Irreducible Factorization Lengths and the Elasticity Problem within $\mathbb{N}$

Matthew O. Jenssen, Daniel Montealegre, and Vadim Ponomarenko

Abstract

A large class of multiplicative submonoids of the natural numbers is presented, which includes congruence monoids as well as numerical monoids (by isomorphism). For monoids in this class, the important factorization property of finite elasticity is characterized.

1 Introduction

The Fundamental Theorem of Arithmetic (FTA) states that each element of $\mathbb{N}$, the set of natural numbers, may be written uniquely (up to order) as the product of elements of P, the set of primes. We consider now subsets of $\mathbb{N}$ that are closed under multiplication and include 1; these are called *submonoids* of $\mathbb{N}$. For submonoids of $\mathbb{N}$, we wish to know if the FTA, or perhaps something weaker, still holds.

For example, set $E = \{2n : n \in \mathbb{N}\} \cup \{1\}$. Note that $6, 18 \in E$, but neither can be factored nontrivially in E, since only one factor could be even and hence the other would have to be 1. We call such elements that can't be further (nontrivially) factored *irreducibles*, or *atoms*. By using the ordering of the naturals, it is easy to prove that all submonoids of $\mathbb{N}$ are "atomic"; that is, each element apart from 1 can be factored into irreducibles (a weak form of the FTA). However, this factorization is typically not unique; for example $36 = 6 \cdot 6 = 2 \cdot 18$ are two different factorizations into irreducibles within E.

It is natural to wish to measure how far a multiplicative system, such as a submonoid of $\mathbb{N}$, is from satisfying the FTA. Indeed, this was one of the original interpretations of the class number of an algebraic number field. As it is well-known that a ring of algebraic integers satisfies the FTA if and only if its class number is 1, algebraic number rings with high class number were considered to be "far" from having unique factorizations of elements into products of irreducibles. While we lose the notion of class number in submonoids of $\mathbb{N}$, we can still measure the notion of differing factorization lengths in a related way.

One of the key invariants in the growing field of factorization theory is the *elasticity*. A recent Monthly paper [3] considers this concept in detail. For a history of elasticity, see the survey [2]. Given an atomic monoid M and $x \in M \setminus \{1\}$, we define the elasticity of x, $\rho(x)$, to be the ratio of the maximum number of atoms in a factorization of x divided by the minimum number of atoms in a factorization of x. If $\rho(x) = 1$, then all factorizations of x have the same length, which is close to FTA. Whereas if $\rho(x)$ is very large, then factorizations of x can vary wildly in size. We define $\rho(M) = \sup_{x \in M} \rho(x)$, which is a cap on how wild factorizations can get in M. It turns out that $\rho(E) = 1$; although factorizations are not unique, the number of irreducibles is always the same. Such monoids are called half-factorial (e.g., see [9]).

Example 1. We demonstrate the notion of elasticity on the set $E = \{2n : n \in \mathbb{N}\}$ described earlier. If $x \in E$ and $4|x$, then we can factor x as the product of two elements of E as $x = 2 \cdot \frac{x}{2}$. On the other hand, if $x = y \cdot z$, with $y, z \in E$, then $4|x$. Hence $x \in E$ is an atom if and only if $4 \nmid x$. Consequently, every factorization of $2^m n$ (n odd) into atoms must comprise of exactly m atoms. Therefore $\rho(E) = 1$. We contrast the situation in E by considering $T = \{6n : n \in \mathbb{N}\}$. The element 6^m may be factored into m atoms as $6 \cdot 6 \cdots 6$, and also into two atoms as $(2 \times 3^{m-1}) \cdot (3 \times 2^{m-1})$. Hence $\rho(T) = \infty$.

2 Definitions

A fundamental question to ask about an atomic monoid is whether its elasticity is finite; if not, then FTA fails to hold quite catastrophically. We propose to answer this question for a class of submonoids which we define below. We will give some examples and then return to the elasticity question in our main result, Theorem 12.

