Publ. Math. Debrecen
94/3-4 (2019), 369–380
DOI: 10.5486/PMD.2019.8319

On the additive and multiplicative structures of the exceptional units in finite commutative rings

By SU HU (Guangzhou) and MIN SHA (Sydney)

Abstract. Let R be a commutative ring with identity. A unit u of R is called exceptional if $1-u$ is also a unit. When R is a finite commutative ring, we determine the additive and multiplicative structures of its exceptional units; and then as an application we find a necessary and sufficient condition under which R is generated by its exceptional units.

1. Introduction

1.1. Background. Let R be a commutative ring with $1 \in R$ and R^* its group of units. A unit $u \in R$ is called *exceptional* if $1-u \in R^*$. We denote by R^{**} the set of exceptional units of R. This concept was introduced by Nagell [7] in 1969 in order to solve certain cubic Diophantine equations. The key idea is that the solution of many Diophantine equations can be reduced to the solution of a finite number of unit equations of type

$$ax + by = 1,$$

where x and y are restricted to units in the ring of integers of some number field (see [2] for a treatise on unit equations). By choosing $a = b = 1$, we obtain the concept of exceptional unit.

Let $\mathbb{Z}_n$ be the residue class ring of the integers $\mathbb{Z}$ modulo a positive integer n. Sander [9, Theorem 1.1] determined the number of representations of an element in $\mathbb{Z}_n$ as the sum of two exceptional units. Recently, Zhang and Ji [12,

Mathematics Subject Classification: 11B13, 11D45, 11T24.
Key words and phrases: exceptional unit, finite commutative ring, character sum.

Theorem 1.5] extended Sander's result to the case when R is a residue class ring of a number field. Using a different approach with the aid of exponential sums, for any integer $k \geq 2$ YANG and ZHAO [11, Theorem 1] obtained an exact formula for the number of ways to represent an element of $\mathbb{Z}_n$ as a sum of k exceptional units. Most recently, MIGUEL [6, Theorem 1] generalized the result of Yang and Zhao to the case of finite commutative rings. SANDER [10] persued another structural perspective by investigating the atom decomposition of sets of exceptional units in $\mathbb{Z}_n$.

1.2. Our situation. In this paper, we consider the additive and multiplicative structures of the exceptional units of a finite commutative ring. We show that as in [6] and [11], there is an exact formula for the number of ways to represent a unit as a product of k exceptional units. As an application and in combination with Miguel's result, we completely determine the additive and multiplicative structures of such exceptional units in our situation (see Theorems 1.7 and 1.10 below); and then as an application we find a necessary and sufficient condition under which R is generated by its exceptional units (see Corollaries 1.8 and 1.11 below).

From now on, R is a finite commutative ring with identity. It is well-known that R can be uniquely expressed as a direct sum of local rings; see [5, page 95]. So, in the following we assume that

$$R = R_1 \oplus \cdots \oplus R_n,$$

where each R_i, for $i = 1, \ldots, n$, is a local ring. Then, each element $c \in R$ can be represented as $(c_1, \ldots, c_n)$ with $c_i \in R_i$, $i = 1, \ldots, n$. For each $i = 1, \ldots, n$, suppose that M_i is the unique maximal ideal of R_i, and put

$$m_i = |M_i|, \qquad q_i = |R_i/M_i|.$$

Here, each residue field R_i/M_i is a finite field, and thus q_i is a power of a prime.

We first state our results in Sections 1.3, 1.4, 1.5 and 1.6, and then we give proofs in Section 2.

1.3. Additive structure of units. Before further work, we first determine the additive structure of R^*. For $c \in R$, we define the set

$$\Psi_{k,R}(c) = \{(x_1, \ldots, x_k) \in (R^*)^k : x_1 + \cdots + x_k = c\},$$

and put

$$\psi_{k,R}(c) = |\Psi_{k,R}(c)|.$$

That is, $\psi_{k,R}(c)$ is the number of ways to represent c as a sum of k units. KIANI and MOLLAHAJIAGHAEI obtained the following formula for $\psi_{k,R}(c)$ (see [3, Theorem 2.5]), which generalizes the result in [8].

