Mathematica Slovaca

SooAh Chang; Scott T. Chapman; William W. Smith

Elasticity in certain block monoids via the Euclidean table

*Mathematica Slovaca*, Vol. 57 (2007), No. 5, [415]--454

Persistent URL: http://dml.cz/dmlcz/136969

VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-007-0037-0
Math. Slovaca **57** (2007), No. 5, 415–454

# ELASTICITY IN CERTAIN BLOCK MONOIDS VIA THE EUCLIDEAN TABLE

SooAh Chang* — Scott T. Chapman** — William W. Smith*

(*Communicated by Stanislav Jakubec*)

ABSTRACT. This paper continues the study begun in [GEROLDINGER, A.: *On non-unique factorizations into irreducible elements II*, Colloq. Math. Soc. János Bolyai **51** (1987), 723–757] concerning factorization properties of block monoids of the form $\mathscr{B}(\mathbb{Z}_n, S)$ where $S = \{\overline{1}, \overline{a}\}$ (hereafter denoted $\mathscr{B}_a(n)$). We introduce in Section 2 the notion of a *Euclidean table* and show in Theorem 2.8 how it can be used to identify the irreducible elements of $\mathscr{B}_a(n)$. In Section 3 we use the Euclidean table to compute the elasticity of $\mathscr{B}_a(n)$ (Theorem 3.4). Section 4 considers the problem, for a fixed value of $n$, of computing the complete set of elasticities of the $\mathscr{B}_a(n)$ monoids. When $n = p$ is a prime integer, Proposition 4.12 computes the three smallest possible elasticities of the $\mathscr{B}_a(p)$.

## 1. Introduction

This paper continues the study begun in [8] and continued in [2], [7] and [12] concerning factorization properties of block monoids of the form $\mathscr{B}(\mathbb{Z}_n, S)$ where $S = \{\overline{1}, \overline{a}\}$ (hereafter denoted $\mathscr{B}_a(n)$). To set the stage for the reader, we open with some basic definitions and a general description of the problem area, before reviewing our specific results.

Given an abelian group $G$ and $S \subseteq G_0 = G \setminus \{0\}$, let $\mathscr{F}(G, S)$ be the free abelian monoid with basis $S$. An element $B$ in $\mathscr{F}(G, S)$ is called a *sequence* and the total number of times that each element $g \in S$ appears in $B$ is called the

2000 Mathematics Subject Classification: Primary 20M14, 20D60.
Keywords: block monoid, elasticity of factorization, non-unique factorization, minimal zero-sequence.

Parts of this work are contained in the first author's Doctoral Dissertation written at the University of North Carolina at Chapel Hill under the direction of the third author.

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

Springer

*multiplicity* of $g$ in $B$, denoted as $v_g(B)$. Each sequence $B$ then has a unique representation of the form $B = \prod_{g \in S} g^{v_g(B)}$. The following are some of the basic notions to be considered:

- For $G$ finite, the *cross number* $k(B) := \sum_{g\in S} \frac{v_g(B)}{|g|}$.
- $C \in \mathscr{F}(G,S)$ *divides* $B$, if $v_g(C) \leqslant v_g(B)$ for every $g \in S$.
- The *length* of $B$: $|B| = \sum_{g \in S} v_g(B) \in \mathbb{N}$.
- The *sum* of $B$: $\sigma(B) = \sum_{g\in S} v_g(B)g$.

The monoid homomorphism

$$\sigma\colon \mathscr{F}(G,S) \to G, \quad \sigma\left(\prod_{g\in S} g^{v_g(B)}\right) = \sum_{g \in S} v_g(B)g$$

maps a sequence to the sum of its elements. Note that $\ker(\sigma)$ forms a submonoid of $\mathscr{F}(G,S)$. A sequence $B$ is called a *block*, if $\sigma(B) = 0$, equivalently, if $B \in \ker(\sigma)$. Let $\mathscr{B}(G,S)$ denote $\ker(\sigma)$, the set of all the blocks in $\mathscr{F}(G,S)$. It is called the *block monoid over $G$ determined by $S$* (see [9] for more information on block monoids). Note that the empty block $1 = \prod_{g\in S} g^0 \in \mathscr{F}(G)$ acts as the identity in $\mathscr{B}(G,S)$. A block $B$ is said to be *irreducible* if any block $C$ that divides $B$ is either the empty block or itself.

The reader should note that block monoids are a central tool for investigating the arithmetic of general Krull monoids (see [10, Chapter 6]). The following related questions concerning arithmetical invariants associated to a block monoid over a finite abelian group $G$ have been studied in the literature.

1) The set of all cross numbers $W(G) = \{k(S) : S \in \mathscr{A}(\mathscr{B}(G))\}$ (see [4]).
2) The system of all sets of lengths $\mathscr{L}(G) = \{L(B) : B \in \mathscr{B}(G)\}$ (see [10]).
3) The set of all elasticities $\{\rho(L) : L \in \mathscr{L}(G)\}$ (see [3]).
4) The set $\Delta^*(G) = \{\min \Delta(\mathscr{B}(G_0)) : G_0 \subset G \text{ with } \rho(\mathscr{B}(G_0) \neq 1\}$ of differences in long sets of lengths (see [10, Chapter 6.8].

Our main interests in the study of block monoids are twofold. The first is to determine all the *irreducible blocks* of $\mathscr{B}(G,S)$. The second is to consider factorizations of blocks as a product of irreducible blocks. Such a study requires the following definition. The *elasticity* of $\mathscr{B}(G,S)$ is defined as

$$\rho(\mathscr{B}(G,S)) = \sup\{\tfrac{m}{n} : B_1 \dots B_n = C_1 \dots C_m \text{ with each } B_i \text{ and } C_j \text{ irreducible in } \mathscr{B}(G,S)\}$$

and measures the degree of non-uniqueness in factorizations of the monoid. A wide array of the recent mathematical literature has considered problems related to elasticity in both monoids and integral domains. The interested reader can find more information concerning elasticity in [1] and [11], while [5] is a good reference for problems in general in the area of non-unique factorization. Moreover, two recent papers by Schmid ([14] and [15]) explore questions related to non-unique factorizations specifically in block monoids.

It has been shown that the elasticity of $\mathscr{B}(G,S)$, or at least certain upper and lower bounds for it, can be obtained by considering the cross number ([6, Corollary 1.7]). In particular, for those block monoids $\mathscr{B}(\mathbb{Z}_{p^n},S)$ with $p$ a prime integer, the elasticity is given by the minimum cross number (see [7]). Our specific interest here is in the case where $G=\mathbb{Z}_n$ and $S$ is a subset of two elements of the form $\{\overline{1},\overline{a}\}$ with $\gcd(a,n)=1$ (for simplicity, we denote such a block monoid by $\mathscr{B}_a(n)$). In [8], Geroldinger studies the irreducible elements of $\mathscr{B}_a(n)$ and the associated sets of lengths for their general blocks, using continued fractions. In [2], Anderson and Chapman study elasticities in the particular case where $n=p^k$ is a power of a prime. They show that if $k=1$ and $\rho(\mathscr{B}_a(p))\neq 1$, then $\rho(\mathscr{B}_a(p))\geq \frac{2p}{p+1}$. The case where $p=2$ and $k>1$ has been recently studied in greater detail by Kattchee in [12]. Chapman and Smith in [7] develop a method, distinct from that of [8] for determining the irreducibles of $\mathscr{B}_a(n)$ using the Euclidean Division Algorithm.

Following the introduction, the results of this paper are broken into 4 sections and can be summarized as follows. We expand upon Geroldinger's study of continued fractions in [8] and in Section 2 introduce the notion of a *Euclidean table.* We show in Theorem 2.8 how it can be used to identify the irreducible elements of $\mathscr{B}_a(n)$. In Section 3 we use the Euclidean table to compute the elasticity of $\mathscr{B}_a(n)$ (Theorem 3.4). Section 4 considers the problem, for a fixed value of $n$, of computing the complete set of elasticities of the $\mathscr{B}_a(n)$ monoids (which we denote by $\Upsilon_2(n)$). When $n=p$ is a prime integer, Proposition 4.12 computes the three smallest possible elasticities of the $\mathscr{B}_a(p)$. Section 5 contains a detailed proof of Proposition 4.12.

## 2. The irreducibles and the Euclidean table

In this section, we consider the irreducible blocks in the block monoid $\mathscr{B}(G,S)$ where $G=\mathbb{Z}_n$ and $S$ is a subset of two elements of the form $\{\bar{a},\bar{b}\}$ with $1<a<b<n$ such that $\gcd(a,b,n)=1$. In [8, Proposition 5], it is shown that there exist $n'\in\mathbb{Z}$ and $1\leqslant a'\leqslant n'-1$ such that $\gcd(c,n')=1$ and that for $S'-\{1,\bar{a}'\}\subseteq\mathbb{Z}_{n'}$, $\mathscr{B}(G,S)$ is isomorphic to $\mathscr{B}(\mathbb{Z}_{n'},S')$. Thus, we may restrict our attention to the block monoids of the form $\mathscr{B}\big(\mathbb{Z}_n,\{\bar{1},\bar{a}\}\big)$ with $\gcd(a,n)=1$.

Following the notation in [7], we denote the block monoid of this type as $\mathscr{B}_a(n)$, that is

$$\mathscr{B}_a(n) = \{\bar{1}^u \bar{a}^v : \text{ where } u, v \geqslant 0 \text{ and } u + av = kn \text{ with } k \geqslant 1\}.$$

The irreducible blocks in $\mathscr{B}_a(n)$ have been previously studied. We first present two previous methods for describing the irreducibles.

**Method I:** In [8], Geroldinger provides a description of the irreducibles in $\mathscr{B}_a(n)$ using the continued fraction of $\frac{n}{q}$, where $q \in \{1, 2, \dots, n-1\}$ is minimal such that $aq + 1 \equiv 0 \pmod{n}$. Let $[b_0, b_1, \dots, b_m]$ be the continued fraction of $\frac{n}{q}$ with the convergents $\frac{p_i}{q_i}$, $i = 1, 2, \dots, m$ and set $p_{-2} = 0$, $p_{-1} = 1$; $q_{-2} = 1$, $q_{-1} = 0$. For each $N \in \mathbb{N}$, he defines the integer $m_N = [N \cdot \frac{n}{q}] + 1$ and the block $B(m_N)$ in $\mathscr{B}_a(n)$ with $v_1(B(m_N)) = m_N$ for which the multiplicity of $\bar{a}$ is minimal. With these notations, he proves the following.

**Proposition 2.1.**

(1) ([8, Proposition 8]) *A block $B \in \mathscr{B}_a(n)$ not equal to $\bar{1}^n$ or $\bar{a}^n$ is irreducible if and only if $B = B(m_N)$ for some $N \in \{0, 1, \dots, q-1\}$.*

(2) ([8, Proposition 10]) *Let $N \in \{0, 1, \dots, q-1\}$. Then $B(m_N)$ is irreducible if and only if $N$ is in one of the following two forms:*
   - (i) *$N = q_{j-1} + c_j q_j$ with $0 < c_j < b_{j+1}$, $0 \leqslant j < m$ with $j$ even.*
   - (ii) *$N = q_j$ with $j = -1$ or $0 \leqslant j < m$ with $j$ odd.*

We note that in (i), each of those $j$'s with $b_{j+1} = 1$ does not yield any value of $N$. Note also that $j = -1$ in (ii), which corresponds to the irreducible block $\bar{1}^1 \bar{a}^q$, is not included in the original theorem.

*Example* 2.2. Consider $\mathscr{B}_8(19)$. Note that $q = 7$ and $[2, 1, 2, 2]$ is the continued fraction of $\frac{19}{7}$ with the convergents $\frac{2}{1}, \frac{3}{1}, \frac{8}{3}; \frac{19}{7}$. Below is the list of $N$ for which $B(m_N)$ is irreducible, the value $m_N$, and the block $B(m_N)$:

| | | |
|---|---|---|
| $N = q_1 + q_2 = 4$ | $m_4 = [4 \cdot \frac{19}{7}] + 1 = 11$ | $\bar{1}^{11}\bar{8}^1$ |
| $N = q_{-1} = 0$ | $m_0 = [0 \cdot \frac{19}{7}] + 1 = 1$ | $\bar{1}^1\bar{8}^7$ |
| $N = q_1 = 1$ | $m_1 = [1 \cdot \frac{19}{7}] + 1 = 3$ | $\bar{1}^3\bar{8}^2$ |

These three with the two trivial irreducibles $\bar{1}^{19}$ and $\bar{8}^{19}$ give all the irreducible blocks in $\mathscr{B}_8(19)$.

**Method II:** The second method by Chapman and Smith (in [7]) provides a different description of the irreducibles in $\mathscr{B}_a(n)$ using the Euclidean Division Algorithm for $n$ and $a$. They classify the irreducibles into two types as follows.

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

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

They then give the condition, distinct from Geroldinger's, for a block to be irreducible of each type.

**Proposition 2.3.** ([7, Theorem 2.1])

a) $\bar{1}^{r_k}\bar{a}^{q_k}$ *is irreducible of* Type 1 *if and only if* $r_k < r_i$*, whenever* $i < k$*, where* $n\cdot k = a\cdot q_k + r_k$ *is the Euclidean division for values of* $k$*,* $1 \leqslant k \leqslant a$*.*

b) $\bar{1}^{u}\bar{a}^{v}$ *is irreducible of* Type 2 *if and only if* $u + av = n$ *and* $0 \leqslant v \leqslant [\frac{n}{a}]$*.*

*Example* 2.4. We revisit our earlier example $\mathscr{B}_8(19)$. Consider the divisions

$$\begin{aligned}
1 \times 19 &= 8\cdot 2 + 3 && \longleftarrow\\
2 \times 19 &= 8\cdot 4 + 6\\
3 \times 19 &= 8\cdot 7 + 1 && \longleftarrow\\
4 \times 19 &= 8\cdot 9 + 4\\
5 \times 19 &= 8\cdot 11 + 7\\
6 \times 19 &= 8\cdot 14 + 2\\
7 \times 19 &= 8\cdot 16 + 5\\
8 \times 19 &= 8\cdot 19 + 0 && \longleftarrow .
\end{aligned}$$

The criteria for Type 1 irreducibles then yields $\bar{1}^3\bar{8}^2$, $\bar{1}^1\bar{8}^7$, and $\bar{1}^{19}\bar{8}^0$. Type 2 irreducibles are $\bar{1}^{19}\bar{8}^0$ and $\bar{1}^{11}\bar{8}^1$.

Our main theorem translates Geroldinger's result in terms of the continued fraction of $\frac{n}{a}$. Before introducing our result, we first set up the main computational tool, namely, *the Euclidean Table.* As is well known, the Euclidean Algorithm applied to two given positive integers, $n$ and $a$, is a very efficient tool to compute the $\gcd(a, n)$ and also to calculate the continued fraction of $\frac{n}{a}$. We describe our notation, which is standard — except we avoid $p$'s and $q$'s for convergents and $r$'s for remainders so as not to cause confusion with the calculation done in [8].

