CHAPTER III

FULL MATRIX RINGS OVER $k\mathbb{Z}_m$

We have mentioned in Chapter I that any ring of the following rings has the intersection property of quasi-ideals.

(1) Commutative rings.

(2) Rings with identity.

(3) Regular rings.

Note that every quasi-ideal in a commutative ring is an ideal.

Let k, m and n be positive integers. The ring $k\mathbb{Z}_m$ need not have an identity and need not be regular. The ring $2\mathbb{Z}_{12}$ is an example. Since for every $x \in \mathbb{Z}$, $12 \nmid 2(2x-1)$, $(2\bar{x})\bar{2} \neq \bar{2}$ in $\mathbb{Z}_{12}$ for all $x \in \mathbb{Z}$. Then $2\mathbb{Z}_{12}$ has no identity. Since $12 \nmid 2(4x-1)$ for all $x \in \mathbb{Z}$, $\bar{2} \neq \bar{2}(2\bar{x})\bar{2}$ in $\mathbb{Z}_{12}$ for all $x \in \mathbb{Z}$. Then $2\mathbb{Z}_{12}$ is not regular.

If $k\mathbb{Z}_m$ is a zero ring, then $M_n(k\mathbb{Z}_m)$ is a zero ring. If $k\mathbb{Z}_m$ has an identity, then the identity $n \times n$ matrix over $k\mathbb{Z}_m$ is the identity of $M_n(k\mathbb{Z}_m)$. If $k\mathbb{Z}_m$ is regular, then by Theorem 1.2, $M_n(k\mathbb{Z}_m)$ is regular. Hence the ring $M_n(k\mathbb{Z}_m)$ has the intersection property of quasi-ideals if $k\mathbb{Z}_m$ is a zero ring, has an identity or is a regular ring.

The aim of this chapter is to give some sufficient conditions of k and m such that $M_n(k\mathbb{Z}_m)$ has the intersection property of quasi-ideals. These sufficient conditions of k and m are given such that $k\mathbb{Z}_m$ is a zero ring, has an identity or is a regular ring.

Let (k, m) denote the greatest common divisor of k and m. We remark that

$$k\mathbf{Z}_m = \left\{\overline{0}, \overline{(k, m)}, 2\overline{(k, m)}, \dots, \left(\frac{m}{(k, m)} - 1\right)\overline{(k, m)}\right\} = (k, m)\mathbf{Z}_m$$

and $|k\mathbf{Z}_m| = \frac{m}{(k, m)}$. We have that $k\mathbf{Z}_m = (k, m)(\frac{k}{(k, m)}\mathbf{Z}_m) \subseteq (k, m)\mathbf{Z}_m$. Since (k, m) is the greatest common divisor of k and m, $(k, m) = xk + ym$ for some $x, y \in \mathbf{Z}$. Then $(k, m)\mathbf{Z}_m = (xk + ym)\mathbf{Z}_m \subseteq k(x\mathbf{Z}_m) + y(m\mathbf{Z}_m) \subseteq k\mathbf{Z}_m + \{\overline{0}\} = k\mathbf{Z}_m$. Hence $k\mathbf{Z}_m = (k, m)\mathbf{Z}_m$. It remains to show that

$k\mathbf{Z}_m \subseteq \left\{\overline{0}, \overline{(k, m)}, 2\overline{(k, m)}, \dots, \left(\frac{m}{(k, m)} - 1\right)\overline{(k, m)}\right\}$ and for $i, j \in \{0, 1, 2, \dots, \frac{m}{(k, m)} - 1\}$, $i\overline{(k, m)} = j\overline{(k, m)}$ implies that $i = j$. Let $a \in \mathbf{Z}$. Then there exist q and r in $\mathbf{Z}$ such that $ak = qm + r$ and $0 \leq r < m$. Then $r = ak - qm$. Since $(k, m) \mid k$ and $(k, m) \mid m$, we have $(k, m) \mid r$. Then $\frac{r}{(k, m)} \in \mathbf{Z}$, $0 \leq \frac{r}{(k, m)} < \frac{m}{(k, m)}$ and in $\mathbf{Z}_m$,

