ON MULTIPLICATIVE SEMIGROUPS OF RESIDUE CLASSES

E. T. PARKER[1]

The set of residue classes, modulo any positive integer, is commutative and associative under the operation of multiplication. The author made the conjecture: *For each finite commutative semigroup, S, there exists a positive integer, n, such that S is isomorphic with a subsemigroup of the multiplicative semigroup of residue classes* (mod n). (A semigroup is a set closed with respect to a single-valued associative binary operation.)

A counter-example to the above follows:

Let S be the set, $\{z, a, b, c\}$, with all products defined to be z except $bc=cb=a$.

Assume that there exists a positive integer, n, and four distinct residue classes, z, a, b, c (mod n) forming a system under multiplication isomorphic with S. Form the residue classes, $0=z-z$, $a'=a-z$, $b'=b-z$, $c'=c-z$. For x and y any ordered pair of z, a, b, c, we have $(x-z)(y-z)=xy-z-z+z=xy-z$. Thus, 0, a', b', c' form a multiplicative semigroup isomorphic with S, where 0 is the zero residue class. The following must hold: b'^2 and c'^2 are each the zero residue class (mod n), but $b'c'$ is a nonzero residue class; i.e., $n|\beta^2$, $n|\gamma^2$, $n\nmid\beta\gamma$, where β and γ are integers in the residue classes b' and c' (mod n) respectively. Since $n|\beta^2$ and $n|\gamma^2$, it follows that $n^2|\beta^2\gamma^2$, and $n|\beta\gamma$. The desired contradiction has been obtained.

We begin the main result of this paper with a

DEFINITION. For each prime-power, p^k, and each positive integer, m, we define a *basic semigroup*, $\sigma(p^k, m)$, with generators x and y, identity 1, annihilator 0, and commutative multiplication defined by:

$$x^ry^s = x^uy^v, \text{ if and only if } \begin{cases} 0 \leqq s = v < m, \text{ and} \\ r \equiv u \pmod{p^k} \end{cases}$$

$$\text{or } \begin{cases} s \geqq m, \text{ and} \\ v \geqq m. \end{cases}$$

(Letters used as exponents denote non-negative integers; the convention is adopted that any element to the zeroth power is 1.)

Received by the editors July 9, 1953 and, in revised form, December 27, 1953.

[1] The author wishes to express his sincere gratitude to the referee for finding an error in the original version of this paper, and for suggesting several clarifying alterations.

It follows that x is a generator of a cyclic group of order p^k, and $y^m = 0$.

We shall prove the

PRINCIPAL THEOREM. *The necessary and sufficient condition that a semigroup, S, be embeddable in a multiplicative semigroup of residue classes, modulo some positive integer, is that S be embeddable in a direct product of finitely many basic semigroups.*

"*Embeddable in* $\cdots$" means "isomorphic with a sub-semigroup (not necessarily proper) of $\cdots$."

We note that if a semigroup is embeddable in a second semigroup, then each sub-semigroup of the former is embeddable in the latter. Thus the principal theorem is equivalent to the following two theorems collectively:

THEOREM I. *Each multiplicative semigroup of residue classes is embeddable in a direct product of finitely many basic semigroups.*

THEOREM II. *Each direct product of finitely many basic semigroups is embeddable in a multiplicative semigroup of residue classes.*

We proceed now to a lemma, which may be in the literature:

LEMMA. *If $n = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes, and $c_1, c_2, \cdots, c_n$ are positive integers, then the multiplicative semigroup of residue classes* (mod n) *is isomorphic with the direct product of the multiplicative semigroups of residue classes* (mod $p_1^{c_1}$), (mod $p_2^{c_2}$), $\cdots$, (mod $p_n^{c_n}$).

PROOF. The result follows immediately by induction once we prove that if $n = n_1 n_2$ with $(n_1, n_2) = 1$, then the multiplicative semigroup of residue classes (mod n) is isomorphic with the direct product of multiplicative semigroups of residue classes (mod n_1) and (mod n_2). First, the correspondence between residue classes (mod n) and ordered pairs of residue classes (mod n_1) and (mod n_2) is one-to-one.[2] Since the sets of residue classes $\equiv 0$ (mod n_1), (mod n_2) constitute ideals, we ignore addition and have our result.[3]

We observe that, if S_1, S_1', S_2, S_2' are semigroups such that S_1 is embeddable in S_1' and S_2 is embeddable in S_2', then the direct product of S_1 and S_2 is embeddable in the direct product of S_1' and S_2'.

