Full Elasticity of Local Singular Arithmetical Congruence Monoids

Cody Allen[1], Whitney Radil[2], Rachel Rankin[3], and Helen Williams[4]

[1]Department of Mathematics and Computer Science, San Diego State University
[2]Department of Mathematics, College of St. Benedict
[3]Department of Mathematics, University of California, Los Angeles
[4]Department of Mathematics, Florida State University

August 27, 2012

Abstract

This paper will examine Local Singular Arithmetical Congruence Monoids (ACM's) and determine if they are fully elastic. This process involves two distinct and important tools. First, we will restrict our view to a submonoid of the given ACM which is chosen so that only two prime numbers divide any element. This submonoid is carefully chosen so that it is fully elastic on an interval. The second step involves defining a transfer homomorphism between the submonoid and a subset of $\mathbb{N}_0^2$. This allows us to more easily define which elements are in the submonoid, classify irreducibles, and prove elasticity formulas. These tools are intregral in classifying the full elasticity of monoids.

1 Outline

2 Introduction

Our goal is to determine which singular local ACMs have full elasticity. Before we can do that, we must go through the basics first to show how full elasticity can be obtained from a generalized set.

An ACM,*Arithmetic Congruence Monoid* [3] , is an arithmetic progression, or sequence, that starts with 1 and is closed under multiplication. It is denoted by $M_{a,b} = \{1\} \cup \{a + b\mathbb{N}_0\}$. Lets use $M_{2,2}$ as an example. By following the given formula, we start with 1 and continuously add increasing multiples of b to a.

$$\begin{aligned} M_{a,b} &= \{1\} \cup \{a + b\mathbb{N}_0\} \\ M_{a,b} &= \{1, a, a+b, a+2b, a+3b\} \\ M_{2,2} &= \{1, 2, 2+2, 2+4, 2+6\} \\ &= \{1, 2, 4, 6, 8, 10\} \end{aligned}$$

Now as much as we want to randomly choose a and b, that cannot be done. There are two restirctions that must be fulfilled in order for an ACM to exist [2] . First $0 < a \leq b$ and secondly $a^2 \equiv a \bmod b$. So we know that $M_{2,2}$ is an ACM by the fact that $2 \equiv 4 \bmod 2$. Through this we know $M_{10,20}$ or $M_{3,4}$ are not moniods though the same restriction.

Another aspect of monoids is their factorizations lengths. As with any given integer, there exist different ways to break them down into the simplest forms. In natural numbers, the simplest forms are primes. There is just one catch, an element, $g \in M_{a,b}$, must be factored into elements of the monoid. Within the monoid $M_{a,b}$, there exists two types of elements, *reducibles* and *irreducibles.* An irreducible is an element within the monoid that cannot be broken down into elements that are within the monoid and the opposite is implied for reducibles.

We have taken factorizations in account for two major reasons; to determine the factorization lengths and to establish factorization length sets. Factorization lengths deal with the number of irreducibles that an element within the monoid can be factored down to. Dealing with $g = 36$ from $M_{2,2}$, we can conclude the following, $36 = (2)(18) = (6)(6)$. So the shortest factorization length, $l(36)$ and the longest factorization lengh, $L(36)$ are equivalent. When an element has two different factorizations, it is known as a *nonunique factorization.* With this known, we can then conclude that the set of factorization lengths, $\mathcal{L}(36) = \{2\}$, since there are two irreducibles in every factorization.

The factorizations lengths are used to determine the elasticity an element, $\rho(g)$. If $M_{a,b}$ is an ACM, then the elasticity of an element [3] , g, is defined as the following:

$$\rho(g) = \frac{\max \mathcal{L}(g)}{\min \mathcal{L}(g)}.$$

The longest factorization length divided by the shortest factorization length. The elasticity of the monoid [2] , $M_{a,b}$ is given by

$$\rho(M_{a,b}) = \sup_{g \in M_{a,b}} \rho(g).$$

In order to calculate the elasticity of a moniod, one must first take the elasticities of the elements in the monoid into account. An ACM, $M_{a,b}$, is fully elastic if for every rational number w with $w \in [1, \rho(M_{a,b}))$ there exists $g \in M_{a,b}$ with $\rho(g) = w$.

This presented a very broad spectrum when determing whether or not a monoid was fully elastic. The following results are taken from *Arithmetical Congruence Monoids: A Survey.* Recall, for $M_{a,b}$, we have defined $gcd(a, b) = d$. If $d = 1$, then $a = 1$ since $a < b$ and our monoid is actually $M_{1,b}$. Such an ACM is called *regular.* If $d \neq 1$ then such an ACM is called *singular.* A *singular* ACM is *local* if $d = gcd(a, b) = p^{\alpha}$ where p^{α} is a power of a prime. For singular ACMs, the elasticity of the monoid can be found: $\rho(M_{a,b}) = \frac{\alpha+\beta-1}{\alpha}$. Before beginning research, we did have previously known results: $M_{b,b}$ is fully elastic if and only if $b = p$ is a prime (because then $M_{b,b}$ is half-factorial). If $M_{a,b}$ is a global singular ACM, then the elasticity of $M_{a,b}$ is infinite and the ACM is NOT fully elastic [1] . There is an infinite family of fully elastic, local singular ACMs [1] . Let p be a prime number and $b_1 > 1$ a positive integer with $gcd(p, b_1) = 1$. If $k = ord_{b1}(p)$, then $M_{p^k,p^k b_1}$ is fully elastic [1] . Let p be a prime number and $b_1 > 1$ a positive integer with $gcd(p, b_1) = 1$. If $k = t(ord_{b1}(p))$ for $t > 1$, then $M_{p^k,p^k b_1}$ is not fully elastic [1] . With this known, we were left with local, singular ACMs to investigate. Using these definitions, we developed a five-step method for determining the full elasticity of local singular monoids. These five steps are as follows:

(i) Define a submonoid, $M \subseteq M_{xp^{\alpha},y^{\alpha}}$

(ii) Classify the set of irreducibles

(iii) For an element of the submonoid, find the length of its shortest factorization.

(iv) For an element of the submonoid, find the length of its longest factorization.

(v) Show that for every $\frac{w}{v} \in [1, \rho(M_{a,b}))$, we can find an element $g \in M$ such that $\rho(g) = \frac{w}{v}$

Let $M = \{p^i q^k : i, k \in \mathbb{N}_0, i \geq \alpha\} \cap M_{xp^{\alpha},yp^{\alpha}}$. We know [3] that $M_{xp^{\alpha},yp^{\alpha}} = M_{p^{\alpha},p^{\alpha}} \cap M_{1,y}$. The gcd$(x, y) = 1$, and $1 < x < y$ and p, q are prime.

Theorem 1. *The submonoid $M \subseteq M_{xp^{\alpha},yp^{\alpha}}$ is closed. i.e. if $c, d \in M$, then $cd \in M$.*

Proof. Assume $c, d \in M$. Then $c = p^{i_c} q^{k_c}$ and $d = p^{i_d} q^{k_d}$ where $i_c, i_d, k_c, k_d \in \mathbb{N}_0$, $i_c, i_d \geq \alpha$, and $c \equiv 1 \bmod y, d \equiv 1 \bmod y$. Then $cd = p^{i_c+i_d} q^{k_c+k_d}$, $i_c, i_d, k_c, k_d \in \mathbb{N}_0$, $i_c + i_d \geq \alpha$ since $i_c, i_d \geq \alpha$, and $cd \equiv 1 \bmod y$ since $cd \equiv (1)(1) \equiv 1 \bmod y$. Thus $cd \in M$.

□

Theorem 2. *The submonoid $M \subseteq M_{xp^\alpha,yp^\alpha}$ is isolated. i.e. if $fg \in M$ and $f,g \in M_{xp^\alpha,yp^\alpha}$, then both $f,g \in M$.*

Proof. Since $fg \in M$, then $fg = p^i q^k$ for primes p and q, where $i,k \in \mathbb{N}_0, i \geq \alpha$ and $fg \equiv 1 \bmod y$. Then we can say by the Fundamental Theorem of Algebra(needs a cite to something), which states that every positive integer $n > 1$ can be represented in *exactly one* way as a product of prime numbers, that $fg = f * g$ implies f and g are products of primes p and q *alone.* Since $f,g \in M_{xp^\alpha,yp^\alpha}$ and $f,g \in \{p^i j^k : i,k \in \mathbb{N}_0\}$, then $f,g \in \{p^i j^k : i,k \in \mathbb{N}_0\} \cap M_{xp^\alpha,yp^\alpha} = m$. Therefore, m is isolated.

□

3 Transfer Homomorphism

Let $M_{xp,yp}$ be an ACM such that $\gcd(x,y) = 1$, p is prime, $\text{ord}(p) = \beta$ (i.e. $p^\beta \equiv 1 \bmod y$), and $q \equiv x \bmod y$ is a prime. Let $M = \{p^i q^k : i,k \in \mathbb{N}_0\} \cap M_{xp,yp}$.

Thus we define $N \subseteq {\mathbb{N}_0}^2$ in the following way:

$$N = \{(i,k) : i,k \in \mathbb{N}_0, i \geq 1, i \equiv k \bmod \beta\}$$

.

Lemma 3. *The order of q, ord(q), equals β, the minimal power of p such that p is in $M_{xp,yp}$.*

Proof. We know that $\text{ord}(p) = \beta$. So $p^\beta \equiv 1 \bmod y$ and for all $b < \beta$, $p^b \not\equiv 1 \bmod y$. Now q was defined so that $pq \equiv 1 \bmod y$ so $1 \equiv (pq)^\beta \equiv p^\beta q^\beta \equiv q^\beta$. So $\text{ord}(q) \leq \beta$. Suppose there exists $b < \beta$ such that $q^b \equiv 1 \bmod y$. Then $1 \equiv (pq)^b \equiv p^b q^b \equiv p^b \not\equiv 1 \bmod y$. So we have a contradiction and therefore $\text{ord}(q) \equiv \beta$.

□

Lemma 4. *If $i \equiv k \bmod \beta$ and $i \geq 1$, then the element $p^i q^k$ is in $M_{xp,yp}$.*

Proof. Since $i \equiv k \bmod \beta$ and $i \geq 1$, there exist $a,b,c \in \mathbb{N}_0$ such that $i = a\beta + c$ and $k = b\beta + c$ where $a + c \geq 1$. So $p^i q^k \equiv p^{a\beta+c} q^{b\beta+c} \equiv (p^\beta)^a (q^\beta)^b (pq)^c \equiv 1^a 1^b 1^c \equiv 1 \bmod y$. So $p^i q^k \equiv 1 \bmod y$. Therefore $p^i q^k \in M_{xp,yp}$.

□

Lemma 5. *If $i \not\equiv k \bmod \beta$ or $i < 1$, then the element $p^i q^k$ is not in $M_{xp,yp}$.*

Proof. (i) Let $i < 1$, then $p \not| p^i q^k$ so $p^i q^k \notin M_{xp,yp}$.

(ii) Let $i \geq 1$ and $i \not\equiv k \bmod \beta$. So $\exists a,b,c,d \in \mathbb{N}_0$ with $c \neq d$ and $c,d < \beta$ where $i = a\beta + c$ and $k = b\beta + d$.

First consider $c < d$. Now $p^i q^k \equiv p^{a\beta+c} q^{b\beta+d} \equiv (p^\beta)^a (q^\beta)^b (pq)^c q^{d-c} \equiv 1^a 1^b 1^c q^{d-c} \equiv q^{d-c} \bmod y$. Since $d - c < d < \beta$ it follows that $q^{d-c} \not\equiv 1 \bmod y$. Since $p^i q^k \not\equiv 1 \bmod y$ then $p^i q^k \notin M_{xp,yp}$. Lastly consider

$d < c$. Now $p^i q^k \equiv p^{a\beta+c} q^{b\beta+d} \equiv (p^\beta)^a (q^\beta)^b (pq)^d p^{c-d} \equiv 1^a 1^b 1^c p^{c-d} \equiv p^{c-d} \bmod y$. Since $c-d < c < \beta$, then $p^{c-d} \not\equiv 1 \bmod y$ and $p^i q^k \not\equiv 1 \bmod y$. Consequently, $p^i q^k \notin M_{xp,yp}$.

□

Corollary 6. *The element $p^i q^k \in M_{xp,yp}$ if and only if $i \equiv k \bmod \beta$ and $i \geq 1$.*

Proof. By Lemma 4 and Lemma 5. □

Define $\psi : M \to N$ to be a function mapping the submonoid, M to the subset N.

Lemma 7. *The function $\psi : M \to N$ is bijective.*

Proof. To be bijective, ψ must be injective and surjective.

(i) Let $s, t \in M$. Then $s = p^{i_s} q^{k_s}$ and $t = p^{i_t} q^{k_t}$ and assume $\psi(s) = \psi(t)$. This implies:

$$(i_s, k_s) = (i_t, k_t)$$
$$p^{i_s} = p^{i_t}, q^{k_s} = q^{k_t}$$
$$p^{i_s} q^{k_s} = p^{i_t} q^{k_t}$$
$$s = t$$

Therefore we can say that ψ is injective.

