COLLOQUIUM MATHEMATICUM

VOL. 108 2007 NO. 1

ON THE ARITHMETIC OF ARITHMETICAL CONGRUENCE MONOIDS

BY

M. BANISTER (Claremont, CA and Santa Barbara, CA),
J. CHAIKA (Iowa City, IA and Houston, TX), S. T. CHAPMAN (San Antonio, TX)
and W. MEYERSON (Cambridge, MA and Los Angeles, CA)

Abstract. Let $\mathbb{N}$ represent the positive integers and $\mathbb{N}_0$ the non-negative integers. If $b \in \mathbb{N}$ and Γ is a multiplicatively closed subset of $\mathbb{Z}_b = \mathbb{Z}/b\mathbb{Z}$, then the set $H_\Gamma = \{x \in \mathbb{N} \mid x + b\mathbb{Z} \in \Gamma\} \cup \{1\}$ is a multiplicative submonoid of $\mathbb{N}$ known as a *congruence monoid*. An *arithmetical congruence monoid* (or *ACM*) is a congruence monoid where $\Gamma = \{\overline{a}\}$ consists of a single element. If H_Γ is an ACM, then we represent it with the notation $M(a, b) = (a + b\mathbb{N}_0) \cup \{1\}$, where $a, b \in \mathbb{N}$ and $a^2 \equiv a \pmod b$. A classical 1954 result of James and Niven implies that the only ACM which admits unique factorization of elements into products of irreducibles is $M(1, 2) = M(3, 2)$. In this paper, we examine further factorization properties of ACMs. We find necessary and sufficient conditions for an ACM $M(a, b)$ to be half-factorial (i.e., lengths of irreducible factorizations of an element remain constant) and further determine conditions for $M(a, b)$ to have finite elasticity. When the elasticity of $M(a, b)$ is finite, we produce a formula to compute it. Among our remaining results, we show that the elasticity of an ACM $M(a, b)$ may not be accepted and show that if an ACM $M(a, b)$ has infinite elasticity, then it is not fully elastic.

1. Introduction and definitions. The notion of unique factorization plays a central role in the basic study of number theory and algebra. While the ring $\mathbb{Z}[\sqrt{-5}]$ is a traditional example of a non-unique factorization domain, simpler examples of non-unique factorization can be constructed using multiplicative monoids. For instance, the celebrated *Hilbert monoid*

2000 *Mathematics Subject Classification*: 20M14, 20D60, 13F05.

Key words and phrases: non-unique factorizations, arithmetical congruence monoid, half-factorial, elasticity of factorization.

The first, second and fourth authors received support for this work under NSF grant DMS-0097366 while participating in the 2003 Trinity University Mathematics REU Program. Prior to their work at Trinity, they spent a 10 day period at the Institute für Mathematik at Karl-Franzens-Universität in Graz, Austria, with NSF support under grant DMS-0303687. The authors wish to thank Professors Franz Halter-Koch and Alfred Geroldinger for their careful presentation of the background material necessary for the completion of this work.

Part of this work was completed while the third author was on an Academic Leave granted by the Trinity University Faculty Development Committee.

(see [7], [17] and [20])

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

fails to have the unique factorization property since $441 = 21 \cdot 21 = 9 \cdot 49$ and 9, 21 and 49 are all irreducible in $1 + 4\mathbb{N}_0$. Notice that an element x is irreducible in $1+4\mathbb{N}_0$ if and only if x is prime in $\mathbb{N}$ or $x = p_1 p_2$ where p_1 and p_2 are primes in $\mathbb{N}$ which are congruent to 3 modulo 4. Using this fact, it is easy to argue that $1+4\mathbb{N}_0$, while not a factorial monoid, does satisfy the following condition: if $x \in 1+4\mathbb{N}_0$ can be written as $x = p_1 \cdots p_t = q_1 \cdots q_k$ with each p_i and q_j irreducible in $1 + 4\mathbb{N}_0$, then $k = t$. In general, an atomic monoid (i.e., one in which each non-unit possesses a factorization into irreducibles) which satisfies the prior factorization property is called *half-factorial*.

Various properties relating to non-unique factorizations in integral domains and monoids have recently been studied in the literature (see [14] for a detailed study of these properties). The $1 + 4\mathbb{N}_0$ example sparked our interest in studying these properties in "Hilbert-like" monoids, and the remainder of this paper is devoted to this investigation. We use $\mathbb{N}$ to represent the positive integers and $\mathbb{N}_0$ the non-negative integers. Let $b \in \mathbb{N}$ and Γ be a multiplicatively closed subset of $\mathbb{Z}_b = \mathbb{Z}/b\mathbb{Z}$. The set

$$H_\Gamma = \{x \in \mathbb{N} \mid x + b\mathbb{Z} \in \Gamma\} \cup \{1\}$$

is a multiplicative submonoid of $\mathbb{N}$ known as a *congruence monoid*. A general discussion of this construction (which can be generalized to any integral domain R) can be found in both [12] and [14]. The papers [17] and [20] contain proofs that a congruence monoid $H_\Gamma \subseteq \mathbb{N}$ is factorial if and only if there exists an $b \in \mathbb{N}$ with

$$H_\Gamma = \{m \in \mathbb{N} \mid \gcd(m, b) = 1\}.$$

An *arithmetical congruence monoid* (or *ACM*) is a congruence monoid where $\Gamma = \{\overline{a}\}$ consists of a single element (hence, the non-units of H_Γ form an arithmetic sequence). If H_Γ is an ACM, then we represent it with the notation $M(a, b)$ where $a, b \in \mathbb{N}$, and $a^2 \equiv a \pmod{b}$. Note that here we are actually setting

$$M(a, b) = (a + b\mathbb{N}_0) \cup \{1\} = \{a + kb \mid k \in \mathbb{N}_0\} \cup \{1\}.$$