**Definition 2.5.** Given $n$, $a$ with $1 < a < n$ and $\gcd(a, n) = 1$, we define finite sequences, $\{a_k\}$ (for $k \geqslant 0$) and $\{x_k\}$, $\{y_k\}$; $\{s_k\}$ (for $k \geqslant -2$) recursively as follows:

(1) For $k \geqslant 0$, $a_k = [\frac{s_{k-2}}{s_{k-1}}]$ with $s_{-2} = n$, $s_{-1} = a$.

(2) $s_k = s_{k-2} - a_k \cdot s_{k-1}$ for $k \geqslant 0$.

(3) $x_{-2} = 1$, $x_{-1} = 0$ and $x_k = x_{k-2} + a_k \cdot x_{k-1}$ for $k \geqslant 0$.

(4) $y_{-2} = 0$, $y_{-1} = 1$ and $y_k = y_{k-2} + a_k \cdot y_{k-1}$ for $k \geqslant 0$.

By the assumption $\gcd(a, n) = 1$, the recursion will continue until one gets $s_{k-1} = 1$ and $s_k = 0$. Let $m$ denote the last index of the continued fraction of $\frac{n}{a}$ such that $s_{m-1} = 1$ and $s_m = 0$. Note that the indexing (starting at $-2$) is simply to provide the standard indexing on the continued fraction. We note the following facts.

**Remarks 2.6.**

(1) The continued fraction of $\frac{n}{a}$ is $[a_0, a_1, \dots, a_m]$.

(2) The convergents are $\frac{y_0}{x_0}, \frac{y_1}{x_1}, \dots, \frac{y_m}{x_m} = \frac{n}{a}$.

(3) We have $x_0 < x_1 < \cdots < x_m = a$ and $y_0 < y_1 < \cdots < y_m \quad n$.

(4) We also have $a > s_0 > \cdots > s_{m-1} = 1$ (the remainders).

(5) For all $k \geqslant 0$, $x_k n - y_k a = (-1)^k s_k$.

In our main theorem, we require that the length of the continued fraction be odd, which can be always done as follows: Let $[a_0, a_1, \dots, a_m]$ be the continued fraction of $\frac{n}{a}$ minimal in length. Minimality in length implies that $a_m > 1$. since otherwise (that is if $a_m = 1$), it can be reduced to $[a_0, a_1, \dots, a_{m-1} + 1]$, which is shorter in length. If $m$ is even, then the length of the continued fraction is odd and hence we are done. Suppose now that $m$ is odd so that the continued fraction has even length. We take $[a_0, a_1, \dots, a_m - 1, 1]$ which still gives the continued fraction of $\frac{n}{a}$ and is in odd length as desired. We call the continued fraction in odd length obtained in each case *the odd continued fraction of* $_a$ and denote it as $[a^o_0, a^o_1, \dots, a^o_{m^o}]$. In a similar manner, we can always make the continued fraction of $\frac{n}{a}$ in even length. Call this *the even continued fractior of* $\frac{n}{a}$ and denote it by $[a^e_0, a^e_1, \dots, a^e_{m^e}]$. Let $\{x^e_k\}$, $\{y^e_k\}$; $\{s^e_k\}$ and $\{x^o_k\}$, $\{y^o_k\}$: $\{s^o_k\}$ respectively denote the corresponding sequences determined by even and odd continued fraction. It is easy to see that if $m$ is even, the odd continued fraction of $\frac{n}{a}$ will be the same as the original continued fraction $[a_0, a_1, \dots, a_n]$ and the even continued fraction of $\frac{n}{a}$ will be $[a_0, a_1, \dots, a_m - 1, 1]$ such that $m^e = m + 1$, $a^e_k = a_k$; $s^e_k = s_k$ for every $k \leqslant m^e - 2$, $a^e_{m^e-1} = a_m - 1$; $s^e_{m^e-1} - 1$ and $a^e_{m^e} = 1$; $s^e_{m^e} = 0$. Similarly, if $m$ is odd, the even continued fraction of $\frac{n}{a}$ will be the same with the original and the odd continued fraction of $\frac{n}{a}$ will be given by $[a_0, a_1, \dots, a_m - 1, 1]$ such that $m^o = m + 1$, $a^o_k = a_k$; $s^o_k = s_k$ for every $k \leqslant m^o - 2$, $a^o_{m^o-1} = a_m - 1$; $s^o_{m^o-1} = 1$ and $a^o_{m^o} = 1$; $s^o_{m^o} = 0$.

We now introduce the *Euclidean Table.* For ease of notation, we will occasionally omit the superscripts as in the following definition, if it does not cause any confusion.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | $x_{-2}$ | $y_{-2}$ | $n$ | – |
| -1 | $x_{-1}$ | $y_{-1}$ | $a$ | |
| 0 | $x_0$ | $y_0$ | $s_0$ | $a_0$ |
| 1 | $x_1$ | $y_1$ | $s_1$ | $a_1$ |
| 2 | $x_2$ | $y_2$ | $s_2$ | $a_2$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| m | $x_m$ | $y_m$ | $s_m$ | $a_m$ |

**Definition 2.7.** Let $[a_0, a_1, \dots, a_m]$ be the odd continued fraction of $\frac{n}{a}$ and $\{x_k\}$, $\{y_k\}$; $\{s_k\}$ the corresponding sequences defined as in Definition 2.5. The table formed above is called the *Euclidean Table for n and a.*

We proceed to show that the irreducible blocks in $\mathscr{B}_a(n)$ can be easily obtained from this table.

**Theorem 2.8.** *Let* $[a_0^o, a_1^o, \dots, a_{m^o}^o]$ *be the odd continued fraction of* $\frac{n}{a}$ *and let* $\{s_k^o\}$, $\{x_k^o\}$ *and* $\{y_k^o\}$, *for* $k = -2, -1, \dots, m^o$ *be the corresponding sequences described as in* Definition 2.5. *Then* $B = \bar{1}^u \bar{a}^v \in \mathscr{B}_a(n)$ *is irreducible for exactly the following values of u.*

$$u = \begin{cases} s_k^o - t_k \cdot s_{k+1}^o, & 0 \leqslant t_k < a_{k+2}^o,\ -2 \leqslant k \leqslant m^o - 2 \textit{ with } k \textit{ even.} \\ s_{m^o}^o \end{cases}$$

*For each of these u, the corresponding v and* $\tau$ *for which* $\tau \cdot n = av + u$ *are given by*

$$v = y_k^o + t_k \cdot y_{k+1}^o, \quad -2 \leqslant k \leqslant m^o - 2 \quad \textit{with } k \textit{ even or } v = y_{m^o}^o;$$

$$\tau = x_k^o + t_k \cdot x_{k+1}^o, \quad -2 \leqslant k \leqslant m^o - 2 \quad \textit{with } k \textit{ even or } \tau = x_{m^o}^o.$$

*Example* 2.9. We again consider the block monoid $\mathscr{B}_8(19)$. The odd continued fraction of $\frac{19}{8}$ is $[2; 2, 1, 1, 1]$. The Euclidean Table for 19 and 8 is given below

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | 19 | – |
| -1 | 0 | 1 | 8 | – |
| 0 | 1 | 2 | 3 | 2 |
| 1 | 2 | 5 | 2 | 2 |
| 2 | 3 | 7 | 1 | 1 |
| 3 | 5 | 12 | 1 | 1 |
| 4 | 8 | 19 | 0 | 1 |

and $\mathscr{B}_8(19)$ has the irreducible blocks,

$$\begin{array}{rlll} k = -2: & u = 19 - 8t & \text{for} \quad 0 \leqslant t < 2 & \longrightarrow \quad \bar{1}^{19}\bar{8}^{0}; \bar{1}^{11}\bar{8}^{1} \\ k = 0: & u = 3 - 2t & \text{for} \quad 0 \leqslant t < 1 & \longrightarrow \quad \bar{1}^{3}\bar{8}^{2} \\ k = 2: & u = 1 - t & \text{for} \quad 0 \leqslant t < 1 & \longrightarrow \quad \bar{1}^{1}\bar{8}^{7} \\ k = 4: & u = 0 & & \longrightarrow \quad \bar{1}^{0}\bar{8}^{19}. \end{array}$$

The rest of the section will be devoted to the proof of Theorem 2.8. As we are translating Geroldinger's result in terms of the continued fraction of $\frac{n}{a}$, we first recognize the relation between the continued fraction of $\frac{n}{a}$ and that of $\frac{n}{q}$, where $q$ is the value described at the beginning of Section 2 in Method I. The following lemma is an elementary exercise in continued fractions (see [13, p.26, Exercise 7]).

**Lemma 2.10.** ([13]) *If $[a_0, a_1, \dots, a_m]$ is the continued fraction of $\frac{n}{a}$, then $[a_m, a_{m-1}, \dots, a_0]$ is the continued fraction of*

a) *$\frac{n}{q}$, where $q$ is the least positive integer with $aq + 1 \equiv 0 \pmod{n}$, when $m$ is odd, and*

b) *$\frac{n}{b}$, where $b$ is the least positive integer with $ab - 1 \equiv 0 \pmod{n}$, when $m$ is even.*

**Lemma 2.11.** *Let $[a_0, a_1, \dots, a_m]$ be the even continued fraction of $\frac{n}{a}$ and $\{s_k\}$ be the corresponding sequence of the remainders. Let $\frac{p_j}{q_j}$ denote the convergents for the continued fraction $[a_m, a_{m-1}, \dots, a_0]$ of $\frac{n}{q}$ with $p_{-2} = 0$; $p_{-1} - 1$. Then for each $j = -2, -1, 0, \dots, m$, $p_j = s_{m-j-2}$.*

Proof. By assumption, $p_{-2} = 0 = s_m = s_{m-(-2)-2}$ and $p_{-1} - 1 = s_{m-1} - s_{m-(-1)-2}$. Suppose that the result holds up to $j - 1$. Then

$$\begin{aligned} p_j &= p_{j-2} + a_{m-j} \cdot p_{j-1} = s_{m-j} + a_{m-j} \cdot s_{m-j-1} \\ &= s_{m-j-2} - a_{m-j} \cdot s_{m-j-1} + a_{m-j} \cdot s_{m-j-1} = s_{m-j-2}. \end{aligned}$$

□

We also need the following result.

**Proposition 2.12.** ([8, Proposition 9])

a) *If $N = \sum_{i=2k}^{j} c_i q_i$ with $0 \leqslant 2k \leqslant j < m$ and $c_{2k} > 0$, then $[N \cdot \frac{n}{q}] = \sum_{i=2k}^{j} c_i p_i$.*

b) *If $N = \sum_{i=2k+1}^{j} c_i q_i$ with $0 \leqslant 2k+1 \leqslant j < m$ and $c_{2k+1} > 0$, then $\left\lceil N \cdot \frac{n}{q} \right\rceil = \sum_{i=2k+1}^{j} c_i p_i - 1$.*

Proof of Theorem 2.8. Note that our theorem requires an odd continued fraction of $\frac{n}{a}$, while Proposition 2.1 does not require any condition on the length of the continued fraction of $\frac{n}{q}$. We will begin with the even continued fraction of $\frac{n}{a}$ with which we can rewrite Geroldinger's result using the previous two lemmas. We then will convert the result in terms of the odd continued fraction. Let $[a_0^e, a_1^e, \dots, a_{m^e}^e]$ be the even continued fraction of $\frac{n}{a}$ and let $b_j = a^e_{m^e-j}$. Then by Lemma 2.10, $[b_0, b_1, \dots, b_m]$ gives the continued fraction of $\frac{n}{q}$. We know that an irreducible block $\neq \bar{1}^n$ or $\bar{a}^n$ in $\mathscr{B}_a(n)$ is of the form $B(m_N)$, where $m_N = v_1(B(m_N))$ by Proposition 2.1. In order to prove the theorem, we will first show that the list of $m_N$ provided in Proposition 2.1, with 1 and $n$ added, is identical to that of $u$ in Theorem 2.8. Using Proposition 2.1 and 2.12,

$m_N$ with 1 and $n$ excluded, is described as follows.

$$\begin{aligned} m_N &= \left[N \cdot \frac{n}{q}\right] + 1 \\ &= \begin{cases} p_{j-1} + c_j \cdot p_j, & \text{if } 0 < c_j < b_{j+1},\ 0 \leqslant j < m^e \text{ with } j \text{ even} \\ p_j, & \text{if } j = -1 \text{ or } 0 \leqslant j < m^e \text{ with } j \text{ odd.} \end{cases} \end{aligned} \tag{1}$$

We rewrite (1) in terms of $a^e_k$ and $s^e_k$ using Lemma 2.11 and obtain

$$m_N = \begin{cases} s^e_{m^e-j-1} + c_j \cdot s^e_{m^e-j-2}, & \text{if } 0 < c_j < a^e_{m^e-j-1}, \\ & 0 \leqslant j < m^e \text{ with } j \text{ even} \\ s^e_{m^e-j-2}, & \text{if } j = -1 \text{ or } 0 \leqslant j < m^e \text{ with } j \text{ odd.} \end{cases} \tag{2}$$

Note that if $j$ is even, $m^e - j - 1$ is even and if $j$ is odd, $m^e - j - 2$ is even also, since $m^e$ is odd. Thus (2) can be simplified to

$$\begin{aligned} m_N &= \begin{cases} s^e_k + c_k \cdot s^e_{k-1}, & \text{if } 0 < c_k < a^e_k;\ 0 \leqslant k \leqslant m^e - 1 \text{ with } k \text{ even} \\ s^e_k, & \text{if } 0 \leqslant k \leqslant m^e - 1 \text{ with } k \text{ even} \end{cases} \\ &= s^e_k - c_k \cdot s^e_{k-1}, \text{ if } 0 \leqslant c_k < a^e_k;\ 0 \leqslant k \leqslant m^e - 1 \text{ with } k \text{ even} \\ &= s^e_{k-2} - a^e_k \cdot s^e_{k-1} + c_k \cdot s^e_{k-1}, \text{ if } 0 \leqslant c_k < a^e_k;\ 0 \leqslant k \leqslant m^e - 1 \text{ with } k \text{ even} \\ &= s^e_{k-2} - t_k \cdot s^e_{k-1}, \text{ if } 0 < t_k = a^e_k - c_k \leqslant a^e_k,\ 0 \leqslant k \leqslant m^e - 1 \text{ with } k \text{ even} \\ &= s^e_k - t_k \cdot s^e_{k+1}, \text{ if } 0 < t_k \leqslant a^e_{k+2},\ -2 \leqslant k \leqslant m^e - 3 \text{ with } k \text{ even.} \end{aligned} \tag{3}$$

To rewrite (3) in terms of the odd continued fraction of $\frac{n}{a}$, we divide into cases according to the length of the original continued fraction of $\frac{n}{a}$. Suppose first that it is even. Then the even continued fraction is the same as the original and the odd continued fraction is given by $[a^e_0, a^e_1, \dots, a^e_{m^e} - 1, 1]$. That is, with $m^o = m^e + 1$, $a^o_k = a^e_k$ for $k \leqslant m^o - 2$, $a^o_{m^o-1} = a^e_{m^e} - 1$ and $a^o_{m^o} = 1$. And accordingly, $s^o_k = s^e_k$ for $k \leqslant m^o - 2$. Thus (3) becomes

$$m_N = s^o_k - t_k \cdot s^o_{k+1}, \qquad 0 < t_k \leqslant a^o_{k+2},\ -2 \leqslant k \leqslant m^o - 4 \text{ with } k \text{ even.} \tag{4}$$

Recall that this list misses $n = s^o_{-2}$ and $0 = s^o_{m^o}$ each of which corresponds to the block $\bar{1}^n \bar{a}^0$ and $\bar{1}^0 \bar{a}^n$ respectively. To include $s^o_{-2}$ to the list, we modify the inequality $0 < t_k \leqslant a^o_{k+2}$ to $0 \leqslant t_k < a^o_{k+2}$ (excluding $a^o_{k+2}$ to avoid repetition). Doing so, we lose $s^o_{m^o-2}$. Allowing $k$ to be $m^o - 2$ will take care of the problem, since $a^o_{(m^o-2)+2} = a^o_{m^o} = 1$ and hence $t_{m^o-2}$ with $0 \leqslant t_{m^o-2} < 1$ can only be 0 whose corresponding value of $m_N$ is $s^o_{m^o-2}$. Finally, by adding $s^o_{m^o}$ to (4), we obtain the complete list of the multiplicities of $\bar{1}$ for the irreducible blocks in $\mathscr{B}_a(n)$:

$$m_N = \begin{cases} s^o_k - t_k \cdot s^o_{k+1}, & 0 \leqslant t_k < a^o_{k+2},\ -2 \leqslant k \leqslant m^o - 2 \text{ with } k \text{ even} \\ s^o_{m^o} \end{cases} \tag{5}$$

and this gives exactly the same set of values of $u$ in Theorem 2.8.

