Elem. Math. 64 (2009) 154 – 159
0013-6018/09/040154-6



**Elemente der Mathematik**

# On a property of the division algorithm and its application to the theory of non-unique factorizations

David F. Anderson, Scott T. Chapman, and William W. Smith

David Anderson received his Ph.D. at the University of Chicago in 1976. He joined the faculty at the University of Tennessee in 1976 and has been associate department head for graduate studies since 2001.

Scott Chapman received his Ph.D at the University of North Texas in 1987. He spent 21 years on the faculty at Trinity University in San Antonio, Texas, before becoming the Scholar in Residence at Sam Houston State University in Huntsville, Texas, in 2008.

William Smith received his Ph.D. at Louisiana State University in 1965. He joined the faculty at the University of North Carolina at Chapel Hill that year. During his tenure in Chapel Hill, he has served terms as department chair, special assistant to the dean and to the provost.

While the Fundamental Theorem of Arithmetic indicates that integers factor uniquely (up to order) as a product of prime integers, not all multiplicative systems possess this property. For instance, in the celebrated *Hilbert Monoid*,

$$1 + 4\mathbb{N}_0 = \{1,\ 5,\ 9,\ 13,\ 17,\ 21,\ 25,\ 29,\ 33,\ 37,\ 41,\ 45,\ 49,\ \ldots\},$$

we have that

$$441 = 9 \cdot 49 = 21 \cdot 21$$

Dividiert man die natürliche Zahl $n$ mit Rest durch die positive natürliche Zahl $a$, so erhält man bekanntlich eindeutig bestimmte natürliche Zahlen $q$ und $r$ derart, dass $n = qa + r$ mit $0 \leq r < a$ gilt. In der vorliegenden Arbeit studieren die Autoren zu vorgegebenen $n$ und $a$ die Zahlenfolge $\{\sigma_{n,a}\}_{n=a+1}^{\infty}$, wobei $\sigma_{n,a} = q + r$ ist. Es stellt sich heraus, dass diese Folge rekursiv definiert werden kann und dass $\sigma_{n,a} \leq \lfloor (n+1)/2 \rfloor$ ist (hierbei bedeutet $\lfloor x \rfloor$ die grösste natürliche Zahl kleiner gleich $x$). Darüber hinaus untersuchen die Autoren, welche Werte die Folge $\{\sigma_{n,a}\}_{n=a+1}^{\infty}$ annimmt und wann der Wert $\lfloor (n+1)/2 \rfloor$ erreicht wird. Die Arbeit schliesst mit einer Anwendung der gewonnenen Erkenntnisse auf Monoide, in denen die Eindeutigkeit der Primfaktorzerlegung verletzt ist.

and none of the integers 9, 21 nor 49 factors in $1 + 4\mathbb{N}_0$. Interest in integral domains and monoids where unique factorization fails has increased over the past few years (see [1], [5] and [10] for further details). Investigating the phenomena of nonunique factorization has led to a reexamination of the basic arithmetic in many algebraic structures. It was during such an investigation that the current authors noticed an interesting property concerning the sum of the quotient and remainder in the Division Algorithm. Before proceeding, we state the Division Algorithm for the convenience of the reader.

**The Division Algorithm.** *Let $n$ and $a$ be integers with $a > 0$. There exists unique integers $q$ and $r$ such that*

$$n = qa + r$$

*with $0 \leq r < a$.*

For positive integers with the condition $1 < a < n$ our interest is in the sum $q + r$ as given by the division above. Using the three conditions

(i) $n = aq + r$, (ii) $0 \leq r < a$, and (iii) $1 < a < n$

one can easily establish the inequality

$$q + r \leq \left\lfloor \frac{n+1}{2} \right\rfloor \qquad (*)$$

since the inequality $q + r \leq \frac{n+1}{2}$ can easily seen to be equivalent to $q(a-2) \geq r - 1$. However, our interest goes beyond the basic inequality $(*)$. We want to analyze the range of values that $q + r$ might obtain as either $n$ or $a$ vary and further determine exactly when this sum reaches its maximum. To that end, we use the following notation.

For $1 < a < n$ set

$$\sigma_{n,a} = q + r$$

where $n = qa + r$ with $0 \leq r < a$. We list the values of $\sigma_{n,a}$ for $2 \leq n \leq 11$ in Table 1 on the next page.