(ii) Let $y \in N$. Then $y = (i, k)$ where $i \geq \alpha$ and $i \equiv k \bmod \beta$. Consider $p^i q^k$, since $i \geq 1$ and $i \equiv k \bmod \beta, p^i q^k \in M$ so that $\psi(p^i q^k) = (i, k) = y \in N$. Since y was arbitrary, we can say that ψ is surjective.

Therefore ψ is bijective and ψ^{-1} exists.

□

Theorem 8. *A transfer homomorphism exists within $M_{xp,yp}$, mapping M to N.*

Proof. (i) Let $\gamma, \delta \in M$. Then $\gamma = p^{i_\gamma} q^{k_\gamma}, \delta = p^{i_\delta} q^{k_\delta}$, where $i_\gamma, k_\gamma, i_\delta, k_\delta \in \mathbb{N}_0$, $i_\gamma, i_\delta \geq 1$, and $i_\gamma \equiv k_\gamma \bmod \beta$, $i_\delta \equiv k_\delta \bmod \beta$.

Therefore

$$\begin{aligned}
\gamma\delta &= (p^{i_\gamma} q^{k_\gamma})(p^{i_\delta} q^{k_\delta}) \\
&= p^{i_\gamma + i_\delta} q^{k_\gamma + k_\delta} \\
\psi(\gamma\delta) &= (i_\gamma + i_\delta, k_\gamma + k_\delta) \\
&= (i_\gamma, k_\gamma) + (i_\delta, k_\delta) \\
&= \psi(\gamma) + \psi(\delta)
\end{aligned}$$

(ii) Let $\psi(g) = s + t$, such that $s, t \in N \subseteq \mathbb{N}_0^2$. Then $\exists\ i_s, k_s, i_t, k_t \in \mathbb{N}_0$, with $s = (i_s, k_s)$ and $t = (i_t, k_t)$. So $i_s, i_t \geq 1, i_s \equiv k_s \bmod \beta$, and $i_t \equiv k_t \bmod \beta$. We can find $v, w \in M$ such that $\psi(v) = s$ and $\psi(w) = t$, , which will result in $g = vw$. Consider $v, w \in M$, where $v = p^{i_s} q^{k_s}$ and $w = p^{i_t} q^{k_t}$. Now, $\psi(v) = \psi(p^{i_s} q^{k_s}) = (i_s, k_s) = s$ and $\psi(w) = \psi(p^{i_t} q^{k_t}) = (i_t, k_t) = t$. Recall that

$$\begin{aligned} \psi(g) &= s + t \\ &= (i_s + i_t, k_s + k_t) \\ g &= \psi^{-1}((i_s + i_t, k_s + k_t)) \\ &= p^{i_s + i_t} q^{k_s + k_t} \end{aligned}$$

So the transfer homomorphism exists, as desired. □

Let M_{xp^α, yp^α} be an ACM such that $\gcd(x, y) = 1$, p is prime, $\alpha \geq 1$, and $\text{ord}(p) = d$ (i.e. $p^d \equiv 1 \bmod y$). Choose y such that $\mathbb{Z}_y^\times \cong \mathbb{Z}_n$, i.e., the group of units of y is cyclic.

Define $f : \mathbb{Z}_y^\times \to \mathbb{Z}_n$ such that $f(g) = 1, f(p) = a$ and $f(q) = b$ where g is a generator of $\mathbb{Z}_y^\times$ and q is a prime not equal to p.

Let $M = \{p^i q^k : i, k \in \mathbb{N}_0\} \cap M_{xp^\alpha, yp^\alpha}$. Let $c = \gcd(n, a)$, then $d = \frac{n}{c}$ and there exists an $a' \in \mathbb{N}_0$ such that $a = ca'$. Since d is minimal and $p^d \equiv 1 \bmod y, da \equiv 0 \bmod n$. Let $w = \gcd(c, b)$ so that $c = wc'$ and $b = wb'$ where $\gcd(b', c') = 1$. Since $p^i q^k \in M$, $p^i q^k \equiv 1 \bmod y$ so $ai + bk \equiv 0 \bmod n$ and then $ai \equiv bk \bmod n$. Now, $ai \equiv -bk \bmod n$ so that $a'i \equiv \frac{-b}{c} k \bmod d$ which implies that $a'i \equiv (-b')(\frac{k}{c'}) \bmod d$, finally implying that i$\equiv (-b')(a'^{-1})(\frac{k}{c'}) \bmod d$.

Thus we define $N \subseteq \mathbb{N}_0^2$ in the following way:

$$N = \{(i, k) : i, k \in \mathbb{N}_0, c' | k, i \geq \alpha, i \equiv (-b')(a'^{-1})(\frac{k}{c'}) \bmod d\}$$

.

Define $\psi : M \to N$ to be a function mapping the submonoid, M to the subset N.

Lemma 9. *The function $\psi : M \to N$ is bijective.*

Proof. To be bijective, ψ must be injective and surjective.

(i) Let $s, t \in M$. Then $s = p^{i_s} q^{k_s}$ and $t = p^{i_t} q^{k_t}$ and assume $\psi(s) = \psi(t)$. This implies:

$$\begin{aligned} (i_s, k_s) &= (i_t, k_t) \\ p^{i_s} &= p^{i_t} \\ q^{k_s} &= q^{k_t} \\ p^{i_s} q^{k_s} &= p^{i_t} q^{k_t} \\ s &= t \end{aligned}$$

Therefore we can say that ψ is injective.

(ii) Let $y \in N$. Then $y = (i,k)$ where $i \geq \alpha$ and $i \equiv (-b')(a'^{-1})(\frac{k}{c'}) \bmod d$. Consider $p^i q^k$, since $i \geq \alpha$ and $i \equiv (-b')(a'^{-1})(\frac{k}{c'}) \bmod d, p^i q^k \in M$ so that $\psi(p^i q^k) = (i,k) = y \in N$. Since y was arbitrary and we can say that ψ is surjective.

Therefore ψ is bijective and ψ^{-1} exists.

□

Theorem 10. *A transfer homomorphism exists within M_{xp^α, yp^α} mapping M to N.*

Proof. (i) Let $\gamma, \delta \in M$. Then $\gamma = p^{i_\gamma} q^{k_\gamma}, \delta = p^{i_\delta} q^{k_\delta}$, where $i_\gamma, k_\gamma, i_\delta, k_\delta \in \mathbb{N}_0$, $i_\gamma, i_\delta \geq \alpha$, and $i_\gamma \equiv (-b')(a'^{-1})(\frac{k_\gamma}{c'}) \bmod d$, $i_\delta \equiv (-b')(a'^{-1})(\frac{k_\delta}{c'}) \bmod d$. Therefore

$$\begin{aligned} \gamma\delta &= (p^{i_\gamma} q^{k_\gamma})(p^{i_\delta} q^{k_\delta}) \\ &= p^{i_\gamma + i_\delta} q^{k_\gamma + k_\delta} \\ \text{then, } \psi(\gamma\delta) &= (i_\gamma + i_\delta, k_\gamma + k_\delta) \\ &= (i_\gamma, k_\gamma) + (i_\delta, k_\delta) \\ &= \psi(\gamma) + \psi(\delta) \end{aligned}$$

(ii) Let $\psi(g) = s + t$, such that $s, t \in N \subseteq \mathbb{N}_0^2$. Then $\exists\ i_s, k_s, i_t, k_t \in \mathbb{N}_0$, with $s = (i_s, k_s)$ and $t = (i_t, k_t)$. So $i_s, i_t \geq \alpha, i_s \equiv (-b')(a'^{-1})(\frac{k_s}{c'}) \bmod d$, and $i_t \equiv (-b')(a'^{-1})(\frac{k_t}{c'}) \bmod d$. We can find $v, w \in M$ such that $\psi(v) = s$ and $\psi(w) = t$, ,which will result in $g = vw$. Consider $v, w \in M$, where $v = p^{i_s} q^{k_s}$ and $w = p^{i_t} q^{k_t}$. Now, $\psi(v) = \psi(p^{i_s} q^{k_s}) = (i_s, k_s) = s$ and $\psi(w) = \psi(p^{i_t} q^{k_t}) = (i_t, k_t) = t$. Recall that

$$\begin{aligned} \psi(g) &= s + t \\ &= (i_s + i_t, k_s + k_t) \\ g &= \psi^{-1}((i_s + i_t, k_s + k_t)) \\ &= p^{i_s + i_t} q^{k_s + k_t} \end{aligned}$$

□

4 $M_{xp,yp}$

Let $M_{xp,yp}$ be a monoid with $\gcd(x,y) = 1$ where p is prime and $x > 1$. Note that if $x = 1$, then $M_{xp,yp}$ is fully elastic since it's half-factorial [1] . Define $\beta \in \mathbb{N}$ to be the smallest natural number such that $p^\beta \in M_{xp,yp}$. So $\forall b \in \mathbb{N}$ such that $0 < b < \beta$, it follows that $p^b \not\equiv 1 \bmod y$ and $p^\beta \equiv 1 \bmod y$. Let q be a prime number such that $q \equiv x \bmod y$. Define the submonoid M to be $M = \{p^i q^k : i, k \in \mathbb{N}_0\} \cap M_{xp,yp}$

Lemma 11. *The order of q modulo y is β.*

Proof. Let q be a prime such that $q \equiv x \bmod y$. Since $q \equiv x \bmod y$, then $pq \equiv 1 \bmod y$ and $pq \in M_{xy,yp}$. Suppose for contradiction that there exists a $\gamma \in \mathbb{N}$ such that $0 < \gamma < \beta$ where $q^\gamma \equiv 1 \bmod y$. Then $1 \equiv pq \equiv (pq)^\gamma \equiv p^\gamma q^\gamma \equiv p^\gamma \not\equiv 1 \bmod y$, since $\gamma < \beta$, and β was defined to be the smallest natural number such that $p^\beta \equiv 1 \bmod y$, so we have a contradiction. Therefore the smallest power of q congruent to 1 mod y is β and thus the order of q is β. □

Lemma 12. *Let $c = p^iq^k$. Then $c \in M, x > 1$ if and only if $i \equiv k \bmod \beta$ and $i \geq 1$.*

Proof. ($\Longrightarrow$) Show that if $i \equiv k \bmod \beta$ and $i \geq 1$, then the element p^iq^k is in M:

Since $i \equiv k \bmod \beta$ and $i \geq 1$, there exist $a, b, c \in \mathbb{N}_0$ such that $i = a\beta + c$ and $k = b\beta + c$ where $a + c \geq 1$. So $p^iq^k \equiv p^{a\beta+c}q^{b\beta+c} \equiv (p^\beta)^a(q^\beta)^b(pq)^c \equiv 1^a1^b1^c \equiv 1 \bmod y$. So $p^iq^k \equiv 1 \bmod y$. Therefore $p^iq^k \in M$

($\Longleftarrow$) Show that if $i \not\equiv k \bmod \beta$ or $i < 1$, then the element p^iq^k is not in $M_{xp,yp}$:

(i) Let $i < 1$, then $p \not| p^iq^k$ so $p^iq^k \notin M$.

(ii) Let $i \geq 1$ and $i \not\equiv k \bmod \beta$. So $\exists a, b, c, d \in \mathbb{N}_0$ with $c \neq d$ and $c, d < \beta$ where $i = a\beta + c$ and $k = b\beta + d$.

   (a) First consider $c < d$. Now $p^iq^k \equiv p^{a\beta+c}q^{b\beta+d} \equiv (p^\beta)^a(q^\beta)^b(pq)^cq^{d-c} \equiv 1^a1^b1^cq^{d-c} \equiv q^{d-c} \bmod y$. Since $d - c < d < \beta$ it follows that $q^{d-c} \not\equiv 1 \bmod y$. Since $p^iq^k \not\equiv 1 \bmod y$ then $p^iq^k \notin M$.

   (b) Lastly consider $d < c$. Now $p^iq^k \equiv p^{a\beta+c}q^{b\beta+d} \equiv (p^\beta)^a(q^\beta)^b(pq)^dp^{c-d} \equiv 1^a1^b1^cp^{c-d} \equiv p^{c-d} \bmod y$. Since $c - d < c < \beta$, then $p^{c-d} \not\equiv 1 \bmod y$ and $p^iq^k \not\equiv 1 \bmod y$. Consequently, $p^iq^k \notin M$.

□

Lemma 13. *There are exactly two types of irreducibles of the form $c \in M$ where $c = p^iq^k$ and $x > 1$:*

(i) $c = pq^{(m\beta+1)}$ *for any* $m \in \mathbb{N}_0$

(ii) $c = p^\beta$.

Proof. We will begin by showing that *(i)* and *(ii)* are irreducible. We will then consider $c \in M$ where $c = p^iq^k$ and is not of the form *(i)* or *(ii)* and show that it is either reducible or not in the monoid.

First, we will show that *(i)* is irreducible. Let $m \in \mathbb{N}$ and $c = pq^{(m\beta+1)}$. To show $c \in M$, we must show that $p|c$ and $c \equiv 1 \bmod y$. Clearly since $c = pq^{(m\beta+1)}$, $p|c$. So $c = p^iq^k = p^{\varphi\beta}p^\zeta q^{\theta\beta}q^\zeta = (p^\beta)^\varphi(q^\beta)^\theta(pq)^\zeta \equiv 1^\varphi1^\theta1^\zeta \equiv 1 \bmod y$. Therefore, $c \equiv 1 \bmod y$, so $c \in M$ Assume c is reducible. Since c has only one copy of p, one of the factors will not contain a copy of p and will therefore not be in the monoid. Therefore $c = pq^{(r\beta+1)}$ is an irreducible in M.

