Proceedings of the Edinburgh Mathematical Society (2003) **46**, 257–267 ©
DOI:10.1017/S0013091502000305 Printed in the United Kingdom

ON FACTORIZATION IN BLOCK MONOIDS FORMED BY $\{\bar{1}, \bar{a}\}$ IN $\mathbb{Z}_n$

SCOTT T. CHAPMAN[1] AND WILLIAM W. SMITH[2]

[1] *Trinity University, Department of Mathematics, 715 Stadium Drive, San Antonio, TX 78212-7200, USA* (schapman@trinity.edu)
[2] *The University of North Carolina at Chapel Hill, Department of Mathematics, Chapel Hill, NC 27599-3250, USA* (wwsmith@email.unc.edu)

(Received 18 March 2002)

Abstract We consider the factorization properties of block monoids on $\mathbb{Z}_n$ determined by subsets of the form $S_a = \{\bar{1}, \bar{a}\}$. We denote such a block monoid by $\mathcal{B}_a(n)$. In § 2, we provide a method based on the division algorithm for determining the irreducible elements of $\mathcal{B}_a(n)$. Section 3 offers a method to determine the elasticity of $\mathcal{B}_a(n)$ based solely on the cross number. Section 4 applies the results of § 3 to investigate the complete set of elasticities of Krull monoids with divisor class group $\mathbb{Z}_n$.

Keywords: block monoid; elasticity of factorization; Krull monoid

2000 *Mathematics subject classification:* Primary 20M14; 20D60; 13F05

1. Introduction

This paper deals with factorization properties of certain block monoids, and we start with some notation and terminology. Let G be an abelian group written additively, $G_0 = G - \{0\}$, and let

$$\mathcal{F}(G) = \left\{ \prod_{g \in G_0} g^{v_g} \,\middle|\, v_g \in \mathbb{Z}^+ \cup \{0\} \right\}$$

be the multiplicative free abelian monoid with basis G_0. Given $F \in \mathcal{F}(G)$, we write $F = \prod_{g \in G_0} g^{v_g(F)}$. The block monoid over G is defined by

$$\mathcal{B}(G) = \left\{ B \in \mathcal{F}(G) \,\middle|\, \sum_{g \in G_0} v_g(B) g = 0 \right\}.$$

Note that the empty block acts as the identity in $\mathcal{B}(G)$. In general, given $S \subseteq G_0$, we set

$$\mathcal{B}(G, S) = \{B \in \mathcal{B}(G) \mid v_g(B) = 0 \text{ for } g \in G_0 \setminus S\}.$$

A summary of some basic facts about block monoids can be found in [**6**]. The particular block monoids in which we have an interest can be described as follows. Let n and a be integers with $n > 2$, $1 < a < n$ and set $\bar{a} = a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. If $S_a = \{\bar{1}, \bar{a}\}$, then

$$\mathcal{B}(\mathbb{Z}_n, S_a) = \{\bar{1}^u \bar{a}^v \mid \text{where } u, v \geqslant 0 \text{ and } u + av = tn \text{ with } t > 0\}.$$

For ease of notation, let $\mathcal{B}_a(n) = \mathcal{B}(\mathbb{Z}_n, S_a)$.

In a recent paper, the first author and Anderson [**2**] explored the possible elasticities of a Krull domain D with divisor class group $\mathbb{Z}_n$. If S is the subset of $\mathbb{Z}_n \backslash \{0\}$ which contains the height-one prime ideals of D, then it is well known that the factorization properties of D relating to lengths of factorizations are identical to those of $\mathcal{B}(\mathbb{Z}_n, S)$ (see [**3**] for an explanation). Our interest in the monoids $\mathcal{B}_a(n)$ stems from their use in [**2**]. In particular, the monoids $\mathcal{B}_a(n)$ are intrinsic in arguing the following: while there is a Krull domain with divisor class group $\mathbb{Z}_{13}$ with elasticity $\frac{13}{5}$ and another with elasticity $\frac{13}{7}$, there is no Krull domain with divisor class group $\mathbb{Z}_{13}$ with elasticity strictly between $\frac{13}{5}$ and $\frac{13}{7}$.