Definition 2. *Let M be a submonoid of $\mathbb{N}$. For any $x \in \mathbb{N}$, we say that x* respects *M if for all $y \in \mathbb{N}$,*

$$xy \in M \text{ if and only if } x^2 y \in M.$$

For $r \in \mathbb{N}$, we say that M is r-respectful *if x^r respects M for each $x \in \mathbb{N}$. We say that M is* R-respectful *if M is r-respectful for some $r \in \mathbb{N}$.*

Note that if x respects M, then for all $y \in \mathbb{N}$, the set $\{xy, x^2y, x^3y, \ldots\}$ is either a subset of M or disjoint from M. Not every submonoid of $\mathbb{N}$ is r-respectful. For example, consider $M = \{x \in \mathbb{N} : \text{for all } p \in P, \nu_p(x) = 0 \text{ or } \nu_p(x) \geq p\}$, where $\nu_p(x)$ denotes the highest power of p dividing x. Then M is not R-respectful.

Definition 3. *For M a submonoid of $\mathbb{N}$, we define its P-*radical *as*

$$\sqrt[P]{M} = \{p \in P : p^k \in M \text{ for some } k \in \mathbb{N}\}.$$

For any $T \subseteq P$ and $x \in \mathbb{N}$, let $T(x)$ denote the number of primes from T dividing x, counted according to multiplicity. Let $\mathbb{N}_0$ denote $\mathbb{N} \cup \{0\}$. For $t \in \mathbb{N}_0$, we say that M is t-modest *if $\sqrt[P]{M}(x) \leq t$ for all irreducibles $x \in M$. We say that M is* T-modest *if M is t-modest for some $t \in \mathbb{N}_0$.*

Note that for any $T \subseteq P$ and any $x, y \in \mathbb{N}$, $T(xy) = T(x) + T(y)$. Also, if $T = T_1 \cup T_2$ for disjoint T_1, T_2, then $T(x) = T_1(x) + T_2(x)$. Lastly, note that if $\sqrt[P]{M} = \emptyset$, then M is 0-modest since $\sqrt[P]{M}(x)$ is identically 0.

Not every R-respectful submonoid of $\mathbb{N}$ is T-modest, as the following example shows.

Example 4. Label P sequentially as $\{q_1, q_2, q_3, \ldots\}$. Set $S = \{q_i^2 : i \in \mathbb{N}\} \cup \{q_1q_2, q_3q_4q_5, q_6q_7q_8q_9, q_{10}q_{11}q_{12}q_{13}q_{14}, \ldots\}$. Set $M = \langle S \rangle = \{\prod_{s \in S} s^{b_s} : b_s \in \mathbb{N}_0\}$, where $\mathbb{N}_0$ denotes $\mathbb{N} \cup \{0\}$ and all but finitely many b_s are zero. Then $M = \{\prod_{i \in \mathbb{N}} q_i^{a_i} : a_1 \equiv a_2, a_3 \equiv a_4 \equiv a_5, a_6 \equiv a_7 \equiv a_8 \equiv a_9 \ldots\}$, where all congruences are modulo 2. Further, M is 2-respectful and $\sqrt[P]{M} = P$. However, M has irreducibles with arbitrarily many prime divisors, so M is not T-modest.

3 Important Examples

By restricting our attention to R-respectful T-modest submonoids, we do lose some submonoids of $\mathbb{N}$. We do not have an anologue of our main theorem for these lost submonoids. However, several important classes of monoids meet these restrictions, as will be shown below.

Example 5. Let $n \in \mathbb{N}$. Let $\Gamma \subseteq \{1, 2, \ldots, n\}$ be closed in the sense that if $x, y \in \Gamma$, then there is some $z \in \Gamma$ with $xy \equiv z \pmod{n}$. Set $M(\Gamma, n) = \{x \in \mathbb{N} : \text{ for some } g \in \Gamma, x \equiv g \pmod{n}\} \cup \{1\}$. This is known as a *congruence monoid*. Further, if $|\Gamma| = 1$ it is known as an *arithmetic congruence monoid*.

For example, set $n = 12$. If we take $\Gamma = \{4\}$, then $M(\Gamma, 12) = \{1, 4, 16, 28, 40, \ldots\}$. If we take $\Gamma = \{1, 4\}$, then $M(\Gamma, 12) = \{1, 4, 13, 16, 25, 28, \ldots\}$. However we may not take $\Gamma = \{5\}$, because $5 \cdot 5 \not\equiv 5 \pmod{12}$.

