CHAPTER III

MULTIPLICATIVE SEMIGROUPS OF INTEGERS MODULO POSITIVE INTEGERS

Recall that for $n \in N$, n is square-free if and only if for every k in N- $\{1\}$, $k^2 \nmid n$. We have from Theorem 1.9 that for $n \in N$, the multiplicative semigroup Z_n is regular if and only if n is square-free. We know from Theorem 1.1 that every regular semigroup belongs to BQ. Then for $n \in N$, if n is square-free, then $(Z_n, \cdot) \in BQ$. Since the positive integer 4 is not square- free, by Theorem 1.9, Z_4 is not regular under multiplication. In fact, it is clear because $\bar{2}\bar{x}\bar{2} = \bar{0} \neq \bar{2}$ in Z_4 for every $x \in Z$. However, it is shown in this chapter that the multiplicative semigroup Z_4 belongs to BQ. We prove in this chapter that for $n \in N$, $(Z_n, \cdot) \in BQ$ if and only if either $n = 4$ or n is square-free.

The proof of Theorem 1.9 given in [4] is short by referring (1) if and only if (2), (2) if and only if (3) and (3) if and only if (4) where $n \in N$-$\{1\}$ and

(1) $(Z_n, \cdot)$ is regular,

(2) for every $a \in Z$, there exists $x \in Z$ such that $\bar{a}^2\bar{x} = \bar{a}$,

(3) for every $a \in Z$, $(a^2, n) \mid a$ where (a^2, n) is the g.c.d.of a^2 and n

and

(4) n is square-free.

To us that (3) if and only if (4) is not easily seen. Then we shall give here a proof of Theorem 1.9 by ourselves. Our proof uses simple knowledge of integers.

Assume that $(Z_n, \cdot)$ is regular. Suppose that n is not square-free. Then there exists a prime $p \in N$ such that $p^2 \mid n$. Since Z_n is regular, $\bar{p}^2\bar{x} = \bar{p}$ for some x $\in Z$. This implies that $n \mid p^2x - p$. But $p^2 \mid n$, so $p^2 \mid p(px - 1)$. Then $p \mid px - 1$ which is a contradiction. Hence n is square-free.

Conversely, assume that n is square-free. Let $p \in N$ be a prime. Then

$p^2 \nmid n$. Since p is prime, $(p^2, n) = 1$ or p. Then $p^2x + ny = 1$ or $p^2x + ny = p$ for some $x, y \in \boldsymbol{Z}$. If $p^2x + ny = p$, then $\bar{p}^2\bar{x} = \bar{p}$. If $p^2x + ny = 1$, then $p^3x + pny = p$, so $\bar{p}^2(\overline{px}) = \bar{p}$. This proves that $\bar{p}$ is regular in $(\boldsymbol{Z_n}, \cdot)$ for every prime $p \in \boldsymbol{N}$. For a general case, let $a \in \boldsymbol{N}$, if $a = 1$, then $\bar{1}$ is regular in $(\boldsymbol{Z_n}, \cdot)$. Suppose that $a > 1$. Then there exist primes $p_1, p_2, \ldots, p_m$ such that $a = p_1p_2 \ldots p_m$ for some $m \in \boldsymbol{N}$. From the above proof, for each $i \in \{1, 2, \ldots, m\}$, there exists $x_i \in \boldsymbol{Z}$ such that $\bar{p}_i{}^2\bar{x}_i = \bar{p}_i$. This implies that $\bar{a}^2(\bar{x}_1\bar{x}_2\bar{x}_3 \ldots \bar{x}_m) = \bar{a}$. Hence $\bar{a}$ is regular. But $\boldsymbol{Z_n} = \{\bar{x} \mid x \in \boldsymbol{Z}\} = \{\bar{x} \mid x \in \boldsymbol{N}\}$, so $(\boldsymbol{Z_n}, \cdot)$ is regular.