Before describing the contents of this article in greater detail, we will review some basic notions and definitions from the theory of non-unique factorizations [14]. Let M be a commutative cancellative monoid and suppose that $M^\bullet$ represents the set of non-units of M. The *irreducibles* (or *atoms*) of M are denoted by $\mathcal{A}(M)$. Hence, when considering ACMs, we have

$$\mathcal{A}(M(a, b)) = \{x \in M(a, b) \mid x = rs \text{ with } r, s \in M(a, b) \text{ implies } r = 1 \text{ or } s = 1\}.$$

If every element of $M^\bullet$ can be written as a product of elements from $\mathcal{A}(M)$, then M is called *atomic*. Given an element $x \in M^\bullet$, suppose that

$$(*) \qquad x = p_1 \cdots p_t = q_1 \cdots q_k$$

where each p_i and q_j is in $\mathcal{A}(M)$. The monoid M is *factorial* if for every $x \in M^\bullet$ and factorization of the form $(*)$, we have $t = k$ and there exists a permutation σ of $\{1, \ldots, t\}$ such that p_i and $q_{\sigma(i)}$ are associates for all i. The monoid M is *half-factorial* (or an *HFM*) if for every $x \in M^\bullet$ and factorization of the form $(*)$, we have $t = k$ (we note that the current authors have recently shown in [7] that for a fixed $b > 2$, if $H_\Gamma = \{m \in \mathbb{N} \mid \gcd(m, b) \neq 1\} \cup \{1\}$, then H_Γ is not factorial but half-factorial).

If $x \in M^\bullet$, then *the set of lengths of* x is

$$\mathcal{L}(x) = \{k \in \mathbb{N} \mid x = a_1 \cdots a_k \text{ where } a_i \in \mathcal{A}(M)\}.$$

If $\mathcal{L}(x) = \{n_1, \ldots, n_t\}$ with the n_i's listed in increasing order, then set $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq t\}$ and

$$\Delta(M) = \bigcup_{x \in M^\bullet} \Delta(x).$$

If $\Delta(M) \neq \emptyset$, then, by [11, Lemma 3], $\min \Delta(M) = \gcd \Delta(M)$. The *elasticity* of an element $x \in M^\bullet$, denoted $\varrho(x)$, is given by the ratio of $\sup(\mathcal{L}(x))$ to $\inf(\mathcal{L}(x))$. The *elasticity of* M is then defined as

$$\varrho(M) = \sup\{\varrho(x) \mid x \in M^\bullet\}.$$

A survey of known results concerning elasticity in integral domains and monoids can be found in [3] and [14]. We say that M has *accepted elasticity* if there exists $x \in M^\bullet$ such that $\varrho(x) = \varrho(M)$. Any finitely generated commutative cancellative monoid has accepted elasticity (see [2, Theorem 7]). In turn, so also do block monoids over finite abelian groups and hence Krull domains with finite divisor class groups. We say that M is *fully elastic* if for all $q \in \mathbb{Q} \cap [1, \varrho(M)]$ (or $[1, \infty)$ if the elasticity is infinite) there exists an $x \in M^\bullet$ such that $\varrho(x) = q$. The notion of full elasticity was introduced in [9], where it is shown that block monoids over certain finite abelian groups are fully elastic, but non-cyclic numerical monoids are not. Moreover, recent work in [6] and [10] shows that rings of algebraic integers, as well as certain rings of integer-valued polynomials, are also fully elastic.

Among our results, we find necessary and sufficient conditions for an ACM to have finite elasticity. When the elasticity of $M(a, b)$ is finite, we then determine a formula for $\varrho(M(a, b))$. The elasticity formula leads to necessary and sufficient conditions for an ACM to be half-factorial. While factorial ACMs are quite scarce, we are able to produce an infinite family of half-factorial ACMs. If $M(a, b)$ is not half-factorial, we show that

$\min \Delta(M(a,b)) = 1$. We examine full and accepted elasticity in ACMs, and obtain the somewhat surprising result that an ACM may not have accepted elasticity. We show that if $M(a,b)$ does not have finite elasticity, then $M(a,b)$ is not fully elastic, but the ACM $M(p^k, p^k b)$ where $\gcd(p,b) = 1$ and $k = \mathrm{ord}_b(p)$ is fully elastic.

2. Finite elasticity, half-factoriality and $\min \Delta(M(a,n))$**.** We will open with some basic results concerning the structure of ACMs.

LEMMA 2.1. *Suppose that $M(a,b)$ is an ACM with $a \neq b$. Then*

(1) *either $a = b+1$ or $a < b$, and*
(2) *if $\gcd(a,b) = 1$, then $a = 1$ or $a = b+1$.*

Proof. For (1), if $b+1 < a$ then $a-b \notin M(a,b)$ but $a - b \equiv a \pmod{b}$. For (2), assume that $a \neq b+1$. Since $M(a,b)$ is an ACM, $a^2 \equiv a \pmod{b}$. Thus $b \mid a(a-1)$. If $\gcd(a,b) = 1$, then $b \mid a-1$ and $b < a$, contradicting (1). ∎

Since $M(1,b) = M(b+1,b)$ for all $b \geq 2$, in the remainder of our work we will assume that all ACMs are written in the form $M(a,b)$ with $1 \leq a \leq b$. We recall briefly a key definition. A commutative cancelative monoid S is a *Krull monoid* if there exists a free Abelian monoid D and a homomorphism $\partial : S \to D$ such that

(1) $x \mid y$ in S if and only if $\partial(x) \mid \partial(y)$ in D, and
(2) every $\beta \in D$ is the greatest common divisor of some set of elements in $\partial(S)$.