Mention of the monoids $\mathcal{B}_a(n)$ in the literature is not isolated to [**2**]. In [**5**], Geroldinger gives an elegant characterization of the irreducible blocks in $\mathcal{B}_a(n)$ using continued fractions. In § 2 we start by offering an alternate characterization of these irreducible blocks based on the division algorithm. We then apply this characterization in §§ 3 and 4 to study concepts related to the lengths of factorizations of elements in $\mathcal{B}_a(n)$ into irreducible elements. In § 3 we show that the elasticity of $\mathcal{B}_a(n)$ is $m_a(n)^{-1}$, where $m_a(n)$ is the minimum value obtained by the Zaks–Skula function (see [**4**]) on $\mathcal{B}_a(n)$. In § 4 we compute this elasticity for various values of a and consider the complete set of elasticities of the $\mathcal{B}_a(n)$ for a fixed value of n with $2 \leqslant a \leqslant n-1$. We then specialize these results to the case where p is a prime integer. We finish, in § 4, with an argument which generalizes the observation mentioned earlier in [**2**] for Krull domains with divisor class group $\mathbb{Z}_{13}$. In particular, for an odd prime $p \geqslant 13$, we show that there is no $\mathcal{B}_a(p)$ with elasticity strictly between

$$\frac{p}{\frac{1}{2}(p+1)} \quad \text{and} \quad \frac{p}{\lfloor \frac{1}{4}(p+3) \rfloor}.$$

2. Irreducibles in $\mathcal{B}_a(n)$

Geroldinger [**5**] provides a description of the irreducibles in $\mathcal{B}_a(n)$. Here we give an alternate description of the irreducibles. Following the notation of [**5**] for $n \geqslant 2$, $1 < a \leqslant n-1$, and $u \geqslant 0$, let

$$B_u = \{\bar{1}^u \bar{a}^x \mid \text{where } x \geqslant 0 \text{ and } u + ax = tn \text{ with } t > 0\}.$$

and then set $B(u) = \bar{1}^u \bar{a}^v$, where $v = \min\{x \mid \bar{1}^u \bar{a}^x \in B_u\}$.

It is easily seen (as in [**5**]) that if B is irreducible in $\mathcal{B}_a(n)$, then $B = B(u)$ for some u (the converse is not true). Proposition 8 of [**5**] determines for each u the value of v in $B(u)$. Proposition 10 of [**5**] then provides a remarkable necessary and sufficient condition for $B(u)$ to be irreducible. The values of u for which $B(u)$ is irreducible are determined by an algorithm involving the convergents of the continued fraction of the multiplicative inverse of $-a$ modulo n.

We provide an alternate description of the irreducibles by classifying the irreducibles as one of the following two types.

Type 1: $\bar{1}^u\bar{a}^v$ with $0 \leqslant u < a$.

Type 2: $\bar{1}^u\bar{a}^v$ with $a \leqslant u \leqslant n$.

Setting $d = \gcd(a, n)$, we introduce the following notation. For $1 \leqslant k \leqslant a/d$ write (by the Division Algorithm) $kn = aq_k + r_k$ with $0 \leqslant r_k < a$. This process yields a sequence of remainders $r_1, r_2, \dots, r_w$ and a sequence of blocks

$$\bar{1}^{r_1}\bar{a}^{q_1}, \dots, \bar{1}^{r_w}\bar{a}^{q_w}, \tag{$\dagger$}$$

where $w = a/d$.

Theorem 2.1. *With the notation given above, the irreducible blocks of $\mathcal{B}_a(n)$ can be described as follows.*

(a) *Type 1 blocks: $\bar{1}^{r_k}\bar{a}^{q_k}$, where $r_k < r_i$ for each $i < k$.*

(b) *Type 2 blocks: $\bar{1}^u\bar{a}^v$, where $u + av = n$ and v is an integer with $0 \leqslant v \leqslant \lfloor n/a \rfloor - 1$.*

Proof. First we prove (a). Note that for $B(u)$ any block of the form $\bar{1}^u\bar{a}^v$ with $0 \leqslant u < a$, we have $u + av = kn$. If $B(u)$ is irreducible it must be the case that $k \leqslant a/d$. Since $0 \leqslant u < a$ we have $u = r_k$ and $v = q_k$. Hence, all irreducible blocks of type 1 lie in the sequence ($\dagger$).

For a block $\bar{1}^{r_k}\bar{a}^{q_k}$ taken from ($\dagger$), we show that if there is an $i < k$ with $r_i \leqslant r_k$, then it is reducible. We have

$$\begin{aligned} in &= aq_i + r_i, \\ kn &= aq_k + r_k. \end{aligned}$$

Since

$$q_i = \left\lfloor \frac{in}{a} \right\rfloor \quad \text{and} \quad q_k = \left\lfloor \frac{kn}{a} \right\rfloor,$$

we know that $q_k \geqslant q_i$. Assuming $r_k \geqslant r_i$ yields

$$(k - i)n = a(q_k - q_i) + (r_k - r_i)$$

and, in fact, $\bar{1}^{r_k}\bar{a}^{q_k} = \bar{1}^{r_i}\bar{a}^{q_i} \cdot \bar{1}^{r_{k-i}}\bar{a}^{q_{k-i}}$.

