# Monoids for Math Majors

**Brian D. Beasley**
**Presbyterian College**

In May of 2007, Trinity University in San Antonio hosted a workshop on "The Art of Factorization in Multiplicative Structures." This weeklong workshop, offered through the Professional Enhancement Program (PREP) of the Mathematical Association of America, featured a variety of topics, with quite a number suitable for undergraduate mathematics majors (Chapman, 2007). After the workshop, the challenge at Presbyterian College became determining which of these topics would be most appropriate for our students as well as the best fit in the curriculum.

In order to address these questions, we begin with some basic definitions. Given a set $G$ and an associative binary operation $*$ on $G$, consider the following properties:

(1) $G$ is closed with respect to $*$.

(2) There is an identity element in $G$ with respect to $*$.

(3) There are inverses in $G$ for all of its elements.

Then we say that a *semigroup* satisfies property (1); a *monoid* satisfies properties (1) and (2); and, most familiar of the three, a *group* satisfies properties (1), (2), and (3).

To gauge how often the terms semigroup and monoid are used, we examined a small sample of abstract algebra textbooks. In Gilbert and Gilbert's *Elements of Modern Algebra*, the book currently in use at Presbyterian College, there are no references to either semigroups or monoids (Gilbert and Gilbert, 2005). The same situation occurs in other abstract algebra texts, including Gallian's *Contemporary Abstract Algebra*, Bland's *The Basics of Abstract Algebra*, and Durbin's *Modern Algebra: An Introduction* (Gallian, 2002; Bland, 2002; Durbin, 2005). Hungerford does make a passing remark in his classic text, noting "Our principal interest is in groups. However, semigroups and monoids are convenient for stating certain theorems in the greatest generality" (Hungerford, 1974; page 24). Also, Fraleigh observes in his abstract algebra book that "binary algebraic structures with weaker axioms than those for a group have also been studied quite extensively. Of these weaker structures, the *semigroup*, a set with an associative binary operation, has perhaps had the most attention. A *monoid* is a semigroup that has an identity element for the binary operation" (Fraleigh, 2003; page 42).

As a quick check on Fraleigh's claim, we searched mathematical journals on JSTOR for references to semigroups or monoids. The term "semigroup" produced 3587 articles, while the terms "semigroup" and "factorization" turned up 322 articles, 162 of which have been published since 1985. In comparison, the term "monoid" produced 789 articles, while the terms "monoid" and "factorization" turned up 132 articles, 87 of which have been published since 1985.

Since our focus will be on factorization in certain types of monoids, we continue with more definitions. Let $M$ be a monoid with respect to multiplication having identity element 1. Then a *unit* $u$ in $M$ divides 1 in $M$; that is, there is an element $v$ in $M$ with $uv = 1$. Next, an *atom* is an irreducible non-unit element of $M$: If an atom $x$ is written as $x = yz$ for $y$ and $z$ in $M$, then either $y$ or $z$ is a unit. Finally, we say that $M$ is *factorial* if every element in $M$ which is not a unit may

be factored uniquely, up to order, as a product of atoms in $M$. (Such a monoid $M$ is also called a *unique factorization monoid.*) We present two examples to illustrate these concepts.

*Example 1.* Let $M_1 = \{m \in \mathbb{N} : \gcd(m, 6) = 1\}$. Note that $M_1$ contains all natural numbers that are equivalent to either 1 or 5 modulo 6:

$$M_1 = \{1, 5, 7, 11, 13, 17, 19, 23, \ldots\}.$$

We may verify that $M_1$ is a monoid with respect to multiplication, with the single unit 1, by observing that the set $A = \{1, 5\}$ is closed under multiplication modulo 6. Furthermore, since its atoms consist of all primes greater than 3, we conclude that $M_1$ is factorial, due to the unique factorization property in $\mathbb{N}$.