(Arithmetic) congruence monoids have received considerable attention recently [4, 6, 8, 12, 14]. In [15] it was shown that a congruence monoid $M(\Gamma, n)$ satisfies the FTA if and only if $\Gamma = \{m : 1 \leq m \leq n \text{ and } \gcd(n, m) = 1\}$. Now consider the case where $\Gamma = \{m\}$, and $\gcd(m, n) > 1$. In [5] it was shown that if $\gcd(m, n)$ is not a prime power, then $\rho(M(\Gamma, n)) = \infty$. Otherwise, we have $\gcd(m, n) = p^k$ and $\rho(M(\Gamma, n)) = \frac{a+k-1}{k}$ where a is the smallest positive integer such that $p^a \in M(\Gamma, n)$.

Lemma 6. *Let $M = M(\Gamma, n)$ be a congruence monoid. Set $T_1 = \{p \in P : p|n, p^k \in M \text{ for some } k \in \mathbb{N}\}$, and $T_2 = \{p \in P : p \nmid n\}$. If there is some $g \in \Gamma$ with $\gcd(g, n) = 1$, then $\sqrt[P]{M} = T_1 \cup T_2$; otherwise $\sqrt[P]{M} = T_1$.*

Proof. Certainly $T_1 \subseteq \sqrt[P]{M}$. If $p|n$ but $p \notin T_1$, then $p \notin \sqrt[P]{M}$.

We now consider $p \in P$ with $p \nmid n$. Suppose first we have $p \in \sqrt[P]{M}$. Since $p^k \in M$ for some $k \in \mathbb{N}$, there is some $g \in \Gamma$ with $p^k \equiv g \pmod{n}$. Since $p \nmid n$, then $\gcd(p^k, n) = 1$ and also $\gcd(g, n) = 1$. Suppose now that there is some $g \in \Gamma$ with $\gcd(g, n) = 1$. Because $g, p \in \mathbb{Z}_n^\times$, by Euler's totient theorem $g^{\phi(n)} \equiv p^{\phi(n)} \equiv 1 \pmod{n}$. But $g^{\phi(n)} \in M$, so there must be some $g' \in \Gamma$ with $g' \equiv 1 \equiv p^{\phi(n)} \pmod{n}$. Hence $p^{\phi(n)} \in M$, so $p \in \sqrt[P]{M}$. $\square$

Let G be a finite abelian group and $g_1, g_2, \ldots, g_t$ elements from G. If $t \geq |G|$, then an elementary argument shows that there exists a subset $T \subseteq \{1, 2, \ldots, t\}$ such that $\prod_{i \in T} g_i = 1$. This idea is central to the following definition, upon which the proof of Proposition 8 relies.

Definition 7. *Let G be a finite abelian group under multiplication. Let $D(G)$ be the smallest positive integer m such that if $g_1, g_2, \ldots, g_m$ are elements of G, then there is some nonempty $S \subseteq \{1, 2, \ldots, m\}$ such that $1 = \prod_{s \in S} g_s$. $D(G)$ is known as the* Davenport constant *of G.*

For an introduction to the subject, or to learn more about the importance and history of $D(G)$, see [13]. By the elementary argument above, $D(G) \leq |G|$. If $G \cong \mathbb{Z}_n$ is cyclic, then $D(\mathbb{Z}_n) = n$. If G is not cyclic, then it is easy to show that $D(G) < |G|$ (in fact $D(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 3$). Its precise value is known if G is of rank 1 or 2, is a p-group, or in several other cases. However, in general, only bounds are known.

Proposition 8. *Let $M = M(\Gamma, n)$ be a congruence monoid. Then it is R-respectful and T-modest.*

Proof. We factor $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$. We then choose an r such that $e_i \leq r$ and $\phi(p_i^{e_i})|r$, for all i. We will now show that $x^{2r} \equiv x^r \pmod{n}$, for all x. If $p_i|x$, then $p_i^{e_i}|x^r$ since $e_i \leq r$. Otherwise x is coprime to p_i and by Euler's totient theorem $x^{\phi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$. Hence $x^r \equiv 1 \pmod{p_i^{e_i}}$. Hence each $p_i^{e_i}$ divides $x^r(x^r - 1)$; so too does their least common multiple, namely n. Now, for any $y \in \mathbb{N}$, the following statements are equivalent: (1) $x^r y \in M$, (2) $x^r y \equiv g \pmod{n}$ for some $g \in \Gamma$, (3) $x^{2r} y \in M$. Thus M is r-respectful.

