On Factorization Properties of Semi-Regular Congruence Monoids

Jessica Bauman
Department of Mathematics
Trinity University REU 2006

July 28, 2006

Abstract

If given $n \in \mathbb{N}$ and Γ, a multiplicatively closed subset of $\mathbb{Z}_n$, then the set $H_\Gamma = \{n \in \mathbb{Z} : x \in \mathbb{N} : x + n\mathbb{Z} \in \Gamma\} \cup \{1\}$ is a multiplicative submonoid of $\mathbb{N}_0$ known as a *congruence monoid*. Much work has been done to characterize the *factorial* (every element has unique factorization) and *half-factorial* (lengths of irreducible factorizations of an element remain constant) properties of such objects. Our paper further examines the specific *semi-regular* case, when Γ contains both units and non-units. We delve into characterizing the half-factoriality problem for semi-regular congruence monoids, as well as finding sufficient conditions for a congruence monoid such that $\min \Delta (H_\Gamma) > 1$.

1 Introduction

For some integer $n > 0$, let Γ be a multiplicatively closed subset of $\mathbb{Z}/n\mathbb{Z}$. Consider the set

$$H_\Gamma = \{n \in \mathbb{Z} : x \in \mathbb{N} : x + n\mathbb{Z} \in \Gamma\} \cup \{1\}$$

under multiplication . H_Γ is refered to as a *Congruence Monoid.* This construction, which can be generalized to any integral domain R (see [4]) is a multiplicative submonoid of $\mathbb{N}_0$, and plays an important role in the study of non-unique factorizations.

In 2003, M. Banister, J. Chaika, S.T Chapman and W. Meyerson wrote a paper on "'The Arithmetic of Congruence Monoids"' which examined and characterized specific cases of factorization for both the general congruence monoid as well as a more specific case the *ACM* (Arithmetical Congruence Monoid), which occurs when Γ contains only a single element (see [1]for more results on *ACM*'s). Much is known about these objects. For example, the trendy *Hilbert monoid*

$$1 + 4\mathbb{N}_0 = \{1, 5, 9, 13, 17, 21\}$$

is characterized as an *ACM* and furthermore demonstrates non-unique factorizations, as can be seen by $441 = 21 * 21 = 9 * 49$ (where 9, 21 and 21 are irreducible in $1 + 4\mathbb{N}_0$, see [6] and [5]). What the *Hilbert Monoid* best demonstrates for this paper is a property called *half factoriality*. Given any congruence monoid H_Γ we define the set of irreducibles as $A(H_\Gamma) = \{x \in H_\Gamma : x = rs \rightarrow r \notin H_\Gamma, s \notin H_\Gamma, r = 1 \text{ or } s = 1\}$ and say that H_Γ is *half factorial* iff for any $x \in H_\Gamma$ such that $x = p_1 \ldots p_t = q_1 \ldots q_k$ with each p_i and $q_j \in A(H_\Gamma)$, then $t = k$. This important property is not so easy to prove in general for congruence monoids. Halter-Koch succeeded in characterizing the case when $\Gamma \subseteq (\mathbb{Z}_n)^x$ (called *regular* (see [4]), while M. Banister, J. Chaika, S.T Chapman and W. Meyerson succeeded in characterizing the case when $\Gamma \cap \mathbb{Z}_n^x = \varnothing$ (called *singular*) (see [1]). Yet the last case remained unclassified. Called *semi-regular*, occuring when H_Γ is neither regular nor singular, the half-factorial semi-regular problem provided a large part of the motivation for the work in this paper. In section 1 we provide strong conditions for a semi-regular congruence monoid to be half-factorial and demonstrate several cases where a semi-regular congruence monoid is not half-factorial.

