Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 62 (2007)

Artikel: On a result of James and Niven concerning unique factorization in congruence semigroups

Autor: Banister, M. / Chaika, J. / Chapman, S.T.

DOI: https://doi.org/10.5169/seals-98911

Elem. Math. 62 (2007) 68 – 72
0013-6018/07/020068-5

Elemente der Mathematik

On a result of James and Niven concerning unique factorization in congruence semigroups

M. Banister, J. Chaika, S.T. Chapman and W. Meyerson

Scott Chapman received his Ph.D. from the University of North Texas in 1987. Since then he has held the positions of assistant, associate and full professor at Trinity University in San Antonio, Texas. The remaining authors of this paper worked under his direction in the 2003 Trinity University Research Experiences for undergraduates in the mathematics program.

Melissa Banister completed her undergraduate degree in 2004 at Harvey Mudd College and is now a graduate student at the University of California at Santa Barbara.

Jonathan Chaika completed his undergraduate degree in 2005 at the University of Iowa and is now a graduate student at Rice University.

William Meyerson completed his undergraduate degree in 2004 at Harvard. After completing the Tripos III Program at Cambridge with Distinction, he has enrolled in the graduate program at the University of California at Los Angeles.

The theory of non-unique factorizations in integral domains and monoids is a very active area of current research (see both [1] and [4] to view recent trends in this work). To demonstrate the phenomena of non-unique factorizations, we consider a result from the classical setting on uniqueness of factorizations by James and Niven [11]. We proceed as follows: Let $\mathbb{N}$ represent the natural numbers and suppose that $M \subseteq \mathbb{N}$ is a multiplicative semigroup. M is called a *congruence semigroup* if there exists a natural number n such

Im Hilbertschen Monoid $1+4\mathbb{N}_0 = \{1, 5, 9, 13, \ldots\}$ ($\mathbb{N}_0$ = natürliche Zahlen inklusive Null) ist die Zerlegung in irreduzible Faktoren nicht eindeutig: Es gilt zum Beispiel $441 = 9 \cdot 49 = 21 \cdot 21$. Hilberts Monoid ist ein Beispiel einer Kongruenz-Halbgruppe. Ein klassisches Resultat von James und Niven besagt, dass in einer Kongruenz-Halbgruppe M genau dann der Fundamentalsatz der Arithmetik gilt, wenn M aus allen Zahlen besteht, die relativ prim zu einer festen Zahl $n \in \mathbb{N}$ sind. Die Autoren der vorliegenden Arbeit untersuchen das andere Extrem, nämlich den Fall, wo M aus allen Zahlen besteht, die *nicht* relativ prim zu einer festen Zahl $n \in \mathbb{N}$ sind. Sie zeigen, dass in diesem Fall wenigstens die *Anzahl* der Primfaktoren bei der Zerlegung einer Zahl eindeutig ist.

that

$$x \in M \text{ and } x \equiv y \pmod{n} \text{ for } y \in \mathbb{N} \text{ implies } y \in M.$$

If M is as above, then we call n a *modulus of definition* of M. It follows directly from the definition that a congruence semigroup M of modulus n is completely determined by n and $M \cap \{1, 2, \ldots, n\}$. In a congruence semigroup M, we call an element x *irreducible* if x cannot be written in the form yz where y and z are nonunits of M (note that M possesses at most one unit, that being 1). The classic proof that all natural numbers can be factored as a product of primes can be easily modified to show that each nonunit of a congruence semigroup can be factored as a product of irreducible elements. In general, such a semigroup is called *atomic*. The interested reader can find more information on congruence semigroups in [8] and a review of basic algebra terminology in [10].

Examples of congruence semigroups can be found throughout the mathematical literature. In particular, Davenport [7, p. 21] uses the "Hilbert monoid"

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

as an example of a multiplicative system where the Fundamental Theorem of Arithmetic fails. To be precise, in this system,

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

and 9, 21 and 49 are all nonassociated irreducibles in $1 + 4\mathbb{N}_0$.

