Werk

Titel: Remarks on the structure of the multiplicative monoid of integers modulo m.

Autor: Konieczny, J.

Jahr: 1993

PURL: https://resolver.sub.uni-goettingen.de/purl?362162808_0046|log38

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Semigroup Forum Vol. 46 (1993) 266–269

SHORT NOTE

Remarks on the Structure of the Multiplicative Monoid of Integers Modulo m

Janusz Konieczny

Communicated by Gerard Lallement

Abstract. This note presents some results concerning $\mathcal{H}$-classes, Schützenberger groups, and regular elements in the multiplicative monoid $\mathbb{Z}_m$ of integers modulo m. It also shows that in $\mathbb{Z}_m$, the product of two $\mathcal{H}$-classes is an $\mathcal{H}$-class.

1. Introduction

Throughout the paper, $\mathbb{Z}$ is the set of integers, and for $x, y \in \mathbb{Z}$, xy is the product of x and y in $\mathbb{Z}$. For an integer $m \geq 1$, let $\mathbb{Z}_m$ be the multiplicative monoid of $\mathbb{Z}/m\mathbb{Z}$, the ring of congruence classes modulo m. For $x \in \mathbb{Z}$, the congruence class of x modulo m is denoted by $\overline{x}$; that is, $\overline{x} = \{ y \in \mathbb{Z} : x \equiv y \pmod{m} \} = \{ x + km : k \in \mathbb{Z} \}$. Then, $\mathbb{Z}_m = \{ \overline{x} : x \in \mathbb{Z} \} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, where $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ are distinct, and the multiplication in $\mathbb{Z}_m$ is given by $\overline{x}\,\overline{y} = \overline{xy}$. For example, in $\mathbb{Z}_{12}$, $\overline{4} \cdot \overline{5} = \overline{4 \cdot 5} = \overline{20} = \overline{8}$.

Denote by U_m the *group of units* of $\mathbb{Z}_m$. The group U_m consists of all congruence classes $\overline{u}$, such that $1 \leq u \leq m$ and $\gcd(u, m) = 1$, where $\gcd(u, m)$ is the greatest common divisor of u and m [2, Proposition 3.3.2]. It follows that $|U_m|$, the cardinality of U_m, is $\varphi(m)$, where φ is the *Euler φ function* [2, p. 20]. Note that as a set, U_m can be identified with the set of integers $\{ u \in \mathbb{Z} : 1 \leq u \leq m \text{ and } \gcd(u, m) = 1 \}$. For example, with this identification, $U_{12} = \{1, 5, 7, 11\}$.

We say that $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ is the *prime decomposition* of a positive integer m if $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $p_1, p_2, \ldots, p_s$ are primes, such that $p_1 < p_2 < \cdots < p_s$, and $\alpha_1, \alpha_2, \ldots, \alpha_s$ are positive integers.

Recall that in a commutative semigroup S, all *Green's relations* [3, p. 25] coincide. Denoting this common relation by $\mathcal{H}$, for $x, y \in S$, $x \mathcal{H} y$ iff $x = yu$ and $y = xv$ for some $u, v \in S^1$, where S^1 is the semigroup S with an identity adjoined. The semigroup S is partitioned into $\mathcal{H}$-classes H_x, $x \in S$.

The $\mathcal{H}$ relation in $\mathbb{Z}_m$ is characterized by an elementary result in number theory stating that for all $x, y \in \mathbb{Z}$:

$$x \equiv yk \pmod{m} \text{ for some } k \in \mathbb{Z} \iff \gcd(y, m) \mid x, \tag{1.1}$$

where for $a, b \in \mathbb{Z}$, $a \mid b$ means that a divides b in $\mathbb{Z}$.