The basis elements of D are called the *prime divisors* of S and the quotient $D/\partial(S)$ is called the *divisor class group of S*, denoted by $\mathcal{C}(S)$. More information on Krull monoids can be found in [8] and [14].

PROPOSITION 2.2. *Suppose that $M(a,b)$ is an ACM.*

(1) *$M(a,b)$ is a Krull monoid if and only if $a = 1$.*
(2) *If $M(a,b)$ is a Krull monoid, then every divisor class of $\mathcal{C}(M(a,b)) = (\mathbb{Z}_b)^\times$ contains a prime divisor.*
(3) *If $a = 1$, then $\varrho(M(1,b)) = D(\mathbb{Z}_b^\times)/2$.*
(4) *If $a = 1$, then $M(1,b)$ is half-factorial if and only if $b = 1, 2, 3, 4,$ or 6.*
(5) *If $a = 1$, and $M(1,b)$ is not half-factorial, then* $\min \Delta(M(1,b)) = 1$.

Proof. Assertion (1) follows directly from [17, Theorem 1], and (2) from [16, Beispiel 2].

For (3), by (1) and (2), $M(1,b)$ is a Krull monoid with divisor class group $(\mathbb{Z}_b)^\times$ with a prime in each divisor class. The result now follows from [4, Proposition 3].

For (4), since $M(1,b)$ is again a Krull and each divisor class of $\mathcal{C}(M(1,b))$ contains a prime divisor, we see that $M(1,b)$ is half-factorial if and only if $|\mathcal{C}(M(1,b))| \leq 2$ [18, Theorem 2(ii)]. This clearly requires that $b = 1,2,3,4$ or 6.

Assertion (5) follows directly from [8, Lemma 3.2 and Proposition 5.3]. ∎

A general criterion for the finite elasticity of a congruence monoid can be found in [13, Theorem 7.8]. We give in Theorem 2.3 a simple condition which not only forces $\varrho(M(a,b))$ to be infinite, but also has implications with respect to full elasticity.

THEOREM 2.3. *Let $M(a,b)$ be an ACM such that* $\gcd(a,b)$ *is not a prime power. Then there exists some $B \in \mathbb{N}$ such that every $z \in M(a,b)$ has a factorization of length at most B. Consequently*, $\varrho(M(a,b)) = \infty$ *and $M(a,b)$ is not fully elastic.*

Proof. Let $q = \gcd(a,b)$, $a = qa_1$, $b = qb_1$, where $a_1, b_1 \in \mathbb{N}$ and $\gcd(a_1,b_1) = 1$. Then $a = qa_1 \equiv 1 \pmod{b_1}$ and $M(a,b) = \{x \in q\mathbb{N} \mid x \equiv 1 \pmod{b_1}\} \cup \{1\}$.

Now let $q = p_1^{n_1} \cdots p_k^{n_k}$ with distinct primes $p_1, \ldots, p_k$, $k \geq 2$, $n_1, \ldots, n_k \geq 1$, and let $t \in \mathbb{N}$ be such that $p_i^{n_i t} \equiv 1 \pmod{b_1}$ for all i (e.g., $t = \varphi(b_1)$). We assert that $B = 4t - 1$ meets our requirements.

Indeed, let $z \in M(a,b)$, $z = p_1^{m_1} \cdots p_k^{m_k} y$, where $m_i \geq n_i$, $y \in \mathbb{N}$, $\gcd(q,y) = 1$ and $z \equiv 1 \pmod{b_1}$. If $m_i < 2n_i t$ for at least one i, then z has a factorization of length less than $2t$. Thus assume that $m_i \geq 2n_i t$ for all i, and set $m_i = n_i t l + m_i'$ with $l \in \mathbb{N}$ and $n_i t \leq m_i' < 2n_i t$. Then $z = z_1 z_2 z_3$, where $z_1 = p_1^{n_1} p_2^{n_2 t(l-1)} \cdots p_k^{n_k t(l-1)}$, $z_2 = p_1^{n_1 t(l-1)} p_2^{n_2 t} \cdots p_k^{n_k t}$ and $z_3 = p_1^{m_1'} \cdots p_k^{m_k'} y$. Clearly, $z_1, z_2, z_3 \in M(a,b)$, z_1 and z_2 have factorizations of length at most t, and z_3 has a factorization of length less than $2t$. Thus z has a factorization of length at most $4t-1$. The final two assertions of the theorem now follow directly. ∎

In Theorem 2.4, we give a formula for $\varrho(M(a,b))$ when its elasticity is finite. Using this, we not only recover the general finiteness condition when applied to an ACM, but also characterize which ACMs are HFMs. Our work will require an important tool in studying elasticity. Let M be an atomic monoid. A function $f : M \to \mathbb{R}_0$ is a *semi-length function* on M if

(1) $f(xy) = f(x) + f(y)$ for all x, y in M, and
(2) $f(x) = 0$ if and only if x is a unit of M.

Given an atomic monoid M which is not factorial with semi-length function f, Anderson and Anderson [1] have shown that

$$(\dagger)\qquad \varrho(M) \le \frac{\sup\{f(x) \mid x \in \mathcal{A}(M) \text{ and } x \text{ not prime}\}}{\inf\{f(x) \mid x \in \mathcal{A}(M) \text{ and } x \text{ not prime}\}}.$$

THEOREM 2.4. *Let $M(a,b)$ be an ACM.*

(1) *If* $\gcd(a,b) = p^k$ *for p a prime and k a natural number then*
$$\varrho(M(a,b)) = \frac{n+k-1}{k}$$
where n is the smallest positive integer such that $p^n \in M(a,b)$.