Now, we will show that *(ii)* is irreducible. Let $c = p^\beta$, then by the definition of β, $p^\beta \in M$. Suppose p^β was reducible. Then at least one of its factors would be p^b with $0 < b < \beta$, which is not congruent to 1 mod y and is therefore not in the monoid. So $c = p^\beta$ is irreducible.

Let $c \in M$ where $c = p^iq^k$ and c is not of the form *(i)* or *(ii)*. There are multiple cases to consider:

(a) $1 < i < \beta$ and $k > 0$

(b) $i = \beta$ and $k > 0$

(c) $i > \beta$.

For case (a), for $c \in M_{xp,yp}$, then $k = i + r\beta$ for some $r \in \mathbb{N}$. So c is reducible into $c = p^iq^k = (pq)^{i-1}(pq^{1+r\beta})$. For case (b) then either $i \not\equiv k \bmod \beta$, and therefore $c \notin M_{xp,yp}$ or c is reducible into $c = p^iq^k = (pq)^{i-1}(pq^{1+r\beta})$. For case (c) then either $i \not\equiv k \bmod \beta$, and therefore $c \notin M_{xp,yp}$ or c can be factored into $(p^\beta)(p^{i-\beta}q^k)$ and is therefore reducible.

In conclusion, there are exactly two types of irreducibles of the form $c \in M_{xp,yp}$ where $c = p^iq^k$:

(i) $c = pq^{(m\beta+1)}$ for any $m \in \mathbb{N}$

(ii) $c = p^\beta$

as desired.

□

Lemma 14. *For all elements $c \in M$, where $c = p^iq^k$ and $x > 1$, $\beta|i$, and $0 < k \leq i$, the shortest factorization of c into irreducibles is $l(c) = \frac{i+\beta(\beta-1)}{\beta}$.*

Proof. A short factorization of c into irreducibles is

$$c = p^iq^k = (p^\beta)^{(\frac{i}{\beta}-1)}(pq)^{(\beta-1)}(pq^{(k-\beta+1)})$$

which has length $\frac{i+\beta(\beta-1)}{\beta}$. It is valid since each of the terms are of form *(i)* or *(ii)* from Lemma 13 and the factorization has exactly i copies of p and k copies of q.

The shortest length worth considering is $\frac{i}{\beta}$, which would require all irreducibles to be of the form *(ii)* in Lemma 13. However, this contradicts the assumption that $k > 0$. Therefore the shortest length must be greater than $\frac{i}{\beta}$.

Since the length $\frac{i}{\beta}$ is not possible and since we have only two categories of irreducibles, the next shortest length possible must have $\frac{i}{\beta} - 1$ copies of the *(ii)* irreducibles from Lemma 13 and then β copies of the *(i)* irreducibles from Lemma 13. This has length $\frac{i}{\beta} - 1 + \beta = \frac{i+\beta(\beta-1)}{\beta}$. The factorization above is a valid factorization into irreducibles and has this length. Therefore the shortest factorization length for an element $c \in M_{xp,yp}$ where $c = p^iq^k$, $\beta|i$, and $0 < k \leq i$ is $l(c) = \frac{i+\beta(\beta-1)}{\beta}$.

□

Lemma 15. *For all elements $c \in M_{xp,yp}$, where $c = p^i q^k$ and $x > 1$, $\beta|i$, and $0 < k \leq i$, the longest factorization of c into irreducibles is $L(c) = \frac{i+k(\beta-1)}{\beta}$.*

Proof. A long factorization of c into irreducibles is

$$c = p^i q^k = (p^\beta)^{\frac{i-k}{\beta}} (pq)^k$$

which has length $\frac{i+k(\beta-1)}{\beta}$. This is valid since each of the terms are of form *(i)* or *(ii)* from Lemma 13 and the factorization has exactly i copies of p and k copies of q. Since this factorization has the maximum number of type *(i)* irreducibles ie, each of the k copies of q from $c = p^i q^k$ is paired with a copy of p, it will be the longest factorization possible.

Therefore the longest factroization length for an element $c \in M_{xp,yp}$ where $c = p^i q^k$ and $x > 1$ and $\beta|i$, is $L(c) = \frac{i+k(\beta-1)}{\beta}$ □

Theorem 16. *Given a local, singular monoid $M_{a,b}$, if $gcd(a,b) = p > 1$ where p is prime, then $M_{a,b}$ is fully elastic.*

Proof. Let $c \in M_{xp,yp}, x > 1$. The elasticity of c, defined previously, is $\rho(c) = \frac{L(c)}{l(c)}$. Since $\rho(M_{xp,yp}) = \frac{\alpha+\beta-1}{\alpha} = \frac{1+\beta-1}{1} = \beta$, then given some arbitrary $\frac{w}{v} \in [1, \rho(M_{a,b}))$ we immediately have $\beta v > w \geq v$ or, equivalently, $\beta > \frac{w}{v} \geq 1$. We define $i = (\beta-1)(\beta^2 v - \beta)$ and $k = \beta^2(w-v) + \beta$ and claim that $i \geq k$. Indeed,

$$\begin{aligned}
k &= \beta^2(w-v) + \beta \\
&\leq \beta^2(\beta v - 1 - v) + \beta \\
&= \beta^2 \beta v - \beta^2 - \beta^2 v + \beta \\
&= \beta^2 v(\beta - 1) - \beta(\beta - 1) \\
&= (\beta-1)(\beta^2 v - \beta) \\
&= i
\end{aligned}$$

Hence, $i \geq k$. , we have $\rho(c) = \frac{L(c)}{l(c)} = \frac{i+(\beta-1)k}{i+(\beta-1)\beta}$ and

$$\begin{aligned}
\frac{i+(\beta-1)k}{i+(\beta-1)\beta} &= \frac{(\beta-1)(\beta^2 v - \beta) + (\beta-1)(\beta^2(w-v)+\beta)}{(\beta-1)(\beta^2 v - \beta) + (\beta-1)\beta} \\
&= \frac{\beta^2 v - \beta + \beta^2 w - \beta^2 v + \beta}{\beta^2 v - \beta + \beta} \\
&= \frac{w}{v}
\end{aligned}$$

Since $\frac{w}{v}$ was arbitrary, we have shown that for any local, singular monoid $M_{xp,yp} = M_{a,b}$ where $gcd(a,b) = p > 1$ and p is prime, we can construct $c \in M_{a,b}$ such that $\rho(c) = \frac{w}{v}$. Therefore, the monoid $M_{xp,yp}$ defined above is fully elastic.

□

An alternate proof may be found here[?] .

5 M_{xp^α,yp^α} with $\mathrm{ord}(p) = 2$

We will show that a local singular Arithmetical Congruence Monoid (ACM) of the form M_{xp^α,yp^α}, where p^α is a prime power, $gcd(x,y) = 1$, $x > 1$, and $\mathrm{ord}(p) = 2$ modulo y is fully elastic. Note that if α is even, then $p^\alpha \equiv 1 \bmod y$. Since $1 \equiv xp^\alpha \equiv x \bmod y$, and $x \leq y$ it follows that $x = 1$. This case is fully solved. [1] It follows that M_{p^α,yp^α} with $\mathrm{ord}(p) = 2$ modulo y is fully elastic if and only if $\alpha = 2$.

So we are left with the case M_{xp^α,yp^α}, where $x > 1$, α odd, and $\mathrm{ord}(p) = 2$ modulo y. Define q to be a prime such that $q \equiv x \bmod y$. So $xp^\alpha \equiv qp^\alpha \equiv 1 \bmod y$. Also, $p \equiv qp^{\alpha+1} \equiv q \bmod y$. Therefore, since $\mathrm{ord}(p) = 2$ modulo y, it follows that $\mathrm{ord}(q) = 2$ modulo y.

Define the submonoid $M = M_{xp^\alpha,yp^\alpha} \cap \{p^i q^k : i, k \in \mathbb{N}_0\}$ where $x > 1$, α odd, q is prime, and $\mathrm{ord}(p) = \mathrm{ord}(q) = 2$ modulo y.

Theorem 17. *An element $g = p^i q^k$ is in the submonoid M if and only if $i \geq \alpha$ and $i + k$ is even.*

Proof. Let $g \in M$. Since $M_{xp^\alpha,yp^\alpha} = M_{p^\alpha,p^\alpha} \cap M_{1,y}$, therfore $p^\alpha | g$ and $g \equiv 1 \bmod y$. Suppose $i < \alpha$, then $p^\alpha \not| x$. So $i \geq \alpha$. Now suppose $i + k = 2z + 1$ for some $z \in \mathbb{N}$. Recall that $p \equiv q \bmod y$. So $p^i q^k \equiv p^{i+k} \equiv (p^2)^z p \equiv p \not\equiv 1 \bmod y$. This gives a contradiction, so $i + k$ is even.

Let $g = p^i q^k$ where $i \geq \alpha$ and $i + k$ is even. Since $i \geq \alpha$, it is clear that $g = p^\alpha(p^{i-\alpha} q^k)$ and so $p^\alpha | g$. Now consider $p^i q^k \equiv p^{i+k} \equiv (p^2)^{\frac{i+k}{2}} \equiv 1 \bmod y$. Therefore $g \in M$. □

Lemma 18. *If $g = p^i q^k \in M$ where $\alpha \leq i < 2\alpha$, then g is irreducible.*

Proof. Suppose $g = p^i q^k \in M$ with $\alpha \leq i < 2\alpha$ is reducible. So g factors into at least 2 irreducibles in the monoid. Since $\frac{i}{2} < \alpha$ it is not possible for p^α to divide both factors. Thus, g is irreducible. □

Lemma 19. *If $g = p^i q^k \in M$ where $i = 2\alpha$ and $k = 0$, then g is irreducible.*

Proof. Suppose $g \in M$ where $g = p^{2\alpha}$ is reducible. So g factors into at least 2 irreducibles in the monoid. Then either one irreducible has less than α copies of p and one has more than α copies of p or both have α copies of p. If one irreducible factor has less than α copies of p, then it is not in the monoid and so not an irreducible in the monoid. If both irreducible factors have α copies of p, since there are no copies of q in g, there are no copies of q in either factor. Therefore in each factor, the number of copies of p plus the number of copies of q is odd, and thus it is not in the monoid. So we have a contradiction and $g = p^{2\alpha}$ is irreducible. □

Lemma 20. *If $g = p^i q^k \in M$ where g is not of the form of Lemma 18 or Lemma 19, then g is reducible.*

Proof. Let $g = p^i q^k \in M$. There are two cases not covered:

(i) $i = 2\alpha$ and $k \neq 0$

(ii) $i > 2\alpha$

In case *(i)*, then k is even and at least 2. So g is reducible into $p^{\alpha}q$ and $p^{\alpha}q^{k-1}$. In case *(ii)*, then g is reducible into $p^{\alpha+1}$ and $p^{i-\alpha-1}q^k$. The second term may or may not be an irreducible, however this is enough to show that g is reducible. □

Lemma 21. *The shortest factorization length for an element $g = p^iq^k \in M$ where $2\alpha \mid i$ and $k \neq 0$ where $\omega = \lfloor \frac{i}{2\alpha} \rfloor$ is $l(g) = \frac{i}{2\alpha} + 1$.*

Proof. Let $g = p^iq^k \in M$ where $2\alpha \mid i$ and $k \neq 0$. Recall that $i \geq \alpha$ and $i + k$ must be even. Let $\omega = \lfloor \frac{i}{2\alpha} \rfloor$.

Suppose $2\alpha \mid i$ and $k \neq 0$. Then a short factorization of x into irreducibles is $(p^{2\alpha})^{\omega-1}(p^{\alpha}q)(p^{\alpha}q^{k-1})$. This cannot be shortened because $i+k$ must remain even in each factorization and the factorizations must, of course, remain irreducible. If $2\alpha \mid i$, then $\frac{i}{2\alpha}$ is an integer and $i = 2\alpha\omega$. Thus we can factor out $\omega - 1$ number of $p^{2\alpha}$'s. Since $k \neq 0$, the remaining $p^{2\alpha}$ can only be divided into two single p^{α} terms in order to remain irreducible. This is because if there are more than two terms, some term does not have alpha copies of p, but if we condense them into one term, then the term is immediately reducible. The first of these terms is $p^{\alpha}q$, and the second contains the remaining terms in the form $p^{\alpha}q^{k-1}$. This gives a length of $l(g) = \omega + 1 = \lfloor \frac{i}{2\alpha} \rfloor + 1 = \lceil \frac{i}{2\alpha} \rceil + 1 = \frac{i}{2\alpha} + 1$.

Although slight variations may be made on the factorizations, their length will only be greater than or equal to the length of either $l(g)$ depending on i.