In addition to establishing in Theorem 6 the inequality $(*)$, we will show in Theorem 1 the recursive nature of the sequence $\sigma_{n,a}$. We will also establish in Corollary 3 the full range of values given by $\sigma_{n,a}$ for a fixed $n$ as $a$ ranges from 2 to $n - 1$. We then offer an application of these matters to a non-unique factorization property in a Diophantine monoid. We begin with Theorem 1.

**Theorem 1.** *If $n$ and $a$ are positive integers with $1 < a < n$, then*

$$\sigma_{n+1,a} = \begin{cases} \sigma_{n,a} + 1 & \text{if} \quad a \nmid (n+1)\,, \\ \sigma_{n,a} + (2-a) & \text{if} \quad a \mid (n+1)\,. \end{cases}$$

*Moreover, $\sigma_{n+1,n} = 2$.*

*Proof.* Write

$$n = qa + r \text{ and } n + 1 = q'a + r'. \qquad (**)$$

| $n\backslash a$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | | | | | | | | |
| 4 | 2 | 2 | | | | | | | |
| 5 | 3 | 3 | 2 | | | | | | |
| 6 | 3 | 2 | 3 | 2 | | | | | |
| 7 | 4 | 3 | 4 | 3 | 2 | | | | |
| 8 | 4 | 4 | 2 | 4 | 3 | 2 | | | |
| 9 | 5 | 3 | 3 | 5 | 4 | 3 | 2 | | |
| 10 | 5 | 4 | 4 | 2 | 5 | 4 | 3 | 2 | |
| 11 | 6 | 5 | 5 | 3 | 6 | 5 | 4 | 3 | 2 |

Table 1

Notice that $q' = q$ if $n+1 \not\equiv 0 \pmod{a}$ and $q' = q+1$ if $n+1 \equiv 0 \pmod{a}$. Hence we consider two cases.

a) If $q' = q$, then $(**)$ implies that $r' = r+1$. Hence $\sigma_{n+1,a} = q' + r' = q + r + 1 = \sigma_{n,a} + 1$.

b) If $q' = q+1$, then $(**)$ implies that $r' = r - a + 1$. Hence, $\sigma_{n+1,a} = q' + r' = (q+1) + (r - a + 1) = \sigma_{n,a} + (2 - a)$. □

With Lemma 2, we begin to explore possible values in the sequences $\{\sigma_{n,a}\}_{a=2}^{n-1}$.

**Lemma 2.** *Let $n$ and $a$ be positive integers with $1 < a < n$.*

(1) *If $n$ is even, then*
   (a) $\sigma_{n,2} = \sigma_{n,(n+2)/2} = n/2$, *and*
   (b) $\sigma_{n,a} = n - a + 1 < \frac{n}{2}$ *for* $a > \frac{n+2}{2}$.

(2) *If $n$ is odd, then*
   (a) $\sigma_{n,2} = \sigma_{n,(n+1)/2} = \frac{n+1}{2}$, *and*
   (b) $\sigma_{n,a} = n - a + 1 < \frac{n+1}{2}$ *for* $a > \frac{n+1}{2}$.

*Proof.* Part (a) of both (1) and (2) can be readily verified. We prove (b) for both (1) and (2).

(1) If $n$ is even and $a > \frac{n+2}{2}$, then $q = 1$ and $r = n - a$. Hence, $\sigma_{n,a} = 1 + n - a < 1 + n - \left(\frac{n+2}{2}\right) = \frac{n}{2}$.

(2) If $n$ is odd and $a > \frac{n+1}{2}$, then $q = 1$ and $r = n - a$. Hence, $\sigma_{n,a} = 1 + n - a < 1 + n - \left(\frac{n+1}{2}\right) = \frac{n+1}{2}$. □

As a consequence of the last result, we obtain the following

**Corollary 3.** *For every $n \geq 3$, the sequence $\{\sigma_{n,a}\}_{a=2}^{n-1}$ takes on all integer values in the interval $\left[2, \left\lfloor \frac{n+1}{2} \right\rfloor\right]$.*

Establishing $(*)$ will require two lemmas.

