ON SMARANDACHE ALGEBRAIC STRUCTURES, I: THE COMMUTATIVE MULTIPLICATIVE SEMIGROUP $A(a,n)$

Maohua Le

Abstract. In this paper, under the Smarandache algorithm, we construct a class of commutative multiplicative semigroups.

Key words. Smarandache algorithm, commutative multiplicative semigroup.

In this serial papers we consider some algebraic structures under the Smarandache algorithm (see [2]). Let $n$ be a positive integer with $n>1$, and let

(1) $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$

be the factorization of $n$, where $p_1,p_2,\ldots,p_r$ are prime with $p_1<p_2<\cdots<p_k$ and $r_1,r_2,\ldots,r_k$ are positive integers. Further, let

(2) $n'=p_1p_2\cdots p_k$.

Then, for any fixed nonzero integer $a$, there exist unique integers $b,c,l,m,l',m'$ such that

(3) $a=bc$, $n=lm$, $n'=l'm'$,

(4) $l'=\gcd(l,n')$, $m'=\gcd(m,n')$,

(5) $l'=\gcd(a,n'),\gcd(c,n)=1$,

and every prime divisor of $b$ divides $l'$. Let

(6) $e=\begin{cases}0, & \text{if } l'=1, \\ \text{the least positive integer} & \text{which make } l' \mid a^e, \\ \text{which make } l' \mid a^e, & \text{if } l'>1. \end{cases}$

Since $\gcd(a,m)=1$, by the Fermat–Euler theorem (see [1, Theorem 72]), there exists a positive integer $t$ such that
Let $f$ be the least positive integer $t$ satisfying (7). For any fixed $a$ and $n$, let the set

$$A(a,n) = \begin{cases} 
\{1, a, \ldots, a^{f-1}\} \pmod n, & \text{if } f=1, \\
\{a, a^2, \ldots, a^{f-1}\} \pmod n, & \text{if } f>1.
\end{cases}$$

In this paper we prove the following result.

**Theorem.** Under the Smarandache algorithm, $A(a,n)$ is a commutative multiplicative semigroup.

**Proof.** Since the commutativity and the associativity of $A(a,n)$ are clear, it suffices to prove that $A(a,n)$ is closed.

Let $d^i$ and $d^j$ belong to $A(a,n)$. If $i+j \leq e+f-1$, then from (8) we see that $a^i a^j = a^{i+j}$ belongs to $A(a,n)$. If $i+j > e+f-1$, then $i+j \geq e+f$. Let $u = i+f-e$. Then there exists unique integers $v, w$ such that

$$u = f v + w, u \geq 0, \quad f > w \geq 0.$$  

Since $a^f \equiv 1 \pmod m$, we get from (9) that

$$a^{i+j} = a^u a^w \equiv a^u - a^w \equiv a^{f v + w} - a^w \equiv a^w a^w \equiv 0 \pmod m.$$  

Further, since $\gcd(l,m) = 1$ and $a^e \equiv 0 \pmod l$ by (6), we see from (10) that

$$a^{i+j} = a^{v+u} \pmod m.$$  

Notice that $e \leq e + w \leq e+f-1$. We find from (11) that $a^{i+j}$ belongs to $A(a,n)$. Thus the theorem is proved.
References


Department of Mathematics
Zhanjiang Normal College
Zhanjiang, Guangdong
P.R. CHINA