(2) *The elasticity of $M(a,b)$ is finite if and only if*
   (i) $a = 1$ *in which case* $\varrho(M(a,b)) = D(\mathbb{Z}_n^{\times})/2$, *or*
   (ii) $\gcd(a,b) = p^k$ *for p a prime and k a natural number.*

(3) *The $M(a,b)$ is half-factorial if and only if*
   (i) $a = 1$ *and* $b = 1, 2, 3, 4$ *or* 6, *or*
   (ii) *a divides b and $a = p$ where p is a prime.*

(4) *Suppose* $\gcd(a,b) = p^k$ *for p a prime. Then $\varrho(M(a,b)) < 2$ if and only if $a = p^k$. Moreover, the following conditions are equivalent:*
   (i) $\varrho(M(a,b)) = 1$.
   (ii) $a = p$.
   (iii) $\varrho(M(a,b)) < 3/2$.

Proof. (1) Suppose the ACM $M(a,b)$ has $\gcd(a,b) = p^k$ for p a prime and k a natural number. Therefore, it can be written in the form $p^k(c+d\mathbb{N}_0)\cup\{1\}$ where c and d are natural numbers such that $d > c > 1$, $\gcd(c,d) = 1$ and $\gcd(p,d) = 1$. If $\overline{x}$ represents the equivalence class of an integer in $\mathbb{Z}_d$, then notice that $\overline{p}$, $\overline{c}$, and $\overline{p^k}$ are all elements of $(\mathbb{Z}_d)^{\times}$. Further, as $a \equiv a^2 \pmod{b}$, $a \equiv a^2 \pmod{d}$, which implies that $1 \equiv a \pmod{d}$. It follows that if w is an integer, then $w \in M(a,b)$ if and only if w has p-adic value at least k and $w \equiv 1 \pmod{d}$.

CLAIM. *There exists $m \in \mathbb{N}$ such that $p^m \in M(a,b)$.*

Proof. Let x be the order of $\overline{p^k}$ in $(\mathbb{Z}_d)^{\times}$. It follows that $p^{kx} = (p^k)^x \equiv 1 \pmod{d}$ and therefore is also an element of $M(a,b)$.

Now let n be the smallest integer in $\mathbb{N}$ such that $p^n \in M(a,b)$ (note that $n \ge k$). Suppose m is an element of $M(a,b)$ which has p-adic value at least $n+k$ (i.e. $m = p^{n+k}z$ for some integer z). However, $m = (p^n)(p^k z)$, which is the product of two elements which have p-adic value at least k and are congruent to 1 modulo d; therefore, m is not an atom. All atoms must therefore have p-adic value at most $n+k-1$ and at least k (as all elements of $M(a,b)$ are divisible by p^k and therefore have p-adic value at least k). Thus the map $f : M(a,b) \to \mathbb{R}_0$ which sends an element to its p-adic value is a semi-length function with both $\sup\{f(x) \mid x \in \mathcal{A}(M(a,b))\} < \infty$ and $\inf\{f(x) \mid x \in \mathcal{A}(M(a,b))\} > 0$. It follows from (†) that $\varrho(M(a,b)) \leq (k+n-1)/k$.

Now observe that by Dirichlet's theorem there exists a prime q in $\overline{p^{1-k}}$ and a prime r in $\overline{p^{-k}}$. It follows that $p^{n+k-1}q$ is an atom in $M(a,b)$, as is any element of $M(a,b)$ with p-adic value $n+k-1$. In particular, $p^k q^n r$ is an atom. Now let $t_c = (p^k q^n r)^{c(k+n-1)+1}$. Observe that as t_c can be written as the product of $c(k+n-1)+1$ atoms with p-adic value k, it has p-adic value $ck^2+cnk-ck+k$ and can be written as the product of at most $c(k+n-1)+1$ atoms. In addition, as the product of ck or fewer atoms must have p-adic value at most

$$ck(k+n-1) = ck^2 + cnk - ck < ck^2 + cnk - ck + k,$$

t_c cannot be expressed as the product of ck or fewer atoms. However,

$$t_c = (p^{k+n-1}q)^{ck}(p^k q^{nck+cn^2-nc+n-ck} r^{c(k+n-1)+1})$$

and therefore can be written as the product of $ck+1$ atoms. This implies that $\varrho(t_c) = (c(k+n-1)+1)/(ck+1)$, which approaches $(k+n-1)/k$ as c approaches infinity. This implies that the elasticity of $M(a,b)$ is equal to $(k+n-1)/k$.

Assertion (2) follows directly from Lemma 2.1 and Theorem 2.3 and part (1) above.

(3) If the ACM is Krull, then we have $a = 1$ and (i) follows from Proposition 2.2(4). If the ACM is not Krull, then from Theorem 2.3 we have $\gcd(a,b) = p^k$, with p a prime. Again, from part (1) the elasticity is $\varrho(M(a,b)) = (n+k-1)/k$ and $\varrho(M(a,b)) = 1 + (n-1)/k = 1$. Thus, we need $n = 1$, meaning that $p \in M(a,b)$ and thus $a = p$, completing the proof.

(4) We prove the first assertion. ($\Rightarrow$) If $(n+k-1)/k < 2$, then $n < k+1$ and hence $n = k$. By the definition of n, $a = p^n = p^k$. ($\Leftarrow$) If $a = p^k$, then $n = k$ and $\varrho(M(a,b)) = (2k-1)/k < 2$.