**Lemma 4.** *Let $a > 2$ be a positive integer. If $n = qa + r$ is a positive integer with $q > 2$ and $0 \le r < a$, then*

(1) $\sigma_{n,a} < \frac{n}{2}$ *if $n$ is even, and* (2) $\sigma_{n,a} < \frac{n+1}{2}$ *if $n$ is odd.*

*Proof.* For $q > 2$ and $a > 3$, we have

$$r < a \le 2a - 4 = 2(a-2) < q(a-2).$$

Hence, $qa + r > 2q + 2r$, which implies that $\sigma_{n,a} = q + r < \frac{qa+r}{2} = \frac{n}{2} < \frac{n+1}{2}$. For the case $a = 3$, if $n = 3q + r$ with $q > 2$ and $0 \le r < 3$, then $r < q$ and $2q + 2r < 3q + r$ implies that $\sigma_{n,3} = q + r < \frac{3q+r}{2} = \frac{n}{2} < \frac{n+1}{2}$. □

We next examine the inequality $(*)$ for $a > 2$ and $q = 1$ or 2. The cases $a = 3$ and $a = 4$, follow from Table 1. The following lemma completes the argument for $a > 4$ and further determines the values where the maximum is obtained.

**Lemma 5.** *Let $n$ and $a > 4$ be positive integers and suppose that $a + 1 \le n \le 3a - 1$. Then*

(1) *for $n$ even, $\sigma_{n,a} < \frac{n}{2}$ unless $n = a + (a-2)$, in which case $\sigma_{n,a} = \frac{n}{2}$.*

(2) *for $n$ odd, $\sigma_{n,a} < \frac{n+1}{2}$ unless $n = a + (a-1)$, in which case $\sigma_{n,a} = \frac{n+1}{2}$.*

*Proof.* Let $a > 4$. If $n = a + (a-2)$, then $n$ is even and

$$\sigma_{a+(a-2),a} = 1 + (a-2) = \frac{a + (a-2)}{2} = \frac{n}{2}.$$

If $n = a + (a-1)$, then $n$ is odd and

$$\sigma_{a+(a-1),a} = 1 + (a-1) = \frac{a + (a-1) + 1}{2} = \frac{n+1}{2}.$$

Now, if $n = a + r$ with $1 \le r < a - 2$, then $2 + 2r < a + r$ implies $1 + r < \frac{a+r}{2}$, which implies $\sigma_{a+r,a} = 1 + r < \frac{a+r}{2} = \frac{n}{2} < \frac{n+1}{2}$. If $n = 2a + r$ with $0 \le r < a$, then $\sigma_{n,a} = 2 + r$ and $r < a < 2a - 4$ implies $4 + 2r < 2a + r$, and hence $\sigma_{n,a} = 2 + r < \frac{2a+r}{2} = \frac{n}{2} < \frac{n+1}{2}$. □

We summarize our results in the following theorem, which completes the argument for $(*)$.

**Theorem 6.** *Let $n$ and $a$ be positive integers with $1 < a < n$. Write $n = qa + r$ with $0 \le r < a$. Then*

(1) $q + r \le \frac{n}{2}$ *if $n$ is even, and* (2) $q + r \le \frac{n+1}{2}$ *if $n$ is odd.*

*Moreover, equality is obtained only in the following cases:*

(a) $a = 2$, (b) *$n$ is even and* $a = \frac{n+2}{2}$,

(c) *$n$ is odd and* $a = \frac{n+1}{2}$, *and* (d) $n = 8$ *and* $a = 3$.

We demonstrate a simple application of Theorem 6 to the theory of non-unique factorizations. A central focus of this area of research is to describe the arithmetic of various algebraic structures. This can be difficult even in simple cases, as we now illustrate. Let $p$ be an odd prime number, $a$ be an integer with $1 < a < p$, and

$$M = \{(x_1, x_2, x_3) \mid x_i \in \mathbb{N}_0 \text{ and } x_1 + ax_2 - px_3 = 0\}.$$