*Example 2.* Let $M_2 = \{1\} \cup \{m \in \mathbb{N} : \gcd(m, 6) \neq 1\}$. Note that $M_2$ contains (in addition to 1) all natural numbers that are equivalent to 0, 2, 3, or 4 modulo 6:

$$M_2 = \{1\} \cup \{2, 3, 4, 6, 8, 9, 10, 12, \ldots\}.$$

Then $M_2$ is also a monoid with respect to multiplication, as the set $A = \{0, 2, 3, 4\}$ is closed under multiplication modulo 6. In order to determine the atoms of $M_2$, we list its reducible elements and use these to "sieve" out the atoms:

$$\{\text{reducible elements}\} = \{4, 6, 8, 9, 12, 16, 18, 20, \ldots\};$$
$$\{\text{atoms}\} = \{2, 3, 10, 14, 15, 21, 22, \ldots\}.$$

In particular, we observe that 2, 3, 10, and 15 are all atoms in $M_2$, but $30 = (2)(15) = (3)(10)$. Hence $M_2$ is not factorial.

The previous examples raise more questions for our consideration. In $M_2$, unique factorization into atoms failed – but will any such factorization of a given element have the same *number* of atoms? We say a monoid is *half-factorial* if for every non-unit $x$, whenever

$$x = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

for atoms $p_i$ and $q_j$, we have $r = s$. In general, when will monoids of the type seen in $M_1$ and $M_2$ possess the factorial or half-factorial property? Such monoids are known as *congruence monoids*, having the form

$$M(A, b) = \{1\} \cup \{m \in \mathbb{N} : m \in A \pmod b\},$$

where $A$ is multiplicatively closed modulo $b$. For certain congruence monoids, the factorial and half-factorial questions have been answered, as seen in the following theorems.

*Theorem 1* (James and Niven, 1954). A congruence monoid is factorial if and only if it consists of all elements relatively prime to a fixed positive integer $n$.

*Theorem 2* (Banister, Chaika, Chapman, and Meyerson, *Elemente der Mathematik*, 2007).
Given a positive integer $n$, the congruence monoid

$$M = \{1\} \cup \{m \in \mathbb{N} : \gcd(m, n) \neq 1\}$$

is half-factorial.

A special case of congruence monoids occurs when $A$ consists of a single element $a$ with $a \leq b$ and $a^2 \equiv a \pmod{b}$:

$$M(a,b) = \{1\} \cup \{m \in \mathbb{N} : m \equiv a \pmod{b}\}$$

is called an *arithmetical congruence monoid* or ACM. The result of James and Niven shows that the only factorial ACM's are $M(1,1) = \mathbb{N}$ and $M(1,2) = \{\text{positive odd integers}\}$. This leaves the problem of classifying the half-factorial ACM's. Before presenting that result, we investigate four examples and determine whether the half-factorial property holds in each.

*Example 3.* Consider $M(1,6) = \{1, 7, 13, 19, 25, \ldots\}$. By Theorem 1, we know that $M(1,6)$ is not factorial; in particular, we note that 25, 55, and 121 are atoms which produce the counterexample $3025 = (25)(121) = 55^2$. In order to determine whether $M(1,6)$ is half-factorial, we find a pattern for its atoms:

$$\{\text{reducible elements}\} = \{49, 91, 133, 169, 175, \ldots\};$$
$$\{\text{atoms}\} = \{7, 13, 19, 25, 31, 37, 43, 55, \ldots\}$$
$$= \{p : \text{prime } p \equiv 1 \pmod{6}\} \cup \{pq : \text{primes } p \equiv q \equiv 5 \pmod{6}\}.$$

Then $x = p_1 p_2 \cdots p_r (q_1 q_2)(q_3 q_4) \cdots (q_{2s-1} q_{2s})$ has $r + s$ atoms in any such factorization, where each $p_i$ is a prime with $p_i \equiv 1 \pmod{6}$, each $q_j$ is a prime with $q_j \equiv 5 \pmod{6}$, and each product of two primes $q_j$ and $q_k$ becomes an atom in $M(1,6)$. Hence the half-factorial property holds for this monoid.

*Example 4.* Next, we examine $M(1,8) = \{1, 9, 17, 25, 33, \ldots\}$. By Theorem 1, we know that $M(1,8)$ is not factorial; one counterexample is $1089 = (9)(121) = 33^2$. However, unlike $M(1,6)$, this monoid is not even half-factorial, as seen by $11025 = (9)(25)(49) = 105^2$.