Now suppose for $\bar{1}^{r_k}\bar{a}^{q_k}$ that $r_k < r_i$ for each $i < k$. If $\bar{1}^{r_k}\bar{a}^{q_k}$ is reducible, then we write $\bar{1}^{r_k}\bar{a}^{q_k} = \bar{1}^u\bar{a}^v \cdot B$, where $\bar{1}^u\bar{a}^v$ is irreducible. So,

$$\begin{aligned} kn &= r_k + aq_k, \\ wn &= u + av \end{aligned}$$

and (by assumption) $wn < kn$. Hence $w < k$. Since $u \leqslant r_k < a$, by the uniqueness implied by the Division Algorithm, we have that $u = r_w$ and $v = q_w$ with $w < k$ and

$r_w \leqslant r_k$, contradicting the assumption. Hence, the block is irreducible, which concludes the proof of (a).

We now prove (b). If $\bar{1}^u\bar{a}^v$ is of the given form, then it is clearly irreducible. Now suppose $u + av = tn$ with $t \geqslant 2$ and $a \leqslant u \leqslant n-1$. Write $n = aq + r$ with $0 \leqslant r < a$ ($\bar{1}^r\bar{a}^q$ is a type 1 irreducible by definition). Then $tn = u + av > n = r + aq$. Thus $(t-1)n = (u-r) + a(v-q)$. But $t-1 \geqslant 1$ and $r < a \leqslant u < n-1$. It follows that $u - r > 0$ and $v - q \geqslant 0$ and that $\bar{1}^r\bar{a}^q \cdot \bar{1}^{u-r}\bar{a}^{v-q} = \bar{1}^u\bar{a}^v$. Thus $t \geqslant 2$ yields that $\bar{1}^u\bar{a}^v$ is reducible and the implication is established, completing the proof. □

We note the division $n = aq_1 + r_1$, $0 \leqslant r_1 < a$, always produces the first type 1 irreducible. Also, $\bar{1}^0\bar{a}^{n/d}$ is type 1 and $\bar{1}^n\bar{a}^0$ is type 2.

We illustrate this description of irreducibles with the following simple example.

Example 2.2. The type 1 irreducibles in $\mathcal{B}_8(19)$ are given by the divisions

$$\begin{aligned}(1)19 &= 8(2) + 3,\\ (3)19 &= 8(7) + 1,\\ (8)19 &= 8(19) + 0.\end{aligned}$$

That is, $\bar{1}^3\bar{8}^2$, $\bar{1}^1\bar{8}^7$, $\bar{1}^0\bar{8}^{19}$ are the type 1 irreducible blocks. The type 2 irreducible blocks are simply $\bar{1}^{19}\bar{8}^0$ and $\bar{1}^{11}\bar{8}^1$.

We use this simple description of the irreducibles in the following sections, where it will be seen that the type 1 irreducibles play a critical role in the study of the elasticity of the block monoid $\mathcal{B}_a(n)$.

3. On the elasticity of $\mathcal{B}_a(n)$

For $\mathcal{B}_a(n)$, the elasticity is defined as

$$\rho(\mathcal{B}_a(n)) = \sup\{m/n \mid B_1 \cdots B_n = C_1 \cdots C_m \\ \text{with each } B_i \text{ and } C_j \text{ irreducible in } \mathcal{B}_a(n)\}.$$

General background for this concept can be found in [**1**]. In [**4**], the Zaks–Skula function is introduced as a tool for studying the elasticity. We interpret the notation and results of that work in the setting of $\mathcal{B}_a(n)$ as follows. For the block $B = \bar{1}^u\bar{a}^v$, the Zaks–Skula constant (or cross number) for B is given by $\Bbbk(B) = (u + dv)/n$. We let

$$M_a(n) = \max\{\Bbbk(B) \mid B \text{ is an irreducible block in } \mathcal{B}_a(n)\}$$

and

$$m_a(n) = \min\{\Bbbk(B) \mid B \text{ is an irreducible block in } \mathcal{B}_a(n)\}.$$

With this notation, we state the following as a lemma (see [**4**, Corollary 1.11]).

https://doi.org/10.1017/S0013091502000305 Published online by Cambridge University Press

Lemma 3.1. *For* $n \geqslant 2$ *and* $1 < a \leqslant n-1$,

$$\max\{M_a(n), m_a(n)^{-1}\} \leqslant \rho(\mathcal{B}_a(n)) \leqslant \frac{M_a(n)}{m_a(n)}.$$

Obviously, the case $a \mid n$ represents the trivial case where $m_a(n) = M_a(n) = \rho(\mathcal{B}_a(n)) = 1$. In this section, we establish an efficient algorithm using the characterization of irreducibles from § 2 to calculate the elasticity. In later sections, we will analyse for a given n the set of elasticities $\{\rho(\mathcal{B}_a(n)) \mid 2 \leqslant a \leqslant n-1\}$. In particular, in this section we will show that $M_a(n) = 1$ and that $m_a(n)$ is determined by the type 1 irreducibles.