In section two we introduce a new concept, that of a Δ-set. Given $x \in H_\Gamma$, then the *set of lengths of x* is

$$L(x) = \{k \in N : x = a_1 \ldots a_k \text{ where } a_i \in A(H_\Gamma).$$

If we order $L(x) = \{n_1, \ldots n_t\}$ from smallest to largest, then we can define $\Delta(x) = \{n_i - n_{i-1} : 2 \leq i \leq t\}$, which one can think of as an indication of how differently x can factor. To delineate how "differently" H_Γ as a whole can factor, we define

$$\Delta(H_\Gamma) = \cup_{1 \neq x \in H_\Gamma} \Delta(x).$$

Much work has been done on the Δ-set's of monoids. One such important result came from A. Geroldinger ([3, lemma 3]), which characterized the minimum of the Δ-set of any monoid, by proving that

$$\min \Delta(H_\Gamma) = \gcd \Delta(H_\Gamma).$$

This gives us a comprehensive tool for finding the minimum of many congruence monoids, especially in the cases of ACM's. But it was not known

whether there existed a congruence monoid with the minimum of the Δ-set $\neq 1$ such that $\Delta(H_\Gamma) \neq \varnothing$. The main result of section two constructs a family of semi-regular congruence monoids with that $\min \Delta(H_\Gamma) > 1$.
To do so we examine a slightly weaker condition than *half factoriality*, namely *congruence half factoriality*. We say that a congruence monoid H_Γ is a *congruence half-factorial monoid of order r (or CHFM)* if $\forall x \in H_\Gamma$ such that $x = p_1 \dots p_t = q_1 \dots q_k$ with each p_i and $q_j \in A(H_\Gamma)$, then $t \equiv k \mod r$. A half-factorial congruence monoid is always CHFM of order r for all $r > 1$, but the converse of this statement does not always hold, as in many examples of CHFMs in the Krull case (see [2]for more examples and information). Finally we end the introduction with the definitions of *elasticity* and *minimal essential H-sets*.

The *elasticity* of an element $x \in H_\Gamma$, denoted $\rho(x)$, is given by the ratio of $\max(L)$ to $\min(L)$, and the *elasticity* of H_Γ is then defined to be

$$\rho(H_\Gamma) = \sup\{\rho(x) : x \in H_\Gamma\}.$$

If H_Γ is half-factorial then $\rho(H_\Gamma) = 1$. Let $G \subseteq N$ be a monoid. A finite set of prime numbers R is called *G-Essential* if there exists $a \in G$ such that R is the set of all primes dividing a. We say R is minimal if it is minimal by set inclusion. A result by Halter-Koch (see [4, lemma 3]) proves that a congruence monoid H_Γ has finite elasticity if and only if every minimal H_Γ-essential set is a singleton. This has an important impact in the types of elements in a half-factorial semi-regular congruence monoid.

I would like to thank Dr. Scott Chapman and Paul Baginki for their priceless support, mentoring and help, and well as my family, and the NSF for funding this project.

1.1 Semi-Regular Congruence Monoids and Half-Factoriality

Let $\mathcal{G} = H_\Gamma \cap \{q : \gcd(q, n) = 1\}$. If $\mathcal{G}$ is a monoid under multiplication, then it can be considered regular with respect to minimal modulus n. We define

$$\phi : \mathcal{G} \to \mathbb{Z}_n$$

such that $\phi(g) = g \mod n \ \forall g \in \mathcal{G}$. Letting G be the image of $\mathcal{G}$ under ϕ, clearly $G \subseteq \mathbb{Z}_n^\times$.

Proposition 1.1. *If H_Γ is a half factorial semi-regular congruence monoid of minimal modulus n then $[\mathbb{Z}_n^\times : G] \leq 2$.*

Proof. Suppose H_Γ is a half-factorial semi-regular confruence monoid with minimal modulus n, such that $[\mathbb{Z}_n^\times : G] > 2$ (by assumption). Let $\alpha \in \mathbb{Z}_n^\times/G$ By Direchlet's theorem $\exists\ \alpha^{-1} \in \mathbb{Z}_n^\times/G$ such that $q_1 G = \alpha$, $q_2 G = \alpha^{-1}$ and $q_1 q_2 \in H_\Gamma$. As $|\mathbb{Z}_n^\times/G| > 2$, $q_1 \neq q_2$ and by definition of G, we can conclude $q_1 \notin H_\Gamma$ and $q_2 \notin H_\Gamma$. There exists a smallest k such that $q_1^k \in H_\Gamma$ and by the properties of inverses $q_2^k \in H_\Gamma$. But that implies $(q_1 q_2)^k = \left(q_1^k\right)\left(q_2^k\right)$. As $q_1 q_2 \in A(H_\Gamma)$, $q_1^k \in A(H_\Gamma)$ and $q_2^k \in A(H_\Gamma)$, factorization is not half-factorial. Hence by contradition half-factoriality implies $[\mathbb{Z}_n^\times : G] \leq 2$. □

Proposition 1.2. *If H_Γ is a semi-regular congruence monoid of minimal modulus $n = p^k$ then H_Γ is not half-factorial.*

Before we prove this proposition, we're going to prove the following lemma.