Let T_1, T_2 be as in Lemma 6. Because $|T_1| < \infty$, we may choose $K > 0$ so that $p^K \in M$ for all $p \in T_1$. For any irreducible $x \in M$, $T_1(x) = \sum_{p \in T_1} \nu_p(x)$. We will show that for any $p \in T_1$, that $\nu_p(x) < (K+1)r$. Suppose otherwise. Because p^r respects M and $p^r \mid x/p^{Kr}$, we in fact have $x/p^{Kr} \in M$. Since $p^K \in M$, then $p^{Kr} \in M$. Hence $x = p^{Kr} \cdot (x/p^{Kr})$ is a factorization in M, which contradicts the irreducibility of x. Hence $T_1(x) \leq |T_1|(K+1)r$. If $\sqrt[P]{M} = T_1$, then M is T-modest; otherwise there is more to do.

We now assume that $\sqrt[P]{M} = T_1 \cup T_2$. By the proof of Lemma 6, there is some $g \in \Gamma$ with $g \equiv 1 \pmod{n}$. Let x be any irreducible of M. Let $\mathbb{Z}_n^\times$ denote the group of units modulo n. Set $v = D(\mathbb{Z}_n^\times)$, the Davenport constant as from Definition 7. Suppose that $T_2(x) > v$. We write $x = q_1 q_2 \cdots q_v x'$, where q_i are (not necessarily distinct) elements of T_2. Hence, there is some subsequence of $q_1 q_2 \cdots q_v$ whose product is 1 in $\mathbb{Z}_n^\times$. We then write $x = q \cdot x''$, where now $q \equiv 1 \equiv g \pmod{n}$, $x'' \neq 1$, and $x'' \equiv x \pmod{n}$. This is a factorization in M. Hence $T_2(x) \leq v$ for all irreducible $x \in M$. Thus $\sqrt[P]{M}(x) \leq |T_1|(K+1)r + v$. $\square$

Example 10 relies upon the following definitions; for an introduction to the subject see [19].

Definition 9. *Let $a_1, a_2, \ldots a_k \in \mathbb{N}$, with $\gcd(a_1, a_2, \ldots, a_k) = 1$. Set $S = \{a_1 b_1 + a_2 b_2 + \cdots + a_k b_k : b_i \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$. S is a monoid under addition known* *as a* numerical monoid*. There is some minimum $F \in \mathbb{N}_0$ such that $x \in S$ for all $x \in \mathbb{N}$ with $x > F$. F is known as the* Frobenius number *of S.*

Numerical monoids have long been the subject of considerable study, e.g. [10, 11, 16, 18]. The precise value of F is known if S has two or three generators, but not in general. The problem of determining F has been revisited many times as the knapsack problem, the coin problem, the postage stamp problem, and the Chicken McNugget problem. It is known to be NP-hard in general, which makes it at least as hard as Sudoku that was shown to be NP-complete in [21].

Example 10. Let S be a numerical monoid under addition. Then $M = \{2^s : s \in S\}$ is a (multiplicative) submonoid of $\mathbb{N}$ with $M \cong S$. Moreover, M is R-respectful and T-modest.

Proof. Let F be the Frobenius number of S, as in Definition 9. For any $x, y \in \mathbb{N}$, we consider $Q = \{x^{F+1}y, x^{2(F+1)}y, x^{3(F+1)}y, \ldots\}$. If $x = 1$, then $Q = \{y\}$ so 1^{F+1} respects M. If x or y is not a power of 2, then Q is disjoint from M. If both x, y are powers of 2, then $Q \subseteq M$, because each element has at least $F+1$ copies of 2. Hence M is $(F+1)$-respectful.