$$\begin{aligned} k\overline{a} &= \frac{ka}{(k, m)}\overline{(k, m)} \\ &= \left(\frac{qm}{(k, m)} + \frac{r}{(k, m)}\right)\overline{(k, m)} \\ &= \frac{qm}{(k, m)}\overline{(k, m)} + \frac{r}{(k, m)}\overline{(k, m)} \\ &= \overline{0} + \frac{r}{(k, m)}\overline{(k, m)} \\ &= \frac{r}{(k, m)}\overline{(k, m)} \end{aligned}$$

which is an element of $\left\{\overline{0}, \overline{(k, m)}, 2\overline{(k, m)}, \dots, \left(\frac{m}{(k, m)} - 1\right)\overline{(k, m)}\right\}$. Next, let $s, t \in \{0, 1, 2, \dots, \frac{m}{(k, m)} - 1\}$ be such that $s \leq t$ and $s\overline{(k, m)} = t\overline{(k, m)}$.

Then $0 \leq t-s < \frac{m}{(k, m)}$ and $m \mid (t-s)(k, m)$. Therefore $\frac{m}{(k, m)} \mid (t-s)$. Since $0 \leq t-s < \frac{m}{(k, m)}$, $t-s=0$, so $s=t$.

Some examples of the previous remark are

$$8\mathbf{Z}_{36} = 4\mathbf{Z}_{36} = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}, \overline{32}\},$$

$$|8\mathbf{Z}_{36}| = \frac{36}{4} = 9,$$

$$125\mathbf{Z}_{15} = 5\mathbf{Z}_{15} = \{\overline{0}, \overline{5}, \overline{10}\},$$

$$|125\mathbf{Z}_{15}| = \frac{15}{5} = 3,$$

$$12\mathbf{Z}_{121} = \mathbf{Z}_{121}$$

and

$$|12\mathbf{Z}_{121}| = 121.$$

First, we give a necessary and sufficient condition of k and m such that $k\mathbf{Z}_m$ is a zero ring.

Theorem 3.1. *Let k and m be a positive integer. Then $k\mathbf{Z}_m$ is a zero ring if and only if $m \mid k^2$. Hence if $m \mid k^2$, then for every positive integer n, $M_n(k\mathbf{Z}_m)$ has the intersection property of quasi-ideals.*

Proof. Assume that $k\mathbf{Z}_m$ is a zero ring. Then $\overline{k}\,\overline{k} = \overline{0}$ in $k\mathbf{Z}_m$ which implies that $m \mid k^2$.

Conversely, if $m \mid k^2$, then $(\overline{k})^2 = \overline{0}$ in $\mathbf{Z}_m$. Thus for $x, y \in \mathbf{Z}$, $(k\overline{x})(k\overline{y}) = (\overline{k})^2\overline{x}\,\overline{y} = \overline{0}$ in $k\mathbf{Z}_m$. Hence $k\mathbf{Z}_m$ is a zero ring. □

From Theorem 3.1, we have as examples that $6\mathbf{Z}_9$ and $48\mathbf{Z}_{64}$ which are $3\mathbf{Z}_9$ and $16\mathbf{Z}_{64}$, respectively are both zero rings, and hence for every positive integer n, $M_n(6\mathbf{Z}_9)$ and $M_n(48\mathbf{Z}_{64})$ have the intersection property of quasi-ideals.

If k is a positive integer, then $2k \mid k^2$ if and only if $2 \mid k$. Hence the next corollary is obtained directly from Theorem 3.1.

Corollary 3.2. *Let k be a positive integer. Then $k\mathbf{Z}_{2k}$ is a zero ring if and only if k is even. Hence if k is even, then for every positive integer n, $M_n(k\mathbf{Z}_{2k})$ has the intersection property of quasi-ideals.*

In the next theorem, a necessary and sufficient condition for positive integers k and m such that $k\mathbf{Z}_m$ has an identity is given.