Lemma 3.1. *$(\boldsymbol{Z_4}, \cdot) \in \boldsymbol{BQ}$.*

Proof. Note that $\bar{1}$ and $\bar{3}$ are all the units of $(\boldsymbol{Z_4}, \cdot)$. Let B be a bi-ideal of $(\boldsymbol{Z_4}, \cdot)$. Then $\bar{0} \in B$. If $\bar{1} \in B$ or $\bar{3} \in B$, then $B = \boldsymbol{Z_4}$ which is a quasi-ideal of $\boldsymbol{Z_4}$. Suppose that $\bar{1} \notin B$ and $\bar{3} \notin B$. Then $B = \{\bar{0}\}$ or $B = \{\bar{0}, \bar{2}\}$. Since for these both cases B is an ideal of $(\boldsymbol{Z_4}, \cdot)$, we have that B is a quasi-ideal of $(\boldsymbol{Z_4}, \cdot)$.

This proves that every bi-ideal of $(\boldsymbol{Z_4}, \cdot)$ is a quasi-ideal. Hence $(\boldsymbol{Z_4}, \cdot) \in \boldsymbol{BQ}$. □

Theorem 3.2. *For $n \in \boldsymbol{N}$, $(\boldsymbol{Z_n}, \cdot) \in \boldsymbol{BQ}$ if and only if either $n = 4$ or n is square-free.*

Proof. Let $n \in \boldsymbol{N}$. If $n = 4$, by Lemma 3.1, $(\boldsymbol{Z_n}, \cdot) \in \boldsymbol{BQ}$. If n is square-free, by Theorem 1.9 $(\boldsymbol{Z_n}, \cdot)$ is regular, so $(\boldsymbol{Z_n}, \cdot) \in \boldsymbol{BQ}$ by Theorem 1.1.

For the converse, suppose that $n \neq 4$ and n is not square-free. Then there exists $a \in \boldsymbol{N} - \{1\}$ such that $a^2 \mid n$.

Case 1: $a > 2$. Since $a^2 \mid n$, $n = a^2x$ for some $x \in \boldsymbol{N}$. Let

$$B = \{\bar{0}, \overline{ax}\}.$$

Since $(\overline{ax}\ )^2 = (\overline{a^2x}\ )\overline{x} = \overline{n}\overline{x} = \overline{0}$, we have $B^2 = \{\overline{0}\}$, so B is a bi-ideal of $(\boldsymbol{Z}_n, \cdot)$. From the fact that $a > 2$, we get $2ax < a^2x = n$. Thus $0 < ax < 2ax < n$ which implies that $\overline{2ax} \neq \overline{0}$ and $\overline{2ax} \neq \overline{ax}$. Consequently, $\overline{2ax} = \overline{2}\,\overline{ax} \in Z_nB - B$. Thus B is not quasi-ideal of $(\boldsymbol{Z}_n, \cdot)$.

Case 2: $a = 2$. Thus $n = 2^k m$ for some $k \in N - \{1\}$ and some odd positive integer m.

Subcase 2.1: $k = 2$. Since $n \neq 4$ and m is odd, $m \geq 3$.

Set

$$B = (\overline{2})_b\,.$$

By Theorem 1.5, $B = \boldsymbol{Z}_n\overline{2}^2 \cup \{\overline{2}\} = \boldsymbol{Z}_n\overline{4} \cup \{\overline{2}\}$. Claim that B is not a quasi-ideal of $(\boldsymbol{Z}_n, \cdot)$. Since $\overline{6} = \overline{3}\,\overline{2}$ and $\overline{2} \in B$, $\overline{6} \in \boldsymbol{Z}_nB$. Suppose that $\overline{6} \in B$. Since $n \geq 12$, $\overline{6} \neq \overline{2}$, so $\overline{6} = \overline{x}\,\overline{4}$ for some $x \in \boldsymbol{Z}$. It follows that $2^2m \mid 4x - 6$ which implies that $2m \mid 2x - 3$. This is a contradiction because $2m$ is even and $2x - 3$ is odd. Hence $\overline{6} \notin B$. This shows that B is not a quasi-ideal of $(\boldsymbol{Z}_n, \cdot)$.