Clearly $\sqrt[P]{M} = \{2\}$. Let $x \in M$ be irreducible. We claim that $\sqrt[P]{M}(x) < 2(F+1)$. Suppose otherwise. Then we may write $x = 2^{F+1} \cdot (x/2^{F+1})$. Since $v_2(x/2^{F+1}) \geq F+1$, both factors are in M, which contradicts the irreducibility of x. Hence M is T-modest. $\square$

Example 11. Let S_1, S_2 be numerical monoids. Let $M = \{2^{s_1}3^{s_2} : s_1, s_2 \geq 1, s_1 \in S_1, s_2 \in S_2\} \cup \{1\}$. Then M is a (multiplicative) submonoid of $\mathbb{N}$ which is R-respectful and T-modest.

Proof. Let $F > 0$ be chosen strictly larger than the Frobenius numbers of both S_1 and S_2. For any $x, y \in \mathbb{N}$, we consider $Q = \{x^F y, x^{2F} y, x^{3F} y, \ldots\}$. If $x = 1$, then $Q = \{y\}$ so 1^{F+1} respects M. If either x or y has any prime factor outside of $\{2, 3\}$, then Q is disjoint from M. If x is a power of 2, then either $Q \subseteq M$ (if $\nu_3(y) \in S_2$) or Q is disjoint from M (otherwise). If x is a power of 3, then either $Q \subseteq M$ (if $\nu_2(y) \in S_1$) or Q is disjoint from M (otherwise). Lastly, if both 2,3 divide x, then $Q \subseteq M$. Hence M is F-respectful.

Clearly $\sqrt[P]{M} \subseteq \{2, 3\}$; however no power of 2 or 3 alone is in M, so $\sqrt[P]{M} = \emptyset$. Hence M is 0-modest.

$\square$

Monoids of this type may be thought of as a form of multi-dimensional numerical monoids, e.g. [1, 17, 20].

4 Theorem

We now present our main result, that characterizes and bounds finite elasticity in R-respectful, T-modest monoids. We note that this bound is typically not sharp; t is a uniform bound on all of $\sqrt[P]{M}$ while a sharper bound may be found by looking at its elements individually. A more abstract version of this result concerning C_0-monoids, attributed to F. Halter-Koch, was cited as a personal communication in the manuscript [7]. This "folklore" motivated the present paper.

Theorem 12. *Suppose that M is an R-respectful, t-modest monoid, for some $t \in \mathbb{N}$. Then the following are equivalent:*

1. *$\rho(M)$ is finite,*
2. *$\rho(M) \le t$, and*
3. *$\sqrt[P]{M}(x) \ge 1$ for all $x \in M \setminus \{1\}$.*

Proof. ($2 \to 1$) Clear.

($1 \to 3$) Suppose there is some $x \in M \setminus \{1\}$ with $\sqrt[P]{M}(x) = 0$. If x has only one prime factor, then x is a prime power and hence $\sqrt[P]{M}(x) = 1$. Hence, x has at least two distinct prime factors. Choose one such, $x = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, with $e_i \in \mathbb{N}$ and m minimal. Set $e = \max(e_1, e_2, \ldots, e_m)$. Because p_1^r respects M, and $x^r = p_1^{re_1} \cdots p_m^{re_m} \in M$, we conclude that $p_1^{r(e-e_1)} x^r = p_1^{re} p_2^{re_2} \cdots p_m^{re_m} \in M$. Repeating this with each of $p_2^r, \ldots, p_m^r$, we may conclude that $y = (p_1 p_2 \cdots p_m)^{re} \in M$. We now choose any $s \in \mathbb{N}$. Set $v = s(m-1)+m$. Consider $\rho(y^v)$. Certainly this may be factored into at least v irreducibles by first factoring into v copies of y. Now set $y_i = y(\frac{p_1 p_2 \cdots p_m}{p_i})^{res}$. The second multiplicand respects M. Because $y \in M$, we in fact have $y_i \in M$. Because $\nu_{p_i}(y_i) = re$, if y_i were to factor into more than re irreducibles, then some irreducible would not have a p_i factor. This would therefore violate the minimality of m in the choice of x. We have $y_1 y_2 \cdots y_m = y^m (p_1 \cdots p_m)^{res(m-1)} = y^{s(m-1)+m} = y^v$. Since each y_i has at most re irreducibles, then this factorization of y^v yields at most mre irreducibles. Thus $\rho(y^v) \ge \frac{v}{mre} = \frac{s(m-1)+m}{mre}$. Since m, r, e are all fixed but s was chosen freely, we may make this fraction arbitrarily large. Consequently, $\rho(M) = \infty$.