$M$ forms a monoid under addition and is a basic example of a Diophantine monoid (see [8] for an indepth study of these monoids). We partially order $M$ by the rule $(x_1, x_2, x_3) \leq (y_1, y_2, y_3)$ if and only if $x_i \leq y_i$ for each $i$. The minimal nonzero elements of $M$ under $\leq$ cannot be properly factored in $M$, and are *irreducible*. Let $\mathcal{I}(M)$ represent the set of irreducibles in $M$ (which is finite by Dickson's lemma [9, Theorem 5.1]). One constant used to describe the arithmetic of $M$ is called the *elasticity* ([3] or [7] are good general references for the elasticity) and is defined as

$$\rho(M) = \sup\left\{\frac{m}{n} \;\middle|\; \exists v_1, \ldots, v_m, u_1, \ldots, u_n \in \mathcal{I}(M) \text{ with } v_1 + \ldots + v_m = u_1 + \ldots + u_n\right\}.$$

By [2, Theorem 7], $\rho(M)$ is finite and rational. The exact value of $\rho(M)$ can be computed using a combinatorial algorithm found in [6]. Theorem 6 can be used to find a lower bound for $\rho(M)$. Let $p = qa + r$ with $0 \leq r < a$. Note that the elements

$$v_1 = (r, q, 1), \; w_1 = (p, 0, 1), \text{ and } w_2 = (0, p, a)$$

are all in $\mathcal{I}(M)$ and

$$\sum_{i=1}^{p} v_1 = \sum_{i=1}^{r} w_1 + \sum_{i=1}^{q} w_2.$$

Hence, using $(*)$ we obtain

$$\rho(M) \geq \frac{p}{q+r} \geq \frac{p}{\frac{p+1}{2}} = \frac{2p}{p+1}.$$

This observation is key to a more general result [4, Theorem 7]. If $M$ is a Krull monoid (see [7]) with divisor class group $\mathbb{Z}/p\,\mathbb{Z}$, then either $\rho(M) = 1$ or $\frac{2p}{p+1} \leq \rho(M) \leq \frac{p}{2}$. We note that the exact value of $\rho(M)$ depends on both $p$ and $a$. For instance, by [4, Lemma 12], if $a = 2$, then $\rho(M) = \frac{2p}{p+1}$, but if $a = 3$, then

$$\rho(M) = \begin{cases} \dfrac{3p}{p+2} & \text{if} \quad p \equiv 1 \pmod 3, \\ \dfrac{3p}{p+4} & \text{if} \quad p \equiv 2 \pmod 3. \end{cases}$$

## References


[1] Anderson, D.D. (ed.): *Factorization in Integral Domains*. Lecture Notes in Pure and Appl. Math. 189, 1997.

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

[3] Anderson, D.F.: Elasticity of factorizations in integral domains: a survey. In [1], 1–30.

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

[5] Chapman, S.T. (ed.): *Arithmetical Properties of Commutative Rings and Monoids*. Lecture Notes in Pure and Appl. Math. Chapman and Hall, 241, 2005.

[6] Chapman, S.T.; García-García, J.I.; García-Sánchez, P.A.; Rosales, J.C.: Computing the elasticity of a Krull monoid. *Linear Algebra Appl.* 336 (2001), 191–200.

[7] Chapman, S.T.; Geroldinger, A.: Krull domains and monoids, their sets of lengths and associated combinatorial problems. In [1], 73–112.

[8] Chapman, S.T.; Oeljeklaus, E.; Krause, U.: On Diophantine monoids and their class groups. *Pacific J. Math.* 207 (2002), 125–147.

[9] García-Sánchez, P.A.; Rosales, J.C.: *Finitely Generated Commutative Monoids*. Nova Science Publishers, Commack, New York 1999.

[10] Geroldinger, A.; Halter-Koch, F.: *Non-unique Factorizations, Algebraic, Combinatorial and Analytic Theory*. Chapman & Hall/CRC, Boca Raton, Florida 2006.



David F. Anderson
The University of Tennessee
Department of Mathematics
Knoxville, Tennessee 37996, USA
e-mail: anderson@math.utk.edu

Scott T. Chapman
Sam Houston State University
Department of Mathematics and Statistics
Box 2206
Huntsville, Texas 77341-2206, USA
e-mail: scott.chapman@shsu.edu

William W. Smith
The University of North Carolina at Chapel Hill
Department of Mathematics
Chapel Hill, North Carolina 27599-3250, USA
e-mail: wwsmith@email.unc.edu