Hence, it is reasonable to ask which congruence semigroups do satisfy the Fundamental Theorem of Arithmetic. This question was answered by James and Niven in [11], where they prove the following interesting result. We will require the following notation: if $n \in \mathbb{N}$, then set

$$A(n) = \{m \mid m \in \mathbb{N} \text{ and } \gcd(m, n) = 1\}$$

and $B(n) = \mathbb{N} - A(n)$.

Theorem (James and Niven [11]). *Let M be a congruence semigroup. M has unique factorization of elements into products of irreducible elements if and only if there exists a positive integer n with $M \cap A(n) = A(n)$ and $M \cap B(n) = \emptyset$. In other words, M has unique factorization if and only if M consists of all elements relatively prime to a fixed positive integer n.*

An alternate proof of this theorem due to Halter-Koch (which uses the *divisor theory* of a commutative cancellative monoid) can be found in [9]. As a byproduct of the theorem, we point out that the modulus for a congruence semigroup is not unique. Notice that letting $n = 2$ or 4 in the theorem produces the same semigroup. Hence, this M can be viewed with modulus of definition 2 or 4. While the modulus is not unique, it is obvious that each congruence semigroup has a unique *minimal modulus*.

We are struck by what happens in the other extreme suggested by the theorem (i.e., when M consists of all elements not relatively prime to a fixed positive integer n). It turns out that such an M also exhibits an interesting factorization property.

Proposition. *Let $n = p_1^{n_1} \cdots p_k^{n_k}$ be a positive integer where the p_i's are distinct primes and the n_i's positive integers. Set*

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

M is a congruence semigroup with minimal modulus $n' = p_1 \cdots p_k$ which satisfies the following factorization property: If $x \in M$ and

$$x = y_1 \cdots y_s = z_1 \cdots z_t \qquad (*)$$

where each y_i and z_j is irreducible in M, then $s = t$.

Proof. Since the product of two numbers not relatively prime to n is again not relatively prime to n, M is closed under multiplication and is a multiplicative semigroup. It follows directly from the hypothesis of the proposition and elementary number theory that M is a congruence semigroup of modulus n. We show that M also has modulus $n' = p_1 \cdots p_k$. Setting

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

we obtain, as above, that M' is a congruence monoid of modulus n'. For $m \in \mathbb{N}$ it follows that $\gcd(m, n) \neq 1$ if and only if $\gcd(m, n') \neq 1$. Hence $M = M'$ and n' is a modulus of definition for M. We argue that this is the minimal modulus. Suppose M is defined by some modulus $d < n'$. Then there exists an i such that $p_i \nmid d$. Now, by definition $p_i \in M$, but note that $p_i^{\varphi(d)} \equiv 1 \pmod{d}$ (where φ represents the Euler φ-function), and hence $1 \in M$, a contradiction.

We now show that M satisfies $(*)$. By the definition of M, if $x \in M$, then $x = p_1^{\alpha_1} \cdots p_k^{\alpha_k} w$ where the α_i's are nonnegative integers (with at least one nonzero) and $w \in \mathbb{N}$ with $\gcd(w, n') = 1$. Define a function $f : M \to \mathbb{N}$ by

$$f(x) = \sum_{i=1}^{k} \alpha_i.$$

It is easy to verify that for x and $y \in M$ we have $f(xy) = f(x) + f(y)$.

Claim: $x \in M$ is irreducible in M if and only if $f(x) = 1$.

Proof of Claim: ($\Rightarrow$) Suppose that $x \in M$ and $f(x) > 1$. Write $x = pqk$ where p and q are not necessarily distinct primes which divide n' and $k \in \mathbb{N}$. By definition, p, q and qk are in M. Hence $pqk = (p)(qk)$ and thus is not irreducible in M.

($\Leftarrow$) Suppose $x = pk$ where p is a prime divisor of n' and $\gcd(k, n') = 1$. If $x = yz$ where y and $z \in M$, then $1 = f(x) = f(yz) = f(y) + f(z)$, which implies that either $f(y)$ or $f(z) = 0$, a contradiction.