Theorem 3.3. *Let k and m be positive integers. Then $k\mathbf{Z}_m$ has an identity if and only if there exists $a \in \mathbf{Z}$ such that $m \mid k(ak-1)$. If such an a exists, then $k\bar{a}$ is the identity of $k\mathbf{Z}_m$ and $M_n(k\mathbf{Z}_m)$ has the intersection property of quasi-ideals for every positive integer n.*

Proof. Assume that $k\mathbf{Z}_m$ has an identity, say $k\bar{a}$ where $a \in \mathbf{Z}$. Since $\bar{k} \in k\mathbf{Z}_m$, $(k\bar{a})\bar{k} = \bar{k}$. Then $m \mid (k^2a - k)$, so $m \mid k(ka-1)$.

Conversely, let $a \in \mathbf{Z}$ be such that $m \mid k(ka-1)$. Then $\overline{k(ak-1)} = \bar{0}$. It follows that $(k\bar{a})\bar{k} = \bar{k}$. Thus for all $x \in \mathbf{Z}$, $(k\bar{a})(\bar{k}\bar{x}) = \bar{k}\bar{x}$. Hence $(k\bar{a})(k\bar{x}) = k\bar{x}$ for all $x \in \mathbf{Z}$. This proves that $k\bar{a}$ is the identity of $k\mathbf{Z}_m$. □

The following theorem is obtained from Theorem 3.3.

Theorem 3.4. *Let k and ℓ be positive integers and p a prime. Then $k\mathbf{Z}_{p^\ell k}$ has an identity if and only if $p \nmid k$. If $p \nmid k$, then for every positive integer n, $M_n(k\mathbf{Z}_{p^\ell k})$ has the intersection property of quasi-ideals.*

Proof. Assume that $k\mathbf{Z}_{p^\ell k}$ has an identity. By Theorem 3.3, there exists $a \in \mathbf{Z}$ such that $p^\ell k \mid k(ak-1)$. Then $p^\ell \mid (ak-1)$, so $p^\ell x = ak-1$ for some $x \in \mathbf{Z}$. Thus $p^\ell(-x) + ka = 1$. This implies that p^ℓ and k are relatively prime. It follows that $p \nmid k$ since p is a prime.

Conversely, assume that $p \nmid k$. Since p is a prime, p^ℓ and k are relatively prime. Then $ak + bp^\ell = 1$ for some $a, b \in \mathbf{Z}$. Then $ak^2 + bp^\ell k = k$, so $(p^\ell k)(-b) = k(ak-1)$. Therefore $p^\ell k \mid k(ak-1)$. By Theorem 3.3, $k\mathbf{Z}_{p^\ell k}$ has an identity. □

We obtain as examples from Theorem 3.4 that each of $7\mathbf{Z}_{28}$ and $4\mathbf{Z}_{44}$ has an identity, and hence for every positive integer n, the full $n \times n$ matrix rings over $7\mathbf{Z}_{28}$ and $4\mathbf{Z}_{44}$ have the intersection property of quasi-ideals.

It follows from Corollary 3.2 that for every positive integer k, $k\mathbf{Z}_{2k}$ is not a zero ring if and only if k is odd. The next theorem shows that a necessary and sufficient condition for the regularity of $k\mathbf{Z}_{2k}$ where k is a positive integer is that k is odd.

Theorem 3.5. *Let k be a positive integer. Then $k\mathbf{Z}_{2k}$ is a regular ring if and only if k is odd.*

Proof. Assume that $k\mathbf{Z}_{2k}$ is a regular ring. Since $k\mathbf{Z}_{2k} = \{\overline{0}, \overline{k}\}$ and $\overline{k} \neq \overline{0}$, $\overline{k}\,\overline{k}\,\overline{k} = \overline{k} \neq \overline{0}$. It follows that $\overline{k}\,\overline{k} \neq \overline{0}$. Then $k\mathbf{Z}_{2k}$ is not a zero ring. By Corollary 3.2, k is odd.

Conversely, assume that k is odd. By Corollary 3.2, $k\mathbf{Z}_{2k}$ is not a zero ring. Since $k\mathbf{Z}_{2k} = \{\overline{0}, \overline{k}\}$, $\overline{k}\,\overline{k} \neq \overline{0}$. Thus $\overline{k}\,\overline{k} = \overline{k}$ and so $\overline{k}\,\overline{k}\,\overline{k} = \overline{k}$. Hence $k\mathbf{Z}_{2k}$ is regular. □

If k is an even positive integer, then by Corollary 3.2, $k\mathbf{Z}_{2k}$ is a zero ring and hence $M_n(k\mathbf{Z}_{2k})$ is a zero ring for every positive integer n. If k is an odd positive integer, then by Theorem 3.5, $k\mathbf{Z}_{2k}$ is a regular ring and hence by Theorem 1.2, $M_n(k\mathbf{Z}_{2k})$ is regular for all positive integers n. Since every zero ring and every regular ring has the intersection property of quasi-ideals, we have the following theorem.