We first note for the irreducibles $\gamma_1 = \{\bar{1}^n\}$ and $\gamma_2 = \{\bar{a}^{n/d}\}$ that $\Bbbk(\gamma_1) = \Bbbk(\gamma_2) = 1$. Hence, $m_a(n) \leqslant 1 \leqslant M_a(n)$. It is also easy to see that if $B = \bar{1}^u \bar{a}^v$ is a type 2 irreducible (i.e. $u \geqslant a$ and $n = u + av$), then

$$\Bbbk(B) = \frac{u + dv}{n} \leqslant \frac{u + av}{n} = 1,$$

since $d \leqslant a$. To show $\Bbbk(B) \leqslant 1$ for B is a type 1 irreducible is slightly more involved.

Theorem 3.2. *For each irreducible block* B *of* $\mathcal{B}_a(n)$, *we have that* $\Bbbk(B) \leqslant 1$. *Thus* $M_a(n) = 1$ *and* $\rho(\mathcal{B}_a(n)) = m_a(n)^{-1}$.

Proof. By the above remark we merely need to prove the result for the type 1 irreducibles in $\mathcal{B}_a(n)$. We use the notation of § 2 and write the irreducible $B = \bar{1}^{r_k} \bar{a}^{q_k}$, where $kn = aq_k + r_k$ and $0 \leqslant r_k < a$. If $r_k = 0$, then $B = \bar{1}^0 \bar{a}^{n/d}$ and $\Bbbk(B) = 1$. Hence, we assume that $r_k \neq 0$. B irreducible implies for the divisions

$$\begin{aligned} n &= aq_1 + r_1, \\ 2n &= aq_2 + r_2, \\ &\vdots \\ (k-1)n &= aq_{k-1} + r_{k-1} \end{aligned}$$

that $r_k < r_i$ for $i = 1, 2, \ldots, k-1$ and $d \mid r_j$ for $1 \leqslant j \leqslant k$. Notice that the remainders $r_1, \ldots, r_{k-1}$ are distinct. To see this, suppose that $r_i = r_j$ with $j \leqslant i < a/d$. Then $in = aq_i + r_i$ and $jn = aq_j + r_j$ implies that $(i-j)n = a(q_i - q_j)$. It follows that a/d divides $(i-j)$ and hence $i = j$. Since $a - dk$ is the largest positive integer less than a that is itself less than $k-1$ distinct integers divisible by d (also less than a), it follows that $r_k \leqslant a - dk$. Since

$$q_k = \left\lfloor \frac{kn}{a} \right\rfloor < \frac{kn}{a},$$

if we assume that $n \leqslant r_k + dq_k < a - dk + (dkn/a)$, then $a(n-a) < dk(n-a)$, a contradiction. Hence $\Bbbk(B) = (r_k + dq_k)/n < 1$. □

Having established $M_a(n) = 1$, we now turn our attention to $m_a(n)$. We show that it is determined by the type 1 irreducibles with the following lemma.

https://doi.org/10.1017/S0013091502000305 Published online by Cambridge University Press

Lemma 3.3. *Let $B = \bar{1}^{r_1}\bar{a}^{q_1}$ be the type 1 irreducible determined by the division $n = aq_1 + r_1$ with $0 \leqslant r_1 < a$. Then $\Bbbk(B) \leqslant \Bbbk(B_i)$ for any type 2 irreducible B_i.*

Proof. Theorem 2.1 (b) implies that type 2 irreducibles exist if and only if $a \leqslant n/2$. In this case, they are the irreducibles of the form $B_t = \bar{1}^{n-ta}\bar{a}^t$ where $1 \leqslant t < \lfloor n/a \rfloor$. Thus $\Bbbk(B_t) = (n - ta + dt)/n$ and $\Bbbk(B) = (r_1 + dq_1)/n$. The result is established if $r_1 + dq_1 \leqslant n - ta + dt$ for $1 \leqslant t < \lfloor n/a \rfloor$. Since $n = aq_1 + r_1$, this inequality reduces to $dq_1 \leqslant aq_1 - ta + dt$ and hence $t(a-d) \leqslant q_1(a-d)$. Again, since we exclude the case $a \mid n$, $a - d > 0$ and $q_1 = \lfloor n/a \rfloor$ yields the desired inequality. □

We summarize the results of this section in the following theorem. Let $\mathcal{B}_a^*(n)$ denote the set of all irreducible blocks of type 1 in $\mathcal{B}_a(n)$.

Theorem 3.4. *Let $1 \leqslant a < n$ and $d = \gcd(a, n)$.*

(1) *If $a \mid n$, then $m_a(n) = 1$.*

(2) *If $a \nmid n$, then*

$$m_a(n) = \min\left\{ \frac{u + dv}{n} \;\middle|\; \bar{1}^u\bar{a}^v \in \mathcal{B}_a^*(n) \right\} < 1.$$

(3) $\rho(\mathcal{B}_a(n)) = m_a(n)^{-1}$.