By (1.1), we have immediately that for $\overline{x}, \overline{y} \in \mathbb{Z}_m$:

$$H_{\overline{x}} = H_{\overline{y}} \iff \gcd(x, m) = \gcd(y, m). \tag{1.2}$$

The condition (1.2) gives a natural 1–1 correspondence between the set of $\mathcal{H}$-classes of $\mathbb{Z}_m$ and the set Div_m of all positive divisors of m. Each $\mathcal{H}$-class contains the congruence class $\overline{d}$ of exactly one divisor d from Div_m. It follows that for $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, the number of $\mathcal{H}$-classes in $\mathbb{Z}_m$ is $(t_1+1) \cdots (t_s+1)$. This is, of course, exactly the same as the number of ideals in the ring $\mathbb{Z}/m\mathbb{Z}$.

2. Computation of $\mathcal{H}$-classes and Schützenberger Groups

Any $\mathcal{H}$-class of $\mathbb{Z}_m$ can be computed from a suitable group of units by a simple multiplication in $\mathbb{Z}$. For $x \in \mathbb{Z}$ and $A \subseteq \mathbb{Z}$, let $xA = \{xa : a \in A\}$ and $\overline{A} = \{\overline{a} : a \in A\}$. In the next theorem, $U_{\frac{m}{d}}$ is identified with the set of integers $\{u \in \mathbb{Z} : 1 \leq u \leq \frac{m}{d} \text{ and } \gcd(u, \frac{m}{d}) = 1\}$.

Theorem 2.1. *For any $\overline{x} \in \mathbb{Z}_m$, $H_{\overline{x}} = \overline{dU_{\frac{m}{d}}}$, where $d = \gcd(x, m)$.*

Proof. Follows from (1.2) and the observation that $dU_{\frac{m}{d}}$ consists of all elements $y \in \mathbb{Z}$, such that $1 \leq y \leq m$ and $\gcd(y, m) = d$. ∎

For example, for $m = 10$ and $\overline{x} = \overline{6}$, $d = \gcd(x, m) = 2$ and $U_{\frac{m}{d}} = U_5 = \{1, 2, 3, 4\}$. Thus, in $\mathbb{Z}_{10}$, $H_{\overline{6}} = \overline{2U_5} = \overline{\{2, 4, 6, 8\}} = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

Corollary 2.2. *For any $\overline{x} \in \mathbb{Z}_m$, $|H_{\overline{x}}| = \varphi(\frac{m}{d})$, where $d = \gcd(x, m)$.*

Proof. By Theorem 2.1, $|H_{\overline{x}}| = |\overline{dU_{\frac{m}{d}}}| = |dU_{\frac{m}{d}}| = |U_{\frac{m}{d}}| = \varphi(\frac{m}{d})$. The second equality follows from the fact that for each element $u \in U_{\frac{m}{d}}$, $1 \leq du \leq m$. ∎

For example, in $\mathbb{Z}_{150}$, $|H_{\overline{28}}| = \varphi(75) = \varphi(3 \cdot 5^2) = 2 \cdot 5 \cdot 4 = 40$.

Given a semigroup S, we can associate with any $\mathcal{H}$-class H of S a permutation group on the set H in the following way. Let $T(H) = \{x \in S^1 : Hx = H\}$, and let $\Gamma(H) = \{\rho_x : x \in T(H)\}$, where for $x \in T(H)$, $\rho_x : H \to H$ is the function defined by $h\rho_x = hx$. The function ρ_x is called the *inner right translation* by x. Then, $\Gamma(H)$ is a permutation group on H [3, Theorem 3.3, p. 32] called the *Schützenberger group* of H.

In the next theorem, $U_{\frac{m}{d}}$ is the group of units of $\mathbb{Z}_{\frac{m}{d}}$; that is, elements of $U_{\frac{m}{d}}$ are congruence classes modulo $\frac{m}{d}$. For $x \in \mathbb{Z}$, the congruence class of x modulo $\frac{m}{d}$ is denoted by $\overline{\overline{x}}$ (to distinguish it from $\overline{x}$, the congruence class of x modulo m).

Theorem 2.3. *For any $\overline{x} \in \mathbb{Z}_m$, the Schützenberger group $\Gamma(H_{\overline{x}})$ is isomorphic to the group of units $U_{\frac{m}{d}}$, where $d = \gcd(x, m)$.*

Proof. Define the function $f : U_{\frac{m}{d}} \to \Gamma(H_{\overline{x}})$ by:

$$f(\overline{\overline{u}}) = \rho_{\overline{u}}, \quad \text{for } \overline{\overline{u}} \in U_{\frac{m}{d}},$$

where $\rho_{\overline{u}}$ is the inner right translation by $\overline{u}$.