Now we suppose that the continued fraction of $\frac{n}{a}$ is in odd length. Then the odd continued fraction is the same as the original and hence the even continued fraction is of the form $[a_0^o, a_1^o, \dots, a_{m^o}^o - 1, 1]$. Thus with $m^e = m^o + 1$ $a_k^e = a_k^o$ for $k \leqslant m^e - 2$, $a_{m^e-1}^e = a_{m^o}^o - 1$ and $a_{m^e}^e = 1$ and accordingly, $s_k^e = s_k^o$ for $k \leqslant m^e - 2$. Then (3) becomes

$$m_N = \begin{cases} s_k^o - t_k \cdot s_{k+1}^o, & 0 < t_k \leqslant a_{k+2}^o, \\ & \text{for } -2 \leqslant k \leqslant m^e - 5 = m^o - 4 \text{ with } k \text{ even} \\ s_{m^o-2}^o - t_{m^o-2} \cdot s_{m^o-1}^o, & 0 < t_k \leqslant a_{m^o}^o - 1, \ \text{ for } k = m^e - 3 = m^o - 2. \end{cases} \tag{6}$$

Allowing $t_{m^o-2} = a_{m^o}^o$ to the second line of (6) yields

$$m_N = s_{m^o-2}^o - t_{m^o-2} \cdot s_{m^o-1}^o, \quad 0 < t_{m^o-2} \leqslant a_{m^o}^o$$

by which 0 has been added to the list. This is because $s_{m^o-2}^o = a_{m^o}^o$ and $s_{m^o-1}^o = 1$ by (3) in Definition 2.5 and hence with $t_{m^o-2} = a_{m^o}^o$, $m_N = s_{m^o-2}^o - a_{m^o}^o \cdot s_{m^o-1}^o = a_{m^o}^o - a_{m^o}^o = 0$. Now (6) becomes

$$m_N = s_k^o - t_k \cdot s_{k+1}^o, \quad 0 < t_k \leqslant a_{k+2}^o, \quad \text{for } -2 \leqslant k \leqslant m^o - 2 \text{ with } k \text{ even.} \tag{7}$$

It remains to add $n = s_{-2}^o$ to the list. This can be done, as in the first case, by modifying the inequality $0 < t_k \leqslant a_{k+2}^o$ in (7) to $0 \leqslant t_k < a_{k+2}^o$. As a result, we obtain

$$m_N = \begin{cases} s_k^o - t_k \cdot s_{k+1}^o, & 0 \leqslant t_k < a_{k+2}^o, -2 \leqslant k \leqslant m^o - 2 \text{ with } k \text{ even} \\ s_{m^o}^o & \end{cases}$$

which is identical to (5). This proves the part of the theorem that describes values of $u$.

To prove the statements on the values of $v$ and $\tau$, we divide the argument into cases. For ease of description, we let $[a_0, a_1, \dots, a_m]$ be the odd continued fraction of $\frac{n}{a}$. We know that when $k = -2$, the corresponding value of $u$ is given by $s_{-2} - t \cdot s_{-1} = n - at$, for $0 \leqslant t < a_0$. Note that $y_{-2} + t \cdot y_{-1} = t$. For each $0 \leqslant t < a_0$, we have $n = at + (n - at) = a \cdot (y_{-2} + t \cdot y_{-1}) + u$. Since $t < a_0 = [\frac{n}{a}]$, we have $a \leqslant u$. Thus, by Proposition 2.3, each $t$ yields the Type 2 irreducible $\bar{1}^u \bar{a}^v$ with $u = s_{-2} - t \cdot s_{-1}$ and $v = y_{-2} + t \cdot y_{-1}$. The corresponding value of $\tau$ is 1 which is equal to $x_{-2} + t \cdot x_{-1}$ as desired. Now consider the case where $0 \leqslant k \leqslant m - 2$ with $k$ even. By 5 in Remarks 2.6, we have

$$x_k \cdot n = a \cdot y_k + s_k \tag{8}$$

$$x_{k+1} \cdot n = a \cdot y_{k+1} - s_{k+1}. \tag{9}$$

Multiplying (9) by $t_k$ and adding it to (8) yields

$$(x_k + t_k \cdot x_{k+1})n = a(y_k + t_k \cdot y_{k+1}) + (s_k - t_k \cdot s_{k+1}), \quad 0 \leqslant t_k < a_{k+2}. \tag{10}$$

Notice that (10) yields the block $\bar{1}^u \bar{a}^v$ with $u = s_k - t_k \cdot s_{k+1}$, which has been shown to be irreducible. The corresponding $v$ and $\tau$ are given respectively as $v = y_k + t_k \cdot y_{k+1}$ and $\tau = x_k + t_k \cdot x_{k+1}$ as desired. Lastly, when $k = m$, (8) becomes $n \cdot a = a \cdot n + 0$ which corresponds to the irreducible block $\bar{1}^0 \bar{a}^n$ with $v = n = y_m$ and $\tau = a = x_m$. This completes the proof. □

The value of the description of the irreducibles given in Theorem 2.8 is related to simplicity and the well-known computational efficiency of the basic Euclidean Algorithm. Obviously, the basic calculation can be done quickly by machines for very large values of $n$. Also, we will see in the next two sections how this description of the irreducibles using the Euclidean Table provides us additional efficient algorithms for determining the elasticity of the block monoid $\mathscr{B}_a(n)$.

## 3. The elasticity of $\mathscr{B}_a(n)$

In this section, some of the previous results regarding the general relation between the elasticity and the cross number will be reviewed. We will then show that the elasticity of the block monoid $\mathscr{B}_a(n)$ can be easily obtained using the Euclidean Table for $n$ and $a$. The results of [6] have shown that there is a strong connection between the elasticity and the cross number. The following proposition describes a lower and upper bound for the elasticity in terms of the cross numbers.

**Proposition 3.1.** ([6, Corollary 1.7]) *Given a block monoid $\mathscr{B}(G,S)$, set*

$$M(\mathscr{B}(G,S)) = \max\{k(B) : \ B \text{ is an irreducible block in } \mathscr{B}(G,S)\},$$
$$m(\mathscr{B}(G,S)) = \min\{k(B) : \ B \text{ is an irreducible block in } \mathscr{B}(G,S)\}.$$

*Then*

$$\max\{M(\mathscr{B}(G,S)), m(\mathscr{B}(G,S))^{-1}\} \leqslant \rho(\mathscr{B}(G,S)) \leqslant M(\mathscr{B}(G,S))m(\mathscr{B}(G,S))^{-1}.$$

We immediately have the following.

**Corollary 3.2.**

(i) *If $M(\mathscr{B}(G,S)) = 1$, then $\rho(\mathscr{B}(G,S)) = m(\mathscr{B}(G,S))^{-1}$.*
(ii) *If $m(\mathscr{B}(G,S)) = 1$, then $\rho(\mathscr{B}(G,S)) = M(\mathscr{B}(G,S))$.*

The elasticity of the block monoid $\mathscr{B}_a(n)$ has been studied in [7] where the following result can be found.

**Proposition 3.3.** ([7, Theorem 3.2]) *For each irreducible block $B$ of $\mathscr{B}_a(n)$, $k(B) \leqslant 1$. Thus $M_a(n) = 1$ and $\rho(\mathscr{B}_a(n)) = m_a(n)^{-1}$, where $M_a(n)$ and $m_a(n)$ denotes $M(\mathscr{B}_a(n))$ and $m(\mathscr{B}_a(n))$ respectively.*

Therefore, to determine the elasticity of $\mathscr{B}_a(n)$, it suffices to compute the minimum cross number of the irreducibles. We now describe how to determine this minimum value and state a result for the special case where $\gcd(a,n) = 1$.

**Theorem 3.4.** *Given $n$ and $1 < a < n$ with $\gcd(a,n) = 1$, let $l$ be the first integer $\geqslant 0$ for which $y_l \geqslant s_l$ in the Euclidean Table for $n$ and $a$. Then*

$$m_a(n) = \begin{cases} \frac{y_l+s_l}{n} & \text{if } l \text{ is even} \\ \frac{y_l\ \ 1+s_l\ \ 1}{n} & \text{if } l \text{ is odd} \end{cases}$$

*and hence*

$$\rho(\mathscr{B}_a(n)) = \begin{cases} \frac{n}{y_l+s_l} & \text{if } l \text{ is even} \\ \frac{n}{y_{l-1}+s_{l-1}} & \text{if } l \text{ is odd.} \end{cases}$$

We only need to prove the first part of the theorem for $m_a(n)$. Notice that for a block $B = \bar{1}^u\bar{a}^v$ in $\mathscr{B}_a(n)$, the cross number $k(B)$ is given by $\frac{u+\imath}{n}$, since $\gcd(a,n) = 1$. Thus to find the minimum cross number, it is enough to find the minimum value of the numerator. This leads us to the following definitions.

**Definition 3.5.** Given a block $B$ in $\mathscr{B}(\mathbb{Z}_n, S)$, set

$$K_2(a,n) := \min\{|B| :\ B \in \mathscr{B}_a(n)\}.$$

The reader should note under the hypothesis above that $|B| = n \cdot k(B)$. The next Corollary now follows easily from Definition 3.5 and Proposition 3.3.

**Corollary 3.6.** *For $n$ and $a$ as in* Theorem 3.4, *we have $m_a(n) = \frac{K_2(a.}{\imath}$ and hence $\rho(\mathscr{B}_a(n)) = \frac{n}{K_2(a,n)}$.*

Proof of Theorem 3.4. Theorem 2.8 provides the description of the irreducibles blocks in $\mathscr{B}_a(n)$.

Let $B_{k,t_k}$ denote the irreducible block $\bar{1}^{s_k - t_k s_{k+1}}\bar{a}^{y_k + t_k y_{k+1}}$, for $0 \leqslant t_k < a_{k+2}$ and $-2 \leqslant k \leqslant m$ with $k$ even, where $[a_0, a_1, \dots, a_m]$ is the odd continued fraction of $\frac{n}{a}$. For each $k$ and $t_k$, we consider

$$\begin{aligned} K_{k,t_k} &:= |B_{k,t_k}| \\ &= y_k + s_k + t_k(y_{k+1} - s_{k+1}), \qquad 0 \leqslant t_k < a_{k+2}. \end{aligned}$$

Note that $K_{k,0} = y_k + s_k$. We need to show that $K_2(a,n) = K_{l,0}$, if $l$ is even or $K_2(a,n) = K_{l-1,0}$, if $l$ is odd. Notice that $y_k$ is increasing and $s_k$ is decreasing and hence $y_k - s_k$ is increasing as $k$ increases. By the assumption, it follows that $y_k - s_k < 0$, if $k < l$ and $y_k - s_k \geqslant 0$, if $k \geqslant l$. With this in mind, we will prove the theorem by dividing it into cases. Suppose first that $l$ is even. For $k$ even with $k < l - 2$,

$$\begin{aligned} K_{k,t_k} &= y_k + s_k + t_k(y_{k+1} - s_{k+1}) \\ &> y_k + s_k + a_{k+2}(y_{k+1} - s_{k+1}) \qquad (\text{since } t_k < a_{k+2};\ y_{k+1} - s_{k+1} < 0) \\ &= y_{k+2} + s_{k+2} > y_{k+2} + s_{k+2} + t_{k+2}(y_{k+3} - s_{k+3}) \\ &= K_{k+2,t_{k+2}}, \end{aligned} \tag{11}$$

since $t_{k+2} \geqslant 0$ and $y_{k+3} - s_{k+3} < 0$. Thus $K_{k,t_k}$ is decreasing as $k$ increases up to $l-2$. For $k = l-2$,

$$\begin{aligned} K_{l-2,t_{l-2}} &= y_{l-2} + s_{l-2} + t_{l-2}(y_{l-1} - s_{l-1}) \\ &> y_{l-2} + s_{l-2} + a_l(y_{l-1} - s_{l-1}) \quad (\text{since } t_{l-1} < a_l;\ y_{l-1} - s_{l-1} < 0) \\ &= y_l + s_l \\ &= K_{l,0} \end{aligned}$$

which is less than or equal to $K_{l,t_l} = y_l + s_l + t_l(y_{l+1} - s_{l+1})$, since $t_l \geqslant 0$; $y_{l+1} - s_{l+1} > 0$. For $k$ even with $k \geqslant l$, we have

$$\begin{aligned} K_{k,0} &= y_k + s_k \leqslant y_k + s_k + t_k(y_{k+1} - s_{k+1}) && (\text{since } t_k \geqslant 0;\ y_{k+1} - s_{k+1} > 0) \\ &< y_k + s_k + a_{k+2}(y_{k+1} - s_{k+1}) && (\text{since } t_k < a_{k+2};\ y_{k+1} - s_{k+1} > 0) \\ &= y_{k+2} + s_{k+2} \\ &\leqslant y_{k+2} + s_{k+2} + t_{k+2}(y_{k+3} - s_{k+3}), && (\text{since } t_{k+2} \geqslant 0;\ y_{k+3} - s_{k+3} > 0) \\ &= K_{k+2,t_{k+2}}, \end{aligned} \tag{12}$$

which shows that $K_{k,t_k}$ is increasing as $k$ increases from $l$. Hence $K_2(a,n) = K_{l,0} = y_l + s_l$. Suppose now that $l$ is odd. A similar argument shows that (11) holds for every $k$ even with $k < l-1$ and (12) holds for $k$ even with $k \geqslant l+1$. Thus $K_{k,t_k}$ is decreasing as $k$ increases up to $l-1$ and is increasing as $k$ increases from $l+1$. When $k = l-1$,

$$\begin{aligned} K_{l-1,0} &= y_{l-1} + s_{l-1} \leqslant y_{l-1} + s_{l-1} + t_{l-1}(y_l - s_l) && (\text{since } t_{l-1} \geqslant 0;\ y_l - s_l \geqslant 0) \\ &< y_{l-1} + s_{l-1} + a_{l+1}(y_l - s_l) && (\text{since } t_{l-1} < a_{l+1};\ y_l - s_l \geqslant 0) \\ &= y_{l+1} + s_{l+1} \\ &\leqslant y_{l+1} + s_{l+1} + t_{l+1}(y_{l+2} - s_{l+2}) && (\text{since } t_{l+1} \geqslant 0;\ y_{l+2} - s_{l+2} > 0) \\ &= K_{l+1,t_{l+1}}. \end{aligned}$$

Thus $K_2(a,n) = K_{l-1,0} = y_{l-1} + s_{l-1}$. □

For an atomic monoid $H$ which contains a nonunit and some $k \in \mathbb{N}$, we set

$$\rho_k(H) = \sup\{\sup L :\ L \in \mathscr{L}(H),\ \min L \leq k\} \in \mathbb{N} \cup \{\infty\}.$$

Using $\rho_k$, here is a further interpretation of the invariant $K_2(a,n)$ which may be of interest.

