Vol. 38 (2018)
No. 4

数 学 杂 志
J. of Math. (PRC)

ON THE UNIT GROUPS OF THE QUOTIENT RINGS OF IMAGINARY QUADRATIC NUMBER RINGS

WEI Yang-jiang, SU Lei-lei, TANG Gao-hua
(*School of Mathematics and Statistics, Guangxi Teachers Education University, Nanning 530023, China*)

Abstract: In this paper, we investigate the unit groups of the quotient rings of the integer rings R_d of the quadratic fields $\mathbb{Q}(\sqrt{d})$ over the rational number field $\mathbb{Q}$. By employing the polynomial expansions and the theory of finite groups, we completely determine the unit groups of $R_d/\langle\vartheta^n\rangle$ for $d = -3, -7, -11, -19, -43, -67, -163$, where ϑ is a prime in R_d, and n is an arbitrary positive integer. The results in this paper generalize the study of the unit groups of $R_d/\langle\vartheta^n\rangle$ for $d = -1$, which obtained by J. T. Cross (1983), G. H. Tang and H. D. Su (2010) and for the case $d = -2$ by Y. J. Wei (2016).

Keywords: imaginary quadratic number ring; quotient ring; unit group; quadratic field
2010 MR Subject Classification: 11R04; 20K01
Document code: A **Article ID:** 0255-7797(2018)04-0602-17

1 Introduction

Let $K = \mathbb{Q}(\sqrt{d})$, the quadratic field over $\mathbb{Q}$, where $\mathbb{Q}$ is the rational number field and d is a square-free integer other than 0 and 1. The ring of algebraic integers of K is denoted by R_d, and it is very important for the study of dynamical systems, e.g., see [1, 2]. We call R_d an imaginary quadratic number ring if $d < 0$. From the work of Stark [3], we know that there are only finite negative integers d such that the complex quadratic ring R_d is a unique-factorization domain, namely, $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. For an arbitrary prime element $\vartheta \in R_d$, and a positive integer n, the unit groups of $R_d/\langle\vartheta^n\rangle$ were determined for the cases $d = -1, -2, -3$ in [4–6], respectively. Moreover, the square mapping graphs for the Gaussian integer ring modulo n is studied in paper [7]. In this paper, we investigate the unit groups of $R_d/\langle\vartheta^n\rangle$ for the cases $d = -3, -7, -11, -19, -43, -67, -163$, and we make some corrections to the case of $d = -3$ in paper [6].

Throughout this paper, we denote by $\mathbb{Z}$ the set of rational integers, $\mathbb{Z}_n$ is the additive cyclic group of order n, $\mathbb{Z}/\langle n\rangle$ is the ring of integers modulo n, and $o(\theta)$ is the order of θ in

* **Received date:** 2017-03-01 **Accepted date:** 2017-06-20
Foundation item: Supported by the National Natural Science Foundation of China (11461010; 11661013; 11661014); the Guangxi Science Research and Technology Development Project (1599005-2-13).

Biography: Wei Yangjiang (1969–), female, born at Nanning, Guangxi, professor, major in commutative algebra.

a group. For a given ring R, let $U(R)$ denote the unit group of R, let $\langle\gamma\rangle$ denote the ideal of R generated by $\gamma \in R$. If γ is an element of a given group G, we also use $\langle\gamma\rangle$ to denote the subgroup of G generated by $\gamma \in G$. The Legendre symbol $(\frac{a}{p})$, where a is an integer, p is a prime and $p \nmid a$, is defined as follows: if there exists an integer x such that $x^2 \equiv a \pmod{p}$, then $(\frac{a}{p}) = 1$, otherwise, $(\frac{a}{p}) = -1$.

Lemma 1.1 [8, Lemma 2.4.2] The ring R_d of algebraic integers of $K = \mathbb{Q}(\sqrt{d})$ is

(1) $R_d = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\}$, if $d \equiv 2, 3 \pmod 4$.

(2) $R_d = \{\frac{1}{2}(a + b\sqrt{d}) : \ a, b \in \mathbb{Z}$ are of the same parity$\}$, if $d \equiv 1 \pmod 4$.

By Lemma 1.1, for $d = -3, -7, -11, -19, -43, -67, -163$, the elements of R_d are all of the form $\frac{1}{2}(a + b\sqrt{d})$, where $a, b \in \mathbb{Z}$ are of the same parity. Moreover, we know that $U(R_d) = \{\pm 1\}$ for all $d = -3, -7, -11, -19, -43, -67, -163$.

Now, we need to identify all primes in the ring R_d. The following theorem is obtained from [9, Theorem 9.29].