For the second assertion, (i) and (ii) are equivalent by part (3). Clearly (i)$\Rightarrow$(iii). Given (iii), the first part of the theorem implies that $a = p^k$ for some k. If $k \geq 2$ then the formula in part (1) clearly implies that $\varrho(M(a,b)) \geq 3/2$. Hence, $k = 1$ and (ii) holds. ∎

Example 2.5. (1) Suppose $M(p^k, p^k b_1)$ is an ACM for some prime p and b_1 with $\gcd(p, b_1) = 1$. We necessarily have $b_1 \mid p^k - 1$ and since $n = k$, Theorem 2.4(1) implies that $\varrho(M(p^k, p^k b_1)) = (2k-1)/k < 2$. Notice that if $p \equiv 1 \pmod{b_1}$, then $p^r \in M(p^k, p^k b_1)$ for all $r \geq k$. Setting $x = (p^k)^{2k-1}$, we find that $x = (p^k)^{2k-1} = (p^{2k-1})^k$ are irreducible factorizations of x of length $2k-1$ and k. Hence, if $p \equiv 1 \pmod{b_1}$, then the elasticity of $M(p^k, p^k b_1)$ is accepted.

(2) Consider $M(4,6)$. Since $4^2 \equiv 4 \pmod 6$, $M(4,6)$ is an ACM. Again applying Theorem 2.4, we have $n=2$ and $k=1$, and hence $\varrho(4+6\mathbb{N}_0)=2$. In general, notice that if $\gcd(a,b)=p^k$ and $M(a,b)$ is an ACM where p^k does not exactly divide a, then $\varrho(M(a,b))\geq 2$.

(3) Let p be an odd prime. Then $p^2 \equiv p \pmod{2p}$ and hence $M(p,2p)$ is an ACM. Since $p+2p\mathbb{N}_0$ is not Krull, it is not factorial, but by Theorem 2.4 it is half-factorial.

Example 2.6. We revisit Example 2.5(2) and show that the ACM $M(4,6)$ with elasticity 2 does not have accepted elasticity. We believe that this is the simplest example known of an atomic monoid with rational elasticity such that the elasticity is not accepted (other examples can be found in [5, Example 3.4] and [15, Proposition 3.8]). Moreover, this example indicates that the sequencing argument used in the proof of Theorem 2.4(1) is unavoidable.

We observe that the atoms of the monoid $M(4,6)$ fall into two types: (A) atoms of the form $2r$ where r is an odd number congruent to $2 \pmod 3$ (to be called "A-type"), and (B) atoms of the form $4s$ where s is a product of odd primes all of which are congruent to $1 \pmod 3$ (to be called "B-type"; if s had a factor $r_1 \equiv 2 \pmod 3$, it would be expressible as r_1r_2 with $r_2 \equiv 2 \pmod 3$ as well; then $4s = (2r_1 2r_2)$).

Now we suppose that there exists an element m in $M(4,6)$ with elasticity two. Letting j be the minimum number of atoms in a decomposition of m and letting k be the maximum number of atoms, it follows that the 2-adic value of m is at least k and at most $2j$; as $k/j=2$ it follows that $k=2j$, which is therefore the 2-adic value of m.

Therefore, the decomposition of m into j atoms requires m to be written as a product of j atoms of type B (the only possible way for the product of j atoms to have 2-adic value $2j$) so m cannot have any odd factors congruent to $2 \pmod 3$. However, the decomposition of m into k atoms requires m to be written as a product of k atoms of type A (the only possible way for the product of k atoms to have 2-adic value k) so m must be a multiple of an atom of type A, and therefore must be a multiple of an odd number congruent to $2 \pmod 3$, producing a contradiction. Therefore, no element of elasticity two can exist in $M(4,6)$.

We close this section by computing $\min \Delta(M(a,b))$ when $M(a,b)$ is not half-factorial.

Theorem 2.7. *Suppose the ACM $M(a,b)$ is not half-factorial. Then*
$$\min \Delta(M(a,b)) = 1.$$

Proof. If $\gcd(a,b)=1$, then the result follows from Lemma 2.1 and Proposition 2.2(5). If $a=b$, then we consider two cases.

(i) Suppose $a = p^k$ for p a prime. If $k \geq 2$, then p^k and p^{k+1} are both atoms and $(p^k)^{k+1} = (p^{k+1})^k$ implies that a product of k irreducibles can be factored as a product of $k+1$. Hence, $\min \Delta(M(a,b)) = 1$. This leaves the option that $a = p$, which by Theorem 2.4(3) implies that $M(a,b)$ is half-factorial.

(ii) Suppose a is not a power of a prime. Then $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where $k \geq 2$ and each p_i is a distinct prime. We see that both $y_1 = (p_1^{\alpha_1})^2(p_2^{\alpha_2}) \cdots (p_k^{\alpha_k})$ and $y_2 = (p_1^{\alpha_1})(p_2^{\alpha_2})^2 \cdots (p_k^{\alpha_k})^2$ are irreducible in $M(a,b)$. Thus $y_1 y_2 = (p_1^{3\alpha_1}) \cdots (p_k^{3\alpha_k}) = a^3$, and a product of two irreducibles can be factored as a product of three, completing the argument for the case $a = b$.