**Lemma 3.7.** *Let $n \in \mathbb{N}_{\geq 2}$, $a \in [1, n-1]$ with $\gcd(a,n) = 1$ and $K_2(a,n) = \min\{|B| :\ B \in \mathscr{B}_a(n)\}$. Then*

$$\rho_k(\mathscr{B}_a(n)) \leq k\rho(\mathscr{B}_a(n)) \leq \frac{kn}{K_2(a,n)}$$

*for every $k \in \mathbb{N}$. Moreover, there is some $N \in \mathbb{N}$ such that*

$$\rho_{kN}(\mathscr{B}_a(n)) = \frac{knN}{K_2(a,n)}$$

*for every $k \in \mathbb{N}$.*

Proof. The first inequality follows from [10, Theorem 3.4.10.4] (with $H$ $\mathscr{B}_a(n)$). Since $\mathscr{B}_a(n)$ is finitely generated, it has accepted elasticity, and hence the second assertion follows from [10, Proposition 1.4.2.3] and Corollary 3.6. □

Our next example illustrates an application of our results.

*Example* 3.8. Consider $\mathscr{B}_{605}(2116)$. There are more than 100 irreducibles in this monoid. However, the elasticity $\frac{n}{y_0+s_0} = \frac{2116}{304}$ is obtained immediately by using Theorem 3.4 and the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | 2116 | |
| -1 | 0 | 1 | 605 | |
| 0 | 1 | 3 | 301 | 3 |
| 1 | 2 | **7** | **3** | 2 |
| 2 | 201 | 703 | 1 | 100 |
| 3 | 404 | 1413 | 1 | 2 |
| 4 | 605 | 2116 | 0 | 1 |

Next, we will consider the case where $a$ and $n$ are not necessarily relatively prime. As briefly mentioned at the beginning of Section 2, the study of the block monoids of the form $\mathscr{B}(\mathbb{Z}_n, \{\bar{a}, b\})$ can be reduced to the case where $b = 1$ and $\gcd(a,n) = 1$. This is due to the following theorem by Geroldinger.

**Proposition 3.9.** ([8, Proposition 5.1]) *Given $n \geqslant 3$ and $1 \quad a, b < n$, l t*

$$n' = \frac{n \cdot \gcd(a,b,n)}{\gcd(a,n) \cdot \gcd(b,n)}.$$

*Then there exists $1 < a' < n'$ with $\gcd(a',n') = 1$ such that $\mathscr{B}(\mathbb{Z}_n, \{a,b\}) \sim \mathscr{B}_{a'}(n')$.*

The explicit description of the value $a'$ is given in the proof of the theorem (see the proof for details). Applying Theorem 3.8 to the case where $b = 1$ yields $a' = \frac{a}{\gcd(a,n)}$. Thus we have the following.

**Corollary 3.10.** *Given $n$ and $1 < a < n$, let $a' = \frac{a}{\gcd(a,n)}$ and $n' = \frac{n}{\gcd\ a,\imath}$. Then $\mathscr{B}_a(n) \cong \mathscr{B}_{a'}(n')$.*

Note that $\gcd(a',n') = 1$. Thus the elasticity of $\mathscr{B}_{a'}(n')$ and hence the elasticity of $\mathscr{B}_a(n)$ can be easily obtained by using the Euclidean Table for $n'$ and $a'$ by Theorem 3.4. Our goal is to describe the result in terms of $n$ and $a$.

not of $n'$ and $a'$. Let $[a_0, a_1, \ldots, a_m]$ and $[a'_0, a'_1, \ldots, a'_m]$ be the odd continued fraction of $\frac{n}{a}$ and $\frac{n'}{a'}$ respectively. And let $\{s_k\}$, $\{x_k\}$; $\{y_k\}$ and $\{s'_k\}$, $\{x'_k\}$; $\{y'_k\}$ respectively denote the corresponding sequences for $\frac{n}{a}$ and for $\frac{n'}{a'}$. The key is to notice that $\frac{n}{a} = \frac{n'}{a'}$ and hence both of the fractions have the same odd continued fraction. That is, $a_k = a'_k$ for every $0 \leqslant k \leqslant m$. Recall that $x'_{-2} = 1 = x_{-2}$; $x'_{-1} = 0 = x_{-1}$ and $y'_{-2} = 0 = y_{-2}$; $y'_{-1} = 1 = y_{-1}$. Thus, by the recursive definition given in Definition 2.5, we must have $x_k = x'_k$ and $y_k = y'_k$ for every $k \geqslant -2$. Then the Euclidean Table for $n$ and $a$ is the same as the Euclidean Table for $n'$ and $a'$ possibly except for the column with the remainders. To see how $\{s_k\}$ and $\{s'_k\}$ are related, consider the division

$$s_{k-2} = s_{k-1} \cdot a_k + s_k.$$

Let $d = \gcd(a, n)$. Since $d|(n = s_{-2})$ and $d|(a = s_{-1})$, $d$ divides $s_0$. Then, by induction, we know that $d$ divides $s_k$ for every $0 \leqslant k \leqslant m$. Dividing each side of the above division by $d$, we obtain,

$$\frac{s_{k-2}}{d} = \frac{s_{k-1}}{d} \cdot a_k + \frac{s_k}{d}. \tag{13}$$

Note that $s_k < s_{k-1}$ implies $\frac{s_k}{d} < \frac{s_{k-1}}{d}$ and hence (13) yields the Euclidean division. Since $s'_{-2} = n' = \frac{n}{d} = \frac{s_{-2}}{d}$ and $s'_{-1} = a' = \frac{a}{d} = \frac{s_{-1}}{d}$, we must have $s'_0 = \frac{s_0}{d}$. Once again, by induction, $s'_k = \frac{s_k}{d}$ for every $0 \leqslant k \leqslant m$. We now apply Theorem 3.4 to the block monoid $\mathscr{B}_{a'}(n')$ and obtain

$$K_2(a', n') = \begin{cases} y'_l + s_l{}' & \text{if } l \text{ is even} \\ y'_{l-1} + s'_{l-1} & \text{if } l \text{ is odd,} \end{cases} \tag{14}$$

where $l$ is the first integer such that $y'_l \geqslant s'_l$. Note that $\rho(\mathscr{B}_a(n)) = \rho(\mathscr{B}_{a'}(n'))$ by Corollary 3.9, where each is given respectively by $\frac{n}{K_2(a,n)}$ and $\frac{n'}{K_2(a',n')}$. Thus we have $\frac{n}{K_2(a,n)} = \frac{n'}{K_2(a',n')} = \frac{\frac{n}{d}}{K_2(a',n')}$ which implies

$$K_2(a, n) = d \cdot K_2(a', n'). \tag{15}$$

With the relation between the sequences described above, we may rephrase (14) as follows.

$$K_2(a, n) = \begin{cases} dy_l + s_l & \text{if } l \text{ is even} \\ dy_{l-1} + s_{l-1} & \text{if } l \text{ is odd,} \end{cases}$$

where $l$ is the first integer such that $y_l \geqslant \frac{s_l}{d}$. Summarizing, we obtain the following.

**Corollary 3.11.** *Given $n$ and $1 < a < n$, let $d = \gcd(a, n)$ and let $l$ be the first integer $\geqslant 0$ for which $y_l \geqslant \frac{s_l}{d}$ in the Euclidean Table for $n$ and $a$. Then*

$$\rho(\mathscr{B}_a(n)) = \begin{cases} \frac{n}{dy_l + s_l} & \textit{if } l \textit{ is even} \\ \frac{n}{dy_{l-1} + s_{l-1}} & \textit{if } l \textit{ is odd.} \end{cases}$$

*Example* 3.12. Let $n = 2^9 = 512$ and $a = 326$. Consider the block monoid $\mathscr{B}_{326}(512)$. Note that $d = \gcd(326, 512) = 4$. The Euclidean Table given below shows that $y_k$ first exceeds $\frac{s_k}{4}$ at $k = 1$. Thus, the elasticity of $\mathscr{B}_{326}(512)$ is given by $\frac{512}{4y_0+s_0} = \frac{512}{8+40} = \frac{32}{3}$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | 512 | |
| -1 | 0 | 1 | 326 | |
| 0 | 1 | 2 | 40 | 2 |
| 1 | 5 | **11** | **36** | 5 |
| 2 | 6 | 13 | 4 | 1 |
| 3 | 53 | 115 | 4 | 8 |
| 4 | 59 | 126 | 0 | 1 |

## 4. The complete set of elasticities

In this section, we will fix a prime $p$ and consider the set of the elasticities of $\mathscr{B}_a(p)$ for $1 < a < p$. In general, let $\Upsilon_2(\mathbb{Z}_n)$ denote the set of the elasticities of $\mathscr{B}_a(n)$ for $1 < a < n$. We know that the elasticity of $\mathscr{B}_a(n)$ is given by $\frac{n}{K_2(a,n}$ by Theorem 3.4. Hence

$$\Upsilon_2(\mathbb{Z}_n) := \left\{\tfrac{n}{K_2(a,n)} : 1 < a < n\right\}.$$

Since $n$ is fixed, $\Upsilon_2(\mathbb{Z}_n)$ is basically determined by the values of $K_2(a,n)$ for $1 < a < n$. With this in mind, given $n$, let

$$\Upsilon^2(\mathbb{Z}_n) := \left\{K_2(a,n) : 1 < a < n\right\}.$$

For ease of notation, we write $\Upsilon^2(\mathbb{Z}_n) = \Upsilon^2(n)$.

Throughout this section, we will focus on the case where $n = p$ is a prime. Using the algorithm based on Theorem 3.4, $\Upsilon^2(p)$ can be computed fairly fast (even for large primes) when run by a machine. Appendix A shows the list of $\Upsilon^2(p)$'s for $5 \leqslant p \leqslant 97$.

The structure of $\Upsilon^2(p)$ has been studied by Chapman and Smith in [7] (Min($p$) is their notation). They observed that each row of Table 1 begins with a string of consecutive numbers followed by a series of 'gaps'. Both of the observations, the length of the string and the top values which determine the gaps, become of interest. The following are two previous results on each part, described in our notation.

**Proposition 4.1.**

(1) ([7, Theorem 4.5]) $\{2, 3, \ldots, s\} \subseteq \Upsilon^2(p)$ *for all prime* $p > s^2 - s$.

(2) ([7, Theorem 4.7]) *Let $p$ be a prime and let $a$ be an integer with $3 \leqslant a \leqslant p-1$ and $a \neq \frac{1}{2}(p+1)$. Then $K_2(a,p) \leqslant \frac{1}{3}(p+4)$.*

It is observed that $\frac{p+1}{2} = K_2(2,p) = K_2(2^{-1},p)$ and $[\frac{p+4}{3}] = K_2(3,p)$ are always in $\Upsilon^2(p)$. [7, Theorem 4.7] verifies that $\frac{p+1}{2}$ is given only by $a = 2$ and $a = 2^{-1} = \frac{p+1}{2}$ and that for any other $a$, $K_2(a,p) \leqslant [\frac{p+4}{3}]$. From this, it follows that:

**Proposition 4.2.** ([7, Theorem 4.8]) *The maximum value in $\Upsilon^2(p)$ is $\frac{p+1}{2}$ and the second largest value is $[\frac{p+4}{3}]$, for $p > 5$.*

Before we move on, we provide an alternate proof to Proposition 4.1(1) using the Euclidean Table.

Alternate Proof of Proposition 4.1(1). Let $t = s-1$ and $a = p-t$. The assumption $p > s^2 - s$ is then equivalent to $p > t^2 + t$. This implies that $\frac{p}{t} > t+1$ and hence $[\frac{p-t}{t}] = [\frac{p}{t} - 1] \geqslant t$. Note that $t^2 \geqslant t$ holds for every $t \geqslant 1$ which, when combined with $p > t^2 + t$, yields $p - t > t$. Thus, the Euclidean Table for $p$ and $p - t$ is given as below

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $p$ | – |
| -1 | 0 | 1 | $p-t$ | – |
| 0 | 1 | 1 | $t$ | 1 |
| 1 | $[\frac{p-t}{t}]$ | $[\frac{p}{t}]$ | $r$ | $[\frac{p-t}{t}]$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and we have $y_1 = [\frac{p}{t}] > [\frac{p}{t} - 1] \geqslant t > r = s_1$. Hence $K_2(a,p) = y_0 + s_0 = t + 1 = s$. □

In the rest of this section, we will be investigating further the largest values in $\Upsilon^2(p)$. We first consider the case where $K_2(a,p) = a$ which is observed in $K_2(\frac{p+1}{2}, p) = \frac{p+1}{2}$ and for other large values as well. The following proposition provides a necessary condition for this to be the case.