Theorem 1.2 For $d = -3, -7, -11, -19, -43, -67, -163$, up to multiplication by units, the primes of R_d are the following three types ($D = -d$):

(1) p, where $p \in \mathbb{Z}$ is a prime satisfying the Legendre symbol $(\frac{p}{D}) = -1$;

(2) π or $\overline{\pi}$, where $q = \pi\overline{\pi} \in \mathbb{Z}$ is a prime satisfying the Legendre symbol $(\frac{q}{D}) = 1$;

(3) $\delta = \sqrt{d}$.

2 Main Results

Throughout this section, $d = -3, -7, -11, -19, -43, -67, -163$. For conveniences, we denote by $D = -d$. Let n be a positive integer, and ϑ is a prime in R_d. We determine the structure of unit groups of $R_d/\langle\vartheta^n\rangle$.

First, we characterize the equivalence classes of $R_d/\langle\vartheta^n\rangle$, where ϑ is prime in R_d. For $\alpha \in R_d$, we denote by $[\alpha] \in R_d/\langle\vartheta^n\rangle$ the equivalence class which α belongs to. Simultaneously, we make corrections to the equivalence classes which are given in [6, Theorem 3.2] for the case $d = -3$.

Theorem 2.3 Let ϑ denote a prime of R_d, $\delta = \sqrt{d}$, $D = -d$. For an arbitrary positive integer n, the equivalence classes of $R_d/\langle\vartheta^n\rangle$ are of the following types:

(1) $R_d/\langle\delta^{2m}\rangle = \big\{[r_1 + r_2\sqrt{d}\,] : \ 0 \leqslant r_i \leqslant D^m - 1, r_i \in \mathbb{Z}, i = 1, 2\big\}$, $m \geqslant 1$;

(2) $R_d/\langle\delta^{2m+1}\rangle = \big\{[r_1 + r_2\sqrt{d}\,] : \ 0 \leqslant r_1 \leqslant D^{m+1} - 1, 0 \leqslant r_2 \leqslant D^m - 1, r_1, r_2 \in \mathbb{Z}\big\}$, $m \geqslant 0$;

(3) $R_d/\langle p^n\rangle = \big\{[r_1 + r_2\sqrt{d}\,] : \ 0 \leqslant r_i \leqslant p^n - 1, r_i \in \mathbb{Z}, i = 1, 2\big\}$, where p is an odd prime in $\mathbb{Z}$ satisfying the Legendre symbol $(\frac{p}{D}) = -1$;

(4) $R_d/\langle\pi^n\rangle = \{[a] : \ 0 \leqslant a \leqslant q^n - 1, a \in \mathbb{Z}\}$, where $q = \pi\overline{\pi}$ is a prime in $\mathbb{Z}$ satisfying the Legendre symbol $(\frac{q}{D}) = 1$;

(5) Suppose that $d \neq -7$. Then

(a) $R_d/\langle 2\rangle = \big\{[0], [1], [\frac{1}{2} + \frac{1}{2}\sqrt{d}\,], [\frac{1}{2} - \frac{1}{2}\sqrt{d}\,]\big\}$;

(b) For $n \geqslant 2$, $R_d/\langle 2^n\rangle = R_1 \cup R_2 \cup R_3$, where

$$\begin{aligned} R_1 &= \left\{[r_1 + r_2\sqrt{d}\,]:\ 0 \leqslant r_i \leqslant 2^{n-1}-1,\ \ r_i \in \mathbb{Z},\ \ i = 1,2\right\}, \\ R_2 &= \left\{[r_1 - r_2\sqrt{d}\,]:\ 0 \leqslant r_1 \leqslant 2^{n-1}-1,\ \ 1 \leqslant r_2 \leqslant 2^{n-1},\ \ r_1, r_2 \in \mathbb{Z}\right\}, \\ R_3 &= \left\{[\frac{r_1}{2} \pm \frac{r_2}{2}\sqrt{d}\,]:\ 1 \leqslant r_i \leqslant 2^n - 1,\ \ r_i \in \mathbb{Z},\ \ 2 \nmid r_i,\ \ i = 1,2\right\}. \end{aligned}$$

Proof (1) As $\delta^{2m} = d^m$, we get that $\langle \delta^{2m}\rangle = \langle D^m\rangle$. Suppose $\alpha = a_1 + a_2\sqrt{d} \in R_d$, where $a_1, a_2 \in \mathbb{Z}$. Let $a_i = D^m k_i + r_i$ with $0 \leqslant r_i \leqslant D^m - 1$, $k_i \in \mathbb{Z}$, $i = 1,2$. Then $\alpha = (r_1 + r_2\sqrt{d}) + D^m(k_1 + k_2\sqrt{d})$. So α and $r_1 + r_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle \delta^{2m}\rangle$.