To complete the argument, we consider the cases where $\gcd(a,b) \neq 1$ and $a \neq b$. First assume $\gcd(b,a) = m \neq 1$ or a and that $a \nmid b$. Let $a = mj$ and $b = mc$. First observe that given a prime p where $p^e \parallel b$ we have $a \equiv 0$ or $1 \pmod{p^e}$ (else $a \not\equiv a^2 \pmod{p^e}$, which yields $a^2 \not\equiv a \pmod{b}$, a contradiction). We have $\gcd(c,m)$=1 because otherwise we deduce in a similar manner that $a \not\equiv a^2$. Moreover, since $\gcd(b,a) = m$ it follows that $\gcd(j,c) = 1$. Hence, $a \equiv 0 \pmod{m}$ and $a \equiv 1 \pmod{c}$. We will need the following three important facts:

(1) By Lemma 2.1(1), $j < c$ (since $mj < mc$). If $j \equiv 1 \pmod{c}$, then $j = 1$, a contradiction. Hence $j \not\equiv 1 \pmod{c}$.
(2) We also have $m \not\equiv 1 \pmod{c}$, since otherwise $a \equiv mj \equiv j \not\equiv 1 \pmod{c}$, another contradiction.
(3) Thus $\mathrm{ord}_c(m) > 1$ and $\mathrm{ord}_c(j) > 1$.

Again we consider two cases.

(a) m is prime. By Dirichlet's theorem, pick a prime number u with $u \equiv m^{-1} \pmod{c}$. We have $um \in M(a,b)$ because $um \equiv 1 \pmod{c}$ and $um \equiv 0 \pmod{m}$. Set $g = \mathrm{ord}_c(u) = \mathrm{ord}_c(m) > 1$. Note that um is an atom because u is prime and $m^2 \nmid um$. For the same reason, $u^{g+1}m$ is also an atom. Since m^g is also an atom, we have $(mu)^{g+1} = (m^g)(u^{g+1}m)$. The left side contains $g+1$ atoms and the right side contains 2 atoms. Since the difference of these two lengths is $g-1$, if $g = 2$, then $\min \Delta(M(a,b)) = 1$. We assume for the remainder of the proof that $g > 2$. Again using Dirichlet's theorem, there exists a prime $q \equiv u^2 \pmod{c}$. Observe that qm^2 is an atom because $qm^2 \equiv (um)^2 \pmod{b}$. Also $qu^{g-1}m \equiv um \pmod{c}$ is an atom because an element of $M(a,b)$ needs to be divisible by m. Thus $(pu^{g-1}m)(m^g) = (pm^2)(um)^{g-1}$. The left side has length 2 and the right side has length g. The difference between these factorizations is $g-2$ so the modulus of factorization must divide $g-2$. But $g-2$ is relatively prime to $g-1$. Therefore $\min \Delta(M(a,b)) = 1$.

(b) m is composite. Write $m = p_1 \cdots p_t$ and $j = q_1 \cdots q_w$ for not necessarily distinct primes p_i and q_j. By Dirichlet's theorem, pick distinct new primes $r_1, \dots, r_t, s_1, \dots, s_w$ with $r_i \equiv p_i \pmod{c}$ and $s_j \equiv q_j \pmod{c}$. Let

$$
\begin{aligned}
x_1 &= ap_1 r_2 \cdots r_t s_1 \cdots s_w, \\
x_2 &= ar_1 p_2 \cdots r_t s_1 \cdots s_w, \\
&\ \vdots \\
x_t &= ar_1 r_2 \cdots r_{t-1} p_t s_1 \cdots s_w, \\
y_1 &= ar_1 r_2 \cdots r_t q_1 s_2 \cdots s_w, \qquad (\ddagger)\\
y_2 &= ar_1 r_2 \cdots r_t s_1 q_2 \cdots s_w, \\
&\ \vdots \\
y_w &= ar_1 r_2 \cdots r_t s_1 s_2 \cdots s_{w-1} q_w, \\
z &= ar_1 r_2 \cdots r_t s_1 s_2 \cdots s_w.
\end{aligned}
$$

Clearly each x_i, y_j and z is congruent to $amj = a^2$ modulo $mc = b$, and hence in $M(a,b)$. Moreover, by construction, each x_i, y_j and z is exactly divisible by m, and hence an atom of $M(a,b)$. Finally,

$$\prod_{i=1}^{t} x_i \cdot \prod_{j=1}^{w} y_j = z^{t+w-1} \cdot a \cdot a$$

and $t+w$ irreducibles factor as $t+w+1$. Thus $\min \Delta(M(a,b)) = 1$.

Our remaining cases yield $a|b$ and $a \neq b$, so suppose that $\gcd(a,b) = a$. If a is prime, then $M(a,b)$ is half-factorial by Theorem 2.4(3). If a is not prime, we are in case (b) above with $w = 0$, completing the argument. ∎

3. ACMs and full elasticity. Using the next two results, we will determine exactly which ACMs of the form $M(p^k, p^k b_1)$ are fully elastic.

LEMMA 3.1. *Let p be a prime number and $b_1 > 1$ a positive integer with $\gcd(p, b_1) = 1$. If $k = \mathrm{ord}_{b_1}(p)$, then $M(p^k, p^k b_1)$ is fully elastic.*

Proof. The elasticity of $M(p^k, p^k b_1)$ is $(2k-1)/k$ by Theorem 2.4(1). By Dirichlet's theorem, choose a prime $q \neq p$ such that $qp \equiv 1 \pmod{b_1}$. For each pair of positive integers e and f let

$$c(e,f) = (p^k)^e (p^{2k-1} q)^{kf}.$$

As $c(e,f)$ has p-adic value $k(e+f(2k-1))$, it can be written as the product of at most $e+f(2k-1)$ atoms because each non-unit element of the monoid—in particular, the atoms—has p-adic value at least k. This can be done by writing $c(e,f) = (p^k)^{e+f(2k-1)-1}(p^k q^{kf})$ (the last term is an atom because it has p-adic value k and $q^{kf} \equiv 1 \pmod{b_1}$). Further, any factorization of $c(e,f)$ must contain at least $e+fk$ atoms. To see this, note that p^k is the only atom which is a power of p, and a factorization of $c(e,f)$ into atoms can contain at most kf atoms with larger p-adic value; if they all have p-adic value $2k-1$ (which is the largest p-adic value) the remaining part has p-adic value ke