Let $\overline{\overline{u}} \in U_{\frac{m}{d}}$. Then, there is $v, 1 \leq v \leq \frac{m}{d}$, such that $\overline{\overline{u}} = \overline{\overline{v}}$. By Theorem 2.1, $\overline{d}\,\overline{v} = \overline{dv} \in H_{\overline{x}}$, and so, since $\overline{d} \in H_{\overline{x}}$, $H_{\overline{x}}\overline{v} \cap H_{\overline{x}} \neq \emptyset$. This implies $H_{\overline{x}}\overline{v} = H_{\overline{x}}$ [3, Lemma 3.2, p. 32], which shows $\rho_{\overline{v}} \in \Gamma(H_{\overline{x}})$. Now, since $u \equiv v \pmod{\frac{m}{d}}$, $du \equiv dv \pmod{m}$, and so $\overline{d}\rho_{\overline{u}} = \overline{d}\rho_{\overline{v}}$. Since $\overline{d} \in H_{\overline{x}}$, it follows that $\overline{h}\rho_{\overline{u}} = \overline{h}\rho_{\overline{v}}$ for every $\overline{h} \in H_{\overline{x}}$, which proves that f is well–defined.

Assume that for $\overline{\overline{u}}, \overline{\overline{v}} \in U_{\frac{m}{d}}$, $\rho_{\overline{u}} = \rho_{\overline{v}}$. Then, in particular, $\overline{du} = \overline{d}\,\overline{u} = \overline{d}\rho_{\overline{u}} = \overline{d}\rho_{\overline{v}} = \overline{d}\,\overline{v} = \overline{dv}$, which implies $m \mid d(u - v)$. Thus, $\frac{m}{d} \mid (u - v)$, and so $\overline{\overline{u}} = \overline{\overline{v}}$. Hence f is 1–1.

Let $\overline{z} \in T(H_{\overline{x}})$; that is, $\overline{z} \in \mathbb{Z}_m$ and $H_{\overline{x}}\overline{z} = H_{\overline{x}}$. Then, $\overline{d}\,\overline{z} \in H_{\overline{x}}$, and so, by Theorem 2.1, $\overline{d}\,\overline{z} = \overline{d}\,\overline{u}$ for some u, such that $1 \leq u \leq \frac{m}{d}$ and

$\gcd(u, \frac{m}{d}) = 1$. This implies that $\overline{\overline{u}} \in U_{\frac{m}{d}}$ and $\overline{h}\overline{z} = \overline{h}\overline{u}$ for every $\overline{h} \in H_{\overline{x}}$. Consequently, $\rho_{\overline{z}} = \rho_{\overline{u}}$, which proves that f is onto.

Assume $\overline{\overline{u}}, \overline{\overline{v}} \in U_{\frac{m}{d}}$, $\overline{h} \in H_{\overline{x}}$. Then, $\overline{h}\rho_{\overline{uv}} = \overline{h}\,\overline{uv} = (\overline{h}\,\overline{u})\overline{v} = (\overline{h}\rho_{\overline{u}})\rho_{\overline{v}} = \overline{h}(\rho_{\overline{u}}\rho_{\overline{v}})$. Thus, f is an isomorphism. ∎

Theorem 2.3 implies that any regular $\mathcal{H}$-class $H_{\overline{x}}$ of $\mathbb{Z}_m$ is isomorphic to $U_{\frac{m}{d}}$, where $d = \gcd(x, m)$. A direct proof of this corollary is contained in [1, Theorem 2.5].

For example, in $\mathbb{Z}_{36}$, $H_{\overline{4}} = \overline{4U_9} = \overline{4\{1,2,4,5,7,8\}} = \{\overline{4}, \overline{8}, \overline{16}, \overline{20}, \overline{28}, \overline{32}\}$. Since $\overline{28}$ is an idempotent in $\mathbb{Z}_{36}$, $H_{\overline{4}}$ is a group and $H_{\overline{4}} \cong U_9 \cong \mathbb{C}_6$, where $\mathbb{C}_6$ is a cyclic group of order 6 (for the structure of U_n see [2, Theorem 3, p. 44]).