Theorem 1.1 ([3]). *For any integer $k \geq 2$ and any $c = (c_1, \ldots, c_n) \in R$, we have*

$$\psi_{k,R}(c) = \prod_{i=1}^{n} m_i^{k-1} q_i^{-1} \mu_{k,R_i}(c_i),$$

where

$$\mu_{k,R_i}(c_i) = \begin{cases} (q_i - 1)^k + (-1)^k (q_i - 1), & \text{if } c_i \in M_i, \\ (q_i - 1)^k + (-1)^{k+1}, & \text{if } c_i \in R_i \setminus M_i. \end{cases}$$

Theorem 1.1 can be directly used to establish the additive structure of the units of R.

Corollary 1.2. *The following hold:*
(i) *If $q_i > 2$ for each $i = 1, \ldots, n$, then we have*

$$R^* + R^* = R.$$

(ii) *If $q_1 = \cdots = q_s = 2$ $(s \geq 1)$ and $q_j > 2$ for each $j > s$, then for any integer $k \geq 2$ we have*

$$\sum_{i=1}^{k} R^* = \begin{cases} (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{j>s} R_j), & \text{if } k \text{ is even}, \\ (\oplus_{i=1}^{s} R_i \setminus M_i) \oplus (\oplus_{j>s} R_j), & \text{otherwise}. \end{cases}$$

In particular, each element of R is a sum of units if and only if $s = 1$.

In Corollary 1.2 (ii), if $s = n$, then the part $\oplus_{j>s} R_j$ does not exist.

Corollary 1.3. *The ring R is generated by its units if and only if there is at most one q_i equal to 2.*

1.4. Additive structure of exceptional units. We now turn our attention to exceptional units. In Theorem 1.1, if we choose $k = 2$ and $c = 1$, then we directly get the size of R^{**}.

Corollary 1.4. *We have*

$$|R^{**}| = \prod_{i=1}^{n} m_i (q_i - 2).$$

We directly have:

Corollary 1.5. *$R^{**} \neq \emptyset$ if and only if each $q_i \geq 3$, $i = 1, \ldots, n$.*

For $c \in R$, define the set

$$\Phi_{k,R}(c) = \{(x_1, \ldots, x_k) \in (R^{**})^k : x_1 + \cdots + x_k = c\},$$

and denote

$$\varphi_{k,R}(c) = |\Phi_{k,R}(c)|.$$

That is, $\varphi_{k,R}(c)$ is the number of ways to represent c as a sum of k exceptional units. Miguel gave an exact formula for $\varphi_{k,R}(c)$; see [6, Theorem 1].

Theorem 1.6 ([6])**.** *For any integer $k \geq 2$ and any $c = (c_1, \ldots, c_n) \in R$, we have*

$$\varphi_{k,R}(c) = \prod_{i=1}^{n} (-1)^k m_i^{k-1} q_i^{-1} \rho_{k,R_i}(c_i),$$

where

$$\rho_{k,R_i}(c_i) = q_i \sum_{\substack{j=0 \\ j \equiv c_i \pmod{M_i}}}^{k} \binom{k}{j} + (2 - q_i)^k - 2^k.$$

Using Theorem 1.6, we completely determine the additive structure of R^{**} in the following theorem. Note that by Corollary 1.5 we need to exclude the case when there is some q_i equal to 2.