We note that $m_a(n)$ is not necessarily obtained by $\bar{1}^{r_1}\bar{a}^{q_1}$. As an example, easy calculations reveal that $m_{11}(19)$ is obtained by $\bar{1}^{r_3}\bar{a}^{q_3}$.

4. The set of elasticities

For a given integer n, we set

$$P(n) = \{\rho(\mathcal{B}_a(n)) \mid 2 \leqslant a \leqslant n - 1\}.$$

In this section, we make some general observations about the set $P(n)$. Due to the results of § 3, we use a simpler notation and describe

$$\mathrm{Min}(n) = \{nm_a(n) \mid 2 \leqslant a < n\}.$$

Hence, $P(n) = \{(n/m) \mid m \in \mathrm{Min}(n)\}$.

Example 4.1. In Example 2.2, it was shown that $m_{11}(19) = \frac{7}{19}$. Additional calculations yield $\mathrm{Min}(19) = \{2, 3, 4, 5, 7, 10\}$.

Lemma 4.2. *The following statements are equivalent.*

(1) $1 \in P(n)$.

(2) $n \in \mathrm{Min}(n)$.

(3) *n is not prime.*

https://doi.org/10.1017/S0013091502000305 Published online by Cambridge University Press

Proof. This has often been observed earlier, since n not prime means there is a divisor a of n with $2 \leqslant a \leqslant n-1$. $\square$

Theorem 4.3. *Let $n > 2$ be a positive integer.*

(a) *For all n we have that $2 \in \mathrm{Min}(n)$. In fact, $\frac{1}{2}n = \rho(\mathcal{B}_a(n))$, where $a = n-1$.*

(b) *If $n > 3$ is an odd integer, then $3 \in \mathrm{Min}(n)$. In fact, $\frac{1}{3}n = \rho(\mathcal{B}_a(n))$ for $a = \frac{1}{2}(n-1)$.*

(c) *If n is odd and $a = \frac{1}{2}(n+1)$, then $\rho(\mathcal{B}_a(n)) = n/(\frac{1}{2}(n+1))$. That is, $\frac{1}{2}(n+1) \in \mathrm{Min}(n)$.*

(d) *$\rho(\mathcal{B}_2(n)) = 1$ if n is even and $\rho(\mathcal{B}_2(n)) = n/(\frac{1}{2}(n+1))$ if n is odd.*

Proof.

(a) In this case, $n = a(1) + 1$ produces the only type 1 irreducible B besides $\bar{a}^n$ and $\Bbbk(B) = 2/n$.

(b) As in the previous case, the fact that $n = a(2) + 1$ implies that there is only one irreducible type 1 block to consider with the desired value.

(c) For $1 \leqslant k \leqslant a-1$ we have $kn = a(2k-1) + (a-k)$. Hence, the remainders $a-1, a-2, \dots, 1$ decrease and each division gives an irreducible $B_k = \bar{1}^{a-k}\bar{a}^{2k-1}$. We note that $\gcd(a, n) = 1$ and hence

$$\Bbbk(B_k) = \frac{(a-k) + (2k-1)}{n} = \frac{a+k-1}{n},$$

which is minimal when $k = 1$, where

$$\Bbbk(B_1) = \frac{a}{n} = \frac{\frac{1}{2}(n+1)}{n}.$$

(d) The statement for n even is trivial since $2 \mid n$. For odd n, we have the isomorphism of $\mathbb{Z}_n$ given by multiplication by 2 carries the set S_a onto S_2, where $a = \frac{1}{2}(n+1)$. Hence part (c) gives the result.

$\square$

We turn our attention to describing the set $P(p)$ for a prime integer p. We discuss this in terms of the set of integers $\mathrm{Min}(p)$, keeping in mind that $x \in \mathrm{Min}(p)$ if and only if $(p/x) \in P(p)$.

To motivate these results, we include the results of calculations of $\mathrm{Min}(p)$ for primes p in the range $41 \leqslant p \leqslant 59$:

p	$\mathrm{Min}(p)$
41	$\{2,3,4,5,6,7,8,9,10,11,14,15,21\}$
43	$\{2,3,4,5,6,7,8,9,10,11,13,15,22\}$
47	$\{2,3,4,5,6,7,8,9,10,11,12,14,16,17,24\}$
53	$\{2,3,4,5,6,7,8,9,10,11,13,14,18,19,27\}$
59	$\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,20,21,30\}$

We note several properties of each $\mathrm{Min}(p)$ already established under the condition that p is prime in Lemma 4.2 and Theorem 4.3. The smallest number in each set is 2, obtained at $a = p-1$. For $p \geqslant 5$, 3 in $\mathrm{Min}(p)$ is obtained at $a = \frac{1}{2}(p-1)$ and $\frac{1}{2}(p+1)$ is obtained at $a = 2$ and $a = \frac{1}{2}(p+1)$.