and therefore must be written as $(p^k)^e$. Since $c(e,f) = (p^k)^e(p^{2k-1}q)^{kf}$ is a factorization into $e + kf$ atoms, it follows that

$$\varrho(c(e,f)) = (e + f(2k-1))/(e + kf).$$

Now suppose a/b is a rational number with $1 < a/b < \varrho(M) = (2k-1)/k$. Rewriting a/b as $a(k-1)/b(k-1)$, it follows that if $f = a - b$ and $e = b(2k-1) - ak$ (which are both positive integers as $1 < a/b < (2k-1)/k$), then

$$a/b = (e + f(2k-1))/(e + kf) = \varrho(c(e,f)).$$

Hence, $M(p^k, p^k b_1)$ is fully elastic. ∎

LEMMA 3.2. *Let p be a prime number and $b_1 > 1$ a positive integer with $\gcd(p, b_1) = 1$. If $k = t \cdot \mathrm{ord}_{b_1}(p)$ for $t > 1$, then $M(p^k, p^k b_1)$ is not fully elastic.*

Proof. Let $s = k + \mathrm{ord}_{b_1}(p)$. Since $p^{\mathrm{ord}_{b_1}(p)} \in 1 + b_1\mathbb{N}_0$ and $\mathrm{ord}_{b_1}(p) < k$, both p^k and p^s are atoms of $M(p^k, p^k b_1)$. The elasticity of M is clearly at least equal to s/k (as exemplified by the element p^{sk}). We show that $M(p^k, p^k b_1)$ has no element with elasticity $(ks^2 + 1)/(ks^2)$.

Assume the contrary. Let A be an element in $M(p^k, p^k b_1)$ with $\varrho(A) = (ks^2 + 1)/ks^2$. As A can be written as the product of at least $ks + 1$ atoms (in fact, at least $ks^2 + 1$ atoms) and all such atoms have p-adic value at least k, it has p-adic value at least $k^2 s + k$; call its p-adic value $v_p(A)$. Let n be the largest multiple of k less than or equal to $v_p(A) - k$; therefore, we can write A in the form $(p^k)^{n/k} B$ for some positive integer B (which is in the monoid as it is congruent to 1 modulo b_1 and has p-adic value at least k). This means that we can write A as the product of at least $n/k + 1$ atoms (i.e., of at least $v_p(A)/k - 1$ atoms).

However, we can now let m be the largest multiple of s less than or equal to $v_p(A) - k$; therefore, we can write A in the form $(p^s)^{m/s} C$ for some positive integer C (which is in the monoid as it is congruent to 1 modulo b_1 and has p-adic value at least k). As C has p-adic value at most $k + s$ (which is less than $3k$ because s is at most $2k - 1$), it can be factored into three or fewer atoms; this means that A can also be written as the product of a number of atoms which has at most $m/s + 3$ atomic factors (i.e. less than $v_p(A)/s + 3$ such factors).

We note that our hypotheses imply that $k \geq 2$, $s \geq 3$ (as $s > k$) and $k - s \leq -1$. Therefore, the elasticity of the element A, because we can express A both as a product of at least $v_p(A)/k - 1$ atoms and as a product of at most $v_p(A)/s + 3$ atoms, is at least

$$(v_p(A)/k - 1)/(v_p(A)/s + 3) = (s/k)(v_p(A) - k)/(v_p(A) + 3s).$$

Because $v_p(A) \geq k^2s + k$, and the function on $[k^2s + k, \infty)$ sending t to $(t - k)/(t + 3s)$ is increasing, we obtain the inequality

$$(1)\qquad \begin{aligned}(s/k)(v_p(A) - k)/(v_p(A) + 3s) &\geq (s/k)(k^2s + k - k)/(k^2s + k + 3s)\\ &= (s/k)(k^2s)/(k^2s + k + 3s) = ks^2/(k^2s + k + 3s).\end{aligned}$$

For the values of k and s under consideration, we will show that

$$(2)\qquad k^2s + k + 3s \leq ks^2 - 1$$

except when $(k, s) = (2, 3)$ or $(k, s) = (3, 4)$. Then (2) combined with (1) yields

$$ks^2/(k^2s + k + 3s) \geq ks^2/(ks^2 - 1) > (ks^2 + 1)/ks^2,$$

which completes the proof for all but these two exceptional cases. Since both sides of (2) are integers, (2) is equivalent to

$$(3)\qquad k^2s + k + 3s < ks^2.$$

We verify (3) by showing

$$(4)\qquad ks(s - k) > k + 3s.$$

To see this, if $s - k \geq 2$, we note that since $s \geq 3$ and $k \geq 2$, the left hand side of (4) is at least $2ks = (1/2)ks + (3/2)ks \geq (3/2)k + 3s > k + 3s$ as desired.

However, if $s - k < 2$ then because $k < s$, we have $s - k = 1$ so (4) is equivalent to $ks > k + 3s$, which implies $k^2 + k > 4k + 3$ and hence $k^2 - 3k - 3 > 0$. The latter inequality holds for $k > 3/2 + (1/2)\sqrt{21}$, which is less than four; therefore (as $k \geq 2$) the only cases where it fails are $(k, s) = (2, 3)$ or $(k, s) = (3, 4)$.

In these two cases, we recall that A can in fact be written as the product of $ks^2 + 1$ atoms, each of p-adic value at least k, so $v_p(A) \geq k^2s^2 + k$.