*Example 5.* We consider an ACM with $a > 1$, specifically $M(5,10) = \{1\} \cup \{5, 15, 25, 35, 45, \ldots\}$. By Theorem 1, we know that $M(5,10)$ is not factorial; a quick check produces $225 = (5)(45) = 15^2$. In order to determine whether $M(5,10)$ is half-factorial, we seek to classify its atoms:

$$\{\text{reducible elements}\} = \{25, 75, 125, 175, 225, \ldots\};$$
$$\{\text{atoms}\} = \{x \in M(5,10) : 5 \text{ divides } x \text{ but } 25 \text{ does not divide } x\}.$$

Then $x = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ for atoms $p_i$ and $q_j$ would require the same number of factors of 5 from the atoms on each side, meaning $r = s$. Hence the half-factorial property holds for this monoid.

*Example 6.* Finally, we examine $M(4,12) = \{1\} \cup \{4, 16, 28, 40, 52, \ldots\}$. By Theorem 1, we know that $M(4,12)$ is not factorial; one counterexample is $1120 = (4)(280) = (28)(40)$. Next, we classify the atoms of this monoid:

$$\{\text{reducible elements}\} = \{16, 64, 112, 160, 208, 256, 304, \ldots\};$$
$$\{\text{atoms}\} = \{x \in M(4,12) : 4 \text{ divides } x \text{ but } 16 \text{ does not divide } x\}.$$

However, unlike $M(5,10)$, this monoid does not have the half-factorial property; one counterexample is $1600 = (4^2)(100) = 40^2$. Here, $x = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ does not require $r = s$, since 4 is not prime.

When students see such examples of ACM's, they naturally begin to seek a pattern to explain exactly which monoids have the half-factorial property. We have seen that $M(1,6)$ and $M(5,10)$ are half-factorial, yet $M(1,8)$ and $M(4,12)$ are not half-factorial. We offer the following additional examples, with particular interest in considering the case $a = 1$ vs. the case $a > 1$: $M(1,4)$ and $M(3,6)$ are half-factorial, yet $M(1,5)$, $M(4,6)$, and $M(9,18)$ are not half-factorial. In fact, the following classification theorem for half-factorial ACM's divides them into precisely these two cases.

*Theorem 3* (Banister, Chaika, Chapman, and Meyerson, *Colloquium Mathematicum*, 2007). Given $a \leq b$ in $\mathbb{N}$ with $a^2 \equiv a \pmod{b}$, $M(a,b)$ is half-factorial if and only if either:

$a = 1$ and $b \in \{1,2,3,4,6\}$; or

$a$ is prime and $a$ divides $b$.

Having outlined some examples and results involving factorization in monoids, we shift our attention to the question of where in the curriculum to place such material. At Presbyterian College, we currently have no number theory course, but we have a year-long sequence in abstract algebra, taught every other year. Last year, the first semester of this sequence included basic definitions and examples of monoids, while the second semester incorporated a brief supplement on factorization. In addition, our department has just started a team-taught senior capstone course, offered each spring. The past two springs, one-third of this course covered factorization in monoids and in rings of algebraic integers.

Two of the advantages of the senior capstone setting are the availability of more time to cover factorization in detail and the opportunity to encourage possible senior projects. The main disadvantage of this setting is that the context of factorization within abstract structures may be lost. In contrast, placing this material in abstract algebra would not only help motivate groups but also emphasize to students that we cannot take unique factorization for granted. Yet the main disadvantage of this approach is the time constraint always present in abstract algebra – which current topics would have to be sacrificed in order to cover the new material?