[2] Uspensky and Heaslet, *Elementary number theory*, New York, McGraw-Hill, 1939, Chapter VI, Section 5.

[3] Birkhoff and MacLane, *A survey of modern algebra*, New York, Macmillan, 1941, p. 360, problem 12 (p. 381 in rev. ed.).

By induction, this is true for any finite number of pairs of semigroups.

Applying the lemma, we may assert that Theorem I will be established when we prove:

THEOREM Ia. *Each multiplicative semigroup of residue classes modulo a prime-power is embeddable in a direct product of finitely many basic semigroups.*

Similarly, Theorem II follows when we prove:

THEOREM IIa. *For each basic semigroup, $\sigma(p^k, m)$, there exist infinitely many primes, q, such that $\sigma(p^k, m)$ is embeddable in the multiplicative semigroup of residue classes* (mod q^m).

PROOF OF THEOREM Ia. Case 1. The modulus is p^c, where p is an odd prime.

It is well known that the residue classes relatively prime to an *odd* prime-power modulus form a cyclic[4] group under multiplication. Let τ be a primitive root of p^c. The multiplicative semigroup of residue classes (mod p^c) is generated by τ and π, with commutative multiplication satisfying

$\tau^r\pi^s \equiv \tau^u\pi^v$ (mod p^c), if and only if

$$\begin{cases} 0 \leqq s = v < c, \text{ and} \\ r \equiv u \pmod{\phi(p^{c-s})}, \text{ where "}\phi\text{" denotes Euler's Function,} \end{cases}$$

or

$$\begin{cases} s \geqq c, \text{ and} \\ v \geqq c. \end{cases}$$

Let $p-1=q_1^{a_1}q_2^{a_2}\cdots q_k^{a_k}$, where $q_1, q_2, \cdots, q_k$ are distinct primes, and $a_1, a_2, \cdots, a_k$ are positive integers.

Let σ_i, with generators x_i and y_i, be $\sigma(q_i^{a_i}, c)$, for $i=1, 2, \cdots, k$.

Let σ_j^*, with generators x_j^* and y_j^*, be $\sigma(p^{c-j}, j)$, for $j=1, 2, \cdots, c-1$.

Form the direct product of the σ_i and the σ_j^*. Let

$$\tau \leftrightarrow (x_1, x_2, \cdots, x_k, \overset{*}{x_1}, \overset{*}{x_2}, \cdots, \overset{*}{x}_{c-1}),$$

$$\pi \leftrightarrow (y_1, y_2, \cdots, y_k, \overset{*}{y_1}, \overset{*}{y_2}, \cdots, \overset{*}{y}_{c-1}).$$

Now $\tau^r\pi^s \leftrightarrow (0, 0, \cdots, 0)$, the annihilator of the direct product, if

[4] Speiser, *Die Theorie der Gruppen von Endlicher Ordnung*, 3d ed., New York, Dover, 1943, Theorem 56, p. 57.

and only if $s \geqq c$. And, if $0 \leqq s < c$, and $\tau^r\pi^s = \tau^u\pi^v$ in the direct product, then $s = v$; for, when $0 \leqq s < c$, $x_1^r y_1^s = x_1^u y_1^v$ only if $s = v$. Further, if $0 \leqq s < c$, and $\tau^r\pi^s = \tau^u\pi^s$, then $r \equiv u \pmod{q_i^{a_i}}$ for $i = 1, 2, \cdots, k$; and $r \equiv u \pmod{p^{c-j}}$ for $j = s+1, s+2, \cdots, c-1$. It follows that $r \equiv u$ modulo the least common multiple of these various moduli; that is, $r \equiv u \pmod{p^{c-s-1}\prod_{(i)} q_i^{a_i}}$; $r \equiv u \pmod{p^{c-s-1}(p-1)}$; or, $r \equiv u \pmod{\phi(p^{c-s})}$. Conversely, if $0 \leqq s < c$, and $r \equiv u \pmod{\phi(p^{c-s})}$, the congruence may be factored into the preceding moduli, and the correspondences hold in the σ_i and the σ_j^*, so that

$$\tau^r\pi^s = \tau^u\pi^s.$$

This completes the proof of Case 1.