Theorem 1.7. *Assume that each $q_i \geq 3$, $i = 1, \ldots, n$. Then, the following hold:*

(i) *If each q_i is greater than 4, $i = 1, \ldots, n$, we have*

$$R^{**} + R^{**} = R.$$

(ii) *If $q_1 = \cdots = q_s = 3$ ($s \geq 1$) and $q_j > 4$ for each $j > s$, then for any $k \geq 2$ we have*

$$\sum_{i=1}^{k} R^{**} = \begin{cases} (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{j>s} R_j), & \text{if } k \equiv 0 \pmod 3, \\ (\oplus_{i=1}^{s} 2 + M_i) \oplus (\oplus_{j>s} R_j), & \text{if } k \equiv 1 \pmod 3, \\ (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{j>s} R_j), & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

(iii) *If $q_1 = \cdots = q_t = 4$ ($t \geq 1$) and $q_j > 4$ for each $j > t$, then for any $k \geq 2$ we have*

$$\sum_{i=1}^{k} R^{**} = \begin{cases} (\oplus_{i=1}^{t} (M_i \cup 1 + M_i)) \oplus (\oplus_{j>t} R_j), & \text{if } k \text{ is even}, \\ (\oplus_{i=1}^{t} (R_i \setminus (M_i \cup 1 + M_i))) \oplus (\oplus_{j>t} R_j), & \text{otherwise}. \end{cases}$$

(iv) *Assume that* $q_1 = \cdots = q_s = 3$ $(s \geq 1)$, $q_{s+1} = \cdots = q_{s+t} = 4$ $(t \geq 1)$, *and* $q_j > 4$ *for each* $j > s + t$. *Then, for any* $k \geq 2$ *we have*

$$\sum_{i=1}^{k} R^{**} = \begin{cases} (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{i=s+1}^{s+t}(M_i \cup 1 + M_i)) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 0 \pmod 6, \\ (\oplus_{i=1}^{s} 2 + M_i) \oplus (\oplus_{i=s+1}^{s+t}(R_i \setminus (M_i \cup 1 + M_i))) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 1 \pmod 6, \\ (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{i=s+1}^{s+t}(M_i \cup 1 + M_i)) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 2 \pmod 6, \\ (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{i=s+1}^{s+t}(R_i \setminus (M_i \cup 1 + M_i))) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 3 \pmod 6, \\ (\oplus_{i=1}^{s} 2 + M_i) \oplus (\oplus_{i=s+1}^{s+t}(M_i \cup 1 + M_i)) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 4 \pmod 6, \\ (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{i=s+1}^{s+t}(R_i \setminus (M_i \cup 1 + M_i))) \oplus (\oplus_{j>s+t} R_j), \\ \qquad\qquad \text{if } k \equiv 5 \pmod 6. \end{cases}$$

Using Theorem 1.7, we directly obtain a necessary and sufficient condition under which every element of R is a sum of its exceptional units.

Corollary 1.8. *Assume that each* $q_i \geq 3$, $i = 1, \ldots, n$. *Then, every element of* R *is a sum of its exceptional units if and only if there is at most one* q_i *equal to* 3 *and at most one* q_j *equal to* 4 *for* $i, j = 1, \ldots, n$.

1.5. Multiplicative structure of exceptional units. Here, we want to determine the multiplicative structure of exceptional units of R.

For a unit $u \in R^*$, define the set

$$\Theta_{k,R}(u) = \{(x_1, \ldots, x_k) \in (R^{**})^k : x_1 x_2 \cdots x_k = u\},$$

and denote

$$\theta_{k,R}(u) = |\Theta_{k,R}(u)|.$$

That is, $\theta_{k,R}(u)$ is the number of ways to represent u as a product of k exceptional units.

By Corollary 1.5, if there is some $q_i = 2$, then $R^{**} = \emptyset$. Certainly we need to exclude this case. Applying the same arguments as in [6], we obtain an exact formula for $\theta_{k,R}(u)$.

Theorem 1.9. *Assume that each $q_i \geq 3$, $i = 1, \ldots, n$. Then, for any integer $k \geq 2$ and any $u = (u_1, \ldots, u_n) \in R^*$, we have*

$$\theta_{k,R}(u) = \prod_{i=1}^{n} m_i^{k-1}(q_i - 1)^{-1}\sigma_{k,R_i}(u_i),$$

where

$$\sigma_{k,R_i}(u_i) = \begin{cases} (q_i - 2)^k + (-1)^k(q_i - 2), & \text{if } u_i \in 1 + M_i, \\ (q_i - 2)^k + (-1)^{k+1}, & \text{if } u_i \notin 1 + M_i. \end{cases}$$

Then, we can determine the multiplicative structure of R^{**}.