**Proposition 4.3.** *Let a prime $p$ and $1 < a < p$ be given. If $K_2(a,p) = a$, then $q + r = a$, where $p = aq + r$ is the Euclidean Division.*

Proof. We will prove the theorem by showing that $K_2(a,p)$ is given by $y_0 + s_0 = q + r$. The result will then immediately follow. Suppose that $K_2(a,p) = y_l + s_l$, for some $l \geqslant 2$. Then, in particular, we must have $y_1 = q[\frac{a}{r}] + 1 < a - r[\frac{a}{r}] = s_1$ which implies that $(q + r)[\frac{a}{r}] < a - 1$. This is a contradiction, since $q + r \geqslant K_2(a,p) = a$ and $[\frac{a}{r}] \geqslant 1$. □

Considering Proposition 4.3, we note that combining the division $p = aq + r$ and $q + r = a$ yields that $a = \frac{p+q}{q+1}$. We will show that every $a$ in this form yields $K_2(a,p) = a$ for certain consecutive values of $q$ under a special condition on $p$. Given an integer $t \geqslant 2$, set $m_t = \operatorname{lcm}\{1, 2, \dots, t\}$. Consider the case where $p \equiv 1 \pmod{m_t}$.

**Lemma 4.4.** *Suppose that $p \equiv 1 \pmod{m_t}$. Then for every $s < t - 1$ $(s+1)|(p+s)$.*

Proof. Write $p = m_t q + 1$. Then $p + s = m_t q + s + 1$. Assuming $s \leqslant t - 1$, or equivalently $s + 1 \leqslant t$, yields $(s+1)|m_t$ and the result follows. □

**Proposition 4.5.** *Let $p$ be such that $p \equiv 1 \pmod{m_t}$. Let $a_s - \frac{p+s}{s+1}$, for ever $1 \leqslant s \leqslant t - 1$. Then $K_2(a_s, p) = a_s$.*

Proof. Solving $a_s = \frac{p+s}{s+1}$ for $p$, we obtain $p \quad a_s s + (a_s - s)$. Clearly $a_s - s < a_s$. Note that for $t \geqslant 4$, $p \geqslant m_t \geqslant t(t-1) \cdot 2 \geqslant (s+1)s \cdot 2 = 2s^2 + 2s$. This implies that $a_s - 2s = \frac{p+s}{s+1} - 2s = \frac{p-2s^2-s}{s+1} > 0$ and hence $a_s - s > s$. Thus the Euclidean Table for $p$ and $a_s$ is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $p$ | |
| -1 | 0 | 1 | $a_s$ | |
| 0 | 1 | $s$ | $a_s - s$ | $s$ |
| 1 | 1 | $s+1$ | $s$ | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

which shows that $K_2(a_s, p) = s + (a_s - s) = a_s$. When $t = 2$, the smallest prime $p$ with $p \equiv 1 \pmod{m_2}$ is $p = 3$ and the only possible $s$ is 1. This gives $a_s = \frac{3+1}{1+1} = 2$ and we have $a_s - s \geqslant s$. For $p \geqslant 5$ with $p \equiv 1 \pmod{m_2}$, $a_s - s > s$ always follows. The Euclidean table for $p$ and $a_s$ is then in the same form as the above and hence $K_2(a_s, p) = a_s$. Let $t - 3$. Then $s \leqslant 2$. For $p \geqslant 13$ with $p \equiv 1 \pmod{m_3}$, $a_s - s \geqslant s$ always for any $s \leqslant 2$ and hence the result follows. Now let $p = 7$. If $s = 1$, then the corresponding $a_s = a_1 - \frac{7+1}{1+1} = 4$ and so $a_s - s > s$ holds. Again the Euclidean table for $p$ and $a_s$ is the same as the above and hence the result follows. If $s = 2$, then $a_s = 3$. From the Euclidean Table for 7 and 3, we easily obtain $K_2(a_s, p) = a_s$. □

We provide an example which illustrates results in Proposition 4.1 and Proposition 4.5.

*Example* 4.6. Let $p = 421$. Below is the full set of $\Upsilon^2(421)$.

$$\begin{aligned}\Upsilon^2(421) = \{&\mathit{2}, \mathit{3}, \mathit{4}, \mathit{5}, \mathit{6}, \mathit{7}, \mathit{8}, \mathit{9}, \mathit{10}, \mathit{11}, \mathit{12}, \mathit{13}, \mathit{14}, \mathit{15}, \mathit{16}, \mathit{17}, \mathit{18}, \mathit{19}, \mathit{20}, \mathit{21},\\ &22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39,\\ &40, 41, 43, 44, 47, 49, 53, 57, \mathbf{61}, 63, \mathbf{71}, \mathbf{85}, 86, \mathbf{106}, \mathbf{141}, \mathbf{211}\}.\end{aligned}$$

Note that $421 \equiv 1 \pmod{420}$ and $420 = m_7$. Thus by Proposition 4.5, for every $1 \leqslant s \leqslant 6$, $a_s = \frac{p+s}{s+1}$ yields $K_2(a_s, p)$ (those values in bold-face) with $K_2(a_s, p) = a_s$. These are not the 6 largest values, but do give 6 of the top 8 values in $\Upsilon^2(421)$. On the other hand, note that every $s \leqslant 21$ satisfies the condition $p > s^2 - s$. Thus the string of the first twenty values in $\Upsilon^2(421)$ (those in italic) are obtained by Proposition 4.1.

We return to the problem of determining the top values in $\Upsilon^2(p)$. We first observe the following, summarizing what gives the two largest values.

**Remark 4.7.**

(i) For every prime $p$, $p \equiv 1 \pmod 2$ and $\frac{p-1}{2}+1 = \left[\frac{p}{2}\right]+1$ gives the maximum value $\frac{p+1}{2}$ in $\Upsilon^2(p)$.

(ii) Given a prime $p$, either $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. In each case, $\frac{p-1}{3} + 1 = \left[\frac{p}{3}\right] + 1$ and $\frac{p-2}{3} + 2 = \left[\frac{p}{3}\right] + 2$ respectively gives the second largest value $\left[\frac{p+4}{3}\right]$ in $\Upsilon^2(p)$.

Thus it seems that the first and the second largest values in $\Upsilon^2(p)$ are determined respectively by what $p$ is congruent to modulo 2 and modulo 3. We will write $\mathrm{Mod}[p, t]$ to denote the least positive residue of $p$ modulo $t$. Through the next two propositions, we will see that for each $t \geqslant 2$, $\mathrm{Mod}[p, t]$ yields at least one value in $\Upsilon^2(p)$ of the form $\left[\frac{p}{t}\right] + r$, for some $r \leqslant \mathrm{Mod}[p, t]$.

**Proposition 4.8.** *Given a prime $p$ and an integer $t \geqslant 2$ with $p \geqslant t^2$,*

$$\left[\frac{p}{t}\right] + j \quad \textit{and} \quad \left[\frac{p}{t}\right] + 1 \tag{16}$$

*are always in $\Upsilon^2(p)$ where $j = \mathrm{Mod}[p, t]$. Each is given respectively by $a = t$ and $a - \frac{(t\quad 1)p+j}{t}$.*

Proof. Let $p \equiv j \pmod t$. Since $p \geqslant t^2$ and $t > j$, it follows that $y_0 = \frac{p-j}{t} \geqslant t\quad 1 \geqslant j = s_0$ in the Euclidean Table for $p$ and $t$ and hence $K_2(t, p) = \frac{p-j}{t} + j$, as desired. Let $a = \frac{(t-1)p+j}{t} = p - \frac{p-j}{t}$. Then $a - \frac{p-j}{t} = \frac{(t-2)p+j}{t} > 0$ due to the assumption $t \geqslant 2$. Thus the Euclidean Table for $p$ and $a$ is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $p$ | $-$ |
| -1 | 0 | 1 | $\frac{(t-1)p+j}{t}$ | $-$ |
| 0 | 1 | 1 | $\frac{p-j}{t}$ | 1 |
| 1 | 1 | $t$ | $j$ | $t-1$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

which shows that $K_2(a,p) = \frac{p-j}{t} + 1$. □

In particular, the first part of Proposition 4.8 tells us immediately what $K_2(a,p)$ is, for every $a$ with $a \leqslant \sqrt{p}$.

**Corollary 4.9.** *Given a prime $p$ and $a \leqslant \sqrt{p}$, $K_2(a,p) = \left[\frac{p}{t}\right] + \operatorname{Mod}[p,a]$.*

*Example* 4.10. Let $p = 79$. Below is the list of the values in $\Upsilon^2\,(79)$ obtained by using Proposition 4.8, for $2 \leqslant t \leqslant 6 < \left[\sqrt{79}\right]$.

$$t = 2 \qquad 79 \equiv 1 \pmod{2} \quad \longrightarrow \quad \left[\frac{79}{2}\right] + 1 = 40$$

$$t = 3 \qquad 79 \equiv 1 \pmod{3} \quad \longrightarrow \quad \left[\frac{79}{3}\right] + 1 = 27$$

$$t = 4 \qquad 79 \equiv 3 \pmod{4} \quad \longrightarrow \quad \begin{cases} \left[\frac{79}{4}\right] + 3 = 22 \\ \left[\frac{79}{4}\right] + 1 = 20 \end{cases}$$

$$t = 5 \qquad 79 \equiv 4 \pmod{5} \quad \longrightarrow \quad \begin{cases} \left[\frac{79}{5}\right] + 4 = 19 \\ \left[\frac{79}{5}\right] + 1 = 16 \end{cases}$$

$$t = 6 \qquad 79 \equiv 1 \pmod{6} \quad \longrightarrow \quad \left[\frac{79}{6}\right] + 1 = 14.$$

Consider the special case where $p \equiv t-1 \pmod{t}$. Then by Proposition 4.8, we obtain two values (unless $t = 2$), $\left[\frac{p}{t}\right] + (t-1)$ and $\left[\frac{p}{t}\right] + 1$. Our next proposition shows that we may obtain values other than these two.

**Proposition 4.11.** *Suppose that $p \equiv t-1 \pmod{t}$. Then for any $s \mid (t-1)$,*

$$\left[\frac{p}{t}\right] + \frac{t-1}{s} \in \Upsilon^2\,(p) \tag{17}$$

*and is given by $a = \frac{s(p+1)}{t}$.*

Proof. Note that $p + 1 \equiv 0 \pmod{t}$ implies $t \mid (p+1)$. For each $s \mid (t-1)$, let $a_s = \frac{s(p+1)}{t}$. Then from the Euclidean Table for $p$ and $a_s$ given below,

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $p$ | – |
| -1 | 0 | 1 | $\frac{s(p+1)}{t}$ | – |
| 0 | 1 | $\frac{t-1}{s}$ | $\frac{p-(t-1)}{t}$ | $\frac{t-1}{s}$ |
| 1 | $s$ | $t$ | $\frac{ts}{s}=t$ | $s$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

we have $y_1 \geqslant s_1$ and hence $K_2(a_s, p) = y_0 + s_0 = \frac{p-(t-1)}{t} + \frac{t-1}{s}$ as in the statement. □

For instance, in Example 4.10, $79 \equiv 4 \pmod 5$ yields one more value in $\Upsilon^2(79)$ other than 19 and 16, namely, $\left[\frac{79}{5}\right] + \frac{5-1}{2} = 17$ by Proposition 4.11.

Thus, for each $t$, $\mathrm{Mod}\,[p, t]$ yields the values described as in (16) and (17). The following list shows these values for $2 \leqslant t \leqslant 4$.

**List 1**

$$
\begin{array}{lll}
t=2 & p \equiv 1 \pmod 2 \longrightarrow & \dfrac{p-1}{2}+1=\left[\dfrac{p}{2}\right]+1 \\[2ex]
t=3 & \begin{cases} p \equiv 1 \pmod 3 \longrightarrow \\ p \equiv 2 \pmod 3 \longrightarrow \end{cases} & \begin{array}{l} \frac{p-1}{3}+1=\left[\frac{p}{3}\right]+1 \\ \begin{cases} \frac{p-2}{3}+2=\left[\frac{p}{3}\right]+2 \\ \frac{p-2}{3}+1=\left[\frac{p}{3}\right]+1 \end{cases} \end{array} \\[4ex]
t=4 & \begin{cases} p \equiv 1 \pmod 4 \longrightarrow \\ p \equiv 3 \pmod 4 \longrightarrow \end{cases} & \begin{array}{l} \frac{p-1}{4}+1=\left[\frac{p}{4}\right]+1 \\ \begin{cases} \frac{p-3}{4}+3=\left[\frac{p}{4}\right]+3 \\ \frac{p-3}{4}+1=\left[\frac{p}{4}\right]+1. \end{cases} \end{array}
\end{array}
$$

Note that considering $\mathrm{Mod}\,[p, 12]$ automatically gives $\mathrm{Mod}\,[p, 2]$, $\mathrm{Mod}\,[p, 3]$ and $\mathrm{Mod}\,[p, 4]$. When we divide the cases according to $\mathrm{Mod}\,[p, 12]$, List 1 can be rephrased as follows.

**List 2**

$$
p \equiv 1 \pmod{12} \longrightarrow \begin{cases} p \equiv 1 \pmod 2 \rightarrow \left[\frac{p}{2}\right]+1 \\ p \equiv 1 \pmod 3 \rightarrow \left[\frac{p}{3}\right]+1 \\ p \equiv 1 \pmod 4 \rightarrow \left[\frac{p}{4}\right]+1 \end{cases}
$$

$$
p \equiv 5 \pmod{12} \longrightarrow \begin{cases} p \equiv 1 \pmod 2 \rightarrow \left[\frac{p}{2}\right]+1 \\ p \equiv 2 \pmod 3 \rightarrow \begin{cases} \left[\frac{p}{3}\right]+2 \\ \left[\frac{p}{3}\right]+1 \end{cases} \\ p \equiv 1 \pmod 4 \rightarrow \left[\frac{p}{4}\right]+1 \end{cases}
$$

$$p \equiv 7 \pmod{12} \quad \longrightarrow \quad \begin{cases} p \equiv 1 \pmod 2 \to \left[\frac{p}{2}\right]+1 \\ p \equiv 1 \pmod 3 \to \left[\frac{p}{3}\right]+1 \\ p \equiv 3 \pmod 4 \to \begin{cases} \left[\frac{p}{4}\right]+3 \\ \left[\frac{p}{4}\right]+1 \end{cases} \end{cases}$$

$$p \equiv 11 \pmod{12} \quad \longrightarrow \quad \begin{cases} p \equiv 1 \pmod 2 \to \left[\frac{p}{2}\right]+1 \\ p \equiv 2 \pmod 3 \to \begin{cases} \left[\frac{p}{3}\right]+2 \\ \left[\frac{p}{3}\right]+1 \end{cases} \\ p \equiv 3 \pmod 4 \to \begin{cases} \left[\frac{p}{4}\right]+3 \\ \left[\frac{p}{4}\right]+1. \end{cases} \end{cases}$$

Our computation suggests that these are the $3^{rd}$, $4^{th}$ and $5^{th}$ largest values in $\Upsilon^2(p)$. Another aspect suggested by the computation is that for a fixed $t$ with $2 \leqslant t \leqslant 4$, $\left[\frac{p}{t}\right] + \operatorname{Mod}[p,t]$ gives the maximum and $\left[\frac{p}{t}\right]+1$ gives the minimum among the values described in (16) and (17). In other words, the next largest value to $\left[\frac{p}{t}\right]+1$ in $\Upsilon^2(p)$ seems to be given by $\left[\frac{p}{t+1}\right] + \operatorname{Mod}[p, t+1]$ for $t = 2, 3$. Notice that for $t = 2$, this has already been verified to hold by Chapman-Smith, since the second largest value $\left[\frac{p+4}{3}\right]$ in $\Upsilon^2(p)$, as mentioned in Remark 4.7(ii), is equal to $\left[\frac{p}{3}\right] + \operatorname{Mod}[p,3]$. A case by case proof establishes that it also holds for $t = 3$ (see Section 5 for the proof). We state the result below.