Lemma 1.3. *Suppose H_Γ is a semi-regular congruence monoid of minimal modulus $n = p^k$ such that $k \geq 2$. Let the subgroup of $\mathbb{Z}_n$ generated by p^i, $\langle p^i \rangle$, be a subset of Γ and $\theta_i = \gcd(i, k)$. Then $p^{\theta_i} \in \langle p^i \rangle$ and is the smallest element of $\langle p^i \rangle$ in H_Γ.*

Proof. We define an mapping

$$\varphi : \left(\mathbb{Z}_n / (\mathbb{Z}_n)^\times, *\right) \to (\mathbb{Z}_k, +)$$

taking p^i to its respective equivalence class in $\mathbb{Z}_k$. By definition, $\exists\ a,\ b \in \mathbb{Z}$ such that $ai + bk = \theta_i$. Modulo k this implies $ai \equiv \theta_i$, and thus $\theta_i \in \mathbb{Z}_k$. By the surjectivity of the mapping we can choose a such that $p_i^\theta \in \langle p^i \rangle$. We will show that this is the smallest element of $\langle p^i \rangle$ in H_Γ by contradiction. Assume that $\exists \gamma \in \mathbb{N}$ such that $\gamma < \theta$ and $p^\gamma \in \langle p^i \rangle$. Under φ $\exists$ a such that $ai \equiv \gamma$ modulo k. But that implies that $\exists$ $c \in \mathbb{Z}$ such that $ai = \gamma + ck$, and therefore $ai - ck = \gamma$, contradicting the gcd-ness of θ. □

Corollary 1.4. *Assuming that H_Γ is a half-factorial semi-regular congruence monoid of minimal modulus $n = p^k$ and $\langle p_1^h \rangle, \langle p_2^i \rangle \ldots \langle p_m^j \rangle \subset \Gamma$ where $\langle p^i \rangle$ refers to the cyclic subgroup of $\mathbb{Z}_n$ generated by $p^i$and m is the number of distinct subgroups, then $\theta_i \neq \theta_j \neq 1$, and $\theta_i \neq n\theta_j$ for any p^i and $p^j \in \Gamma$ and $n \in \mathbb{Z}$.*

Proof. If $\theta_i = 1$ and $G = \mathbb{Z}_n^\times$, then $p \in \Gamma$ and $H_\Gamma = \mathbb{N}_0$. If $\theta_i = 1$ and $[\mathbb{Z}_n^\times : G] = 2$, then $p \in \Gamma$ and we can construct irreducibles given any prime unit $q_j \notin G$, $q_1 q_2 \in A(H_\Gamma)$, and $qp^k \in A(H_\Gamma)$. We know $q_1 q_2 \in A(H_\Gamma)$ because G is index 2. The multiplicative structure of $\langle p^i \rangle$ implies that the only multiples of p^j (for any $j < k$) in H_Γ are units $g \in G$. Thus, since $0 \in \Gamma$, the smallest power j of p such that $qp^j \in H_\Gamma$ is k, and $qp^k \in A(H_\Gamma)$. But that implies that $\left(qp^k\right)^2 = (q^2)\, p^k$ which has a factorization length difference of $p^k - 1$, also implying that H_Γ is very much not half-factorial. If $\theta_i = n\theta_j$ for any p^i and $p^j \in \Gamma$ and $n \in \mathbb{Z}$, then $\langle p^j \rangle \subseteq \langle p^i \rangle$, and the subgroups are not distinct, contradicting the given assumption. $\square$

Now we will finally prove Proposition (1.2)!

Proof. Let H_Γ be a semi-regular congruence monoid of minimal modulus $n = p^k$ such that Γ is generated by $\{G, \langle p_1^i \rangle, \dots \langle p_m^j \rangle\}$ where $\langle p_m^i \rangle$ is defined as above, and $\theta_i \neq n\theta_j$ for any $n \in \mathbb{Z}$ and θ_i and θ_j defined as above.

