, \langle b,0 \rangle \}$, $A'_3 = A'_4 = \{\langle a,-x \rangle, \langle a+b,0 \rangle \}$, and $B'_1 = \ldots = B'_5 = \{\langle a,-x \rangle, \langle b,0 \rangle \}$, $B'_6 = \{\langle a,-x \rangle \}$, 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 $\bigcup_{i=1}^{4} A'_i = \{\langle a,-x \rangle, \langle b,0 \rangle \}$, $\langle a+b,0 \rangle \}$ is met. And conditions (1'), (5') of theorem 1.3.2 are met.

None of $A'_1, \ldots, A'_4$ have internal sums in $\{\langle a,x \rangle, \langle 0,-x \rangle \}$, so condition (2') of theorem 1.3.2 is met.
Meeting conditions (3') and (4') of theorem 1.3.2, we have $\sum A'_1 = \ldots = \sum A'_4 = \langle a, 0 \rangle$, and $\sum B'_1 = \ldots = \sum B'_4 = \langle 0, -x \rangle$.

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

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

So let $A'_1 = \{\langle 0, x \rangle^4, \langle 0, -x \rangle^2\}$, $A'_2 = \{\langle a, 0 \rangle^4, \langle 0, -x \rangle\}$. And let $B'_1 = \ldots = B'_3 = \{\langle a, 0 \rangle, \langle 0, x \rangle\}$, $B'_4 = \{\langle a, 0 \rangle, \langle 0, x \rangle, \langle 0, -x \rangle^3\}$, 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 $\bigcup_{j=1}^{2} A'_j = \{\langle 0, x \rangle^4, \langle 0, -x \rangle^3, \langle a, 0 \rangle^4\} = \bigcup_{j=1}^{4} B'_j$, and conditions (1'), (5') of theorem 1.3.2 are met.

Neither $A'_1$ nor $A'_2$ 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 $\sum A'_1 = \ldots = \sum A'_4 = \langle 0, -x \rangle$, and $\sum B'_1 = \ldots = \sum B'_4 = \langle a, x \rangle$.

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

\[\Box\]

References