Subcase 2.2: $k > 2$ and k is even. Then $k = 2t$ for some $t \in N - \{1\}$, so $n = 2^{2t}m$. Let

$$B = \{\ \overline{0}\ ,\ \overline{2^t m}\ \}.$$

Since $(\overline{2^t m}\ )^2 = (\ \overline{2^{2t} m})\overline{m} = \overline{n}\overline{m} = \overline{0}$, $B^2 = \{\overline{0}\}$. Therefore B is a bi-ideal of $(\boldsymbol{Z}_n, \cdot)$. Since $t > 1$, we have $0 < 2^t m < 2^{t+1}m < 2^{2t}m = n$. Then $\overline{2^{t+1}m} \neq \overline{0}$ and $\overline{2^{t+1}m} \neq \overline{2^t m}$, so $\overline{2^{t+1}m} = \overline{2}(\overline{2^t m}) \in \boldsymbol{Z}_nB - B$. Hence B is not a quasi-ideal of $(\boldsymbol{Z}_n, \cdot)$.

Subcase 2.3: $k > 2$ and k is odd. Then $k = 2r + 1$ for some $r \in N$. Therefore we have $n = 2^{2r+1}m$. Set

$$B = \{\overline{0}\ ,\ \overline{2^r m}\ ,\ \overline{2^{2r} m^2}\ \}.$$

We have $B^2 = \{\overline{0}\ ,\ \overline{2^{2r} m^2}\ \}$ because $(\overline{2^r m})^2 = \overline{2^{2r} m^2}$, $(\overline{2^r m})(\overline{2^{2r} m^2}) = (\overline{2^{2r+1} m})(\overline{2^{r-1} m^2}) = \overline{n}(\overline{2^{r-1} m^2}) = \overline{0}$ and $(\overline{2^{2r} m^2})^2 = (\overline{2^{2r+1} m})(\overline{2^{2r-1} m^3}) =$

$\bar{n}(\overline{2^{2r-1}m^3})=\bar{0}$. To show that $Z_nB^2 \subseteq B$, let $x \in \boldsymbol{Z}$. If x is even, then $x = 2u$ for some $u \in \boldsymbol{Z}$, so $\bar{x}(\overline{2^{2r}m^2})=(\overline{2^{2r+1}m})(\overline{um})=\bar{n}(\overline{um})=\bar{0} \in B$. Next assume that x is odd. Then $x = v + 1$ for some even integer v. From the above proof, $\bar{v}(\overline{2^{2r}m^2})=\bar{0}$ which implies that $\bar{x}(\overline{2^{2r}m^2})=\overline{2^{2r}m^2} \in B$. Hence B is a bi-ideal of $(\boldsymbol{Z}_n, \cdot)$. Since $r + 1 \geq 2$, we have $2^{r+1} \geq 4 > 3$. Then $0 < 2^r m < 3(2^r m) < 2^{r+1}2^r m = 2^{2r+1}m = n$. This implies that $\overline{3(2^r m)} \neq \overline{2^r m}$. Suppose that $\overline{3(2^r m)} = \overline{2^{2r} m^2}$. Then $2^{2r+1}m \mid 2^{2r}m^2 - 3(2^r m)$, so $2^{r+1} \mid 2^r m - 3$ which is impossible since 2^{r+1} is even and $2^r m - 3$ is odd. Thus $\overline{3(2^r m)} \neq \overline{2^{2r} m^2}$. Therefore $\overline{3(2^r m)} \notin B$, so $\overline{3(2^r m)} = \bar{3}(\overline{2^r m}) \in \boldsymbol{Z}_nB - B$. This shows that B is not a quasi-ideal of $(\boldsymbol{Z}_n, \cdot)$.

Hence the theorem is completely proved. □