Case 1: Let $G = \mathbb{Z}_n^\times$ and $\langle p^i \rangle \subset \Gamma$, (ie $m = 1$). Then we can find many an $N \in \mathbb{N}$ such that $iN \geq k$ and $(p^i)^N \in H_\Gamma$, which implies that $0 \in H_\Gamma$ and therefore $hp^k \in H_\Gamma$ for any $h \in \mathbb{N}_0$. Now, $pp^k \in H_\Gamma$, and furthermore is an atom (as $1 + k \neq n \gcd(i,k)$ because any prime dividing $\gcd(i,k)$ also divides k, and therefore will not divide $k+1$). But $p^\theta \in A(H_\Gamma)$, and thus we can do the old switcheroo, $\left(pp^k\right)^\theta = \left(p^\theta\right)\left(p^k\right)^\theta$, which has a factorization length difference of $k + 1 - \theta > 0$.

Now, if $G = \mathbb{Z}_n^\times$ and $m = 2$, say $\langle p^i \rangle, \langle p^j \rangle \subset \Gamma$, then $\gcd(\theta_i, \theta_j) = 1$ or, (suprisingly enough!), $\gcd(\theta_i, \theta_j) \neq 1$. If $\gcd(\theta_i, \theta_j) = 1$, then $\langle p^{\theta_i} \rangle \cap \langle p^{\theta_j} \rangle = \varnothing$, and p^{θ_i} and $p^{\theta_j} \in A(H_\Gamma)$. Again, we apply the old switcheroo: $\left(p^{\theta_i}\right)^{\theta_j} = \left(p^{\theta_j}\right)^{\theta_i}$. By Corollary (1.4), $\theta_i \neq \theta_j$ and the factorization is non-half factorial. If $\gcd(\theta_i, \theta_j) \neq 1$ then $\langle p^{\theta_i} \rangle \cap \langle p^{\theta_j} \rangle \neq \varnothing$, but by Corollary (1.4) $\theta_i \neq n\theta_j$ for any $n \in \mathbb{N}$. Furthermore, by Lemma (1.3), p^{θ_i} and p^{θ_j} are still the smallest elements of $\langle p^i \rangle$ and $\langle p^j \rangle$ respectively. Thus p^{θ_i} and p^{θ_j} are still in $A(H_\Gamma)$ and $\left(p^{\theta_i}\right)^{\theta_j} = \left(p^{\theta_j}\right)^{\theta_i}$ (no time to switch on the old switcheroo).

Case 2: Let $[\mathbb{Z}_n^\times : G] = 2$ and $\langle p^i \rangle \subset \Gamma$, (ie $m = 1$). Like above, we can raise (p^i) to some $N \in \mathbb{N}$ power such that $iN \geq k$, which implies that $0 \in H_\Gamma$ and therefore $p^k \in H_\Gamma$. Also as shown above in the proof of Corollary (1.4), given any prime unit $q \notin G$, we have $q_1 q_2 \in A(H_\Gamma)$, and $qp^k \in A(H_\Gamma)$ are true. By Lemma (1.3), $p^{\theta_i} \in A(H_\Gamma)$. If we suppose $r\theta_i = k$ and apply a twisteroo (if you will a twist on the old switch), then $\left(p^k q\right)^2 = \left(p^{r\theta_i} q\right)^2 = \left(p^{\theta_i}\right)^{2r}(q^2)$, fostering a fancy factorization difference of $2r - 1$, and thus H_Γ is not half-factorial.

If $m \neq 1$ then assuming that each $\langle p_1^i \rangle, \dots \langle p_m^j \rangle$ is distinct and $\theta_i \neq n\theta_j$ (for any p^i and $p^j \in \Gamma$ and $n \in \mathbb{Z}$), then $\theta_i, \dots \theta_j \in A(H_\Gamma)$, and given any two, $\left(p^{\theta_i}\right)^{\theta_j} = \left(p^{\theta_j}\right)^{\theta_i}$, rendering factorization not half-factorial.