3. Regular Elements

Recall that an element x of a commutative semigroup S is regular iff $x = x^2k$ for some $k \in S$, or equivalently $x\mathcal{H}x^2$. For a prime number p, denote by $\operatorname{ord}_p(m)$ the nonnegative integer α, such that p^α divides m and $p^{\alpha+1}$ does not divide m. For example, for $m = 12 = 2^2 3$, $\operatorname{ord}_2(m) = 2$ and $\operatorname{ord}_5(m) = 0$.

Theorem 3.1. *Let $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ be the prime decomposition of m. An element $\overline{x} \in \mathbb{Z}_m$ is regular if and only if for every prime number p:*

$$\operatorname{ord}_p(x) > 0 \implies \operatorname{ord}_p(x) \geq \operatorname{ord}_p(m). \tag{3.1}$$

Proof. By (1.2), $\overline{x}$ is regular in $\mathbb{Z}_m$ if and only if $\gcd(x, m) = \gcd(x^2, m)$, which happens if and only if (3.1) holds for every prime p. ∎

For example, in the monoid $\mathbb{Z}_{12}$, $\overline{8}$ is regular, while $\overline{10}$ is nonregular, since $\operatorname{ord}_2(10) = 1 < 2 = \operatorname{ord}_2(12)$.

Corollary 3.2.

(1) *$\mathbb{Z}_m$ has 2^s idempotents, where s is the number of primes dividing m.*

(2) *$\mathbb{Z}_m$ is regular if and only if m is a product of distinct primes.*

Proof. To prove (1), assume $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$. By Theorem 3.1, the congruence class $\overline{d}$ of a divisor d of m is regular in $\mathbb{Z}_m$ iff $d = p_{i_1}^{\alpha_{i_1}}p_{i_2}^{\alpha_{i_2}}\cdots p_{i_q}^{\alpha_{i_q}}$, where $q \geq 0$ and $1 \leq i_1 < i_2 < \cdots < i_q \leq s$. Thus, the number of divisors d, such that $\overline{d}$ is regular in $\mathbb{Z}_m$ is 2^s, which proves (1), since each $\mathcal{H}$-class of $\mathbb{Z}_m$ contains the congruence class of exactly one divisor of m.

(2) is immediate by Theorem 3.1. ∎

For example, $140 = 2^2 \cdot 5 \cdot 7$, and so, $\mathbb{Z}_{140}$ contains $2^3 = 8$ idempotents. The monoid $\mathbb{Z}_{140}$ is not regular, while $\mathbb{Z}_{70}$ is regular, since $70 = 2 \cdot 5 \cdot 7$.

The formula for the number of idempotents in $\mathbb{Z}_m$ is contained in [1, Theorem 2.2]. Corollary 3.2 can also be deduced from the fact that for $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, the ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to the direct sum of $\mathbb{Z}/p^{\alpha_i}\mathbb{Z}$, $i = 1, \ldots, s$ [2, p. 36], and consequently:

$$\mathbb{Z}_m \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_s}}. \tag{3.2}$$

This implies Corollary 3.2, since each $\mathbb{Z}_{p^{\alpha_i}}$ has 2 idempotents, and $\mathbb{Z}_{p^{\alpha_i}}$ is regular iff $\alpha_i = 1$.

4. Multiplication of $\mathcal{H}$-classes

The multiplication in any semigroup S induces a multiplication in the set $\mathcal{P}(S)$ of all subsets of S:

$$AB = \{ ab : a \in A, b \in B \}.$$

If S is commutative, then $\mathcal{H}$ is a congruence in S, which implies that for any $x, y \in S$, $H_x H_y \subseteq H_{xy}$. In the monoid $\mathbb{Z}_m$, the reverse inclusion also holds. Actually, even more is true: an $\mathcal{H}$-class $H_{\overline{x}\,\overline{y}}$ of $\mathbb{Z}_m$ can be obtained by multiplying $H_{\overline{y}}$ by any element from $H_{\overline{x}}$. The proof of this fact will be based on the following lemma, which states that any two elements from the same $\mathcal{H}$-class of $\mathbb{Z}_m$ differ by a unit.