Theorem 1.10. *The following hold:*
(i) *If each $q_i > 3$, $i = 1, \ldots, n$, then we have*

$$R^{**} \cdot R^{**} = R^*.$$

(ii) *If $q_1 = \cdots = q_s = 3$ $(s \geq 1)$ and $q_j > 3$ for each $j > s$, then for any integer $k \geq 2$ we have*

$$\prod_{i=1}^{k} R^{**} = \begin{cases} (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{j>s} R_j^*), & \text{if } k \text{ is even}, \\ (\oplus_{i=1}^{s} R_i^* \setminus 1 + M_i) \oplus (\oplus_{j>s} R_j^*), & \text{otherwise}. \end{cases}$$

In particular, every unit of R is a product of its exceptional units if and only if $s = 1$.

Finally, we determine under which condition the ring R can be generated by its exceptional units (that is, every element of R can be represented as either a sum of exceptional units or a sum of products of exceptional units).

Corollary 1.11. *Assume that each $q_i \geq 3$, $i = 1, \ldots, n$. Then, the ring R is generated by its exceptional units if and only if there is at most one q_i equal to 3.*

1.6. Applications. So far, there have been extensive studies on additive unit representations in global fields; see [1] for a survey. Here, we apply our main results to the case of exceptional units in Dedekind domains.

Let D be a Dedekind domain. Notice that every exceptional unit of D automatically yields an exceptional unit in D/I for any ideal I of D. By Corollary 1.5 (or noticing the simple fact that the binary field has no exceptional unit), we immediately have:

Corollary 1.12. *If D has a prime ideal of norm 2, then $D^{**} = \emptyset$.*

In view of quadratic number fields, one can see that the condition in Corollary 1.12 is sufficient but not necessary. In fact, by definition it is easy to see that the only exceptional units in quadratic fields are the roots of the four polynomials:

$$X^2 - X + 1, \qquad X^2 - 3X + 1, \qquad X^2 - X - 1, \qquad X^2 + X - 1.$$

They correspond to the quadratic fields $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$. For each of the two fields, the ring of integers is generated by its exceptional units.

Using Corollaries 1.8 and 1.12, we directly obtain:

Corollary 1.13. *Not every element of D is a sum of its exceptional units if one of the following conditions holds:*

- *D has a prime ideal of norm 2;*
- *D has at least two prime ideals of norm 3;*
- *D has at least two prime ideals of norm 4.*

The following is a direct consequence of Corollary 1.11.

Corollary 1.14. *D cannot be generated by its exceptional units if D has at least two prime ideals of norm 3.*

We remark that Corollary 1.14 can be proved by the following simple argument without using Corollary 1.11: if P and Q are two prime ideals of norm 3, then every element of D, which is congruent to 0 modulo P and to 1 modulo Q, cannot be a sum of exceptional units or a sum of products of exceptional units, because the only exceptional unit modulo P is 2.

The condition in Corollary 1.14 is also only sufficient.

Example 1.15. Choose D to be the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{21})$. Then, the prime 2 is inert and the prime 3 is ramified in D. By Corollary 1.11, for any non-zero ideal I the quotient ring D/I is generated by its exceptional units. However, D has no exceptional unit.

2. Proofs

2.1. Proof of Corollary 1.2. (i) Notice that for any $c = (c_1, \ldots, c_n) \in R$, if $q_i > 2$, then

$$\mu_{2,R_i}(c_i) > 0.$$

This, together with Theorem 1.1, implies the result in (i).