Case 2. The modulus is 2^c. For $c \geqq 3$, using some known results,[5] we may assert that the multiplicative semigroup of residue classes is generated by -1, -3, 2, and that

$$(-1)^\alpha(-3)^\beta 2^\gamma \equiv (-1)^{\alpha'}(-3)^{\beta'}2^{\gamma'} \pmod{2^c}$$

if and only if

$$\begin{cases} \gamma \geqq c, \text{ and} \\ \gamma' \geqq c \end{cases}$$

$$\text{or} \quad \gamma = \gamma' = c - 1$$

$$\text{or} \quad \begin{cases} 0 \leqq \gamma = \gamma' \leqq c - 2 \\ \alpha \equiv \alpha' \pmod{2} \\ \beta \equiv \beta' \pmod{2^{c-\gamma-2}}. \end{cases}$$

Form the direct product of the following σ_i, with generators x_i and y_i respectively: $\sigma_i = \sigma(2^i, c-i-1)$ for $i = 1, 2, 3, \cdots, c-2$; $\sigma_{c-1} = \sigma(2, c-1)$; $\sigma_c = \sigma(2, c-1)$; $\sigma_{c+1} = \sigma(p, c)$, p any prime. When we let

$$\begin{aligned} -1 &\leftrightarrow (1, 1, 1, \cdots, 1; x_c; 1), \\ -3 &\leftrightarrow (x_1, x_2, x_3, \cdots, x_{c-2}; x_{c-1}; 1; 1), \\ 2 &\leftrightarrow (y_1, y_2, y_3, \cdots, y_{c-2} = 0; y_{c-1}; y_c; y_{c+1}), \end{aligned}$$

we have the desired automorphism.

For $c = 2$, we note that under multiplication

$$\{0, 4, 1, 3\} \pmod{8} \sim \{0, 2, 1, 3\} \pmod{4}.$$

For $c = 1$, the proof is trivial.

Proof of Theorem IIa. Let q be a prime, $q \equiv 1 \pmod{p^k}$. By Dirichlet's theorem, there exist infinitely many such primes, q. The multiplicative semigroup of residue classes $\pmod{q^m}$ is generated by

[5] Speiser, op. cit., Theorem 56 and preceding paragraph.

t and q subject to the conditions,

$$t^r q^s \equiv t^u q^v \pmod{q^m}, \text{ if and only if}$$

$$\begin{cases} 0 \leqq s = v < m, \text{ and} \\ r \equiv u \pmod{\phi(q^{m-s})} \end{cases}$$

$$\text{or } \begin{cases} s \geqq m, \text{ and} \\ v \geqq m. \end{cases}$$

Let $\bar{t} = t^{\phi(q^m)/p^k}$. Then $\bar{t}^r q^s \equiv \bar{t}^u q^v \pmod{q^m}$ if and only if

$$\begin{cases} 0 \leqq s = v < m, \text{ and} \\ \dfrac{\phi(q^m)}{p^k} r \equiv \dfrac{\phi(q^m)}{p^k} u \pmod{\phi(q^{m-s})} \end{cases}$$

$$\text{or } \begin{cases} s \geqq m, \text{ and} \\ v \geqq m. \end{cases}$$

Using $\phi(q^m) = q^{m-1}(q-1)$ and the assumption that $(q-1)/p^k$ is an integer, an elementary calculation shows that the first of these conditions holds if and only if $r \equiv u \pmod{p^k}$.

Thus, the semigroup generated by $\bar{t}$ and q is isomorphic with $\sigma(p^k, m)$, and the proof is complete.

Final remarks. The principal theorem is rather analogous with the "Basis Theorem for Abelian groups." Trivially, if Σ is a semigroup embeddable in a multiplicative semigroup of residue classes, then such is also true for each sub-semigroup of Σ. Another immediate corollary is that if two semigroups are embeddable in multiplicative semigroups of residue classes, then their direct product is likewise embeddable. (This latter property was the crucial question in the investigations leading to this paper.)

From another standpoint, the analogy with the Basis Theorem breaks down. There exists a semigroup embeddable in a multiplicative semigroup of residue classes having a homomorphic image which fails to have this property. Let p be an odd prime. The residue classes (mod p^3) containing $0, p^2, -p^2, p, -p$ are distinct, and form a multiplicative semigroup. Let 0 and p^2 correspond to z, $-p^2$ to a, p to b, and $-p$ to c. We have a homomorphic image with S (at the beginning of the paper).

UNIVERSITY OF TEXAS