On the other hand, let $\beta = \frac{1}{2}(b_1 + b_2\sqrt{d}) \in R_d$, where b_1 and b_2 are odd integers. Since D is odd for $i = 1,2$, there exists a unique integer $g_i \in \{0, 1, \cdots, D^m - 1\}$ satisfying the congruence $2g_i \equiv b_i \pmod{D^m}$. Hence, there exists an odd integer x_i such that $b_i = D^m x_i + 2g_i$, $i = 1,2$. Therefore, $\gamma = \frac{x_1}{2} + \frac{x_2}{2}\sqrt{d} \in R_d$, and $\beta = (g_1 + g_2\sqrt{d}) + D^m\gamma$, which implies that β and $g_1 + g_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle \delta^{2m}\rangle$. Finally, it is easy to verify that the classes of (1) are distinct.

(2) As $\delta^{2m+1} = d^m\delta$, we get that $\langle \delta^{2m+1}\rangle = \langle D^m\sqrt{d}\,\rangle$. Suppose $\alpha = a_1 + a_2\sqrt{d} \in R_d$, where $a_1, a_2 \in \mathbb{Z}$. Let $a_1 = D^{m+1}k_1 + r_1$ with $0 \leqslant r_1 \leqslant D^{m+1} - 1$. Let $a_2 = D^m k_2 + r_2$ with $0 \leqslant r_2 \leqslant D^m - 1$. Then $\alpha = (r_1 + r_2\sqrt{d}) + D^m\sqrt{d}(k_2 - k_1\sqrt{d})$. So α and $r_1 + r_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle \delta^{2m+1}\rangle$.

On the other hand, let $\beta = \frac{1}{2}(b_1 + b_2\sqrt{d}) \in R_d$, where b_1 and b_2 are odd integers. Since D is odd, there exists a unique integer $g_1 \in \{0, 1, \cdots, D^{m+1} - 1\}$ satisfying congruence $2g_1 \equiv b_1 \pmod{D^{m+1}}$. Analogously, there exists a unique integer $g_2 \in \{0, 1, \cdots, D^m - 1\}$ satisfying congruence $2g_2 \equiv b_2 \pmod{D^m}$. Therefore, there exist odd integers x_1, x_2 such that $b_1 = D^{m+1}x_1 + 2g_1$, and $b_2 = D^m x_2 + 2g_2$. Hence, $\gamma = \frac{x_2}{2} - \frac{x_1}{2}\sqrt{d} \in R_d$, and $\beta = (g_1 + g_2\sqrt{d}) + D^m\sqrt{d}(\frac{x_2}{2} - \frac{x_1}{2}\sqrt{d})$, which implies that β and $g_1 + g_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle \delta^{2m+1}\rangle$.

Finally, it is easy to verify that the classes of (2) are distinct.

(3) It can be proved with the similar method to (1). Suppose $\alpha = a_1 + a_2\sqrt{d} \in R_d$, where $a_1, a_2 \in \mathbb{Z}$. Let $a_i = p^n k_i + r_i$ with $0 \leqslant r_i \leqslant p^n - 1$, $k_i \in \mathbb{Z}$, $i = 1,2$. Then $\alpha = (r_1 + r_2\sqrt{d}) + p^n(k_1 + k_2\sqrt{d})$. So α and $r_1 + r_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle p^n\rangle$.

On the other hand, let $\beta = \frac{1}{2}(b_1 + b_2\sqrt{d}) \in R_d$, where b_1 and b_2 are odd integers. Since p is odd for $i = 1,2$, there exists a unique integer $g_i \in \{0, 1, \cdots, p^n - 1\}$ satisfying the congruence $2g_i \equiv b_i \pmod{p^n}$. Hence, there exists an odd integer x_i such that $b_i = p^n x_i + 2g_i$, $i = 1,2$. Therefore, $\gamma = \frac{x_1}{2} + \frac{x_2}{2}\sqrt{d} \in R_d$, and $\beta = (g_1 + g_2\sqrt{d}) + p^n\gamma$, which implies that β and $g_1 + g_2\sqrt{d}$ belong to the same equivalence class of $R_d/\langle p^n\rangle$. Finally, it is easy to verify that the classes of (3) are distinct.