($3 \to 2$) Suppose now that $\sqrt[P]{M}(x) \ge 1$ for all $x \in M \setminus \{1\}$. Let $x \in M$. Suppose that $x = u_1 u_2 \cdots u_j = v_1 v_2 \cdots v_k$ are factorizations into irreducibles where j is maximal and k is minimal. We also have $\sqrt[P]{M}(u_i) \ge 1$ and $\sqrt[P]{M}(v_i) \le t$. Consequently, $j \le \sqrt[P]{M}(x) \le kt$. Hence $\rho(x) = \frac{j}{k} \le t$.

□

Recall the 1-respectful monoid E. We have $\sqrt[P]{E} = \{2\}$. Also, E is 1-modest. Hence Theorem 12 shows that $\rho(E) = 1$. Theorem 12 also shows that $\rho(M) < \infty$ in Example 10. On the other hand, $\rho(M) = \infty$ in similar Example 11. In Example 5, $\rho(M)$ may be finite or infinite depending only on Γ and n, as will be shown by the following.

Proposition 13. *Let $M = M(\Gamma, n)$ be a congruence monoid. Let T_1, T_2 be as in Lemma 6. Set $\Gamma_1 = \{x \in \Gamma : \gcd(x, n) > 1\}$. Then $\rho(M) < \infty$, if and only if $T_1(x) \ge 1$ for all $x \in \Gamma_1$.*

Proof. Suppose first that there is some $x \in \Gamma_1$ with $T_1(x) = 0$. If $\sqrt[p]{M} = T_1$, then already $\sqrt[p]{M}(x) = 0$. Otherwise, write $x = x_1 x_2$, where $T_2(x_1) = 0$. We must have $x_1 > 1$ since $x \in \Gamma_1$. Set $y = x_1^{\phi(n)}$. Note that $x_2^{\phi(n)} \equiv 1 \pmod{n}$. Hence, $y \equiv x_1^{\phi(n)} x_2^{\phi(n)} = x^{\phi(n)} \pmod{n}$. Also we have $x^{\phi(n)} \in M$ because $x \in M$. Therefore, $y \in M$. However $\sqrt[p]{M}(y) = 0$. Hence, in both cases, Theorem 12 implies that $\rho(M) = \infty$.

Now suppose that $T_1(x) \geq 1$ for all $x \in \Gamma_1$. Let $y \in M \setminus \{1\}$. We have $y \equiv x \pmod{n}$, for some $x \in \Gamma$. If $x \notin \Gamma_1$, then $\gcd(x, n) = 1 = \gcd(y, n)$ and hence $T_1(y) = 0$. We have $\sqrt[p]{M}(y) = T_1(y) + T_2(y) = T_2(y) \geq 1$, since y has some prime divisor. Otherwise $x \in \Gamma_1$. Since $T_1(x) \geq 1$, there is some $p \in T_1$ with $p|x$. But also $p|n$, so $p|y$. Hence $T_1(y) \geq 1$. We conclude that $\sqrt[p]{M}(y) \geq T_1(y) \geq 1$. In both cases Theorem 12 implies that $\rho(M) < \infty$.

□

Acknowledgments. The authors would like to thank Paul Baginski and Scott Chapman for suggesting this problem, and several anonymous referees for their helpful suggestions. This research was supported in part by NSF REU grant 1061366.

References

[1] J. Amos, I. Pascu, V. Ponomarenko, E. Treviño, and Y. Zhang, The multidimensional Frobenius problem, *Involve* **4** (2011) 187–197.

[2] D. F. Anderson, Elasticity of factorizations in integral domains: a survey, in *Factorization in integral domains (Iowa City, IA, 1996)*, Lecture Notes in Pure and Appl. Math., vol. 189, Dekker, New York, 1997, 1–29.