A review of the values given in the above table indicates that $\mathrm{Min}(p)$ begins with a string of consecutive integers and appears to always have $\frac{1}{2}(p+1)$ as the maximum value with a gap below it. We establish this pattern for the general case. We require several results from elementary number theory whose proofs are left to the reader.

Lemma 4.4. *Suppose $n \geqslant 2$ and a is an integer with $1 < a < n$.*

(a) $\dfrac{n-1}{a-1} \leqslant 2\left\lfloor \dfrac{n}{a} \right\rfloor$.

(b) *If $n \geqslant 13$ and $3 \leqslant a \leqslant \frac{1}{2}(n-1)$, then*

$$\frac{n-2}{a-1} \leqslant \frac{3}{2}\left\lfloor \frac{n}{a} \right\rfloor.$$

(c) *If $n = aq + r$ and $0 \leqslant r < a$, then $q + r \leqslant \frac{1}{2}(n+1)$.*

Using our earlier notation, an immediate corollary of Lemma 4.4 is that $\frac{1}{2}(p+1)$ is indeed the maximum element of $\mathrm{Min}(p)$. Moreover, $\mathrm{Min}(p) \subseteq \{2, 3, \dots, \frac{1}{2}(p+1)\}$ for all prime $p \geqslant 3$. The next result establishes that for any integer $s \geqslant 2$, the values $2, 3, \dots, s$ are in $\mathrm{Min}(p)$ for p sufficiently large.

Theorem 4.5. *$\{2, \dots, s\} \subseteq \mathrm{Min}(p)$ for all primes $p > s^2 - s$.*

Proof. Let $t = s-1$. We will show that $m_a(p) = s$ for $a = p-t$. We use the divisions from § 2 to consider the type 1 irreducibles. For $k < (p-t)/t$, we have $kt < a$ and $kp = a(k) + kt$. That is, in the notation of § 2, $q_k = k$ and $r_k = kt$. Clearly, $r_1 < r_2 < \cdots$ and the only type 1 irreducible formed for $k < (p-t)/t$ is from the division $p = a(1) + t$ and $q_1 + r_1 = t + 1$. The other type 1 irreducibles will be determined by divisions $kp = aq_k + r_k$ for $0 \leqslant r_k < a - 1$ with $k \geqslant (p-t)/t$.

However, $kp = ak + kt$ and $k \geqslant (p-t)/t$ implies $kt \geqslant p - t = a$. Write $kt = au + v$ with $0 \leqslant v < a$, which gives $kp = a(k+u) + v$. Hence $q_k = k + u$ and $r_k = v$. Noting that $u \geqslant 1$, we have

$$q_k + r_k = k + u + v \geqslant k + 1 \geqslant \frac{p-t}{t} + 1 \geqslant \frac{p}{t}.$$

https://doi.org/10.1017/S0013091502000305 Published online by Cambridge University Press

However, $p > t + t^2$ yields $(p/t) > t + 1$. Hence $q_k + r_k > t + 1$. This establishes that $\rho(\mathcal{B}_a(n))$ is determined by $B = \bar{1}^{r_1}\bar{a}^{q_1}$ (the block with minimal $\Bbbk(B)$ value) and hence $m_a(p) = t + 1$. □

It would seem that the previous result may not be the best possible. For example, it states that $\{2, \dots, 10\} \subseteq \mathrm{Min}(p)$ for all primes $p > 90$. Calculations indicate that this is actually the case for all primes $p \geqslant 41$. In fact, further calculations show that $\{2, \dots, 17\} \subseteq \mathrm{Min}(97)$.

We now turn our attention to the large values in $\mathrm{Min}(p)$. Before doing so, we record the following result in the spirit of our earlier calculations.

Lemma 4.6. *Let $n > 3$.*

(a) *If $3 \mid n$, then $m_3(n) = 1$, $n \in \mathrm{Min}(n)$ and $\rho(\mathcal{B}_3(n)) = 1$.*

(b) *If $3 \nmid n$, then $m_3(n) = \lfloor \frac{1}{3}(n+4) \rfloor$, $\lfloor \frac{1}{3}(n+4) \rfloor \in \mathrm{Min}(n)$ and*

$$\rho(\mathcal{B}_3(n)) = \frac{n}{\lfloor \frac{1}{3}(n+4) \rfloor}.$$

Proof. The case $3 \mid n$ has already been established in Theorem 3.4 (1). The argument for $3 \nmid n$ considers the two cases $n \equiv 1 \pmod 3$ and $n \equiv 2 \pmod 3$. We have used the notation $\lfloor \frac{1}{3}(n+4) \rfloor$ to unify the result, but note that $\lfloor \frac{1}{3}(n+4) \rfloor = \lfloor \frac{1}{3}n \rfloor + 1$ when $n \equiv 1 \pmod 3$ and $\lfloor \frac{1}{3}(n+4) \rfloor = \lfloor \frac{1}{3}n \rfloor + 2$ when $n \equiv 2 \pmod 3$.