Lemma 4.1. *For any elements $\overline{x}, \overline{y} \in \mathbb{Z}_m$, such that $\overline{x} \mathcal{H} \overline{y}$, there is a unit $\overline{u} \in U_m$, such that $\overline{x} = \overline{y}\,\overline{u}$.*

Proof. By (3.2), we may assume that $m = p^\alpha$, where p is a prime and $\alpha \geq 0$. Since $\overline{x} \mathcal{H} \overline{y}$, $\gcd(x, m) = \gcd(y, m) = p^\beta$ for some $\beta, 0 \leq \beta \leq \alpha$.

If $\beta = \alpha$, then $\overline{x} = \overline{y} = \overline{0}$, and so $\overline{x} = \overline{y}\,\overline{1}$.

Assume $\alpha - \beta > 0$ and consider $x_1 = \frac{x}{p^\beta}$ and $y_1 = \frac{y}{p^\beta}$. Then, $\gcd(x_1, p^{\alpha-\beta}) = \gcd(y_1, p^{\alpha-\beta}) = 1$, which implies $x_1 \equiv y_1 u \pmod{p^{\alpha-\beta}}$ for some $u \in \mathbb{Z}$, such that $\gcd(u, p^{\alpha-\beta}) = 1$. Since $\alpha - \beta > 0$, $\gcd(u, p^{\alpha-\beta}) = 1$ implies $\gcd(u, p^\alpha) = 1$, which shows that $\overline{u} \in U_m$. Finally, since $x_1 \equiv y_1 u \pmod{p^{\alpha-\beta}}$, $p^\beta x_1 \equiv p^\beta y_1 u \pmod{p^\alpha}$, and so $\overline{x} = \overline{p^\beta x_1} = \overline{p^\beta y_1 u} = \overline{p^\beta y_1}\,\overline{u} = \overline{y}\,\overline{u}$. ∎

Theorem 4.2. *For any $\overline{x}, \overline{y} \in \mathbb{Z}_m$, $H_{\overline{x}} H_{\overline{y}} = \overline{x} H_{\overline{y}} = H_{\overline{x}}\,\overline{y} = H_{\overline{x}\,\overline{y}}$.*

Proof. Since the inclusions $\overline{x} H_{\overline{y}}, H_{\overline{x}}\,\overline{y} \subseteq H_{\overline{x}} H_{\overline{y}} \subseteq H_{\overline{x}\,\overline{y}}$ are obvious, it suffices to prove $H_{\overline{x}\,\overline{y}} \subseteq \overline{x} H_{\overline{y}}$ ($H_{\overline{x}\,\overline{y}} \subseteq H_{\overline{x}}\,\overline{y}$ will follow by symmetry).

Assume $\overline{z} \in H_{\overline{x}\,\overline{y}}$. By Lemma 4.1, there is a unit $\overline{u} \in U_m$, such that $\overline{z} = \overline{x}\,\overline{y}\,\overline{u}$. Since $\overline{u}$ is a unit, $\overline{y}\,\overline{u} \in H_{\overline{y}}$, and so $\overline{z} = \overline{x}\,\overline{y}\,\overline{u} \in \overline{x} H_{\overline{y}}$. ∎

References

[1] Hewitt, E., and H. S. Zuckerman, *The Multiplicative Semigroup of Integers Modulo m*, Pacific J. Math. **10** (1960), 1291–1308.

[2] Ireland, K., and M. Rosen, "A Classical Introduction to Modern Number Theory," Springer-Verlag, New York, 1982.

[3] Lallement, G., "Semigroups and Combinatorial Applications," John Wiley & Sons, New York, 1979.

Department of Mathematics
Pennsylvania State University
University Park, PA 16802

Received April 8, 1992
and in final form May 5, 1992