□

Lemma 22. *The longest factorization for $g = p^iq^k \in M$ with $k \leq \lfloor \frac{i}{\alpha} \rfloor$ has length $L(g) = k + \lfloor \frac{i-\alpha k}{\alpha+1} \rfloor$.*

Proof. Let $g = p^iq^k \in M$ with $k \leq \lfloor \frac{i}{\alpha} \rfloor$. So $i \geq \alpha$ and $i + k$ even. Let $t = \lfloor \frac{i}{\alpha} \rfloor$ and $s = \lfloor \frac{i-\alpha k}{\alpha+1} \rfloor$.

Suppose $k \leq \lfloor \frac{i}{\alpha} \rfloor$. The explicit factorizations for g must be in cases dependent on if k is odd or even.

Since k is even, then a long factorization of g is

$$(p^{\alpha}q)^k(p^{\alpha+1})^{s-1}(p^{i-\alpha k-(s-1)(\alpha+1)}).$$

Since each irreducible with α copies of p must be paired with a q, there are as many irreducibles with α copies of p as possible. Also, since

$$\alpha \leq i - \alpha k - (s-1)(\alpha+1) < 2\alpha,$$

were there one more irreducible with $\alpha + 1$ copies of p, there would be an irreducible with less than α copies of p, which would not be in the monoid. So this factorization of g is as long as possible. Thus, $L(g) = k + \lfloor \frac{i-\alpha k}{\alpha+1} \rfloor$. □

Corollary 23. *The elasticity for an element $g = p^i q^k \in M$ with $k \leq \lfloor \frac{i}{\alpha} \rfloor$ and $2\alpha \mid i$ and $k \neq 0$ is $\rho(g) = \frac{k+\lfloor \frac{i-\alpha k}{\alpha+1} \rfloor}{\frac{i}{2\alpha}+1}$.*

Proof. Since $\rho(g) = \frac{L(g)}{l(g)}$ and by Lemma 21 we know $l(g) = \frac{i}{2\alpha} + 1$. Also, by Lemma 22 we know $L(g) = k + \lfloor \frac{i-\alpha k}{\alpha+1} \rfloor$. Therefore $\rho(g) = \frac{k+\lfloor \frac{i-\alpha k}{\alpha+1} \rfloor}{\frac{i}{2\alpha}+1}$. □

Theorem 24. *An Arithmetical Congruence Monoid of the type M_{xp^α, yp^α} where $x > 1$, $\alpha > 1$ is odd, and $ord(p) = 2$ modulo y is fully elastic.*

Proof. For an element of the submonoid $g = p^i q^k \in M$, we have the elasticity of g defined as $\rho(g) = \frac{L(g)}{l(g)}$. Then given some $\frac{w}{v} \in [1, \rho(M_{xp^\alpha, yp^\alpha}))$, we have we have $2v > w \geq v$ or, equivalently, $2 > \frac{w}{v} \geq 1$ since $\rho(M_{xp^\alpha, yp^\alpha}) = \frac{\alpha+\beta-1}{\alpha} = 2$ when $x > 1$ and $ord(p) = 2$ modulo y. Consider $i = 2\alpha(v-1)$ and $k = w(\alpha+1) - 2\alpha(v-1)$. We claim that $i \geq k$ which implies that:

$$\begin{aligned} & 2\alpha(v-1) \geq w(\alpha+1) - 2\alpha(v-1) \\ \iff & \frac{4\alpha}{\alpha+1} \geq \frac{w}{v-1} \end{aligned}$$

Assume not, then $i < k$ and we have:

$$\begin{aligned} \implies & \frac{4\alpha}{\alpha+1} < \frac{w}{v-1} \\ \iff & \frac{4\alpha}{\alpha+1} < \frac{w}{v-1} < \frac{2v}{v-1} \\ \iff & \frac{4\alpha}{\alpha+1} < (\frac{3}{3})\frac{2v}{v-1} = \frac{6v}{3v-3} < \frac{6v}{3v-1} \end{aligned}$$

But $\alpha > 1$ and α is odd, so $\alpha \geq 3$. Then, since $f(\alpha) = \frac{4\alpha}{\alpha+1}$ is an increasing function (confirmed by the derivative test) on [3,∞), it attains its minimum at $\alpha = 3$. We also note that $h(v) = \frac{v}{3v-1}$ is a decreasing function (confirmed by the derivative test) on [1,∞) and attains its maximum value at $v = 1$. Hence,

$$\frac{4\alpha}{\alpha+1} = \frac{4(3)}{(3)+1} = 3 < 3 = 6(\frac{1}{3(1)-1}) = \frac{6v}{3v-1}$$

but $3 < 3$ is a contradiction and since $\frac{4\alpha}{\alpha+1} > \frac{6v}{3v-1} > \frac{2v}{v-1} > \frac{w}{v-1}$ for all other values of α and v, we must have $i \geq k$. Since $2\alpha \mid i$ and $k \neq 0$, we have $\rho(g) = \frac{k+\lfloor \frac{i-\alpha k}{\alpha+1} \rfloor}{\frac{i}{2\alpha}+1}$.

$$\begin{aligned}\frac{k+\lfloor\frac{i-\alpha k}{\alpha+1}\rfloor}{\frac{i}{2\alpha}+1} &= \frac{w(\alpha+1)-2\alpha(v-1)+\lfloor\frac{2\alpha(v-1)-\alpha(w(\alpha+1)-2\alpha(v-1))}{\alpha+1}\rfloor}{\frac{2\alpha(v-1)}{2\alpha}+1} \\ &= \frac{w(\alpha+1)-2\alpha(v-1)+\lfloor\frac{2\alpha(v-1)+2(\alpha)^2(v-1))-(\alpha w(\alpha+1))}{\alpha+1}\rfloor}{v} \\ &= \frac{w(\alpha+1)-2\alpha(v-1)+\lfloor\frac{2\alpha(\alpha+1)(v-1))-(\alpha w(\alpha+1))}{\alpha+1}\rfloor}{v} \\ &= \frac{(w\alpha)+(w)-2\alpha(v-1)+2\alpha(v-1)-(w\alpha)}{v} \\ &= \frac{w}{v}\end{aligned}$$

Therefore for all $\frac{w}{v} \in [1,2)$ the element $g = p^{2\alpha(v-1)}q^{w(\alpha+1)-2\alpha(v-1)}$ has an elasticity of $\rho(g) = \frac{w}{v}$. So M_{xp^α,yp^α} where $x > 1$, $\alpha > 1$ is odd, and $ord(p) = 2$ modulo y is fully elastic.

□

6 $M_{xp^2,21p^2}$

It can be shown from the group structure of $\mathbb{Z}_{21}^\times = \mathbb{Z}_2 \times \mathbb{Z}_6$, that for $M_{xp^\alpha,21p^\alpha}$ to be a monoid, one of the following must hold: $p \equiv 1 \bmod 21, p^2 \equiv 1 \bmod 21, p^3 \equiv 1 \bmod 21, p^6 \equiv 1 \bmod 21$. Recall that if the $\operatorname{ord}(p)$ modulo 21 divides α then it follows that $x = 1$ and so the case has been solved. [1] Further, $\operatorname{ord}(p) \bmod 21$ divides α then M_{xp^α,yp^α} is fully elastic if and only if $\operatorname{ord}(p) = \alpha$.

Consider $M_{xp^2,21p^2}$. There are four cases, the $\operatorname{ord}(p)$ modulo 21 can be either $1, 2, 3$ or 6. Note that since $\alpha = 2$ if $\operatorname{ord}(p) = 1, 2$ then the case has been solved and if $\operatorname{ord}(p) = 3, 6$ then the case is open.

Corollary 25. *If the order of p modulo 21 is equal to 1, then $M_{xp^2,21p^2}$ is not fully elastic. If the order of p modulo 21 is equal to 2, then $M_{xp^2,21p^2}$ is fully elastic.*

Proof. Lemma 3.1, 3.2 in On the Arithmetic of Arithmetical Congruence Monoids.

□

Now we will be considering the full elasticity of $M_{xp^2,21p^2}$ when the order of p modulo 21 is equal to 3. Therefore the elasticity of the monoid is $\rho(M_{xp^2,21p^2}) = \frac{\alpha+\beta-1}{\alpha} = \frac{2+3-1}{2} = 2$.

Define r to be a prime such that $r \equiv p^2 \bmod 21$. So $pr \equiv 1 \bmod 21$ and the order of r modulo 21 is also 3. Now define the submonoid $M_1 = \{p^i r^j : i, j \in \mathbb{N}_0\} \cap M_{xp^2,21p^2}$.

Lemma 26. *The element $g = p^i r^j \in M_1$ if and only if $i \geq 2$ and $i \equiv j \bmod 3$.*

Proof. Let $g = p^i r^j \in M_1$. Then $p^2 | g$ so $i \geq 2$. Suppose without loss of generality $i \geq j$. Since $g \in M_1$, then $1 \equiv g \equiv p^i r^j \equiv (pr)^j (p)^{i-j} \equiv p^{i-j} \bmod 21$. The order of p modulo 21 is 3, it follows that $1 \equiv p^{i-j} \bmod 21$ exactly when $i \equiv j \bmod 3$. So when $g \in M_1$, then $i \geq 2$ and $i \equiv j \bmod 3$.

Let $g = p^i r^j$ where $i \geq 2$ and $i \equiv j \bmod 3$. Since $i \geq 2$, then it is clear that $p^2 | g$. Since $i \equiv j \bmod 3$, there exist $A, B, C \in \mathbb{N}_0$ such that $i = 3A + C$ and $j = 3B + C$. So $p^i r^j \equiv (p^3)^A (pr)^C (r^3)^B \equiv (1)^A (1)^C (1)^B \equiv 1 \bmod 21$. Therefore $g \in M_1$.

□

Lemma 27. *The following are the only irreducibles in M_1:*

(i) $p^2 r^{2+3m}$ *where* $m \in \mathbb{N}_0$

(ii) $p^3 r^{3m}$ *where* $m \in \mathbb{N}_0$

(iii) $p^4 r$

Proof. For *(i)* and *(ii)*, clearly $i \equiv j \bmod 3$ and $i \geq 2$, so they are in M_1. Suppose they are reducible. Then at least one factor would not be divisible by p^2, and would therefore not be in the monoid. Therefore, *(i)* and *(ii)* are irreducible. For *(iii)* suppose it was reducible. Then, either one factor will have more than 2 copies p and one will have less, in which case not both factors will be in the monoid. The other case is both will have exactly 2 copies of p. However, since there is only one copy of q, it is not possible for both factors to satisfy the condition that $i \equiv j \bmod 3$. So *(i)*, *(ii)* and *(iii)* are irreducible.

There are two cases not considered, first $p^4 r^{1+3m}$ where $m \in \mathbb{N}_0$ and $m > 0$, and second $p^i r^j$ with $i \geq 5$. Consider $p^4 r^{1+3m}$ where $m \in \mathbb{N}_0$ and $m > 0$. Then there are at least four copies of r. So $p^4 r^{1+3m}$ where $m \in \mathbb{N}_0$ and $m > 0$ is reducible into $(p^2 r^2)(p^2 r^{2+3(m-1)})$. Now consider $p^i r^j$ with $i \geq 5$. This is reducible into $(p^3)(p^{i-3} r^j)$.

Therefore the following are the only irreducibles in M_1:

(i) $p^2 r^{2+3m}$ where $m \in \mathbb{N}_0$

(ii) $p^3 r^{3m}$ where $m \in \mathbb{N}_0$

(iii) $p^4 r$.

□

Lemma 28. *For any element $g = p^i r^j \in M_1$ where $i = 2(2\phi + 1)$ and $j = 3t + \phi + 2$ with $\phi, t \in \mathbb{N}$, the shortest length factorization is $l(g) = \phi + 1$.*

Proof. The absolute shortest factorization length is $\frac{i}{4}$ since our irreducible that utilizes the most copies of p is $p^4 r$. Any element in the monoid with factorization length shorter than this would necessarily have some factor with more than 4 copies of p in it, and would then be reducible. Now, $\frac{i}{4} = \frac{2(2\phi+1)}{4} = \phi + \frac{1}{2}$. Consider the element $g \in M$ where $g = p^i r^j = (p^4 r)^{\phi} (p^2 r^{2+3t})$. Since ϕ is an integer, $\phi + \frac{1}{2}$ is not an integer and we have, $\phi < \phi + \frac{1}{2} < \phi + 1$. Therefore, $\phi + 1$ is the shortest length factorization.

□

Lemma 29. *For any element $g = p^i r^j \in M_1$ where $i = 3\gamma + 2\theta$ and $j = 2\theta$ with $\gamma, \theta \in \mathbb{N}$, the longest length factorization is $L(g) = \gamma + \theta$.*

Proof. We show that $L(g) = \gamma + \theta$ is maximal. Let $t, m \in \mathbb{N}_0$, then with reference to lemma 27, we find the following; A longest factorization can have at most one type (iii) irreducible since $(p^4r)(p^4r)^m = (p^2r^2)(p^3)^2(p^4r)^{m-1}$, where $m \in \mathbb{N}$.

If there is one type (iii) and one type (ii) with $m \geq 1$ in the factorization, then the factorization length is not maximal since $(p^4r)(p^3r^{3m}) = (p^4r)(p^3r^{3(m-1)+3}) = (p^2r^2)^2(p^3r^{3(m-1)})$.