(ii) Now, assume that $q_i = 2$, then by Theorem 1.1, we have

$$\mu_{k,R_i}(c_i) = \begin{cases} 1 + (-1)^k, & \text{if } c_i \in M_i, \\ 1 + (-1)^{k+1}, & \text{if } c_i \in R_i \setminus M_i. \end{cases} \tag{2.1}$$

Then, letting k be even and applying (2.1), we obtain

$$\sum_{i=1}^{k} R^* = (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{j>s} R_j).$$

Similarly, letting k be odd and using (2.1), we obtain the second identity.

2.2. Proof of Theorem 1.7. (i) Notice that given $c = (c_1, \ldots, c_n) \in R$, for each $i = 1, \ldots, n$,

$$\rho_{2,R_i}(c_i) > 0, \quad \text{if } q_i > 4.$$

This, together with Theorem 1.6, implies the result in (i).

(ii) If $q_i = 3$, we have

$$\rho_{2,R_i}(c_i) = 3 \left(\sum_{\substack{j=0 \\ j \equiv c_i \pmod{M_i}}}^{2} \binom{2}{j} - 1 \right), \quad \text{for any } c_i \in R_i.$$

As $q_i = 3$, the residue classes modulo M_i can be represented by 0, 1, 2, respectively. So, $\rho_{2,R_i}(c_i) \neq 0$ if and only if $c_i \in 1 + M_i$. Then, using Theorem 1.6, we get

$$R^{**} + R^{**} = (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{j>s} R_j). \tag{2.2}$$

We again have

$$\rho_{3,R_i}(c_i) = 3 \left(\sum_{\substack{j=0 \\ j \equiv c_i \pmod{M_i}}}^{3} \binom{3}{j} - 3 \right), \quad \text{for any } c_i \in R_i.$$

Thus, $\rho_{3,R_i}(c_i) \neq 0$ if and only if $c_i \in M_i$. So, by Theorem 1.6 we obtain

$$R^{**} + R^{**} + R^{**} = (\oplus_{i=1}^{s} M_i) \oplus (\oplus_{j>s} R_j). \tag{2.3}$$

Then, combining (2.2) with (2.3), we get the identities in (ii).

(iii) If $q_i = 4$, for even k we have

$$\rho_{k,R_i}(c_i) = 4 \sum_{\substack{j=0 \\ j \equiv c_i \pmod{M_i}}}^{k} \binom{k}{j}, \quad \text{for any } c_i \in R_i.$$

So, $\rho_{k,R_i}(c_i) \neq 0$ if and only if $c_i \in M_i$ or $c_i \in 1 + M_i$, where one should note that the characteristic of the residue field R_i/M_i is 2 (because $q_i = 4$). Thus, by using Theorem 1.6, we get the first identity in (iii).

For the second identity, we note that for odd k we have

$$\rho_{k,R_i}(c_i) = 4 \left(\sum_{\substack{j=0 \\ j \equiv c_i \pmod{M_i}}}^{k} \binom{k}{j} - 2^{k-1} \right), \quad \text{for any } c_i \in R_i.$$

Since the characteristic of the residue field R_i/M_i is 2, if $c_i \in M_i$, then $j \equiv c_i \equiv 0 \pmod{M_i}$ for any even integer j. Also, if $c_i \in 1 + M_i$, then $j \equiv c_i \equiv 1 \pmod{M_i}$ for any odd integer j. Thus, $\rho_{k,R_i}(c_i) \neq 0$ if and only if $c_i \notin M_i$ and $c_i \notin 1 + M_i$. So, similarly we obtain the second identity.

(iv) The desired results in (iv) follow directly from (ii) and (iii).

2.3. Proof of Theorem 1.9. Applying the same arguments as in [6], we have the following two lemmas, whose proofs we omit.