Theorem 3.6. *For any positive integers n and k, $M_n(k\mathbf{Z}_{2k})$ has the intersection property of quasi-ideals.*

The next theorem gives some sufficient conditions for a positive integer m such that $k\mathbf{Z}_m$ is a regular ring for every positive integer k. The following three lemmas are proved first.

Lemma 3.7. *For any positive integer m and integer x,*

$$m \mid x(x-1)(x-2)\ldots(x-m+1).$$

Proof. Let m be a positive integer and $x \in \mathbf{Z}$. Then there exist $q, r \in \mathbf{Z}$ such that $x = qm + r$ and $0 \leq r < m$. Then $m \mid (x-r)$ which implies that

$m \mid x(x-1)(x-2)\ldots(x-m+1)$ since $r \in \{0, 1, 2, \ldots, m-1\}$. □

Lemma 3.8. *Let m be an odd positive integer.*

(1) *If* $m \geq 2$, *then* $2 \mid (x^m - x)$ *for every integer* x.

(2) *If* $m \geq 3$, *then* $3 \mid (x^m - x)$ *for every integer* x.

Proof. Let x be an integer. If $m = 2$, then $x^m - x = x(x-1)$, so $2 \mid (x^m - x)$ by Lemma 3.7. Assume that $m > 2$. Since m is odd, $m-2$ is an odd positive integer. Then

$$\begin{aligned} x^m - x &= x(x^{m-1} - 1) \\ &= x(x-1)(x^{m-2} + x^{m-3} + \ldots + x + 1) \\ &= x(x-1)[(x^{m-2} + x^{m-3}) + (x^{m-4} + x^{m-5}) + \ldots + (x+1)] \\ &= x(x-1)[x^{m-3}(x+1) + x^{m-5}(x+1) + \ldots + (x+1)] \\ &= x(x-1)(x+1)(x^{m-3} + x^{m-5} + \ldots + 1). \end{aligned}$$

By Lemma 3.7, $2 \mid x(x-1)$ and $3 \mid x(x-1)(x+1)$. Hence $2 \mid (x^m - x)$ and $3 \mid (x^m - x)$. □

Lemma 3.9. *Let p be a prime. Then the following statements hold.*

(1) *If* $p > 2$, *then for every* $x \in \mathbb{Z}$, $(\bar{x})^p = \bar{x}$ *in* $\mathbb{Z}_{2p}$.

(2) *If* $p > 3$, *then for every* $x \in \mathbb{Z}$, $(\bar{x})^p = \bar{x}$ *in* $\mathbb{Z}_{3p}$.

Proof. Let $x \in \mathbb{Z}$. By Fermat's Theorem, $x^p \equiv x \pmod{p}$. Then $p \mid (x^p - x)$.

(1) Assume that $p > 2$. Then 2 and p are relatively prime. By Lemma 3.8, $2 \mid (x^p - x)$. Since $p \mid (x^p - x)$, $2p \mid (x^p - x)$. Then $(\bar{x})^p = \bar{x}$ *in* $\mathbb{Z}_{2p}$.

(2) Assume that $p > 3$. Then 3 and p are relatively prime. Since $3 \mid (x^p - x)$ by Lemma 3.7, $3p \mid (x^p - x)$. Hence $(\bar{x})^p = \bar{x}$ *in* $\mathbb{Z}_{3p}$. □

Theorem 3.10. (1) *Let k be a positive integer and p a prime such that $p > 2$. Then $k\mathbf{Z}_{2p}$ is a regular ring. Hence for every positive integer n, $M_n(k\mathbf{Z}_{2p})$ has the intersection property of quasi-ideals.*

(2) *Let k be a positive integer and p a prime such that $p > 3$. Then $k\mathbf{Z}_{3p}$ is a regular ring. Hence for every positive integer n, $M_n(k\mathbf{Z}_{3p})$ has the intersection property of quasi-ideals.*

Proof. (1) By Lemma 3.9(1), for every $x \in \mathbf{Z}$, $(k\bar{x})^p = k\bar{x}$ in $\mathbf{Z}_{2p}$ and so $(k\bar{x})(k\bar{x})^{p-2}(k\bar{x}) = k\bar{x}$ in $\mathbf{Z}_{2p}$. This proves that $k\mathbf{Z}_{2p}$ is a regular ring.