If the maximum length factorizaion contains a type (iii) irreducible, then it is of the form $(p^3)^\gamma(p^4r)$ and can only contain one copy of r:

(a) Both $(p^3r^{3m})^\gamma(p^4r)$ and $(p^3)^\gamma(p^4r)^\theta$, $\theta > 1$ are addressed at the beginning of this proof.

(b) $(p^3)^\gamma(p^4r)(p^2r^2) = (p^3)^{\gamma+1}(p^3r^3)$, which does not contain any (p^4r).

(c) $(p^3)^\gamma(p^4r)(p^2r^{2+3t}) = (p^3)^{\gamma-1}(p^2r^{2+3(t-1)})(p^2r^2)^2(p^3)$, which does not contain any (p^4r).

If a longest factorization contains a type (i) irreducible and a type (ii) irreducible, it can be written with all copies of r in the type (ii) irreducible since, $(p^3r^{3m})(p^2r^{2+3t}) = (p^3)(p^2r^{2+3(m+t)})$ have equal lengths.

A longest factorization cannot be written as $(p^3)^a(p^2r^2)^b(p^2r^{2+3t})$ if both $a \geq 2$ and $t \geq 2$ since this factorization length can be increased:

$$(p^3)^{a-2}(p^2r^2)^{b+3}(p^3r^{2+3(t-2)})$$

.

Therefore, all longest factorizations can be written as $(p^3)^a(p^2r^2)^b(p^2r^{2+3t})$ if $a < 2$ or $t < 2$, where $a, b \in \mathbb{N}$. Therefore, $g = (p^3)^\gamma(p^2r^2)^\theta$ is maximal length since $i = 3\gamma + 2\theta > 2\theta = j$ implies $t = 0$ in (p^2r^{2+3t}) and $a = \gamma$ and $b = \theta - 1$. □

Lemma 30. *M_1 is fully elastic on the interval $[\frac{3}{2}, 2)$.*

Proof. First note that, $g \in M_1$ implies that $g = (p^4r)^\phi(p^2r^{2+3t}) = (p^3)^\gamma(p^2r^2)^\theta$. Hence, $\gamma = \phi - t$ and $\theta = \frac{1}{2}(\phi + 3t + 2)$ since,

$$\begin{aligned} g &= (p^3)^\gamma(p^2r^2)^\theta \\ &= (p^3)^{\phi-t}(p^2r^2)^{\frac{1}{2}(\phi+3t+2)} \\ &= p^{3\phi-3t+\phi+3t+2}r^{\phi+3t+2} \\ &= (p^4r)^\phi(p^2r^{2+3t}) \end{aligned}$$

Therefore,

$$\begin{aligned}\rho(g) &= \frac{\gamma+\theta}{\phi+1} \\ &= \frac{\phi - t + \frac{1}{2}(\phi+3t+2)}{\phi+1} \\ &= \frac{(2\phi+2)+(\phi+t)}{2\phi+2} \\ &= 1 + \frac{\phi+t}{2(\phi+1)}\end{aligned}$$

Therefore, it suffices to show that $0 \leq \frac{w}{v} < \frac{1}{2}$ for $w, v \in \mathbb{N}$. Set $\phi = 2v-1$ and $t = 4w - 2v + 1$. Then we have,

$$\frac{\phi+t}{2(\phi+1)} = \frac{2v-1+4w-2v+1}{2(2v-1)} = \frac{4w}{4v} = \frac{w}{v}$$

Therefore, M_1 is fully elastic on $[\frac{3}{2}, 2)$. □

Now let us consider a different submonoid. Define q to be a prime such that $q \equiv p \bmod 21$. So $p^2q \equiv q^2p \equiv 1 \bmod 21$ and the order of q modulo 21 is also 3. Now define the submonoid $M_2 = \{p^iq^k : i, k \in \mathbb{N}_0\} \cap M_{xp^2,21p^2}$.

Lemma 31. *The element $g = p^iq^k \in M_2$ if and only if $i \geq 2$ and $i \equiv 2k \bmod 3$.*

Proof. Let $g = p^iq^k \in M_2$. Then $p^2|g$ so $i \geq 2$. Since $g \in M_2$, then $1 \equiv g \equiv p^iq^k \equiv p^{i+k} \bmod 21$. So $i + k \equiv 0 \bmod 3$. This is equivalent to saying $i \equiv 2k \bmod 3$. So if $g \in M_2$ then $i \geq 2$ and $i \equiv 2k \bmod 3$.

Let $g = p^iq^k$ where $i \geq 2$ and $i \equiv 2k \bmod 3$. Since $i \geq 2$, then it is clear that $p^2|g$. Since $i \equiv 2k \bmod 3$, there exist $A, B, C \in \mathbb{N}_0$ such that $i = 3A + 2C$ and $j = 3B + C$. So $p^iq^k \equiv (p^3)^A(p^2q)^C(r^3)^B \equiv (1)^A(1)^C(1)^B \equiv 1 \bmod 21$. Therefore $g \in M_2$.

□

Lemma 32. *The following are the only irreducibles in M_2:*

(i) p^2q^{1+3m} *where* $m \in \mathbb{N}_0$

(ii) p^3q^{3m} *where* $m \in \mathbb{N}_0$

Proof. For *(i)* and *(ii)*, clearly $i \equiv 2k \bmod 3$ and $i \geq 2$, so they are in M_1. Suppose they are reducible. Then at least one factor would not be divisible by p^2, and would therefore not be in the monoid. Therefore, *(i)* and *(ii)* are irreducible.

There are two cases not considered, first p^4q^{2+3m} where $m \in \mathbb{N}_0$, and second p^iq^k with $i \geq 5$. Consider p^4q^{2+3m} where $m \in \mathbb{N}_0$. This is reducible into $(p^2q)(p^2q^{1+3m})$. Now consider p^iq^k with $i \geq 5$. This is reducible into $(p^3)(p^{i-3}q^k)$.

Therefore the following are the only irreducibles in M_2:

(i) p^2q^{1+3m} where $m \in \mathbb{N}_0$

(ii) p^3q^{3m} where $m \in \mathbb{N}_0$.

□

Lemma 33. *For any element $g = p^iq^k \in M_2$ where $i = 3n$ and $k = 3r$ with $n, r \in \mathbb{N}$, the shortest length factorization is $l(g) = n$.*

Proof. Since the most copies of p possible in an irreducible is 3, the shortest conceivable factorization length is n. Consider the following factorization of $g = p^iq^k$:

$$(p^3)^{n-1}(p^3q^{3r})$$

which has length n. Therefore, the shortest length factorization for an element $g = p^iq^k \in M_2$ where $i = 3n$ and $k = 3r$ with $n, r \in \mathbb{N}$ is $l(g) = n$.

□

Lemma 34. *For any element $g = p^iq^k \in M_2$ where $i = 3n$ and $k = 3r$ with $n, r \in \mathbb{N}$ and $2r \leq n$, the longest length factorization is $L(g) = n + r$.*

Proof. Consider the following factorization of p^iq^k:

$$(p^2q)^{3r}(p^3)^{n-2r}$$

which has length $L(g) = n + r$. Since p^2q is minimal for both p's and q's, and it was used as many times as possible, this is the longest length factorization. □

Corollary 35. *For any element $g = p^iq^k \in M_2$ where $i = 3n$ and $k = 3r$ with $n, r \in \mathbb{N}$ and $2r \leq n$, the elasticity is $\rho(g) = \frac{n+r}{n}$.*

Proof. Since $l(g) = n$ and $L(g) = n + r$, it follows that $\rho(g) = \frac{n+r}{n}$. □

Theorem 36. *M_2 is fully elastic on $[1, \frac{3}{2})$.*

Proof. Let $\frac{w}{v} \in [1, \frac{3}{2}]$. Now consider $g = p^iq^k$ with $i = 3n$ where $n = v$ and $k = 3r$ where $r = w - v$. Note since $1 \leq v \leq w$, r and n are in $\mathbb{N}$. Also, since $w \leq \frac{3v}{2}$, then $r \leq \frac{v}{2}$, and $2r \leq n$. So $\rho(g) = \frac{n+r}{n} = \frac{v+w-v}{v} = \frac{w}{v}$. Therefore, M_2 is fully elastic on $[1, \frac{3}{2})$. □

Theorem 37. *$M_{xp^2,21p^2}$ where the order of p modulo y is 3 is fully elastic.*

Proof. Recall that $\rho(M_{xp^2,21p^2}) = 2$. Also, the submoniod M_1 is fully elastic on $[\frac{3}{2}, 2)$ by Theorem 30. Similarly, the submoniod M_2 is fully elastic on $[1, \frac{3}{2})$ by Theorem 36. Therefore $M_{xp^2,21p^2}$ where the order of p modulo y is 3 is fully elastic.

□

Now we will be considering the full elasticity of $M_{xp^2,21p^2}$ when the order of p modulo 21 is equal to 6. Therefore the elasticity of the monoid is $\rho(M_{xp^2,21p^2}) = \frac{\alpha+\beta-1}{\alpha} = \frac{2+6-1}{2} = \frac{7}{2}$.

Define r to be a prime such that $r \equiv p^5 \bmod 21$. So $pr \equiv 1 \bmod 21$ and the order of r modulo 21 is also 6. Now define the submonoid $M_1 = \{p^i r^j : i,j \in \mathbb{N}_0\} \cap M_{xp^2,21p^2}$.

Lemma 38. *The element $g = p^i r^j \in M_1$ if and only if $i \geq 2$ and $i \equiv j \bmod 6$.*

Proof. Let $g = p^i r^j \in M_1$. Then $p^2|g$ so $i \geq 2$. Suppose without loss of generality $i \geq j$. Since $g \in M_1$, then $1 \equiv g \equiv p^i r^j \equiv (pr)^j (p)^{i-j} \equiv p^{i-j} \bmod y$. The order of p modulo y is 6, it follows that $1 \equiv p^{i-j} \bmod y$ exactly when $i \equiv j \bmod 6$. So when $g \in M_1$, then $i \geq 2$ and $i \equiv j \bmod 6$.

Let $g = p^i r^j$ where $i \geq 2$ and $i \equiv j \bmod 6$. Since $i \geq 2$, then it is clear that $p^2|g$. Since $i \equiv j \bmod 6$, there exist $A, B, C \in \mathbb{N}_0$ such that $i = 6A + C$ and $j = 6B + C$. So $p^i r^j \equiv (p^6)^A (pr)^C (r^6)^B \equiv (1)^A (1)^C (1)^B \equiv 1 \bmod y$. Therefore $g \in M_1$.

□

Lemma 39. *The following are the only irreducibles in M_1:*

(i) $p^2 r^{2+6m}$ *where* $m \in \mathbb{N}_0$

(ii) $p^3 r^{3+6m}$ *where* $m \in \mathbb{N}_0$

(iii) p^6

(iv) $p^7 r$

Proof. For *(i)* and *(ii)*, clearly $i \equiv j \bmod 6$ and $i \geq 2$, so they are in M_1. Suppose they are reducible. Then at least one factor would not be divisible by p^2, and would therefore not be in the monoid. Therefore, *(i)* and *(ii)* are irreducible. For *(iii)* and *(iv)*, suppose they were reducible. Then, at least one factor will have less than 6 copies p with no copies of q. So the $i \equiv j \bmod 6$ condition is broken and the factor is not in the monoid. So *(i)*, *(ii)*, *(iii)* and *(iv)* are irreducible.

There are three cases not considered, first $p^h r^{h+6m}$ where $m \in \mathbb{N}_0$ and $h = 4$ or 5, second $p^7 r^{1+6m}$ where $m \in \mathbb{N}_0$ and $m > 0$, and third $p^i r^j$ with $i \geq 8$. Consider $p^h r^{h+3m}$ where $m \in \mathbb{N}_0$ and $h = 4$ or 5. So $p^h r^{h+3m}$ where $m \in \mathbb{N}_0$ and $h = 4$ or 5 is reducible into $(p^2 r^2)(p^{h-2} r^{h-2+6m})$. Now consider $p^7 r^{1+6m}$ where $m \in \mathbb{N}_0$ and $m > 0$. So there are at least 7 copies of q. So $p^7 r^{1+6m}$ where $m \in \mathbb{N}_0$ and $m > 0$ is reducible into $(p^2 r^2)(p^5 r^{5+6(m-1)}$. Now consider $p^i r^j$ with $i \geq 8$. This is reducible into $(p^6)(p^{i-6} r^j)$.

Therefore the following are the only irreducibles in M_1:

(i) $p^2 r^{2+6m}$ where $m \in \mathbb{N}_0$

(ii) $p^3 r^{3+6m}$ where $m \in \mathbb{N}_0$

(iii) p^6

(iv) p^7r

□

Lemma 40. *For any element $g = p^ir^j \in M_1$ where $i = 7\gamma+3$ and $j = \gamma+3+6m$ for some $\gamma, m \in \mathbb{N}_0$, the shortest factorization length is $l(g) = \gamma + 1$.*

Proof. The shortest consevable length of factorization is $\frac{i}{7} = \gamma + \frac{3}{7}$ since the most copies of p in any irreducible is 7. However, this is not an integer. So the shortest possible length is $\gamma + 1$. Consider the following factorization of $g = p^ir^j$:

$$(p^7r)^\gamma(p^3r^{3+6m})$$

which has length $\gamma+1$. Therefore for any element $g = p^ir^j \in M_2$ where $i = 7\gamma+3$ and $j = \gamma + 3 + 6m$ the shortest factorization length is $l(g) = \gamma + 1$. □

Lemma 41. *For any element $g = p^ir^j \in M_1$ where $i = 2\theta + 6\phi$ and $j = 2\theta$ for some $\theta, \phi \in \mathbb{N}_0$, the longest factorization length is $L(g) = \theta + \phi$.*

Proof. Recall the irreducibles,

(i) p^2r^{2+6m} where $m \in \mathbb{N}_0$

(ii) p^3r^{3+6m} where $m \in \mathbb{N}_0$

(iii) p^6

(iv) p^7r.