**Proposition 4.12.** *Given a prime $p \neq 29$ and $1 < a < p$, we have either $K_2(a,p) \leqslant \left[\frac{p}{4}\right] + \operatorname{Mod}[p,4]$ or $K_2(a,p) \geqslant \left[\frac{p}{3}\right]+1$.*

The result does not extend to $t = 5$. Note that $p \equiv 1 \pmod{60}$ implies $p \equiv 1 \pmod{12}$ which yields three largest values as described in List 1. It also implies $p \equiv 1 \pmod 5$ which yields $\frac{p+4}{5} = \left[\frac{p}{5}\right]+1$ by Proposition 4.8 and this is expected to be the next largest value. However, computation shows that

$$\frac{p+9}{5} \in \Upsilon_2(p) \tag{18}$$

and gives the 4th largest value in $\Upsilon^2(p)$. It turns out that this is a particular example of the following general fact.

**Proposition 4.13.** *Given an odd integer $t \geqslant 5$, let $p$ be a prime such that $p \equiv 1 \pmod t$ with $p > t^2$. Then*

$$\left[\frac{p}{t}\right] + \frac{t-1}{2} \in \Upsilon^2(p) \tag{19}$$

*and is given by $a = \left(\frac{t+1}{2}\right)\left(\frac{p-1}{t}\right)+1$.*

Proof. Write $p = tq+1$ and let $a = \left(\frac{t+1}{2}\right)q+1$. For $t \geqslant 5$, $\left(\frac{t-1}{2}\right)q > q+1$ and clearly $t > \frac{t-1}{2}$. Thus the Euclidean Table for $p$ and $a$ is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $p$ | – |
| -1 | 0 | 1 | $\left(\frac{t+1}{2}\right)q+1$ | – |
| 0 | 1 | 1 | $\left(\frac{t-1}{2}\right)q$ | 1 |
| 1 | 1 | 2 | $q+1$ | 1 |
| 2 | $\frac{t-1}{2}$ | $t-2$ | $q-\left(\frac{t-1}{2}\right)+1$ | $\frac{t-3}{2}$ |
| 3 | $\frac{t+1}{2}$ | $t$ | $\frac{t-1}{2}$ | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

and $K_2(a,p) = y_2 + s_2 = t-2+q-\left(\frac{t-1}{2}\right)+1 = \frac{p-1}{t}+\frac{t-1}{2}$.

We note that $\frac{p+9}{5}$ in (18) is equal to $\frac{p-1}{5}+\frac{5-1}{2}$, in the form of (19) with $t=5$.

## 5. Proof of Proposition 4.12

The proof will be a case by case analysis with the first two major cases being the residue of $p$ modulo 4.

Case 1 $p = 4k+1$:
We will assume $k \geqslant 25$ with the finite number of cases $k < 25$ easily verified by direct calculations (such as in the table in Appendix A).

There are three subcases required to show that the desired inequalities hold for $K_2(a,p)$ for integers $j$ where $a \equiv j \pmod{k}$:

Subcase 1A $0 \leqslant j \leqslant 5$;
Subcase 1B $6 \leqslant j \leqslant \left[\frac{k}{3}\right]$;
Subcase 1C $\left[\frac{k}{3}\right] < j \leqslant k-1$.

Subcase 1A $0 \leqslant j \leqslant 5$: Each case here is verified by considering the appropriate Euclidean Table. Since the calculations are routine, we only illustrate this with one example $j=3$. If $a \equiv 3 \pmod{k}$, then

$$a = 3, \quad k+3, \quad 2k+3, \quad \text{or} \quad 3k+3,$$

since $2 \leqslant a \leqslant k-1$.

(i) It has already been established $K_2(3,p) = \left[\frac{p}{3}\right] + \mathrm{Mod}\,[p,3]$.

For the other values, we get the relevant values from the Euclidean tables as follows:

(ii) For $a = k+3$, $y_0 = 3$; $s_0 = k-8$, so $K_2(a,p) \leqslant k-5 < k+1$.

(iii) For $a = 2k+3$, $y_2 \leqslant 2\left(\frac{2k-2}{5}\right)+1$; $s_2 \leqslant 4$, so $K_2(a,p) \leqslant \frac{4k+21}{5} \leqslant k+1$.

(iv) For $a = 3k+3$, $y_0 = 1$; $s_0 = k-2$, so $K_2(a,p) \leqslant k-1 < k+1$.

In all cases, since $k+1 \leqslant \left[\frac{p}{4}\right] + \mathrm{Mod}\,[p,4]$, we have the desired inequality. The other values of $j$ where $0 \leqslant j \leqslant 5$ are verified in the same way.

<u>*Subcase 1B*</u> $6 \leqslant j \leqslant \left[\frac{k}{3}\right]$:

(i) $a = j$: Since $a = j \geqslant 6$ and $\mathrm{Mod}\,[p, a] < a$, it follows that $K_2\,(a.p)$ $K_2\,(j,p) \leqslant \left[\frac{p}{j}\right] + \mathrm{Mod}\,[p,j] \leqslant \left[\frac{p}{6}\right] + \left[\frac{k}{3}\right] \leqslant \frac{4k+1}{6} + \frac{k}{3} \leqslant \frac{6k+1}{6} < k+1$.

(ii) $a = k+j$: $K_2\,(a,p) \leqslant y_0 + s_0 = k - 3j + 4 \leqslant k+1$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | |
| -1 | 0 | 1 | $k+j$ | |
| 0 | 1 | 3 | $k-3j+1$ | 3 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

(iii) $a = 2k + j$: Note that $6 \leqslant j \leqslant \left[\frac{k}{3}\right]$ implies $6 \leqslant j \leqslant \frac{2k+2}{3}$. Then the Euclidean Table is given by the below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | |
| -1 | 0 | 1 | $2k+j$ | |
| 0 | 1 | 1 | $2k-j+1$ | 1 |
| 1 | 1 | 2 | $2j-1$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ For $\frac{2k+4}{7} < j \leqslant \left[\frac{k}{3}\right]$, $\left[\frac{2k-j+1}{2j-1}\right] = 2$ and $\mathrm{Mod}\,[2k-j+1, 2j-1] - 2k - 5j + 3$. Thus $K_2\,(a,p) \leqslant y_2 + s_2 = 5 + 2k - 5j + 3 = 2k - 5j + 8 < 2k - 5\left(\frac{2k+4}{7}\right) + 8 = \frac{4k+36}{7}$ and this is less than or equal to $k+1$.

$*$ Consider the case $6 \leqslant j \leqslant \frac{2k+4}{7}$. Note that $K_2\,(a,p) \leqslant y_2 + s_2 < 2\left(\frac{2k-j+1}{2j-1}\right)+1+2j-2$. Since $\frac{2k-j+1}{2j-1}$ attains maximum at $j = 6$ and $2j-2$ attains maximum at $j = \frac{2k+4}{7}$, $K_2\,(a,p) \leqslant 2\left(\frac{2k-5}{11}\right)+1+2\left(\frac{2k+4}{7}\right)-2 = \frac{72k-59}{77} \leqslant k+1$.

(iv) $a = 3k + j$: $K_2\,(a,p) \leqslant y_0 + s_0 = k - j < k+1$, by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | |
| -1 | 0 | 1 | $3k+j$ | – |
| 0 | 1 | 1 | $k-j+1$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

<u>*Subcase 1C*</u> $\left[\frac{k}{3}\right] < j \leqslant k-1$:

(i) $a = j$ : Note that $\left[\frac{p}{a}\right] \geqslant 4$, since $\left[\frac{p}{a}\right] \geqslant \frac{4k+1}{k-1} = 4\left(\frac{4k+1}{k\ \ 1}\right) > 5$, for $k \leqslant 6$ which is not the case. Also $\left[\frac{p}{a}\right] \leqslant 11$. To see this, we divide into cases.

$*$ When $k = 3m$, $p = 12m + 1$ and $\left[\frac{k}{3}\right] = m$ and hence $\left[\frac{p}{a}\right] \leqslant \frac{p}{\left[\frac{k}{3}\right]+1} = \frac{12m+1}{m+1} = 11$.

$*$ Similarly when $k = 3m + 1$, $p = 12m + 5$ and $\left[\frac{k}{3}\right] = m$ and hence $\left[\frac{p}{a}\right] \leqslant \frac{p}{\left[\frac{k}{3}\right]+1} = \frac{12m+5}{m+1} = 11$.

Let $q = \left[\frac{p}{a}\right]$. Note that $K_2\left(a,p\right) \leqslant q + \text{Mod}\left[p, a\right] = q + (4k + 1 - qj)$ with $4k + 1 - qj < j$ which implies $j > \frac{4k+1}{q+1}$. Then $q + 4k + 1 - qj \leqslant (q + 1) + 4k - q\left(\frac{4k+1}{q+1}\right)$. Suppose that $(q + 1) + 4k - q\left(\frac{4k+1}{q+1}\right) \leqslant k + 1$. Then $(q + 1)^2 - q\left(\frac{4k+1}{q+1}\right) \leqslant (-3k + 1)\left(q + 1\right)$ which implies $q^2 - qk + 3k \leqslant 0$. This will hold for $\frac{k-\sqrt{k^2-12k}}{2} \leqslant q \leqslant \frac{k+\sqrt{k^2-12k}}{2}$ and it includes $4 \leqslant q \leqslant 11$.

(ii) $a = k + j$: We divide into cases.

- If $k = 3m$, then $p = 12m + 1$ and $m + 1 \leqslant j \leqslant 3m - 1$.

$*$ When $j = m + 1$, $K_2\left(a,p\right) = 4m + 1 = \frac{p-1}{3} + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 1$ | |
| -1 | 0 | 1 | $4m + 1$ | |
| 0 | 1 | 2 | $4m - 1$ | 2 |
| 1 | 1 | 3 | 2 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m + 2$, $K_2\left(a,p\right) \leqslant y_2 + s_2 \leqslant 3\left(\frac{4m-3}{5}\right) + 2 + 4 = \frac{12m+21}{5}$ and this will be less than or equal to $3m + 1 = k + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 1$ | – |
| -1 | 0 | 1 | $4m + 2$ | |
| 0 | 1 | 2 | $4m - 3$ | 2 |
| 1 | 1 | 3 | 5 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ Suppose that $m + 3 \leqslant j \leqslant \frac{12m+3}{8}$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 1$ | |
| -1 | 0 | 1 | $3m + j$ | |
| 0 | 1 | 2 | $6m - 2j + 1$ | 2 |
| 1 | 1 | 3 | $3j - 3m - 1$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

We have $K_2(a,p) \leqslant y_2+s_2 \leqslant 3\left[\frac{6m-2j+1}{3j-3m-1}\right]+2+3j-3m-2$. Note that $\left[\frac{6m-2j+1}{3j-3m-1}\right]$ attains maximum when $j = m+3$ and $3j-3m-2$ attains maximum when $j = \frac{12m+3}{8}$. Then $K_2(a,p) \leqslant 3\left(\frac{4m-5}{8}\right)+\frac{12m+3}{8} = \frac{24m-15}{8} \leqslant 3m+1 = k+1$.

$*$ Suppose that $\frac{12m+3}{8} < j \leqslant 3m-1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+1$ | – |
| -1 | 0 | 1 | $3m+j$ | – |
| 0 | 1 | 2 | $6m-2j+1$ | 2 |
| 1 | 1 | 3 | $3j-3m-1$ | 1 |
| 2 | 2 | 5 | $9m-5j+2$ | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

From the Euclidean Table above, we have $K_2(a,p) \leqslant y_2+s_2 = 5+9m-5j+2 \leqslant 9m-5\left(\frac{12m+3}{8}\right)+7 = \frac{12m+41}{8}$ and this is less than or equal to $3m+1 = k+1$.

- If $k = 3m+1$ $(p = 12m+5)$, then $m+1 \leqslant j \leqslant 3m$.

$*$ When $j = m+1$, $K_2(a,p) = 4m+3 \geqslant 4m+2 = \left[\frac{p}{3}\right]+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $4m+2$ | – |
| 0 | 1 | 2 | $4m+1$ | 2 |
| 1 | 1 | 3 | 1 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$*$ When $j = m+2$, $K_2(a,p) \leqslant y_2+s_2 = 3m+2 = k+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $4m+3$ | – |
| 0 | 1 | 2 | $4m-1$ | 2 |
| 1 | 1 | 3 | 4 | 1 |
| 2 | $m$ | $3m-1$ | 3 | $m-1$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$*$ When $j = m+3$, $K_2(a,p) \leqslant y_2+s_2 \leqslant 3\left(\frac{4m-3}{7}\right)+2+6 = \frac{12m+47}{7}$ by the Euclidean Table below and this is less than or equal to $3m+2 = k+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | |
| -1 | 0 | 1 | $4m+4$ | |
| 0 | 1 | 2 | $4m-3$ | 2 |
| 1 | 1 | 3 | 7 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m+4$, $K_2\left(a,p\right) \leqslant y_2 + s_2 \leqslant 3\left(\frac{4m-5}{10}\right) + 2 + 9 = \frac{12m-95}{10}$ which is less than or equal to $3m+2 = k+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $4m+5$ | – |
| 0 | 1 | 2 | $4m-5$ | 2 |
| 1 | 1 | 3 | 10 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $m+5 \leqslant j \leqslant \frac{12m+15}{8}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $3m+j$ | – |
| 0 | 1 | 2 | $6m-2j+5$ | 2 |
| 1 | 1 | 3 | $3j-3m-5$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2\left(a,p\right) \leqslant y_2 + s_2 \leqslant 3\left[\frac{6m-2j+5}{3j-3m-5}\right] + 2 + 3j - 3m - 6$. Note that $\left[\frac{6m-2j+5}{3j-3m-5}\right]$ attains maximum when $j = m+5$ and $3j-3m-6$ attains maximum when $j = \frac{12m+15}{8}$. Then $K_2\left(a,p\right) \leqslant 3\left(\frac{4m-5}{10}\right) + 2 + 3\left(\frac{12m+15}{8}\right) - 3m - 6 = \frac{76m+15}{40}$ which is always less than or equal to $3m+2 = k+1$.