(2) If $x \in \mathbf{Z}$, then by Lemma 3.9(2), $(k\bar{x})^p = k\bar{x}$ in $\mathbf{Z}_{3p}$ and so $(k\bar{x})(k\bar{x})^{p-2}(k\bar{x}) = k\bar{x}$ in $\mathbf{Z}_{3p}$. Hence $k\mathbf{Z}_{3p}$ is a regular ring. □

We give as examples that $6\mathbf{Z}_{10}$ and $9\mathbf{Z}_{21}$ are regular rings by Theorem 3.10. Hence for every positive integer n, $M_n(6\mathbf{Z}_{10})$ and $M_n(9\mathbf{Z}_{21})$ have the intersection property of quasi-ideals.

We give a remark about all possible rings given in Theorem 3.10.

Remark. Let k be a positive integer and p a prime.

(1) Assume that $p > 2$.

(1.1) If $2 \mid k$ and $p \mid k$, then $k\mathbf{Z}_{2p} = \{\bar{0}\}$.

(1.2) If $2 \mid k$ and $p \nmid k$, then $k\mathbf{Z}_{2p} = 2\mathbf{Z}_{2p} = \{\bar{0}, \bar{2}, \dots, (p-1)\bar{2}\}$ which is isomorphic to the field $\mathbf{Z}_p$.

(1.3) If $2 \nmid k$ and $p \mid k$, then $k\mathbf{Z}_{2p} = p\mathbf{Z}_{2p} = \{\bar{0}, \bar{p}\}$ which is isomorphic to the field $\mathbf{Z}_2$.

(1.4) If $2 \nmid k$ and $p \nmid k$, then $k\mathbf{Z}_{2p} = \mathbf{Z}_{2p}$.

(2) Assume that $p > 3$.

(2.1) If $3 \mid k$ and $p \mid k$, then $k\mathbf{Z}_{3p} = \{\bar{0}\}$.

(2.2) If $3 \mid k$ and $p \nmid k$, then $k\mathbf{Z}_3 = 3\mathbf{Z}_{3p} = \{\overline{0}, \overline{3}, \dots, (p-1)\overline{3}\}$ which is isomorphic to the field $\mathbf{Z}_p$.

(2.3) If $3 \nmid k$ and $p \mid k$, then $k\mathbf{Z}_{3p} = p\mathbf{Z}_{3p} = \{\overline{0}, \overline{p}, 2\overline{p}\}$ which is isomorphic to the field $\mathbf{Z}_3$.

(2.4) If $3 \nmid k$ and $p \nmid k$, then $k\mathbf{Z}_{3p} = \mathbf{Z}_{3p}$.

Proof. (1.1) If $2 \mid k$ and $p \mid k$, then $2p \mid k$ since 2 and p are relatively prime which implies that $k\mathbf{Z}_{2p} = \{\overline{0}\}$.

(1.2) Assume that $2 \nmid k$ and $p \nmid k$. Since 2 and p are relatively prime, $2p$ and k are relatively prime. Then $k\mathbf{Z}_{2p} = \mathbf{Z}_{2p}$.