Now, suppose that $x \in M$ and

$$x = y_1 \cdots y_s = z_1 \cdots z_t$$

where each y_i and z_j is irreducible in M. Then $f(x) = \sum_{i=1}^{s} f(y_i) = \sum_{i=1}^{t} f(z_i)$. Since each $f(y_i) = 1 = f(z_i)$, we have that $f(x) = s = t$ and the result follows. $\square$

We close with some comments concerning the proposition.

(1) An atomic semigroup (or monoid) which satisfies $(*)$ is called *half-factorial*. More information on the half-factorial property can be found in [5].

(2) The James and Niven result indicates that the set of odd integers, when viewed as a semigroup, has unique factorization. On the other hand, the proposition indicates that the set of even integers is half-factorial. As the proof indicates, a non-unique factorization in the set of even integers is given by

$$6 \cdot 10 = 2 \cdot 30,$$

where 2, 6, 10 and 30 are all irreducible as even integers.

(3) Not all half-factorial congruence semigroups are of the form M in the proposition. The Hilbert Monoid, $H = 1 + 4\mathbb{N}_0$ is also half-factorial. To see this, notice that $x \in H$ is irreducible if and only if

(i) x is prime in $\mathbb{N}$, or

(ii) $x = q_1 q_2$ where q_1 and q_2 are not necessarily distinct primes in $\mathbb{N}$ which are congruent to $3 \pmod 4$.

Hence, if $x \in H$ is of the form

$$x = p_1 \cdots p_s q_1 \cdots q_t$$

where each p_i is a prime congruent to $1 \pmod 4$ and each q_j is a prime congruent to $3 \pmod 4$, then any irreducible factorization of x in H has length $s + \frac{t}{2}$ (note that t will necessarily be even). Half-factorial congruence semigroups which are also arithmetic sequences have been characterized in [3, Theorem 2.6].

(4) To exhibit a congruence semigroup which is neither factorial nor half-factorial, let $M = 1 + 5\mathbb{N}_0$. In M we have

$$81 \cdot 2401 = 21 \cdot 21 \cdot 21 \cdot 21$$

and each of 81, 2401 and 21 are irreducible in M. A good general reference on monoids which do not satisfy the unique factorization property is [6].

(5) The function f in the proof of the proposition is known as a *semi-length function* on M. The reader can find more information on semi-length functions in [2].

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

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

References

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

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

[3] Banister, M.; Chaika, J.; Chapman, S.T.; Meyerson, W.: On the arithmetic of arithmetical congruence monoids. To appear in *Colloq. Math.*

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

[5] Chapman, S.T.; Coykendall, J.: Half-factorial domains: a survey. Non-Noetherian Ring Theory. *Math. Appl.* 520 (2000), 97–115.

[6] Chapman, S.T.; Geroldinger, A.: Krull Domains and Monoids, Their Sets of Lengths, and Associated Combinatorial Problems. In: [1], 73–112.

[7] Davenport, H.: *The Higher Arithmetic*. Dover Publications, New York 1983.

[8] Geroldinger, A.; Halter-Koch, F.: Congruence Monoids. *Acta Arith.* 112 (2004), 263–296.

[9] Halter-Koch, F.: Arithmetical semigroups defined by congruences. *Semigroup Forum* 42 (1991), 59–62.

[10] Hungerford, T.: *Abstract Algebra. An Introduction*. Brooks Cole, 1997.

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

M. Banister
Harvey Mudd College
Department of Mathematics
1250 N. Dartmouth Ave.
Claremont, CA 91711, USA
Current address:
University of California at Santa Barbara
Department of Mathematics
Santa Barbara, CA 93106
e-mail: bluerose91711@yahoo.com

J. Chaika
The University of Iowa
Department of Mathematics
14 MacLean Hall
Iowa City, IA 52242, USA
Current address:
Rice University
Department of Mathematics
6100 S. Main St.
Houston, TX 77005-1892, USA

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

W. Meyerson
Harvard University
Department of Mathematics
One Oxford Street
Cambridge, MA 02138, USA
Current address:
University of California at Los Angeles
Department of Mathematics
Box 951555
Los Angeles, CA 90095-1555, USA
e-mail: emannigis73@hotmail.com