Case 1. $n \equiv 1 \pmod 3$. In this case $n = 3q + 1$ provides the only type 1 irreducible and $q + 1 = \lfloor \frac{1}{3}n \rfloor + 1$.

Case 2. $n \equiv 2 \pmod 3$. Here there are two type 1 irreducibles given by $n = 3q + 2$ and $2n = 3(2q + 1) + 1$. The second yields a quotient plus remainder value of $2q + 2$, which is greater than $q + 2$ (as $n > 3$). Thus the minimum value that gives $\rho(\mathcal{B}_3)$ is $q + 2 = \lfloor \frac{1}{3}n \rfloor + 2$. □

The previous lemma yields that the value $\lfloor \frac{1}{3}(p+4) \rfloor$ will be in $\mathrm{Min}(p)$ for all primes $p \geqslant 5$. We will now show that for all primes $p \geqslant 13$, this value is the second largest value of $\mathrm{Min}(p)$. Hence, for $p \geqslant 13$ there will always be a gap (increasing in length as p increases) between the two largest values of $\mathrm{Min}(p)$, namely $\lfloor \frac{1}{3}(p+4) \rfloor$ and $\frac{1}{2}(p+1)$. This 'gap' was observed for small values of p in [**2**].

Theorem 4.7. *Let p be an odd prime and let a be an integer with $3 \leqslant a \leqslant p - 1$ and $a \neq \frac{1}{2}(p+1)$. Then $m_a(p) \leqslant \frac{1}{3}(p+4)$ and hence*

$$\rho(\mathcal{B}_a(p)) \geqslant \frac{p}{\frac{1}{3}(p+4)}.$$

Proof. We split the proof into two cases.

https://doi.org/10.1017/S0013091502000305 Published online by Cambridge University Press

Case 1. Suppose that $3 \leqslant a \leqslant \frac{1}{2}(p-1)$. If $p = aq + r$ with $0 \leqslant r < a$, we will then argue that $q + r \leqslant \frac{1}{3}(p+4)$, which implies that

$$\rho(\mathcal{B}_a(p)) \geqslant \frac{p}{\frac{1}{3}(p+4)}.$$

Now, $q = \lfloor p/a \rfloor$ and $r = p - a\lfloor p/a \rfloor$. Hence $q + r = p + \lfloor p/a \rfloor(1-a)$. By Lemma 4.4 (b), since $1 - a < 0$,

$$\left\lfloor \frac{p}{a} \right\rfloor (1-a) \leqslant \frac{2}{3}\left(\frac{p-2}{a-1}\right)(1-a) = \tfrac{2}{3}(2-p).$$

Therefore, $q + r \leqslant p + \frac{2}{3}(2-p) = \frac{1}{3}(p+4)$.

Case 2. Suppose that $p-1 \geqslant a > \frac{1}{2}(p+1)$. For $1 \leqslant c < \frac{1}{2}(p-1)$ set $a = \frac{1}{2}(p+1)+c = \frac{1}{2}(p+2c+1)$. We fix $c \geqslant 1$ and consider all primes p. It is sufficient to get the result if we know there exists $t \geqslant 1$ so that $tp = aq_t + r_t$ with $0 \leqslant r_t < a$ and $q_t + r_t \leqslant \frac{1}{3}(p+4)$ (i.e. we need not be concerned with 'irreducibility' as an irreducible factor will have even smaller '$q + r$'). Let $b = 2c + 1$ (an odd integer greater than or equal to 3) and $b < p$. First note that $p = a(1) + (p-a) = a(1) + \frac{1}{2}(p-b)$ and $q_1 + r_1 = \frac{1}{2}(p-b+2) \leqslant \frac{1}{3}(p+4)$ whenever $p \leqslant 3b + 2$. For other primes $p > 3b + 2 > 3b$, choose $k \geqslant 1$ so that

$$b(2k+1) = b + 2bk < p \leqslant b + 2b(k+1). \tag{$*$}$$

We have the following identity

$$(k+1)p = (\tfrac{1}{2}(p+b))(2k+1) + (\tfrac{1}{2}(p - b(2k+1))).$$

The condition $(*)$ gives $0 \leqslant \frac{1}{2}(p-b(2k+1)) < a = \frac{1}{2}(p+b)$ and that $k+1 \leqslant a-1$. Hence, this is the result of the division algorithm when $(k+1)p$ is divided by a. Now $q_{k+1}+r_{k+1} = \frac{1}{2}(2(2k+1) + p - b(2k+1))$. We claim that $\frac{1}{2}(2(2k+1) + p - b(2k+1)) \leqslant \frac{1}{3}(p+4)$ (i.e. $6(2k+1)+3p-3b(2k+1) \leqslant 2p+8$ and hence $p \leqslant 3b(2k+1)-6(2k+1)+8$ is needed). By $(*)$, $p \leqslant b+2b(k+1)$, so we need only show $p \leqslant b+2b(k+1) \leqslant 3b(2k+1)-6(2k+1)+8$ or $b+2bk+2b \leqslant 6bk+3b-12k+2$ or $0 \leqslant 4bk-12k+2$ or $6k \leqslant 2bk+1$. But this is true if $b \geqslant 3$, which it is (recall for $b = 1$ and $c = 0$ that $a = \frac{1}{2}(p+1)$, which has elasticity $p/(\frac{1}{2}(p+1))$). □