(1.3) Assume that $2 \mid k$ and $p \nmid k$. Then $(2p, k) = 2$, so $k\mathbf{Z}_{2p} = 2\mathbf{Z}_{2p} = \{\overline{0}, \overline{2}, \dots, (p-1)\overline{2}\}$ and $|k\mathbf{Z}_{2p}| = p$. To show that the ring $k\mathbf{Z}_{2p}$ is a field of order p, it suffices to show that $2\mathbf{Z}_{2p}$ has no zero divisor. Let $x, y \in \mathbf{Z}$ be such that $(2\overline{x})(2\overline{y}) = \overline{0}$ in $\mathbf{Z}_{2p}$. Then $2p \mid 4xy$. Thus $p \mid 2xy$. Since 2 and p are relatively prime, $p \mid xy$. Then $p \mid x$ or $p \mid y$ since p is a prime. Hence $2p \mid 2x$ or $2p \mid 2y$. Consequently, $2\overline{x} = \overline{0}$ or $2\overline{y} = \overline{0}$ in $\mathbf{Z}_{2p}$. Therefore $2\mathbf{Z}_{2p}$ has no zero divisor. Then $k\mathbf{Z}_{2p}$ is a field of order p, so it is isomorphic to $\mathbf{Z}_p$.

(1.4) Assume $2 \nmid k$ and $p \mid k$. Then $(2p, k) = p$, so $k\mathbf{Z}_{2p} = p\mathbf{Z}_{2p} = \{\overline{0}, \overline{p}\}$ and $|k\mathbf{Z}_{2p}| = 2$. If $2p \mid p^2$, then $2 \mid p$, a contradiction. Thus $\overline{p}\,\overline{p} \neq \overline{0}$ in $\mathbf{Z}_{2p}$. Therefore $k\mathbf{Z}_{2p}$ has no zero divisor. It follows that the ring $k\mathbf{Z}_{2p}$ is isomorphic to the field $\mathbf{Z}_2$.

(2.1) If $3 \mid k$ and $p \mid k$, then $3p \mid k$ since 3 and p are relatively prime which implies that $k\mathbf{Z}_{3p} = \{\overline{0}\}$.

(2.2) Assume that $3 \nmid k$ and $p \nmid k$. Since 3 and p are relatively prime, $3p$ and k are relatively prime. Then $k\mathbf{Z}_{3p} = \mathbf{Z}_{3p}$.

(2.3) Assume that $3 \mid k$ and $p \nmid k$. Then $(3p, k) = 3$, so $k\mathbf{Z}_{3p} = 3\mathbf{Z}_{3p} = \{\overline{0}, \overline{3}, \ldots, (p-1)\overline{3}\}$ and $|k\mathbf{Z}_{3p}| = p$. To show that the ring $3\mathbf{Z}_{3p}$ has no zero divisor, let $x, y \in \mathbf{Z}$ be such that $(3\overline{x})(3\overline{y}) = \overline{0}$ in $\mathbf{Z}_{3p}$. Then $3p \mid 9xy$, so $p \mid 3xy$. Since 3 and p are relatively prime, $p \mid xy$. Then $p \mid x$ or $p \mid y$. Then $3p \mid 3x$ or $3p \mid 3y$. It follows that $3\overline{x} = \overline{0}$ or $3\overline{y} = \overline{0}$ in $\mathbf{Z}_{3p}$. Therefore the ring $k\mathbf{Z}_{3p}$ is isomorphic to the field $\mathbf{Z}_p$.

(2.4) Assume $3 \nmid k$ and $p \mid k$. Then $(3p, k) = p$. Therefore $k\mathbf{Z}_{3p} = p\mathbf{Z}_{3p} = \{\overline{0}, \overline{p}, 2\overline{p}\}$ and $|k\mathbf{Z}_{3p}| = 3$. Since $3p \nmid p^2$, $3p \nmid 2p^2$ and $3p \nmid 4p^2$, it follows that $\overline{p}\,\overline{p} \neq \overline{0}$, $\overline{p}(2\overline{p}) \neq \overline{0}$ and $(2\overline{p})(2\overline{p}) \neq \overline{0}$ in $\mathbf{Z}_{3p}$. This proves that $k\mathbf{Z}_{3p}$ has no zero divisor. Hence the ring $k\mathbf{Z}_{3p}$ is isomorphic to the field $\mathbf{Z}_3$. □

Observe from the remarks that the rings in Theorem 3.10(1) and 3.10(2) always have an identity. Then without referring their regularity, we can obtain that for any positive integer n, the full $n \times n$ matrix rings over each of those rings has the intersection property of quasi-ideals. However, Theorem 3.10 shows that those rings are also regular.