□

Proposition 1.5. *Let H_Γ be congruence monoid of minimal modulus $n = p_1^{e_1} \dots p_k^{e_k}$ such that each p_j is distinct and $\Gamma = \mathbb{Z}_n^\times \cup \{\langle p_1 \rangle \cup \dots \cup \langle p_i \rangle\}$. Then H_Γ is not semi-regular (contrary to what one might want to believe!), and in fact is regular of minimal modulus $n = {p_{i+1}}^{e_{i+1}} \dots p_k^{e_k}$.*

Proof. We will show that for every p_i which is introduced into Γ, the modulus of H_Γ decreases. As the modulus is decreasing, no non-units get introduced into H_Γ and thus it stays regular. To see this, note first that if $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ and $n' = p_2^{e_2} \dots p_k^{e_k}$, that since $\gcd(p_1, n') = 1$ that $\langle p_1 \rangle \subset \mathbb{Z}_{n'}^\times$ and furthermore, $\langle p_1 \rangle \cup {\mathbb{Z}_n}^\times = \mathbb{Z}_{n'}^\times$. Let $n'' = p_3^{e_3} \dots p_k^{e_k}$. Then since $\gcd(p_1, p_2, n'') = 1$, we can deduce that $\{\langle p_1 \rangle \cup \langle p_2 \rangle\} \subset \mathbb{Z}_{n''}^\times$ and $\{\langle p_1 \rangle \cup \langle p_2 \rangle\} \cup {\mathbb{Z}_n}^\times = \mathbb{Z}_{n''}^\times$. Repeating this process i times, if we denote $n^i = {p_{i+1}}^{e_{i+1}} \dots {p_k}^{e_k}$, then clearly $\{\langle p_1 \rangle \cup \dots \cup \langle p_i \rangle\} \cup {\mathbb{Z}_n}^\times = \mathbb{Z}_{n^i}^\times$. But now, the assumption that $\Gamma = \langle p_1 \rangle \cup \dots \cup \langle p_i \rangle \cup \mathbb{Z}_n^\times$ implies that $\Gamma = \mathbb{Z}_{n^i}^\times$. But then H_Γ no longer has minimal modulus n; it has minimal modulus n^i. When considered under modulus n^i, H_Γ is no longer semi-regular, and it's half factorial properties can be found in [1]. □

Proposition 1.6. *Let H_Γ be a semi-regular congruence monoid of minimal modulus $n = p_1^{e_1} \dots p_k^{e_k}$ such that each p_j is distinct and $\exists$ at least one prime p_i with $p_i \| n$. If $\Gamma = \mathbb{Z}_n^\times \cup \langle p_i \rangle \cup \{0\}$, where $p_i \| n$ then H_Γ is a half-factorial semi-regular congruence monoid.*

Proof. Note: If $\langle p_1 \rangle \not\subset \Gamma$ and $0 \in \Gamma$ then the minimal essential H-Set of $n = \{p_1, p_2 \dots p_k\}$ and H_Γ has infinite elasticity. By a result in [4], this would imply that H_Γ is not half-factorial.

Let $\langle p_i \rangle \subset \Gamma$ and refer to those that $p_j \mid n$ but $p_j \notin H_\Gamma$ with a subscript j. Then $n = p_i p_{j_1}^{e_1} \dots {p_{j_y}}^{e_y}$ where $1 + y = k$ and letting $G = \mathbb{Z}_n^\times$, $\Gamma = G \cup \langle p_i \rangle \cup \{0\}$. Given any element $x \in H_\Gamma$ $x = q * p_{j_1}^{e_1} \dots {p_{j_y}}^{e_y} * {p_i}^{f_1}$ where $\gcd(q, n) = 1$. The only irreducibles of H_Γ are:

1. q such that q is prime and $\gcd(q, n) = 1$.
2. p_i.
3. $p_{j_1}^{e_1} \dots {p_{j_y}}^{e_y} * p_i$ such that $p_{j_1}^{e_1} \dots {p_{j_y}}^{e_y} \mid n$.

While the first two irreducible classes are obvious (as primes in H_Γ), the third results from $0 \in \Gamma$, allowing every multiple of $n \in H_\Gamma$. These are the only irreducibles as $p_j \notin \Gamma$. □

1.2 Δ-Sets and CHFM

We will now construct a CHFM of minimal modulus $n = p^k$ and order $r > 1$ such that $\min(\Delta(H_\Gamma)) \neq 1$.