The longest irreducible can have at most one irreducible of type *(ii)* or at most one type *(iv)* since

$$(p^3r^{3+6m_1})(p^3r^{3+6m_2}) = (p^2r^2)^2(p^2r^{2+6(m_1+m_2)})$$
$$(p^7r)^2 = (p^2r^2)(p^6)^2$$
$$(p^7r)(p^3r^{3+6m}) = (p^6)(p^2r^2)(p^2r^{2+6m}).$$

If a longest factorization contains a type *(i)* and a type *(iii)* irreducible, then $m = 0$. Suppose $m > 0$, it can be made longer by the following,

$$(p^2r^{2+6m})(p^6) = (p^2r^2)^3(p^2r^{2+6(m-1)})$$

Consider the following factorization of $g = p^ir^j$:

$$(p^2r^2)^\theta(p^6)^\phi$$

which has length $\theta + \phi$. Since we have an even number of r's, if we had a type *(ii)* or a type *(iv)* irreducible, we would need two. But this could be made longer. So our longest factorization must contain only type *(i)* and type *(iii)* irreducibles. Since for all factors $m = 0$, this is the longest factorization.

□

Corollary 42. *Any element $g = p^i r^j \in M_1$ that satisfies Lemma 40 and Lemma 41 has elasticity $\rho(g) = \frac{3\gamma+4m+3}{2\gamma+2}$.*

Proof. Solving the system of equations:

$$\begin{aligned} i &= 7\gamma + 3 \\ i &= 2\theta + 6\phi \\ j &= \gamma + 3 + 6m \\ j &= 2\theta. \end{aligned}$$

We see that $\phi = \gamma - m$, so $\gamma \geq m$. We also see that $\theta = (1/2)(\gamma + 3 + 6m)$, so γ must be odd.

The clear elasticity is $\rho(g) = \frac{\theta+\phi}{\gamma+1}$. And substituting gives $\rho(g) = \frac{\theta+\phi}{\gamma+1} = \frac{\gamma-m+(1/2)(\gamma+3+6m)}{\gamma+1} = \frac{2\gamma-2m+\gamma+3+6m}{2\gamma+2} = \frac{3\gamma+4m+3}{2\gamma+2}$. □

Theorem 43. *M_1 is fully elastic on $(\frac{3}{2}, \frac{7}{2})$.*

Proof. Let $\frac{w}{v} \in (\frac{3}{2}, \frac{7}{2})$. So $3v < 2w < 7v$ and $2w \leq 7v - 1$. Consider $\gamma = 4v - 1$, and $m = 2w - 3v$. Therefore $m = 2w - 3v \leq 7v - 1 - 3v = 4v - 1 = \gamma$, and γ is odd.

So $\rho(g) = \frac{3\gamma+4m+3}{2\gamma+2} = \frac{3(4v-1)+4(2w-3v)+3}{2(4v-1)+2} = \frac{12v-3+8w-12v+3}{8v-2+2} = \frac{8w}{8v} = \frac{w}{v}$. Therefore, M_1 is fully elastic on $(\frac{3}{2}, \frac{7}{2})$. □

Now let us consider a different submonoid. Define q to be a prime such that $q \equiv p^4 \bmod 21$. So $p^2 q \equiv 1 \bmod 21$ and the order of q modulo 21 is 3. Now define the submonoid $M_2 = \{p^i q^k : i, k \in \mathbb{N}_0\} \cap M_{xp^2, 21p^2}$.

Lemma 44. *The element $g = p^i q^k \in M_2$ if and only if $i \geq 2$ and $i \equiv 2k \bmod 6$.*

Proof. Let $g = p^i q^k \in M_2$. Then $p^2 | g$ so $i \geq 2$. Since $g \in M_2$, then $1 \equiv g \equiv p^i q^k \equiv p^{i+4k} \bmod 21$. So $i + 4k \equiv 0 \bmod 6$. This is equivalent to saying $i \equiv 2k \bmod 6$. So if $g \in M_2$ then $i \geq 2$ and $i \equiv 2k \bmod 6$.

Let $g = p^i q^k$ where $i \geq 2$ and $i \equiv 2k \bmod 6$. Since $i \geq 2$, then it is clear that $p^2 | g$. Since $i \equiv 2k \bmod 6$, there exist $A, B, C \in \mathbb{N}_0$ such that $i = 6A + 2C$ and $k = 3B + C$. So $p^i q^k \equiv (p^6)^A (p^2 q)^C (r^3)^B \equiv (1)^A (1)^C (1)^B \equiv 1 \bmod 21$. Therefore $g \in M_2$.

□

Note that since $i \equiv 2k \bmod 6$, it must be true that i is even.

Lemma 45. *The following are the only irreducibles in M_2:*

(i) $p^2 q^{1+3m}$ *where* $m \in \mathbb{N}_0$

(ii) p^6

Proof. For *(i)*, clearly $i \equiv 2k \bmod 6$ and $i \geq 2$, so it is in M_2. Suppose they are reducible. Then at least one factor would not be divisible by p^2, and would therefore not be in the monoid. Therefore, *(i)* is irreducible. Suppose p^6 was reducible. Since i must be even, one of the factors will contain 2 copies of p, but no copies of q. Therefore the factor would not be in the monoid. So *(i)*, and *(ii)* are irreducible in M_2.

There are two cases not considered, first p^4q^{2+3m} where $m \in \mathbb{N}_0$, and second p^iq^k with $i \geq 8$. Consider p^4q^{2+3m} where $m \in \mathbb{N}_0$. This is reducible into $(p^2q)(p^2q^{1+3m})$. Now consider p^ir^j with $i \geq 8$. This is reducible into $(p^6)(p^{i-6}r^j)$.

Therefore the following are the only irreducibles in M_2:

(i) p^2q^{1+3m} where $m \in \mathbb{N}_0$

(ii) p^6.

□

Lemma 46. *For any element $g = p^iq^k \in M_2$ where $i = 6n$ and $k = 3r$ with $n, r \in \mathbb{N}$, the shortest length factorization is $l(g) = n + 2$.*

Proof. Since the maximum copies of p possible in an irreducible is 6, the shortest consevable factorization length is n. Since the next largest number of copies of p possible in an irreducible is 2, the next shortest facotrization length is $(n-1)+3 = n+2$. Further, since $k \neq 0$, it is not possible to have a factorization length of n. Consider the following factorization of p^iq^k:

$$(p^6)^{n-1}(p^2q)^2(p^2q^{2+3(r-1)})$$

which has length $n + 2$. Therefore, the shortest length factorization for an element $g = p^iq^k \in M_2$ where $i = 6n$ and $k = 3r$ with $n, r \in \mathbb{N}$ is $l(g) = n+2$. □

Lemma 47. *For any element $g = p^iq^k \in M_2$ where $i = 6n$ and $k = 3r$ with $n, r \in \mathbb{N}$ and $r \leq n$, the longest length factorization is $L(g) = n + 2r$.*

Proof. Consider the following factorization of p^iq^k:

$$(p^2q)^{3r}(p^6)^{n-r}$$

which has length $L(g) = n+2r$. Since p^2q is minimal for both p's and q's, and it was used as many times as possible, this is the longest length factorization. □

Corollary 48. *For any element $g = p^iq^k \in M_2$ where $i = 6n$ and $k = 3r$ with $n, r \in \mathbb{N}$ and $r \leq n$, the elasticity is $\rho(g) = \frac{n+2r}{n+2}$.*

Proof. Since $l(g) = n + 2$ and $L(g) = n + 2r$, it follows that $\rho(g) = \frac{n+2r}{n+2}$. □

Theorem 49. *M_2 is fully elastic on $[1, 3)$.*

Proof. Let $\frac{w}{v} \in [1, 3)$. Now consider $g = p^i q^k$ with $i = 6n$ where $n = 2v - 2$ and $k = 3r$ where $r = w - v + 1$. Note since $1 \leq v \leq w$, r and n are in $\mathbb{N}$. So $\rho(g) = \frac{n+2r}{n+2} = \frac{2v-2+2w-2v+2}{2v-2+2} = \frac{2w}{2v} = \frac{w}{v}$. Therefore, M_2 is fully elastic on $[1, 3)$. □

Theorem 50. *$M_{xp^2,21p^2}$ where the order of p modulo 21 is 6 is fully elastic.*

Proof. Recall that $\rho(M_{xp^2,21p^2}) = \frac{7}{2}$. Also, the submoniod M_1 is fully elastic on $[3, \frac{7}{2})$ by Theorem 43. Similarly, the submoniod M_2 is fully elastic on $[1, 3)$ by Theorem 49. Therefore $M_{xp^2,21p^2}$ where the order of p modulo 21 is 6 is fully elastic.

□

Theorem 51. *$M_{xp^2,21p^2}$ is fully elastic if and only if the order of p modulo 21 is not equal to 1.*

Proof. By the group structure of $\mathbb{Z}_{21}^{\times}$ the order of p modulo y must be $1, 2, 3, 6$ to be a monoid. By Corollary 25 if the order of p modulo 21 is 1 then $M_{xp^2,21p^2}$ is not fully elastic. By Corollary 25 if the order of p modulo 21 is 2 then $M_{xp^2,21p^2}$ is fully elastic. By Theorem 37 if the order of p modulo 21 is 3 then $M_{xp^2,21p^2}$ is fully elastic. By Theorem 50 if the order of p modulo 21 is 6 then $M_{xp^2,21p^2}$ is fully elastic. Therefore $M_{xp^2,21p^2}$ is fully elastic if and only if the order of p modulo 21 is not equal to 1. □

7 M_{xp^α,yp^α} with $\alpha \leq \frac{ord(p)}{2}$

In this section we will show the full elasticity of M_{xp^α,yp^α} with $\alpha \leq \frac{\text{ord}(p)}{2}$. Note that since $\alpha < 2\alpha \leq \text{ord}(p)$, it follows that the smallest power of p such that $p^\beta \in M_{xp^\alpha,yp^\alpha}$ is $\beta = \text{ord}(p)$. Let q be prime such that $q \equiv x \bmod y$. Define the submonoid $M_1 = M_{xp^\alpha,yp^\alpha} \cap \{p^i q^k : i, k \in \mathbb{N}_0\}$.

Lemma 52. *For $\alpha \leq \frac{\beta}{2}$ the irreducible with the largest power of p in M_1 is p^β.*

Proof. Since $\alpha \leq \frac{\beta}{2}$ it follows that $\beta \geq 2\alpha$. Let $p^i q^k$ be an element of the submonoid such that $i \geq 2\alpha$ with $k \neq 0$. Then $p^i q^k$ is reducible into $(p^\alpha q)(p^{i-\alpha} q^{k-1})$. Since $p^i q^k \equiv p^\alpha q \equiv 1 \bmod y$ it follows that $p^{i-\alpha} q^{k-1} \equiv 1 \bmod y$. Also, since $i \geq 2\alpha$ it follows that $i - \alpha \geq \alpha$ and so $p^\alpha | p^{i-\alpha} q^{k-1}$ and $p^{i-\alpha} q^{k-1} \equiv 1 \bmod y$. Therefore $p^i q^k$ is reducible when $i \geq 2\alpha$ and $k \neq 0$. Let $p^i q^k$ be an element of the submonoid such that $i \geq 2\alpha$ with $k = 0$. Then $\beta | i$, suppose not. Then $p^i = (p^\beta)^{\frac{i}{\beta}}$ but $\frac{i}{\beta}$ is not an integer. Let $i = m\beta + r$ where $m, r \in \mathbb{N}_0$ and $0 < r < \beta$. Then, $(p^\beta)^{\frac{i}{\beta}} = (p^\beta)^m (p^r)$. We know that $p^\beta \equiv 1 \bmod y$ is minimal, and since $0 < r < \beta$, we have $p^r \notin M$. So $i = \theta\beta$ where $\theta \in \mathbb{N}$. So $p^i q^k = (p^\beta)^\theta$. Therefore if $\theta > 1$, then the element is reducible. Therefore any $p^i q^k$ in the submonoid with $i \geq 2\alpha$ and $i \neq \beta$ is reducible. So the irreducible with the largest power of p is p^β. □

Lemma 53. *Given some Arithmetical Congruence Monoid (ACM) M_{xp^α, yp^α} where $p^\beta \equiv 1 \bmod y$ and $\alpha > 1$, let $c = gcd(\alpha, \beta)$ so that there exists some $n, m \in \mathbb{N}$ such that $\beta = cm$ and $\alpha = cn$. Then m is minimal for $q^m \equiv 1 \bmod y$.*