Following are more specifics from the senior capstone in the spring of 2009. After covering factorization in rings of algebraic integers and examining the question of unique vs. non-unique factorization into products of atoms, the course moved into a study of factorization in monoids. Of the five seniors enrolled in capstone, two worked on a final project involving arithmetical congruence monoids. By Theorem 3, we know that for a prime $b \geq 5$, $M(1,b)$ is not half-factorial. The goal of the project was to find a specific element in $M(1,b)$ as a counterexample to the half-factorial property. For example, how does one find the counterexample

$$15^6 = (3^6)(5^6) = (729)(15625)$$

in $M(1,7)$ without simply checking many possible factorizations?

One way to tackle this question is to use the following number theoretic result from abstract algebra. For any prime $b > 3$, there exist distinct $x$ and $y$ in $\{1,2,3,\ldots,b-1\}$ such that both $x$ and $y$ have order $b-1$ modulo $b$ and $xy \equiv 1 \pmod{b}$; that is, $x$ and $y$ are primitive roots and inverses modulo $b$ (Burton, 1997). Applying this result to find such $x$ and $y$, we then let $z = xy$ and note that $z \in M(1,b)$. Also, $z^{b-1} = x^{b-1} \cdot y^{b-1}$ provides a specific counterexample to the half-factorial property, with $b-1 > 2$ atoms on the left but only 2 atoms on the right. (Note that $x^{b-1}$ and $y^{b-1}$

must be atoms in $M(1, b)$, since $x$ and $y$ are primitive roots modulo $b$.) Returning to our previous example, we find the primitive roots 3 and 5 modulo 7, noting that 3 and 5 are inverses modulo 7. This allows us to use $15^6 = (3^6)(5^6) = (729)(15625)$ as a counterexample to the half-factorial property in $M(1, 7)$.

In considering where to place factorization material in the abstract algebra sequence, we note that the Gilbert and Gilbert text covers divisibility in Section 2.3 and the Unique Factorization Theorem for $\mathbb{N}$ in Section 2.4, with the definition of a group in Section 3.1 (Gilbert and Gilbert, 2005). Accordingly, the first-semester abstract algebra course last fall introduced arithmetical congruence monoids right after the Unique Factorization Theorem as a contrast. Formal definitions of monoids and groups were included later with Section 3.1. In the second semester, the coverage of rings in Chapter 6 was supplemented with additional material on factorization in monoids and in rings of algebraic integers.

In the interest of fairness, we conclude by noting that the use of non-unique factorization within the context of abstract algebra is not exactly a new idea. In fact, C. C. MacDuffee's text *An Introduction to Abstract Algebra* used what we call $M(1, 7)$ as an example where unique factorization fails, leaving $M(1, 5)$ as a similar homework exercise – and MacDuffee published his text almost seventy years ago (MacDuffee, 1940).

**References**


Banister, M.; Chaika, J.; Chapman, S. T.; Meyerson, W. On a result of James and Niven concerning unique factorization in congruence semigroups. *Elemente der Mathematik* 62 (2007), 68-72.

Banister, M.; Chaika, J.; Chapman, S. T.; Meyerson, W. On the arithmetic of arithmetical congruence monoids. *Colloquium Mathematicum* 108 (2007), 105-118.

Bland, P. *The Basics of Abstract Algebra.* W. H. Freeman, 2002.

Burton, D. *Elementary Number Theory.* McGraw-Hill, 1997 (3rd edition).

Chapman, S. T. Workshop reading list for "The Art of Factorization in Multiplicative Structures," 2007. Available on-line at http://www.trinity.edu/schapman/background.htm.

Durbin, J. *Modern Algebra: An Introduction.* Wiley & Sons, 2005 (5th edition).

Fraleigh, J. *A First Course in Abstract Algebra.* Addison Wesley, 2003 (7th edition).

Gallian, J. *Contemporary Abstract Algebra.* Houghton Mifflin, 2002 (5th edition).

Gilbert, J.; Gilbert, L. *Elements of Modern Algebra.* Thomson Brooks/Cole, 2005 (6th edition).

Hungerford, T. *Algebra.* Springer-Verlag, 1974.

James, R. D.; Niven, I. Unique factorization in multiplicative systems. *Proceedings of the American Mathematical Society* 5 (1954), 834-838.

MacDuffee, C. C. *An Introduction to Abstract Algebra.* Wiley & Sons, 1940.