Proposition 1.7. *Let H_Γ be a semi-regular congruence monoid with minimal modulus $n = p^k$ and $\Gamma = \{G, \langle p \rangle\}$ such that $\left[(\mathbb{Z}_n)^\times : G\right] = 2$. For every $k \in N$ that $2k-1 \in \mathbb{P}$, $\exists$ a family of CHFM (namely H_Γ of minimal modulus p^k) which has $\min(\Delta(H_\Gamma)) = 2k-1$.*

*A note: G is unique and generated by a primitive root squared under a theorem by [1]. There also exists a common primitive root of $\left(\mathbb{Z}_{p^k}\right)^\times$ for any $k \in \mathbb{N}$ dependant upon p and we will assume that G is generated by the smallest primitive root of $(\mathbb{Z}_p)^\times$ (when more than one exists).

Before proving Proposition (1.7), we will prove two Lemma's.

If we are going to change the minimal modulus of H_Γ from $n = p^k$ to $n = p^i$, we will deliniate the change by writing the modulus as a subscript. So, let $\mathcal{G}_{p^i} = H_\Gamma \cap \{q : \gcd(q, p^i) = 1\}$ and recall the previous definition

$$\phi : \mathcal{G}_{p^i} \to \mathbb{Z}_{p^i}$$

such that $\phi(g) = g \mod p^i \ \forall g \in \mathcal{G}_{p^i}$. Let G_i be the image of $\mathcal{G}_{p^i}$ under ϕ.

Lemma 1.8. *If H_Γ is defined as above such that for any $i \leq k$, $\left[\left(\mathbb{Z}_{p^i}\right)^\times : G_{p^i}\right] = 2$, then, $\mathcal{G}_p = \mathcal{G}_{p^i}$.*

Proof. By a result from [1] we know that a regular congruence monoid under modulus of definition n is regular under any of its possible moduli of definition n' where $n' \mid n$. As $G_{p^i} \subset \left(\mathbb{Z}_{p^i}\right)^\times$, $\mathcal{G}_{p^i}$ (as a multiplicative sub-congruence monoid of H_Γ with modulus $n = p^i$) is regular. However, we know that G_{p^i} is generated by the same primitive root squared as G_p (like all G_{p^l} for $l \leq k$ are). Thus, if we consider $\mathcal{G}_{p^i}$ as its own congruence monoid independant from H_Γ, p^i is not a minimal modulus at all; it's logically p. Therefore $\mathcal{G}_p = \mathcal{G}_{p^i}$. □

Corollary 1.9. *For $g \in \mathcal{G}_{p^k}$, $a \leq k$ and $l \in Z$, the element $(g + p^a l) \in \mathcal{G}_{p^k}$.*

Proof. Since modulo p, $(g + p^a l) \equiv g$, we know that $(g + p^a l) \in \mathcal{G}_p$. But Lemma (1.8) implies that $(g + p^\tau l) \in \mathcal{G}_{p^k}$. □

Lemma 1.10. *If H_Γ is a semi-regular congruence monoid with minimal modulus $n = p^k$ with $\Gamma = \{G, \langle p \rangle\}$ such that $\left[(\mathbb{Z}_n)^\times : G\right] = 2$, then the only irreducible elements are of the form:*

1. *n such that n is prime in $\mathbb{Z}$ and $n \mod p^k \in G$.*

2. *p.*

3. *$q_1 q_2$, where q_1 and q_2 are prime in $\mathbb{Z}$, and q_1 and $q_2 \in \left(\mathbb{Z}_{p^k}\right)^{\times} \backslash G$ (we will refer to these as prime involutions in the class group of G).*

4. *$p^k q_1$ where q_1 is a prime involution in the class group of G.*

Proof. Let $x \in A\left(H_\Gamma\right)$. By the definition of Γ, we know that $x = p^\tau g \mod p^k$ or $x = 0 \mod p^k$, where $0 \leq \tau \leq k$, and $g \in G$.