Lemma 2.1. *For any $u = (u_1, \ldots, u_n) \in R^*$, we have*

$$\theta_{k,R}(u) = \prod_{i=1}^{n} \theta_{k,R_i}(u_i).$$

Lemma 2.2. *For each $i = 1, \ldots, n$ and for any unit $u_i \in R_i^*$, we have*

$$\theta_{k,R_i}(u_i) = m_i^{k-1} \theta_{k,R_i/M_i}(u_i).$$

Let $\mathbb{F}_q$ be a finite field of q elements. Recall that a multiplicative character χ of $\mathbb{F}_q^*$ is a homomorphism from $\mathbb{F}_q^*$ to the complex roots of unity. The trivial character χ_0 is the one sending every element of $\mathbb{F}_q^*$ to 1. Let G_q be the group of multiplictive characters of $\mathbb{F}_q^*$, and let $G_q^* = G_q \setminus \{\chi_0\}$. Then, $|G_q| = q - 1$. Furthermore, we have the following orthogonality relations (for instance, see [4]):

$$\sum_{a \in \mathbb{F}_q^*} \chi(a) = \begin{cases} q - 1, & \text{if } \chi = \chi_0, \\ 0, & \text{otherwise;} \end{cases}$$

and

$$\sum_{\chi\in G_q}\chi(a)=\begin{cases}q-1, & \text{if } a=1,\\ 0, & \text{otherwise.}\end{cases}$$

Proof of Theorem 1.9. Based on the above lemmas, we only need to calculate $\theta_{k,\mathbb{F}_q}(c)$ for $c\in\mathbb{F}_q^*$ and $q>2$. Using the above formulas about multiplicative characters, we obtain

$$\begin{aligned}\theta_{k,\mathbb{F}_q}(c)&=|\{(x_1,\dots,x_k)\in\left(\mathbb{F}_q^{**}\right)^k : x_1x_2\cdots x_k=c\}|\\ &=\sum_{x_1\in\mathbb{F}_q^{**}}\sum_{x_2\in\mathbb{F}_q^{**}}\cdots\sum_{x_k\in\mathbb{F}_q^{**}}\frac{1}{q-1}\sum_{\chi\in G_q}\chi(x_1\cdots x_k/c)\\ &=\frac{1}{q-1}\sum_{\chi\in G_q}\left(\sum_{x_1\in\mathbb{F}_q^{**}}\chi(x_1)\right)\cdots\left(\sum_{x_k\in\mathbb{F}_q^{**}}\chi(x_k)\right)\chi(c^{-1})\\ &=\frac{1}{q-1}\left(\sum_{\chi\in G_q^*}\left(\sum_{x_1\in\mathbb{F}_q^{**}}\chi(x_1)\right)\cdots\left(\sum_{x_k\in\mathbb{F}_q^{**}}\chi(x_k)\right)\chi(c^{-1})+(q-2)^k\right),\end{aligned}$$

since $\mathbb{F}_q^{**}=\mathbb{F}_q^*\setminus\{1\}$.

Notice that for any $\chi\in G_q^*$, we have

$$0=\sum_{x_i\in\mathbb{F}_q^*}\chi(x_i)=1+\sum_{x_i\in\mathbb{F}_q^{**}}\chi(x_i).$$

Then, we further have

$$\begin{aligned}\theta_{k,\mathbb{F}_q}(c)&=\frac{1}{q-1}\left((q-2)^k+(-1)^k\sum_{\chi\in G_q^*}\chi(c^{-1})\right)\\ &=\begin{cases}\frac{1}{q-1}\left((q-2)^k+(-1)^k(q-2)\right), & \text{if } c=1,\\ \frac{1}{q-1}\left((q-2)^k+(-1)^{k+1}\right), & \text{if } c\neq 1.\end{cases}\end{aligned}$$

This, together with Lemma 2.1 and Lemma 2.2, implies the desired result. □

2.4. Proof of Theorem 1.10. (i) Notice that given $u=(u_1,\dots,u_n)\in R^*$, for each $i=1,\dots,n$, we have

$$\sigma_{2,R_i}(u_i)>0,\quad \text{if } q_i>3.$$

This, together with Theorem 1.9, implies the result in (i).