$*$ When $\frac{12m+15}{8} < j \leqslant 3m$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $3m+j$ | – |
| 0 | 1 | 2 | $6m-2j+5$ | 2 |
| 1 | 1 | 3 | $3j-3m-5$ | 1 |
| 2 | 2 | 5 | $9m-5j+10$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2(a,p) \leqslant y_2 + s_2 = 5 + 9m - 5j + 10 \leqslant 9m - 5\left(\frac{12m+15}{8}\right) + 15 = \frac{12m+45}{8}$ which is less than or equal to $3m + 2 = k + 1$.

(iii) $a = 2k + j$: We divide into cases.

• Consider the case where $\left[\frac{k}{3}\right] < j \leqslant \frac{2k+2}{3}$. Then the Euclidean Table is given by the below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | – |
| -1 | 0 | 1 | $2k+j$ | – |
| 0 | 1 | 1 | $2k-j+1$ | 1 |
| 1 | 1 | 2 | $2j-1$ | 1 |
| 2 | 1 | $2q+1$ | $r$ | $q$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ For $j > \frac{2k+3}{5}$, $q = 1$ and $r = 2k - 3j + 2$. Then $K_2(a,p) \leqslant 2q + 1 + r = 3 + 2k - 3j + 2 < 5 + 2k - 3\left(\frac{2k+3}{5}\right) = \frac{4k+16}{5}$ and this is less than or equal to $k + 1$.

$*$ Suppose that $\left[\frac{k}{3}\right] \leqslant j \leqslant \frac{2k+3}{5}$. This implies $\frac{2k+4}{7} \leqslant j \leqslant \frac{2k+3}{5}$, since $\frac{2k+4}{7} \leqslant \left[\frac{k}{3}\right]$. Then $q = 2$ and $r = 2k - 5j + 3$ and hence $K_2(a,p) \leqslant 2q + 1 + r = 2k - 5j + 8 \leqslant 2k - 5\left(\frac{2k+4}{7}\right) + 8 = \frac{4k+36}{7}$ which is less than or equal to $k + 1$.

• Consider the case where $\frac{2k+2}{3} \leqslant j \leqslant k - 1$.

a) Suppose that $\frac{6k+3}{7} < j \leqslant k - 1$. The Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | – |
| -1 | 0 | 1 | $2k+j$ | – |
| 0 | 1 | 1 | $2k-j+1$ | 1 |
| 1 | 2 | 3 | $3j-2k-1$ | 2 |
| 2 | 3 | 4 | $4k-4j+2$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2(a,p) \leqslant y_2 + s_2 = 4 + 4k - 4j + 2 \leqslant 4k - 4\left(\frac{6k+3}{7}\right) + 6 = \frac{4k+30}{7}$ which is less than or equal to $k + 1$.

b) Suppose now that $\frac{2k+2}{3} < j \leqslant \frac{6k+3}{7}$. We divide into cases.

$*$ If $k = 3m$, then $p = 12m + 1$ and $2m + 1 \leqslant j \leqslant \frac{18m+3}{7}$.

$**$ When $j = 2m + 1$, $K_2(a,p) = 4m + 1 = \left[\frac{p}{3}\right] + 1$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+1$ | – |
| -1 | 0 | 1 | $8m+1$ | – |
| 0 | 1 | 1 | $4m$ | 1 |
| 1 | 2 | 3 | 1 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $j = 2m+2$, $K_2(a,p) = 3m+1 = k+1$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+1$ | – |
| -1 | 0 | 1 | $8m+2$ | – |
| 0 | 1 | 1 | $4m-1$ | 1 |
| 1 | 2 | 3 | 4 | 2 |
| 2 | $2m-1$ | $3m-2$ | 3 | $m-1$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $j = 2m+3$, $K_2(a,p) \leqslant y_2 + s_2 \leqslant 3\left(\frac{4m-2}{7}\right) + 1 + 6 = \frac{12m+43}{7}$ which is less than or equal to $3m+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+1$ | |
| -1 | 0 | 1 | $8m+3$ | – |
| 0 | 1 | 1 | $4m-2$ | 1 |
| 1 | 2 | 3 | 7 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $2m+4 \leqslant j \leqslant \frac{18m+3}{7}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+1$ | – |
| -1 | 0 | 1 | $6m+j$ | – |
| 0 | 1 | 1 | $6m-j+1$ | 1 |
| 1 | 2 | 3 | $3j-6m-2$ | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2(a,p) \leqslant y_2 + s_2 \leqslant 3\left(\frac{6m-j+1}{3j-6m-2}\right) + 1 + 3j - 6m - 3$. Note that $\frac{6m-j+1}{3j-6m-2}$ attains maximum at $j = 2m+4$ and $3j-6m-3$ attains maximum at $j = \frac{18m+3}{7}$. Thus $K_2(a,p) \leqslant 3\left(\frac{4m-3}{10}\right) + 1 + 3\left(\frac{18m+3}{7}\right) - 6m - 3 \leqslant \frac{204m-113}{70}$ and this is always less than or equal to $3m+1$.

$*$ If $k = 3m+1$, then $p = 12m+5$ and $2m+2 \leqslant j \leqslant \frac{18m+9}{7}$.

$**$ When $j = 2m+2$, Then $K_2\left(a,p\right) = 4m+2 = \left[\frac{p}{3}\right]+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $8m+4$ | – |
| 0 | 1 | 1 | $4m+1$ | 1 |
| 1 | 2 | 3 | 2 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $j = 2m+3$, $K_2\left(a,p\right) \leqslant y_2+s_2 \leqslant 3\left(\frac{4m}{5}\right)+1+4 = \frac{12m+25}{5}$ which is less than or equal to $3m+2 = k+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $8m+5$ | – |
| 0 | 1 | 1 | $4m$ | 1 |
| 1 | 2 | 3 | 5 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $j = 2m+4$, $K_2\left(a,p\right) \leqslant y_2+s_2 \leqslant 3\left(\frac{4m-1}{8}\right)+1+7 = \frac{12m+61}{8}$ which is less than or equal to $3m+2 = k+1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $8m+6$ | – |
| 0 | 1 | 1 | $4m-1$ | 1 |
| 1 | 2 | 3 | 8 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$**$ When $2m+5 \leqslant j \leqslant \frac{18m+9}{7}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+5$ | – |
| -1 | 0 | 1 | $6m+j+2$ | – |
| 0 | 1 | 1 | $6m-j+3$ | 1 |
| 1 | 2 | 3 | $3j-6m-4$ | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2\left(a,p\right) \leqslant y_2+s_2 \leqslant 3\left(\frac{6m-j+3}{3j-6m-4}\right)+1+3j-6m-5$. Note that $\frac{6m-j+3}{3j-6m-4}$ attains maximum at $j = 2m+5$ and $j \leqslant \frac{18m+9}{7}$. Thus $K_2\left(a,p\right) \leqslant 3\left(\frac{4m-2}{11}\right)+$

$1 + 3\left(\frac{18m+9}{7}\right) - 6m - 5 \leqslant \frac{216m-24}{77}$ and this is always less than or equal to $3m + 2 = k + 1$.

(iv) $a = 3k + j$: By the Euclidean Table below, $K_2(a,p) \leqslant k - j < k + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+1$ | – |
| -1 | 0 | 1 | $3k+j$ | – |
| 0 | 1 | 1 | $k-j+1$ | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

Case 2 $\quad p = 4k + 3$:
Again we assume $k \geqslant 25$ and the argument is then given along the same lines as the previous cases showing the desired inequality for the three subcases determined by $j$ where $a \equiv j \pmod{k}$:

Subcase 2A $\quad 0 \leqslant j \leqslant 5$;<br>
Subcase 2B $\quad 6 \leqslant j \leqslant \left[\frac{k}{3}\right]$;<br>
Subcase 2C $\quad \left[\frac{k}{3}\right] < j \leqslant k - 1$.

Subcase 2A $\quad 0 \leqslant j \leqslant 5$: This case (with the six possible values of $j$) is handled in exactly the same manner as was illustrated in the case $p \equiv 1 \pmod{4}$. We will not repeat the argument for this case.

Subcase 2B $\quad 6 \leqslant j \leqslant \left[\frac{k}{3}\right]$:

(i) $a = j$: Since $a = j \geqslant 6$ and $\operatorname{Mod}[p,a] < a$, it follows that $K_2(a,p) \leqslant \left[\frac{p}{j}\right] + \operatorname{Mod}[p,j] \leqslant \left[\frac{p}{6}\right] + \left[\frac{k}{3}\right] \leqslant \frac{4k+3}{6} + \frac{k}{3} = \frac{6k+3}{6} < k + 3 = \left[\frac{p}{4}\right] + \operatorname{Mod}[p,4]$.

(ii) $a = k+j$: By the Euclidean Table below, $K_2(a,p) \leqslant y_0 + s_0 = k - 3j + 6 < k + 3$

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+3$ | – |
| -1 | 0 | 1 | $k+j$ | – |
| 0 | 1 | 3 | $k-3j+3$ | 3 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

(iii) $a = 2k + j$: The Euclidean Table is given by the below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+3$ | – |
| -1 | 0 | 1 | $2k+j$ | – |
| 0 | 1 | 1 | $2k-j+3$ | 1 |
| 1 | 1 | 2 | $2j-3$ | 1 |
| 2 | $q+1$ | $2q+1$ | $r$ | $q$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

We divide into cases.

$*$ For $\frac{2k+12}{7} < j \leqslant \left[\frac{k}{3}\right]$, we have $q = 2$ and $r = 2k - 5j + 9$. Then $K_2\,(a,p) < 2q + 1 + r = 5 + 2k - 5j + 9 = 2k - 5j + 14 \leqslant 2k - 5\left(\frac{2k+12}{7}\right) + 14 = \frac{4k+38}{7}$ and this is less than or equal to $k + 3$.

$*$ For $6 \leqslant j \leqslant \frac{2k+12}{7}$, $\frac{2k-j+3}{2j-3}$ attains maximum at $j = 6$ and $2j - 4$ attains maximum at $j = \frac{2k+12}{7}$. Thus $K_2\,(a,p) \leqslant y_2 + s_2 \leqslant 2\left(\frac{2k-j+3}{2j-3}\right) + 1 + 2j - 4$ $2\left(\frac{2k-3}{9}\right) + 1 + 2\left(\frac{2k+12}{7}\right) - 4 = \frac{61k-15}{63}$ which is always less than or equal to $k+3$.

<u>*Subcase 2C*</u> $\left[\frac{k}{3}\right] < j \leqslant k - 1$:

(i) $a = j$: We have $\left[\frac{p}{a}\right] = \frac{4k+3}{k-1} \leqslant 4$. Also $\left[\frac{p}{a}\right] \leqslant 11$. To see this, we divide the cases.

$*$ When $k = 3m + 1$, $p = 12m + 7$ and $\left[\frac{k}{3}\right] + 1 = m + 1$ and hence $\left[\frac{p}{a}\right] < \frac{p}{\left[\frac{k}{3}\right]+1} = \frac{12m+7}{m+1} = 11$.

$*$ When $k = 3m + 2$, $p = 12m + 11$ and $\left[\frac{k}{3}\right] + 1 = m + 1$ and hence $\left[\frac{p}{a}\right] < \frac{p}{\left[\frac{k}{3}\right]+1} = \frac{12m+11}{m+1} = 11$.

Let $q = \left[\frac{p}{a}\right]$. Note that $K_2\,(a,p) \leqslant q + \mathrm{Mod}\,[p,a] = q + (4k + 3 - qj)$ with $4k + 3 - qj < j$ which implies $j > \frac{4k+3}{q+1}$. Then $q + 4k + 3 - qj \leqslant (q + 3) + 4k - q\frac{4k+3}{q+1}$. Suppose that $(q + 3) + 4k - q\frac{4k+3}{q+1} \leqslant k + 3$. Then $(q + 3)^2$ $q\frac{4k+3}{q+1} \leqslant (-3k + 3)\,(q + 1)$. Then $q^2 - (k + 2)\,q + 3k \leqslant 0$ and this will hold for $\frac{k+2-\sqrt{k^2-8k+4}}{2} \leqslant q \leqslant \frac{k+2+\sqrt{k^2-8k+4}}{2}$ which includes $4 \leqslant q \leqslant 11$.

(ii) $a = k + j$: We divide the cases.

- If $k = 3m + 1$, then $p = 12m + 7$ and $m + 1 \leqslant j \leqslant 3m$.

$*$ When $j = m + 1$, $K_2\,(a,p) = 4 \leqslant k + 3$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | |
| -1 | 0 | 1 | $4m+2$ | |
| 0 | 1 | 3 | 1 | 3 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m + 2$, $K_2\,(a,p) = y_0 + s_0 = 4m + 3$ which is equal to $\left[\frac{p}{3}\right] + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | |
| -1 | 0 | 1 | $4m+3$ | |
| 0 | 1 | 2 | $4m+1$ | 2 |
| 1 | 1 | 3 | 2 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

* When $j = m+3$, $K_2\left(a,p\right) \leqslant y_2 + s_2 = 3\left[\frac{4m-1}{5}\right] + 2 + 4 \leqslant 3\left(\frac{4m-1}{5}\right) + 6 = \frac{12m+27}{5}$ which is less than or equal to $3m+4 = k+3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $4m+4$ | – |
| 0 | 1 | 2 | $4m-1$ | 2 |
| 1 | 1 | 3 | 5 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

* When $m+4 \leqslant j \leqslant \frac{12m+13}{8}$, the Euclidean Table is given as follows.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $3m+j+1$ | – |
| 0 | 1 | 2 | $6m-2j+5$ | 2 |
| 1 | 1 | 3 | $3j-3m-4$ | 1 |
| 2 | $q+1$ | $3q+2$ | $r$ | $q$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

Then $K_2\left(a,p\right) \leqslant y_2 + s_2 = 3q+2+r \leqslant 3\left[\frac{6m-2j+5}{3j-3m-4}\right] + 2 + 3j - 3m - 5$. Note that $\left[\frac{6m-2j+5}{3j-3m-4}\right]$ attains maximum when $j = m+4$ and $3j-3m-5$ attains maximum when $j = \frac{12m+13}{8}$. Then $K_2\left(a,p\right) \leqslant 3\left(\frac{4m-3}{8}\right) + 2 + 3\left(\frac{12m+13}{8}\right) - 3m - 5 = \frac{24m+6}{8}$ which is always less than or equal to $3m+4 = k+3$.

* When $\frac{12m+13}{8} < j \leqslant 3m$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $3m+j+1$ | – |
| 0 | 1 | 2 | $6m-2j+5$ | 2 |
| 1 | 1 | 3 | $3j-3m-4$ | 1 |
| 2 | 2 | 5 | $9m-5j+9$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2\left(a,p\right) \leqslant 5 + 9m - 5j + 9 \leqslant 9m - 5\left(\frac{12m+13}{8}\right) + 14 = \frac{12m+47}{8}$ and this is less than or equal to $3m+4 = k+3$.

- If $k = 3m + 2$, then $p = 12m + 11$ and $m + 1 \leqslant j \leqslant 3m + 1$.