Case 1: If $\tau = 0$, then $x = g \mod p^k$, and either x is prime, in which case it's automatically irreducible (case 1), or $x = g + lp^k$. If $x = g + lp^k$, as $p \not| x$, $x \in \mathcal{G}_{p^k}$, and is the product of at least two elements $q_1 q_2$ such that q_1 and $q_2 \in \left(\mathbb{Z}_n\right)^{\times}$. In addition, G_{p^k} is index two which implies that given two involutions q_1 and q_2 (not neccessarily prime), that $q_1 q_2 \in H_\Gamma$. Thus x must be the product of an even number of prime involutions in the class group of G, otherwise one would be able to factor out some prime $g \in G$. The smallest even number is 2 and thus (case 3) $q_1 q_2$ is an atom (when q_1 and q_2 are prime involutions).

Case 2: If $\tau > 0$ and $g = 1$ then $x = p^\tau \mod p^k$ and clearly for $x \in A\left(H_\Gamma\right)$, $\tau = 1$ and $x = p$ (case 2). If $\tau > 0$ and $g \neq 1$, then $x = gp^\tau + lp^k = (p)^\tau\left(g + lp^a\right)$ where $\tau + a = k$. But p is an atom and by Corollary (1.9), $\left(g + lp^a\right) \in \mathcal{G}_{p^k}$. As $\mathcal{G}_{p^k} \subset H_\Gamma$, we can see $\left(g + lp^a\right) \in H_\Gamma$ and thus $x \notin A\left(H_\Gamma\right)$.

Case 3: If $x \equiv 0$ modulo p^k, then $x = qp^k$ for some $q \in \mathbb{Z}$. q must be prime, otherwise it would be itself reducible, and it must be an involution oftherwise x would be reducible. Referencing a result in Corollary (1.4), the smallest power m of p such that $qp^m \in H_\Gamma$ is $m = k$. Thus $x = qp^k$ and these are the only irreducibles. □

We will now prove the main theorem of section 2!

Proof. As the atoms of H_Γ are of the forms n, p, $q_1 q_2$, $p^k q_1$ (consistant with the definitions given in Lemma (1.10)), to describe differences in factorization lengths of any element $z \in H_\Gamma$, we need only consider atoms of the last three types (as the first type are primes). Thus, factoring $z = (p)^x (q)^y$ into irreducibles, $z = \left(p^k q\right)^a \left(q_1 q_2\right)^b (p)$, we get a relationship between the number of atoms in a factorization $a + b + c$ and x and y, namely, as $x = ka + c$ and $y = a + 2b$, $2x + y = 2ka + a + 2b + 2c = 2a + 2b + 2c + a(2k - 1)$. Modulus

$2k-1$, $2a+2b+2c$ is determined by x and y uniquely, and as $2k-1$ is odd and $2a+2b+2c$ is even, modulus $2k-1$ we can see that $a+b+c$ is as well. Furthermore, $p^{2k}n^{2k} = \left(p^{2k}\right)\left(n^2\right) = \left(p^k n\right)^2$ has a difference of factorization lengths of $2k-1$. This implies that if H_Γ is to be CHFM of order r, that $r \mid (2k-1)$. Thus, as $2k-1$ is prime, r must equal $2k-1$. However by definiton of CHFM, this implies that $\gcd\left(\Delta\left(H_\Gamma\right)\right) = 2k-1$. But we know that $\gcd\left(\Delta\left(H_\Gamma\right)\right) = \min\left(\Delta\left(H_\Gamma\right)\right)$. Thus, $\min\left(\Delta\left(H_\Gamma\right)\right) = 2k-1$. □

References

[1] M. Banister J. Chaika S.T Chapman and W. Meyerson. On the arithmetic of congruence monoids. *Colloquium Mathematicum (submitted for publication)*, 2005.

[2] S.T Chapman and W.W Smith. On the hfd, chfd, and k-hfd properties in dedekind domains. *Comm. Algebra*, 1992.

[3] A. Geroldinger. On the arithmetic of certain not integrally closed neotherian integral domains. *Comm. Algebra*, 1991.

[4] A. Geroldinger and F. Halter-Koch. Congruence monoids. *ACTA Arith.*, 2004.

[5] R.D James and I. Niven. Unique factorization in multiplicative systems. *Proc. Amer. Math. Soc.*, 1954.

[6] F. Halter Koch. Arithmetical semigroups defined by congruences. *Semigroup Forum*, 1991.