(ii) If $q_i = 3$, we have

$$\sigma_{k,R_i}(u_i) = \begin{cases} 1 + (-1)^k, & \text{if } u_i \in 1 + M_i, \\ 1 + (-1)^{k+1}, & \text{if } u_i \notin 1 + M_i. \end{cases} \tag{2.4}$$

Then, letting k be even and applying (2.4), we get

$$\prod_{i=1}^{k} R^{**} = (\oplus_{i=1}^{s} 1 + M_i) \oplus (\oplus_{j>s} R_j^*).$$

This completes the proof of the first identity.

Similarly, letting k be odd and using (2.4), we obtain the second identity.

2.5. Proof of Corollary 1.11. The sufficient part follows directly from Corollary 1.2 (i) and Theorem 1.10.

For the necessary part, we suppose that $q_1 = q_2 = 3$. By assumption, the ring R is generated by its exceptional units. Then, the ring $R_1 \oplus R_2$ is also generated by its exceptional units, and so is the ring $R_1/M_1 \oplus R_2/M_2$. On the other hand, since both finite fields R_1/M_1 and R_2/M_2 have only three elements, we in fact have

$$(R_1/M_1 \oplus R_2/M_2)^{**} = \{(2, 2)\},$$

which generates the subset

$$\{(0, 0), (1, 1), (2, 2)\}.$$

So, the ring $R_1/M_1 \oplus R_2/M_2$ cannot be generated by its unique exceptional unit. This leads to a contradiction.

Acknowledgements. The authors would like to thank the referees for careful reading and valuable comments. This work was supported by the National Natural Science Foundation of China, Grant No. 11501212. The research of Min Sha was supported by the Macquarie University Research Fellowship.

References

[1] F. Barroero, C. Frei and R. F. Tichy, Additive unit representations in global fields – a survey, *Publ. Math. Debrecen* **79** (2011), 291–307.

[2] J.-H. Evertse and K. Győry, Unit Equations in Diophantine Number Theory, *Cambridge University Press*, *Cambridge*, 2015.

[3] D. Kiani and M. Mollahajiaghaei, On the addition of units and non-units in finite commutative rings, *Rocky Mountain J. Math.* **45** (2015), 1887–1896.

[4] R. Lidl and H. Niederreiter, Finite Fields, Second Edition., *Cambridge University Press*, *Cambridge*, 1997.

[5] B. R. McDonald, Finite Rings With Identity. Pure and Applied Mathematics, Vol. **28**, *Marcel Dekker, Inc.*, *New York*, 1974.

[6] C. Miguel, On the sumsets of exceptional units in a finite commutative ring, *Monatsh. Math.* **186** (2018), 315–320.

[7] T. Nagell, Sur un type particulier d'unités algébriques, *Ark. Mat.* **8** (1969), 163–184.

[8] J. W. Sander, On the addition of units and nonunits mod m, *J. Number Theory* **129** (2009), 2260–2266.

[9] J. W. Sander, Sums of exceptional units in residue class rings, *J. Number Theory* **159** (2016), 1–6.

[10] J. W. Sander, Multiplicative atom decomposition of sets of exceptional units in residue class rings, *J. Number Theory* **173** (2017), 254–271.

[11] Q.-H. Yang and Q.-Q. Zhao, On the sumsets of exceptional units in $\mathbb{Z}_n$, *Monatsh. Math.* **182** (2017), 489–493.

[12] X. Zhang and C.-G. Ji, Sums of generators of ideals in residue class ring, *J. Number Theory* **174** (2017), 14–25.

SU HU
DEPARTMENT OF MATHEMATICS
SOUTH CHINA UNIVERSITY
OF TECHNOLOGY
GUANGZHOU 510640
CHINA

E-mail: mahusu@scut.edu.cn

MIN SHA
DEPARTMENT OF COMPUTING
MACQUARIE UNIVERSITY
SYDNEY, NSW 2109
AUSTRALIA

E-mail: shamin2010@gmail.com

(Received April 19, 2018; revised December 28, 2018)