$*$ When $j = m + 1$, $K_2(a,p) = 5 \leqslant k + 3$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | – |
| -1 | 0 | 1 | $4m + 3$ | – |
| 0 | 1 | 3 | 2 | 3 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m + 2$, $K_2(a,p) = 4m + 5 > \left[\frac{p}{3}\right] + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | – |
| -1 | 0 | 1 | $4m + 4$ | – |
| 0 | 1 | 2 | $4m + 3$ | 2 |
| 1 | 1 | 3 | 1 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m + 3$, $K_2(a,p) = 3m + 3 < 3m + 5 = k + 3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | – |
| -1 | 0 | 1 | $4m + 5$ | – |
| 0 | 1 | 2 | $4m + 1$ | 2 |
| 1 | 1 | 3 | 4 | 1 |
| 2 | 2 | $3m + 2$ | 1 | $m$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $j = m + 4$, $K_2(a,p) \leqslant y_0 + s_0 \leqslant 3\left(\frac{4m-1}{7}\right) + 2 + 6 = \frac{12m+53}{7}$ by the Euclidean Table given below and this is less than or equal to $3m + 5 = k + 3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | – |
| -1 | 0 | 1 | $4m + 6$ | – |
| 0 | 1 | 2 | $4m - 1$ | 2 |
| 1 | 1 | 3 | 7 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

$*$ When $m + 5 \leqslant j \leqslant \frac{12m+17}{8}$, the Euclidean Table is given by the below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+11$ | – |
| -1 | 0 | 1 | $3m+j+2$ | – |
| 0 | 1 | 2 | $6m-2j+7$ | 2 |
| 1 | 1 | 3 | $3j-3m-5$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

Note that $\left[\frac{6m-2j+7}{3j-3m-5}\right]$ attains maximum when $j=m+5$ and $3j-3m-6$ attains maximum when $j=\frac{12m+17}{8}$. Thus $K_2(a,p)\leqslant y_2+s_2\leqslant 3\left[\frac{6m-2j+7}{3j-3m-5}\right]+2+3j-3m-6\leqslant 3\left(\frac{4m-3}{10}\right)+2+3\left(\frac{12m+17}{8}\right)-3m-6=\frac{108m+59}{40}$ which is always less than or equal to $3m+5=k+3$.

$*$ When $\frac{12m+17}{8}<j\leqslant 3m+1$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+11$ | – |
| -1 | 0 | 1 | $3m+j+2$ | – |
| 0 | 1 | 2 | $6m-2j+7$ | 2 |
| 1 | 1 | 3 | $3j-3m-5$ | 1 |
| 2 | 2 | 5 | $9m-5j+12$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2(a,p)\leqslant y_2+s_2=5+9m-5j+12\leqslant 9m-5\left(\frac{12m+17}{8}\right)+17=\frac{12m+51}{8}$ which is less than or equal to $3m+5$ for every $m$.

(iii) $a=2k+j$: Consider the following cases.

- For $\left[\frac{k}{3}\right]\leqslant j\leqslant\frac{2k+6}{3}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+3$ | – |
| -1 | 0 | 1 | $2k+j$ | – |
| 0 | 1 | 1 | $2k-j+3$ | 1 |
| 1 | 1 | 2 | $2j-3$ | 1 |
| 2 | $q+1$ | $2q+1$ | $r$ | $q$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

We divide into cases.

$*$ For $j>\frac{2k+9}{5}$, $q=1$ and $r=2k-3j+6$. Then $K_2(a,p)\leqslant y_2+s_2=2q+1+r=3+2k-3j+6<9+2k-3\left(\frac{2k+9}{5}\right)=\frac{4k+18}{5}$ which is less than or equal to $k+3$.

$*$ For $\left[\frac{k}{3}\right] \leqslant j \leqslant \frac{2k+9}{5}$, $q = 2$ and $r = 2k-5j+9$. Then $K_2(a,p) \leqslant 2q+1+r = 5 + 2k - 5j + 9 = 2k - 5j + 14 \leqslant 2k - 5\left(\frac{2k+12}{7}\right) + 14 = \frac{4k+38}{7}$ and this is less than or equal to $k+3$.

- Consider the case where $\frac{2k+6}{3} \leqslant j \leqslant k-1$.

a) For $\frac{6k+15}{7} < j \leqslant k-1$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+3$ | – |
| -1 | 0 | 1 | $2k+j$ | – |
| 0 | 1 | 1 | $2k-j+3$ | 1 |
| 1 | 2 | 3 | $3j-2k-6$ | 2 |
| 2 | 3 | 4 | $4k-4j+9$ | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

and $K_2(a,p) \leqslant y_2 + s_2 = 4 + 4k - 4j + 9 \leqslant 4k - 4\left(\frac{6k+15}{7}\right) + 13 = \frac{4k+31}{7}$ which is less than or equal to $k+3$ for every $k \geqslant 3$.

b) For $\frac{2k+6}{3} < j \leqslant \frac{6k+15}{7}$, we divide the cases:

$*$ If $k = 3m+1$, then $p = 12m+7$ and $2m+2 \leqslant j \leqslant \frac{18m+21}{7}$.

$**$ When $j = 2m+2$, Then $K_2(a,p) = 5 < k+3$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $8m+4$ | – |
| 0 | 1 | 1 | $4m+3$ | 1 |
| 1 | 1 | 2 | $4m+1$ | 1 |
| 2 | 2 | 3 | 2 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$**$ When $j = 2m+3$, $K_2(a,p) = 4m+3 = \left[\frac{p}{3}\right] + 1$ by the Euclidean Table below.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $8m+5$ | – |
| 0 | 1 | 1 | $4m+2$ | 1 |
| 1 | 2 | 3 | 1 | 2 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$**$ When $j = 2m+4$, $K_2(a,p) \leqslant y_2 + s_2 = 3m+2 < 3m+4 = k+3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $8m+6$ | – |
| 0 | 1 | 1 | $4m+1$ | 1 |
| 1 | 2 | 3 | 4 | 2 |
| 2 | $2m+1$ | $3m+1$ | 1 | $m$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$**$ When $j=2m+5$, $K_2\left(a,p\right)\leqslant y_2+s_2\leqslant 3\left(\frac{4m}{7}\right)+1+6=\frac{12m+49}{7}$ which is less than or equal to $3m+4=k+3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $8m+7$ | – |
| 0 | 1 | 1 | $4m$ | 1 |
| 1 | 2 | 3 | 7 | 2 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

$**$ When $2m+6\leqslant j<\frac{18m+21}{7}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+7$ | – |
| -1 | 0 | 1 | $6m+j+2$ | – |
| 0 | 1 | 1 | $6m-j+5$ | 1 |
| 1 | 2 | 3 | $3j-6m-8$ | 2 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

and $K_2\left(a,p\right)\leqslant y_2+s_2\leqslant 3\left(\frac{6m-j+5}{3j-6m-8}\right)+1+3j-6m-9$. Note that $\frac{6m-j+5}{3j-6m-8}$ attains maximum at $j=2m+6$ and $3j-6m-9$ attains maximum at $j=\frac{18m+21}{7}$. Thus $K_2\left(a,p\right)\leqslant 3\left(\frac{4m-1}{10}\right)+1+3\left(\frac{18m+21}{7}\right)-6m-9\leqslant\frac{204m+49}{70}$ and this is always less than or equal to $3m+4$.

$*$ If $k=3m+2$, then $p=12m+11$ and $2m+3\leqslant j\leqslant\frac{18m+27}{7}$.

$**$ When $j=2m+3$, then $K_2\left(a,p\right)=4<k+3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m+11$ | – |
| -1 | 0 | 1 | $8m+7$ | – |
| 0 | 1 | 1 | $4m+4$ | 1 |
| 1 | 1 | 2 | $4m+3$ | 1 |
| 2 | 2 | 3 | 1 | 1 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

** When $j = 2m + 4$, $K_2(a,p) = 4m + 4 = \left[\frac{p}{3}\right] + 1$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | – |
| -1 | 0 | 1 | $8m + 8$ | – |
| 0 | 1 | 1 | $4m + 3$ | 1 |
| 1 | 2 | 3 | 2 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

** When $j = 2m + 5$, $K_2(a,p) \leqslant y_2 + s_2 \leqslant 3\left(\frac{4m+2}{5}\right) + 1 + 4 = \frac{12m+31}{5}$ which is less than or equal to $3m + 5 = k + 3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | |
| -1 | 0 | 1 | $8m + 9$ | – |
| 0 | 1 | 1 | $4m + 2$ | 1 |
| 1 | 2 | 3 | 5 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

** When $j = 2m + 6$, $K_2(a,p) \leqslant y_2 + s_2 \leqslant 3\left(\frac{4m+1}{8}\right) + 1 + 7 = \frac{12m+67}{8}$ which is less than or equal to $3m + 5 = k + 3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | |
| -1 | 0 | 1 | $8m + 10$ | |
| 0 | 1 | 1 | $4m + 1$ | 1 |
| 1 | 2 | 3 | 8 | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

** When $2m + 7 \leqslant j < \frac{18m+27}{7}$, the Euclidean Table is given by

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $12m + 11$ | |
| -1 | 0 | 1 | $6m + j + 4$ | |
| 0 | 1 | 1 | $6m - j + 7$ | 1 |
| 1 | 2 | 3 | $3j - 6m - 10$ | 2 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

and $K_2(a,p) \leqslant y_2 + s_2 \leqslant 3\left(\frac{6m-j+7}{3j-6m-10}\right) + 1 + 3j - 6m - 11$. Note that $\frac{6m-j+7}{3j-6m\quad 10}$ attains maximum at $j = 2m + 7$ and $j \leqslant \frac{18m+27}{7}$. Thus $K_2(a,p) \leqslant 3\left(\frac{4m}{11}\right) + 1 + 3\left(\frac{18m+27}{7}\right) - 6m - 11 \leqslant \frac{216m+121}{77}$ and this is always less than or equal to $3m + 5 = k + 3$.

(iv) $a = 3k + j$: $K_2(a,p) \leqslant y_0 + s_0 = k - j + 2 < k + 3$.

| k | $x_k$ | $y_k$ | $s_k$ | $a_k$ |
|---|---|---|---|---|
| -2 | 1 | 0 | $4k+3$ | – |
| -1 | 0 | 1 | $3k+j$ | – |
| 0 | 1 | 1 | $k-j+3$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

This completes the proof. □

## Appendix A. Computation of $\Upsilon^2(p)$ for $5 \leq p \leq 97$

| p | $\Upsilon^2$ (p) |
|---|---|
| 5 | $\{2,3\}$ |
| 7 | $\{2,3,4\}$ |
| 11 | $\{2,3,4,5,6\}$ |
| 13 | $\{2,3,4,5,7\}$ |
| 17 | $\{2,3,4,5,6,7,9\}$ |
| 19 | $\{2,3,4,5,7,10\}$ |
| 23 | $\{2,3,4,5,6,7,8,9,12\}$ |
| 29 | $\{2,3,4,5,6,7,8,9,10,11,15\}$ |
| 31 | $\{2,3,4,5,6,7,8,10,11,16\}$ |
| 37 | $\{2,3,4,5,6,7,8,9,10,13,19\}$ |
| 41 | $\{2,3,4,5,6,7,8,9,10,11,14,15,21\}$ |
| 43 | $\{2,3,4,5,6,7,8,9,11,13,15,22\}$ |
| 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 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,20,21,30\}$ |
| 61 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,16,21,31\}$ |
| 67 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,19,23,34\}$ |
| 71 | $\{2,3,4,5,6,7,8,9,10,11,12,13,15,16,18,20,24,25,36\}$ |
| 73 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,19,25,37\}$ |
| 79 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,19,20,22,27,40\}$ |
| 83 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,17,18,19,21,23,28,29,42\}$ |
| 89 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,18,19,21,23,30,31,45\}$ |
| 97 | $\{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,19,20,21,25,33,49\}$ |

## REFERENCES

[1] ANDERSON, D. F.: *Elasticity of factorizations in integral domains: a survey.* In: Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, New York, 1997, pp. 1 30.

[2] ANDERSON, D. F.—CHAPMAN, S. T.: *On the elasticities of Krull domains with finite cyclic divisor class group*, Comm. Algebra **28** (2000), 2543–2553.

[3] BAGINSKI, P.—CHAPMAN, S. T.—HOLDEN, M.—MOORE, T.: *Asymptotic elasticity in atomic monoids*, Semigroup Forum **72** (2006), 134–142.

[4] CHAPMAN, S. T.—GEROLDINGER, A.: *On cross numbers of minimal zero sequences*, Australas. J. Comb. **14** (1996), 85–92.

[5] CHAPMAN, S. T.—GEROLDINGER, A.: *Krull domains and monoids, their sets of lengths and associated combinatorial problems.* In: Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, New York, 1997, pp. 73–112.

[6] CHAPMAN, S. T.—SMITH, W. W.: *An Anlysis using the Zaks-Skula constant of element factorizations in Dedekind domains*, J. Algebra **159** (1993), 176–190.

[7] CHAPMAN, S. T.—SMITH, W. W.: *On factorization in block monoids formed by* $\{\bar{1}, \bar{a}\}$ *in* $\mathbb{Z}_n$, Proc. Edinb. Math. Soc. (2) **46** (2003), 257–267.

[8] GEROLDINGER, A.: *On non-unique factorizations into irreducible elements II*, Colloq. Math. Soc. János Bolyai **51** (1987), 723–757.

[9] GEROLDINGER, A.—HALTER-KOCH, F.: *Nonunique factorizations in block semigroups and their arithmetical applications*, Math. Slovaca **42** (1992), 641–661.

[10] GEROLDINGER, A.—HALTER-KOCH, F.: *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, Vol. 278*, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[11] HALTER-KOCH, F.: *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux **7** (1995), 367–385.

[12] KATTCHEE, K. M.: *On Factorization in Krull domains with divisor class group* $\mathbb{Z}_{2^k}$. In: Arithmetical Properties of Commutative Rings and Monoids, Chapman & Hall/CRC, Boca Raton, FL, 2005, pp. 325–336.

[13] OLDS, C. D.: *Continued Fractions.* New Mathematical Library 9, Random House Inc., New York, 1961.

[14] SCHMID, W. A.: *Arithmetic of block monoids*, Math. Slovaca **54** (2004), 503–526.

[15] SCHMID, W. A.: *On invariants related to non-unique factorizations in block monoids and rings of algebraic integers*, Math. Slovaca **55** (2005), 21–37.

Received 19. 12. 2005
Revised 27. 3. 2006

* *The University of North Carolina at Chapel Hill*
*Department of Mathematics*
*Phillips Hall*
*Chapel Hill, NC 27599-3250*
*E-mail*: sooah@email.unc.edu
wwsmith@email.unc.edu

** *Trinity University*
*Department of Mathematics*
*One Trinity Place*
*San Antonio, TX 78212-7200*
*E-mail*: schapman@trinity.edu