We summarize what we have for $\mathbb{Z}_p$ regarding elasticity in terms of the set $\mathrm{Min}(p)$ (where p is prime). The lower end of the set has consecutive numbers $2, 3, \dots$ (Theorem 4.5). At the other extreme, the largest value is $\frac{1}{2}(p+1)$. The next possible value less than $\frac{1}{2}(p+1)$ is $\lfloor \frac{1}{3}(p+4) \rfloor$. These are equal for $p = 3$ and 5 and differ by one for $p = 7$ and 11. However, for $p \geqslant 13$ there is a gap between these two values and since $\frac{1}{2}(p+1) - \frac{1}{3}(p+4) = \frac{1}{6}(p-5)$, this gap between values gets large as p increases in size. We end this section with an application of the above in a slightly more general setting.

In [**2**], the following set of elasticities is considered (where p is an odd prime):

$$\Upsilon(p) = \{\rho(\mathcal{B}(\mathbb{Z}_p, S)) \mid \emptyset \neq S \subseteq \mathbb{Z}_p \backslash \{0\}\}.$$

In that work, they observed that

$$\Upsilon(p) \subseteq \{\tfrac{1}{2}p, \tfrac{1}{3}p, \dots, p/(\tfrac{1}{2}(p+1)), 1\}.$$

They also noted there were 'gaps' in the sets $\Upsilon(p)$ for $p = 13$, 17, 19 and 23. With the simple observation that

$$\rho(\mathcal{B}(\mathbb{Z}_p, S \cup T)) \geqslant \max\{\rho(\mathcal{B}(\mathbb{Z}_p, S)), \rho(\mathcal{B}(\mathbb{Z}_p, T))\}$$

and the fact that

$$\rho(\mathcal{B}_a(n)) = \frac{p}{\frac{1}{2}(p+1)}$$

for $a = 2$ or $a = \frac{1}{2}(p+1)$, we easily use the analysis of this section to conclude that the only possible set S that could have $\rho(\mathcal{B}(\mathbb{Z}_p, S))$ between $p/(\frac{1}{2}(p+1))$ and $p/\lfloor\frac{1}{4}(p+3)\rfloor$ would be $S = \{\bar{1}, \bar{2}, \overline{\frac{1}{2}(p+1)}\}$. However, in [**2**, Lemma 12 (c)] it is shown that $\rho(\mathbb{Z}_p, \{\bar{1}, \bar{2}, \overline{\frac{1}{2}(p+1)}\})$ is not between these values. Hence, we have the following theorem.

Theorem 4.8. *Let $p \geqslant 13$ be a prime. There is no subset $S \subseteq \mathbb{Z}_p \backslash \{0\}$ with*

$$\frac{p}{\frac{1}{2}(p+1)} < \rho(\mathcal{B}(\mathbb{Z}_p, S)) < \frac{p}{\lfloor\frac{1}{4}(p+3)\rfloor}. \qquad (**)$$

Hence, for such a prime p, there is no Krull domain D with divisor class group $\mathbb{Z}_p$ whose elasticity $\rho(D)$ satisfies the inequality $(**)$.

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

References

1. D. F. Anderson, *Elasticity of factorizations in integral domains: a survey*, Lecture Notes in Pure and Applied Mathematics, vol. 189, pp. 1–29 (Marcel Dekker, New York, 1997).
2. D. F. Anderson and S. T. Chapman, On the elasticities of Krull domains with finite cyclic divisor class group, *Commun. Alg.* **28** (2000), 2543–2553.
3. S. T. Chapman and A. Geroldinger, Krull monoids, their sets of lengths and associated combinatorial problems, *Factorization in integral domains*, Lecture Notes in Pure and Applied Mathematics, vol. 189, pp. 73–112 (Marcel Dekker, New York, 1997).
4. S. T. Chapman and W. W. Smith, An analysis using the Zaks–Skula constant of element factorizations in Dedekind domains, *J. Alg.* **159** (1993), 176–190.
5. A. Geroldinger, On non-unique factorizations into irreducible elements, II, *Colloq. Math. Soc. Janos Bolyai* **51** (1987), 723–757.
6. A. Geroldinger and F. Halter-Koch, Non-unique factorizations in block semigroups and arithmetical applications, *Math. Slovaca* **42** (1992), 641–661.