Proof. Assume that $c = gcd(\alpha, \beta)$, $\beta = cm$ and $\alpha = cn$. Then, immediately we have $gcd(m, n) = 1$ and the $lcm(\alpha, \beta) = cmn$. Consider,

$$q^m \equiv q^m (p^\beta)^n \equiv q^m p^{\alpha m} \equiv (qp^\alpha)^m \equiv 1 \bmod y$$

Therefore, $q^m \equiv 1 \bmod y$. Now, suppose there exists $m' \in \mathbb{N}$ such that $0 < m' < m$ and $q^{m'} \equiv 1 \bmod y$. Then,

$$(qp^\alpha)^{m'} \equiv q^{m'} p^{\alpha m'} \equiv p^{\alpha m'} \equiv p^{cnm'} \bmod y$$

We have $cnm' < cnm$, but $\beta \nmid cnm'$ since, $\beta = cm \mid cnm'$ implies $m \mid nm'$ but $gcd(n, m) = 1$ so that we have $m \mid m'$ which is a contradiction, for $m' < m$. Hence, $p^{cnm'} \not\equiv 1 \bmod y$. Thus, $q^m \equiv 1 \bmod y$ where m is minimal. □

Lemma 54. *The element $p^\alpha q^{1+\theta m} \in M_1$ where $ord(q) = m$ is irreducible.*

Proof. First, we will show that $p^\alpha q^{1+\theta m} \equiv 1 \bmod y$. So $p^\alpha q^{1+\theta m} \equiv (p^\alpha q)(q^m)^\theta \equiv (1)(1)^\theta \equiv 1 \bmod y$. Suppose $p^\alpha q^{1+\theta m}$ was reducible. Since there are exactly α copies of p, at least one of the factors would not be divisible by p^α and thus not be in the monoid. Therefore $p^\alpha q^{1+\theta m}$ is irreducible, as desired. □

Lemma 55. *If $\beta \geq 2\alpha$ then the shortest length factorization of $c \in M \subset M_{xp^\alpha, yp^\alpha}$ is $l(c) = \frac{i}{\beta} + 1 - \frac{\alpha}{\beta}$.*

Proof. First note that the shortest possible factorization length of any element $c \in M \subset M_{xp^\alpha, yp^\alpha}$ is $\frac{i}{\beta}$. This is seen by noting the lemma above, that is, the irreducible that utilizes the most copies of p is p^β. Therefore, for any element $c \in M_{xp^\alpha, yp^\alpha}$, none of the individual factors of c can contain more than β copies of p. Hence, a shorter factorization of $c \in M_{xp^\alpha, yp^\alpha}$ does not exist.

To find the shortest factorization length of an element $c \in M$, we choose i such that $\beta \mid i - \alpha$. Then, a shortest factorization of $c \in M_{xp^\alpha, yp^\alpha}$ of the form $c = p^i q^k$ is $(p^\beta)^{\frac{i-\alpha}{d}} (p^\alpha q^{1+\omega m})$ with $\omega \in \mathbb{N}_0$. Here l(c) $= \frac{i-\alpha}{\beta} + 1 = \frac{i+\beta+\alpha}{\beta} = \frac{i}{\beta} + 1 - \frac{\alpha}{\beta}$. Since $\beta > \alpha$, clearly $\frac{\alpha}{\beta} < 1$. Therefore, $0 < 1 - \frac{\alpha}{\beta} < 1$. But this also implies $\beta \nmid i$ since $1 - \frac{\alpha}{\beta}$ is not an integer. Therefore, $\frac{i}{\beta}$ is not an integer. Since $l(c)$ must be an integer, and $\frac{i}{\beta} < \frac{i}{\beta} + (1 - \frac{\alpha}{\beta}) < \frac{i}{\beta} + 1$, $l(c)$ is a minimal length factorization of c. □

Lemma 56. *If $\beta \geq 2\alpha$ then the longest length factorization of $c \in M_{xp^\alpha, yp^\alpha}$ is $L(c) = k + \frac{i - \alpha k}{\beta}$.*

Proof. First note that the longest possible factorization length of any element $c \in M_{xp^\alpha, yp^\alpha}$ is $\frac{i}{\alpha}$. This is seen by noting the lemma above, that is, the irreducible that utilizes the least copies of p is $p^a q$ since we must have $p^\alpha | c$. Therefore, for any element $c \in M_{xp^\alpha, yp^\alpha}$, none of the individual factors of c can contain less than α copies of p. Hence, a longer factorization of $c \in M_{xp^\alpha, yp^\alpha}$ does not exist. To find the longest factorization length of an element $c \in M$, we choose i such that $i \geq \alpha k$. Then, a longest factorization of $c \in M_{xp^\alpha, yp^\alpha}$ of the form $c = p^i q^k$ is $(p^\alpha q)^k (p^\beta)^{\frac{i-\alpha k}{\beta}}$. Here L(c) $= k + \frac{i - \alpha k}{\beta}$. This factorization length is maximal since we have a maximal number of factors $p^\alpha q$. We note that the factor $p^\alpha q$ has minimal copies of p and of q. Any other irreducible must have at least α copies of p and at least one copy of q. The only exception is the irreducible, p^β. Since we have exhausted our copies of q, any additional copies of p must be put into the form p^β which is precisely what we have.

□

Lemma 57. *M_1 is fully elastic over the interval* $[1, \frac{\beta}{\alpha})$.

Proof. For $c \in M_1$, we have the elasticity of c defined as $\rho(c) = \frac{L(c)}{l(c)}$. Then given some $\frac{w}{v} \in [1, \frac{\beta}{\alpha})$. We define $i = (\beta - \alpha)(\beta v - 1)$ and $k = \beta(w - v) + 1$. We claim that $i \geq \alpha k$, indeed,

$$\begin{aligned} \alpha k &= \alpha\beta w - \alpha\beta v + \alpha \\ &\leq \beta(\beta v - 1) - \alpha\beta v + \alpha \\ &= \beta\beta v - \beta - \alpha\beta v + \alpha \\ &= (\beta - \alpha)\beta v - (\beta - \alpha) \\ &= (\beta - \alpha)(\beta v - 1) = i \end{aligned}$$

Therefore, $i \geq \alpha k$. Then,

$$\begin{aligned} \rho(c) = \frac{i + k(\beta - \alpha)}{i + \beta - \alpha} &= \frac{(\beta - \alpha)(\beta v - 1) + (\beta(w - v) + 1)(\beta - \alpha)}{(\beta - \alpha)(\beta v - 1) + (\beta - \alpha)} \\ &= \frac{(\beta v - 1) + (\beta w - \beta v + 1)}{\beta v} \\ &= \frac{\beta w}{\beta v} \\ &= \frac{w}{v} \end{aligned}$$

Thus, M_1 is fully elastic over the interval $[1, \frac{\beta}{\alpha})$. □

Let M_{xp^α, yp^α} be a monoid such that $\alpha \leq \frac{\mathrm{ord}(p)}{2} = \frac{\beta}{2}$. Let r be prime such that $r \equiv p^{\beta - 1} \bmod y$. Then $pr \equiv 1 \bmod y$. Define the submonoid $M_2 = M_{xp^\alpha, yp^\alpha} \cap \{p^i r^j : i, j \in \mathbb{N}_0\}$.

Lemma 58. *The order of r modulo y is β.*

Proof. Since $1 \equiv pr \equiv (pr)^\beta \equiv p^\beta r^\beta \equiv r^\beta \bmod y$, it follows that $ord(r) \leq \beta$. Suppose there was a $b < \beta$ such that the order of r modulo y was b. Then $1 \equiv pr \equiv (pr)^b \equiv p^b r^b \equiv p^b \not\equiv 1 \bmod y$, and we have a contradiction. Therefore, it follows that $ord(r) = \beta$. □

Lemma 59. *The element $g = p^i r^j$ is in M_2 if and only if $i \geq \alpha$ and $i \equiv j \bmod \beta$.*

Proof. Let $g = p^i r^j \in M_2$. Then $p^\alpha | g$, and so $i \geq \alpha$. Suppose that $i \geq j$. Since $g = p^i r^j \in M_2$, then $1 \equiv g \equiv p^i r^j \equiv (pr)^j (p)^{i-j} \equiv (p)^{i-j} \bmod y$. Since the order of p modulo y is β, it follows that $i - j \equiv 0 \bmod \beta$. Therefore $i \equiv j \bmod \beta$. Suppose that $i < j$. Since $g = p^i r^j \in M_2$, then $1 \equiv g \equiv p^i r^j \equiv (pr)^i (r)^{j-i} \equiv (r)^{j-i} \bmod y$. Since the order of r modulo y is β, it follows that $j - i \equiv 0 \bmod \beta$. Therefore $i \equiv j \bmod \beta$.

Let $g = p^i r^j$ where $i \geq \alpha$ and $i \equiv j \bmod y$. Clearly, $p^\alpha | g$. Since $i \equiv j \bmod y$, there exist $A, B, C \in \mathbb{N}_0$ such that $i = A\beta + C$ and $j = B\beta + C$. Therefore $p^i r^j \equiv (p^\beta)^A (r^\beta)^B (pr)^C \equiv 1^A 1^B 1^C \equiv 1 \bmod y$. So $g \in M_2$. □

Lemma 60. *Any element in M_2 can be written as $g = p^i r^j = (p^\beta)^u (pr)^v (r^\beta)^w$ where $\beta u + v \geq \alpha$ and $uw = 0$.*

Proof. Since for all $p^i r^j$ in the submonoid, $i \equiv j \bmod \beta$, it follows that there exist $u', v', w' \in \mathbb{N}_0$ such that $i = \beta u' + v'$ and $j = \beta w' + v'$. If $u' \geq w'$, then $p^i r^j$ can be written as $(p^\beta)^u (pr)^v (r^\beta)^w$ where $w = 0$, $u = u' - w'$ and $v = v' + \beta w'$. If $u' < w'$, then $p^i r^j$ can be written as $(p^\beta)^u (pr)^v (r^\beta)^w$ where $u = 0$, $w = w' - u'$ and $v = v' + \beta u'$. □

Lemma 61. *An irreducible in M_2 is one of the following:*

- $u = 0$ *and* $\alpha \leq v < 2\alpha$ *and* $w \in \mathbb{N}_0$
- $u = 1$ *and* $0 \leq v < \alpha$ *and* $w = 0$

Proof. Let $g = p^i r^j = (p^\beta)^u (pr)^v (r^\beta)^w$ where $\beta u + v \geq \alpha$ and $uw = 0$ be in the submonoid.

Suppose $u = 0$, then since $uw = 0$, it follows that $w \in \mathbb{N}_0$. If $v < \alpha$, then g is not in the monoid since $p^\alpha \not| g$. If $v \geq 2\alpha$, then g is reducible into $(p^\alpha r^\alpha)(p^{v-\alpha} r^{v+w\beta-\alpha})$. Consider the first factor. Clearly, $i \geq \alpha$ and $i \equiv j \bmod \beta$. Consider the second factor. Since $v \geq 2\alpha$, then $v - \alpha \geq \alpha$ and so $i \geq \alpha$. Also, $i \equiv j \bmod \beta$. So if $v \geq 2\alpha$, then g is reducible. If $\alpha \leq v < 2\alpha$, then suppose g was reducible. Then since there are less than 2α copies of p, one of the factors must have less than α copies of p and therefore not be in the monoid. So we have a contradiction. Therefore if $u = 0$ and $w \in \mathbb{N}_0$, then g is irreducible if and only if $\alpha \leq v < 2\alpha$.

Suppose $u = 1$, then since $uw = 0$, it follows that $w = 0$. If $v \geq \alpha$ then g is reducible into $(p^\beta)(p^v r^v)$ If $0 \leq v < \alpha$, then g is irreducible. Since there are less than α copies of r, then it is not possible to factor g where one factor has $\alpha \leq i < \beta$ copies of p. This is because $i \equiv j \bmod \beta$. So any irreducible with $\alpha \leq i < \beta$ copies of p requires i copies of r which are not available. Therefore, all factors must have at least β copies of p. Since $i = \beta + v < \beta + \alpha < 2\beta$, it follows that g is irreducible. Therefore if $u = 1$ and $w = 0$, then g is irreducible if and only if $0 \leq v < \alpha$.

Suppose $u \geq 2$, then g is reducible into $(p^{\beta})^{u-1}(p^{\beta+v}r^{v})$. It is clear that for all factors $i \geq \alpha$ and $i \equiv j \bmod \beta$. So if $u \geq 2$ then $g = p^i r^j = (p^{\beta})^u (pr)^v (r^{\beta})^w$ is reducible.

□

Lemma 62. *The shortest factorization for an element $g = p^i r^j \in M_2$ where $i = (\alpha+\beta-1)\gamma + 2\alpha - 1$ and $j = (\alpha-1)\gamma + 2\alpha - 1 + m\beta$ for some $\gamma, m \in \mathbb{N}_0$ is $l(g) = \gamma + 1$.*

Proof. Note that the most copies of p present in any one irreducible comes from the case where $u = 1$, $w = 0$, and $v = \alpha - 1$. Therefore it is not possible for an irreducible to have more than $\alpha+\beta-1$ copies of p. So the shortest factorization length comes from every factor having exactly $\alpha+\beta-1$ copies of p. So the shortest length possible to factor an element of M_2 is $\frac{i}{\alpha+\beta-1}$. Since the length of factorization must be an integer, the shortest length possible to factor an element of M_2 is $\lceil \frac{i}{\alpha+\beta-1} \rceil$.