This means that the elasticity of the element A is at least

$$(v_p(A)/k - 1)/(v_p(A)/s + 3) \geq ((k^2s^2 + k)/k - 1)/((k^2s^2 + k)/s + 3).$$

In the case where $k = 2$ and $s = 3$, we note $k^2s^2 + k = 38$, so the elasticity of A is at least $(38/2 - 1)/(38/3 + 3) > 18/16 > 19/18 = (ks^2 + 1)/ks^2$.

In the case where $k = 3$ and $s = 4$, we note that $k^2s^2 + k = 147$, so the elasticity of A is at least $(147/3 - 1)/(147/4 + 3) > 48/40 > 49/48 = (ks^2 + 1)/ks^2$.

In every possible case, we therefore see that the elasticity of A is greater than $(ks^2 + 1)/ks^2$, which contradicts the presumption that the elasticity of A is equal to $(ks^2 + 1)/ks^2$, and therefore our monoid has no element of this elasticity. ■

With the last two lemmas, we have established the following.

Corollary 3.3. *Let p be a prime number, $b_1 > 1$ a positive integer with* $\gcd(p, b_1) = 1$ *and* $k = t \cdot \mathrm{ord}_{b_1}(p)$ *for some* $t \geq 1$. *The following statements are equivalent*:

(1) $M(p^k, p^k b_1)$ *is fully elastic.*
(2) $t = 1$.

Acknowledgements. The authors wish to thank the referee for many helpful comments and suggestions.

REFERENCES

[1] D. D. Anderson and D. F. Anderson, *Elasticity of factorization in integral domains*, J. Pure Appl. Algebra 80 (1992), 217–235.

[2] D. D. Anderson, D. F. Anderson, S. T. Chapman and W. W. Smith, *Rational elasticity of factorizations in Krull domains*, Proc. Amer. Math. Soc. 117 (1993), 37–43.

[3] D. F. Anderson, *Elasticity of factorizations in integral domains*: *a survey*, in: Factorization in Integral Domains, Lecture Notes in Pure and Appl. Math. 189, Dekker, New York, 1997, 1–29.

[4] D. F. Anderson and S. T. Chapman, *On the elasticities of Krull domains with finite cyclic divisor class group*, Comm. Algebra 28 (2000), 2543–2553.

[5] D. F. Anderson, S. T. Chapman and W. W. Smith, *Some factorization properties of Krull domains with infinite cyclic divisor class group*, J. Pure Appl. Algebra 96 (1994), 97–112.

[6] P. Baginski, S. T. Chapman, C. Crutchfield, K. G. Kennedy and M. Wright, *Elastic properties and prime elements*, Results Math. 49 (2006), 1–14.

[7] M. Banister, J. Chaika, S. T. Chapman and W. Meyerson, *On a result of James and Niven concerning unique factorization in congruence semigroups*, Elem. Math., to appear.

[8] S. T. Chapman and A. Geroldinger, *Krull domains and monoids*, *their sets of lengths*, *and associated combinatorial problems*, in: Factorization in Integral Domains, Lecture Notes in Pure and Appl. Math. 189, Dekker, New York, 1997, 73–112.

[9] S. T. Chapman, M. Holden and T. Moore, *Full elasticity in atomic monoids and integral domains*, Rocky Mountain J. Math. 36 (2006), 1437–1455.

[10] S. T. Chapman and B. McClain, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra 293 (2005), 595–610.

[11] A. Geroldinger, *On the arithmetic of certain not integrally closed noetherian integral domains*, Comm. Algebra 19 (1991), 685–698.

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

[13] —, —, *Transfer principles in the theory of non-unique factorizations*, in: Arithmetical Properties of Commutative Rings and Monoids, Lecture Notes in Pure and Appl. Math. 241, Chapman & Hall/CRC, Boca Raton, FL, 2005, 114–141.

[14] —, —, *Non-Unique Factorizations*: *Algebraic*, *Combinatorial and Analytic Theory*, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[15] N. Gonzalez, S. Pellerin and R. Robert, *Elasticity of $A + XI[X]$ domains where A is a UFD*, J. Pure Appl. Algebra 160 (2001), 183–194.

[16] F. Halter-Koch, *Halbgruppen mit Divisorentheorie*, Exposition. Math. 8 (1990), 27–66.

[17] —, *Arithmetical semigroups defined by congruences*, Semigroup Forum 42 (1991), 59–62.

[18] —, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux 7 (1995), 367–385.

[19] —, *C-monoids and congruence monoids in Krull domains*, in: Arithmetical Properties of Commutative Rings and Monoids, Lecture Notes in Pure and Appl. Math. 241, Chapman & Hall/CRC, Boca Raton, FL, 2005, 71–98.

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

M. Banister
Department of Mathematics
Harvey Mudd College
1250 N. Dartmouth Ave.
Claremont, CA 91711, U.S.A.

Current address:
Department of Mathematics
University of California at Santa Barbara
Santa Barbara, CA 93106, U.S.A.
E-mail: bluerose91711@yahoo.com

J. Chaika
Department of Mathematics
The University of Iowa
14 MacLean Hall
Iowa City, IA 52242, U.S.A.

Current address:
Mathematics Department, MS 136
Rice University
6100 S. Main St.
Houston, TX 77005-1892, U.S.A.
E-mail: Jonathan.M.Chaika@rice.edu

S. T. Chapman
Department of Mathematics
Trinity University
One Trinity Place
San Antonio, TX 78212-7200, U.S.A.
E-mail: schapman@trinity.edu

W. Meyerson
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138, U.S.A.

Current address:
Mathematics Department
University of California at Los Angeles
Box 951555
Los Angeles, CA 90095-1555, U.S.A.
E-mail: meyerson@math.ucla.edu

Received 29 March 2005;
revised 30 August 2006 (4612)