[3] P. Baginski and S. T. Chapman, Factorizations of algebraic integers, block monoids, and additive number theory, *Amer. Math. Monthly* **118** (2011) 901–920.

[4] P. Baginski, S. T. Chapman, and G. J. Schaeffer, On the delta set of a singular arithmetical congruence monoid, *J. Théor. Nombres Bordeaux* **20** (2008) 45–59.

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

[6] ———, A theorem on accepted elasticity in certain local arithmetical congruence monoids, *Abh. Math. Semin. Univ. Hambg.* **79** (2009) 79–86.

[7] M. Banister, J. Chaika, and W. Meyerson, Tech. report, Trinity University REU, 2003.

[8] S. T. Chapman and D. Steinberg, On the elasticity of generalized arithmetical congruence monoids, *Results Math.* **58** (2010) 221–231.

[9] S. T. Chapman and J. Coykendall, Half-factorial domains, a survey, in *Non-Noetherian commutative ring theory*, Math. Appl., vol. 520, Kluwer Acad. Publ., Dordrecht, 2000, 97–115.

[10] D. Cibul′skite, The distribution of generating elements in free numerical semigroups. I, II, III, *Litovsk. Mat. Sb.* **10** (1970) 397–415; ibid. 10 (1970), 593–610; ibid. 10 (1970), 835–844.

[11] R. Fröberg, C. Gottlieb, and R. Häggkvist, On numerical semigroups, *Semigroup Forum* **35** (1987) 63–83.

[12] A. Geroldinger and F. Halter-Koch, Congruence monoids, *Acta Arith.* **112** (2004) 263–296.

[13] ______, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006, Algebraic, combinatorial and analytic theory.

[14] F. Halter-Koch, C-monoids and congruence monoids in Krull domains, in *Arithmetical properties of commutative rings and monoids*, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, Boca Raton, FL, 2005, 71–98.

[15] R. D. James and I. Niven, Unique factorization in multiplicative systems, *Proc. Amer. Math. Soc.* **5** (1954) 834–838.

[16] N. Kaplan, Counting numerical semigroups by genus and some cases of a question of Wilf, *J. Pure Appl. Algebra* **216** (2012) 1016–1032.

[17] B. V. Novikov, On the structure of subsets of a vector lattice that are closed with respect to addition, *Ukrain. Geom. Sb.* (1992) 99–103, 164.

[18] V. Ponomarenko and R. Rosenbaum, Numerical semigroups from open intervals, *Involve* **3** (2010) 333–340.

[19] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, vol. 20, Springer, New York, 2009.

[20] R. J. Simpson and R. Tijdeman, Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester, *Proc. Amer. Math. Soc.* **131** (2003) 1661–1671 (electronic).

[21] T. Yato and T. Seta, Complexity and completeness of finding another solution and its application to puzzles., *IEICE Trans. Fundamentals* **E86-A** (2003) 1052–1060.

Matthew O. Jenssen completed his B.A. in Mathematics at the University of Cambridge in 2012 and is currently studying for an M.Math via Part III of the Cambridge Mathematical Tripos. His mathematical interests include Algebra, Combinatorics, Number Theory and researching the work of fellow

countrymen Niels Henrik Abel, Sophus Lie and Atle Selberg. He enjoys 20th century American literature and music, writing poetry and collecting 78rpm records for his gramophone.
Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB

Daniel Montealegre was born and raised in Colombia. At the age of seventeen he moved to the United States. He is now a student at the University of California, Los Angeles; currently working on a joint B.S/M.A. degree in mathematics. He plans to attend graduate school Fall of 2013 and hopes to work in either algebra or discrete mathematics.
Department of Mathematics, University of California at Los Angeles, 520 Portola Plaza, Los Angeles CA 90095-1555

Vadim Ponomarenko received his B.A. from the University of Michigan in 1992, and his Ph.D. from the University of Wisconsin-Madison in 1999. He currently teaches at San Diego State University and directs an REU program there. He enjoys collaborating with students, and invites anyone eligible and interested to direct their browser to *http://www.sci.sdsu.edu/math-reu/index.html*
Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego CA 92182-7720
vponomarenko@mail.sdsu.edu