Consider the following factorization of g:

$$(p^{\alpha+\beta-1}r^{\alpha-1})^{\gamma}(p^{2\alpha-1}r^{2\alpha-1+m\beta})$$

which has length $\gamma+1$. Now, $\lceil \frac{i}{\alpha+\beta-1} \rceil = \lceil \frac{(\alpha+\beta-1)\gamma+2\alpha-1}{\alpha+\beta-1} \rceil = \lceil \gamma + \frac{2\alpha-1}{\alpha+\beta-1} \rceil = \gamma+1$. Therefore, there is a valid factorization with length $\lceil \frac{i}{\alpha+\beta-1} \rceil$. So $l(g) = \gamma+1$. □

Lemma 63. *The longest factorization for an element $g = p^i r^j \in M_2$ where $i = \alpha\theta + \beta\phi$ and $j = \alpha\theta$ for some $\theta, \phi \in \mathbb{N}_0$ is $L(g) = \theta + \phi$.*

Proof. Recall the types of irreducibles:

(i) $u = 0$ and $\alpha \leq v < 2\alpha$ and $w \in \mathbb{N}_0$

(ii) $u = 1$ and $0 \leq v < \alpha$ and $w = 0$.

Also, consider the following factorization of g:

$$(p^{\alpha}r^{\alpha})^{\theta}(p^{\beta})^{\phi}$$

which has length $\theta+\phi$. Also note that the factorization has θ type *(i)* irreducibles and ϕ type *(ii)* irreducibles. Suppose a longer factorization was possible. Then that factorization would either have to have more than θ type *(i)* irreducibles or more than ϕ type *(ii)* irreducibles.

Now, note that it is not possible to have a type *(i)* irreducible with less than α copies of r. Therefore the maximum number of type *(i)* irreducibles is $\frac{j}{\alpha} = \frac{\alpha\theta}{\alpha} = \theta$. So the longer factorization must have more than ϕ type *(ii)* irreducibles so that the factorization length is greater than $\theta+\phi$.

Since $2\alpha \leq \beta$ and a type *(ii)* contains at least β copies of p and a type *(i)* irreducible may not contain more than β copies of p, it would take at least one type *(i)* irreducibles from the previous factorization to create one new type *(ii)* irreducible. Therefore if the number of type *(ii)* irreducibles is more than ϕ, then there is an $A \in \mathbb{N}$ so that the number of type *(ii)* irreducibles is $\phi + A$. And the factorization length $\hat{L}(g)$ is $\hat{L}(g) \leq (\theta - A) + (\phi + A) = \theta + \phi$. Therefore it is not possible to create a longer factorization with more than ϕ type *(ii)* irreducibles.

Therefore the longest factorization for an element $g = p^i r^j \in M_2$ where $i = \alpha\theta + \beta\phi$ and $j = \alpha\theta$ for some $\theta, \phi \in \mathbb{N}_0$ is $L(g) = \theta + \phi$.

□

Corollary 64. *The elasticity for any element $g = p^i r^j \in M_2$ where $i = (\alpha + \beta - 1)\gamma + 2\alpha - 1 = \alpha\theta + \beta\phi$ and $j = (\alpha - 1)\gamma + 2\alpha - 1 + m\beta = \alpha\theta$ for some $\gamma, m, \theta, \phi \in \mathbb{N}_0$ is $\rho(g) = \frac{(2\alpha-1)\gamma + (\beta-\alpha)m + 2\alpha - 1}{\gamma+1}$.*

Proof. Solving the system of equations:

$$\begin{aligned} i &= (\alpha + \beta - 1)\gamma + 2\alpha - 1 \\ i &= \alpha\theta + \beta\phi \\ j &= (\alpha - 1)\gamma + 2\alpha - 1 + m\beta \\ j &= \alpha\theta \end{aligned}$$

gives $\phi = \gamma - m$ and $\theta = \gamma + 2 + (1/\alpha)(m\beta - \gamma - 1)$.

By Lemma 62 the shortest factorization for an element $g = p^i r^j \in M_2$ where $i = (\alpha + \beta - 1)\gamma + 2\alpha - 1$ and $j = (\alpha - 1)\gamma + 2\alpha - 1 + m\beta$ for some $\gamma, m \in \mathbb{N}_0$ is $l(g) = \gamma + 1$. Also, by Lemma 63 the longest factorization for an element $g = p^i r^j \in M_2$ where $i = \alpha\theta + \beta\phi$ and $j = \alpha\theta$ for some $\theta, \phi \in \mathbb{N}_0$ is $L(g) = \theta + \phi$. So $\rho(g) = \frac{L(g)}{l(g)} = \frac{\theta+\phi}{\gamma+1} = \frac{\alpha\gamma + 2\alpha + m\beta - \gamma - 1 + \alpha\gamma - \alpha m}{\gamma+1} = \frac{(2\alpha-1)\gamma + (\beta-\alpha)m + 2\alpha - 1}{\gamma+1}$ □

Following the corollary above, we wish to show that for all rationals $\frac{w}{v} \in [\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$ there is an element $g \in M_2$ such that $\rho(g) = \frac{w}{v}$. The first step in proving this is to show that $\gamma, m, \theta, \phi \in \mathbb{N}_0$ for a given choice of γ and m.

Lemma 65. *Given the constructions above, $\gamma, m, \theta, \phi \in \mathbb{N}_0$.*

Proof. Let $\frac{w}{v} \in [\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$. Also let $\gamma = (\beta - \alpha)v - 1$ and $m = \alpha w - (2\alpha - 1)v = \alpha(w - 2v) + v$. First we note that $\beta \geq 2\alpha > \alpha > 1$. With this observation, we examine:

$$\gamma = (\beta - \alpha)v - 1$$

Since $\beta \geq 2\alpha$, $(\beta - \alpha) \geq 1$. Since $v \in \mathbb{N}$, $v \geq 1$. By the previous two observations, $(\beta - \alpha)v > 1$ which implies $\gamma = (\beta - \alpha)v - 1 > 0$. Now consider,

$$m = \alpha w - (2\alpha - 1)v = \alpha(w - 2v) + v$$

Since both α and v are positive integers, it suffices to show that $w - 2v > 0$. Since $\frac{w}{v} \in [\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$, he have the following,

$$\frac{\beta}{\alpha} < \frac{w}{v} < \frac{\alpha + \beta - 1}{\alpha}$$

$$\beta v < \alpha w < v(\alpha+\beta-1) \tag{1}$$

But since $\beta \geq 2\alpha > \alpha > 1$, we have,

$$2\alpha v \leq \beta v < \alpha w$$

Thus, $2\alpha v < \alpha w$ which implies that $2v < w$ since $\alpha > 1$. Therefore, $m = \alpha w - (2\alpha - 1)v > 0$ as desired. From above, we know that both γ and m are positive integers so it suffices to show that $\gamma \geq m$ to prove ϕ is also a positive integer.

$$\begin{aligned}
m &= \alpha w - (2\alpha-1)v \\
&\leq v(\alpha+\beta-1) - 1 - (2\alpha-1)v && \text{from (1) above} \\
&= (\alpha+\beta-1-2\alpha+1)v - 1 \\
&= (\beta-\alpha)v - 1 \\
&= \gamma
\end{aligned}$$

Therefore, $\gamma \geq m$ as desired. Lastly, we show that

$$\theta = \gamma + 2 + \beta w - 2v\beta + v$$

is a positive integer. This is seen by noting that $\beta w - 2v\beta = \beta(w-2v) \geq 0$. Since $\gamma, v \in \mathbb{N}_0$, it follows that $\theta \in \mathbb{N}_0$. □

Lemma 66. *Given m, γ and β from above, $m \leq \gamma \leq \beta m$.*

Proof. We have already shown that $m \leq \gamma$ in the lemma 65 proof. Therefore, it suffices to show that $\gamma \leq \beta m$. Note that $\gamma = \beta v - \alpha v - 1 \leq \beta v$ since $2v \leq w$, $\alpha\beta(w-2v) \geq 0$.

$$\begin{aligned}
\gamma &= \beta v - \alpha v - 1 \\
&\leq \beta v \\
&\leq \beta v + \alpha\beta w - 2\alpha\beta v \\
&= \beta(\alpha w - v(2\alpha-1)) \\
&= \beta m
\end{aligned}$$

Therefore, $\gamma \leq \beta m$. □

Theorem 67. *M_2 is fully elastic on $[\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$.*

Proof. Let $\frac{w}{v} \in [\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$. Consider $g = p^i r^j \in M_2$ such that $i = (\alpha+\beta-1)\gamma + 2\alpha - 1$ and $j = (\alpha-1)\gamma + 2\alpha - 1 + m\beta$. Consider $\gamma = (\beta-\alpha)v - 1$ and

$m = \alpha w - (2\alpha - 1)v = \alpha(w - 2v) + v$. So from the previous lemmas, we know

$$\begin{aligned}
\rho(g) &= \frac{(2\alpha-1)\gamma + (\beta-\alpha)m + 2\alpha - 1}{\alpha(\gamma+1)} \\
&= \frac{(2\alpha-1)((\beta-\alpha)v - 1) + (\beta-\alpha)(\alpha w - (2\alpha-1)v) + (2\alpha-1)}{\alpha((\beta-\alpha)v - 1 + 1)} \\
&= \frac{(\beta-\alpha)v(2\alpha-1) - (2\alpha-1) + (\beta-\alpha)\alpha w - (2\alpha-1)v(\beta-\alpha) + (2\alpha-1)}{\alpha(\beta-\alpha)v} \\
&= \frac{\alpha(\beta-\alpha)w}{\alpha(\beta-\alpha)v} \\
&= \frac{w}{v}
\end{aligned}$$

Therefore M_2 is fully elastic on $[\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$, as desired.

□

Theorem 68. *M_{xp^α, yp^α} where the $\frac{ord(p)}{2} \geq \alpha$ is fully elastic.*

Proof. Recall that the elasticity of the monoid is $\frac{\alpha+\beta-1}{\alpha}$. Also, by Theorem 57, M_1 is fully elastic on $[1, \frac{\alpha}{\beta})$. By Theorem 67, M_2 is fully elastic on $[\frac{\beta}{\alpha}, \frac{\alpha+\beta-1}{\alpha})$. Therefore, M_{xp^α, yp^α} where the $\frac{\mathrm{ord}(p)}{2} \geq \alpha$ is fully elastic. □

8 Conclusion

The question of whether or not a local singular ACM is fully elastic has proven to be a very difficult. To construct elements such that every elasicity in the interval $[1, \rho(M))$ is a very complex problem. In an attempt to simplify the problem, we considered submonoids. Some monoids were fully elastic on the entire interval, and some were fully elastic on only parts of the interval. Other submonoids were restrictive in such a way that not all fractions in any interval were met. The submonoid that seemed to be the most helpful in determining full elasticity was when $M_{xp^\alpha, yp^\alpha} \cap \{p^i, q^k : q \equiv x \bmod y, q \text{ prime, and } i, k \in \mathbb{N}_0\}$. The benefit to a submonoid was that the prime factorization of any element included only two primes. This avoided complicated interactions between different congruence classes.

Another difficulty that this problem presented was that in general, it is very difficult to classify what is and is not an element in the submonoid. We were able to establish a transfer homomorphism between the submonoid and a subset of $\mathbb{N}_0^2$ when the units of y were isomorphic to a cyclic group. This enabled us to classify which elements were and were not in the monoid effectively and efficiently. The goal was to use this transfer homomorphism to help classify irreducibles in general, and hopefully find a submonoid which was fully elastic on an interval. If different submonoids are fully elastic on different intervals, and those intervals overlap, then the monoid is fully elastic.

We were able to show that many monoids are fully elastic. First, $M_{xp,yp}$ is fully elastic. Also $M_{xp^{\alpha},yp^{\alpha}}$ where the order of p modulo y is 2 is fully elastic if and only if $x > 1$ or $\alpha = 2$. We were also able to show that $M_{xp^2,21p^2}$ is fully elastic if and only if the order of p modulo y is not equal to 1. Also, we were able to show that $M_{xp^{\alpha},yp^{\alpha}}$ with $\alpha \leq \frac{\text{ord}(p)}{2}$ has a submonoid that is fully elastic on $[1, \frac{\alpha+\beta-1}{\alpha})$ We also have some partial results. For example, we were able to establish a transfer homomorphism between a submonoid and a subset of $\mathbb{N}_0^2$ when the units of y were cyclic. This should lead to some results regarding full elasticity since all classifications of what is and is not in the monoid are determined. Overall, we are pleased with the results from our research.

References

1 . M. Banister, J.Chaika, S. T. Chapman, W. Meyerson 2007. *On the Arithmetic of Arithmetical Congruence Monoids*, Colloquium Mathematicum

2 . S.T. Chapman, D. Steinberg, 2010. *On the Elasticity of Generalized Arithmetical Congruence Monoids*, Results In Mathematics

3 . P. Baginski, S.T. Chapman, 2010. *Arithmetic Congruence Monoids: A Survey*