(4) Let $q = \pi\overline{\pi}$ be a prime in $\mathbb{Z}$ satisfying the Legendre symbol $(\frac{q}{D}) = 1$. Let $\pi^n = \frac{1}{2}(s + t\sqrt{d})$, where $s, t \in \mathbb{Z}$ are of the same parity. Then it is clear that $q \nmid st$. Suppose that

$\beta = \frac{1}{2}(b_1+b_2\sqrt{d}) \in R_d$, where $b_1, b_2 \in \mathbb{Z}$ are of the same parity. We show that in the quotient ring $R_d/\langle \pi^n \rangle$, β belongs to the equivalence class $[a]$ for some $a \in \{0, 1, \cdots, q^n - 1\}$. Indeed, Let $\gamma = \frac{1}{2}(x + y\sqrt{d}) \in R_d$, where $x, y \in \mathbb{Z}$ are of the same parity, such that $\beta = a + \pi^n\gamma$. Then the following equations hold

$$a + \frac{1}{4}xs + \frac{1}{4}dyt = \frac{1}{2}b_1, \tag{2.1}$$

$$\frac{1}{4}ys + \frac{1}{4}xt = \frac{1}{2}b_2. \tag{2.2}$$

Now we solve the integer a from the above equations. By equation (2.1), we obtain

$$4as + xs^2 + dyts = 2b_1s. \tag{2.3}$$

And by equation (2.2), we get $-dyts - dt^2x = -2b_2dt$. Eliminating $dyts$ between this equation and (2.3), we obtain

$$4as + x(s^2 - dt^2) = 2(b_1s - db_2t). \tag{2.4}$$

Note that $q = \pi\overline{\pi}$ and $\pi^n = \frac{1}{2}(s + t\sqrt{d})$, we have $s^2 - dt^2 = 4q^n$. Substituting this into (2.4), it follows that

$$4as + 4q^nx = 2(b_1s - db_2t). \tag{2.5}$$

Moreover, since $s, t \in \mathbb{Z}$ are of the same parity and $b_1, b_2 \in \mathbb{Z}$ are of the same parity and note that d is odd, we derive $b_1s - db_2t$ is even. Hence, equation (2.5) can be written as $as + q^nx = \frac{1}{2}(b_1s - db_2t)$, which implies that

$$as \equiv \frac{1}{2}(b_1s - db_2t) \pmod{q^n}. \tag{2.6}$$

Because $q \nmid s$, the last congruence (2.6) in a has a unique solution $a \in \{0, 1, \cdots, q^n - 1\}$. Therefore, β belongs to the equivalence class $[a]$, as desired.

Finally, it is easy to verify that the classes of (4) are distinct.

(5) Suppose $d \neq -7$.

(a) We first determine the structure of the quotient ring $R_d/\langle 2 \rangle$. Suppose $\alpha_1 = a \in \mathbb{Z}$. If a is even, then $\frac{a}{2} \in R_d$. It follows from $\alpha_1 = 0 + 2 \times \frac{a}{2}$ that α_1 belongs to the equivalence class $[0]$ in the quotient ring $R_d/\langle 2 \rangle$. If a is odd, then $a = 1 + 2k$ for some $k \in \mathbb{Z}$. Then clearly α_1 belongs to the equivalence class $[1]$.

Suppose $\alpha_2 = b\sqrt{d}$, where $b \in \mathbb{Z}$. If b is even, then $\frac{b}{2}\sqrt{d} \in R_d$. We have

$$\alpha_2 = b\sqrt{d} = 0 + 2 \times \frac{b}{2}\sqrt{d}.$$

So clearly α_2 belongs to the equivalence class $[0]$. If b is odd, then

$$\alpha_2 = b\sqrt{d} = 1 + 2(-\frac{1}{2} + \frac{b}{2}\sqrt{d}).$$

Therefore, α_2 belongs to the equivalence class $[1]$.

Suppose $\alpha_3 = s + t\sqrt{d} \in R_d$, where $s, t \in \mathbb{Z}$. If s and t are of the same parity, then $\frac{s}{2} + \frac{t}{2}\sqrt{d} \in R_d$. Moreover, we have $s + t\sqrt{d} = 0 + 2(\frac{s}{2} + \frac{t}{2}\sqrt{d})$. Hence, α_3 belongs to the equivalence class $[0]$. If s and t are not of the same parity, then $\frac{s-1}{2} + \frac{t}{2}\sqrt{d} \in R_d$. Since $s + t\sqrt{d} = 1 + 2(\frac{s-1}{2} + \frac{t}{2}\sqrt{d})$, we obtain that α_3 belongs to the equivalence class $[1]$.

Now, suppose $\alpha_4 = \frac{x}{2} + \frac{y}{2}\sqrt{d}$, where $x = 2k_1+1$, $y = 2k_2+1$, $k_1, k_2 \in \mathbb{Z}$. If k_1 and k_2 are of the same parity, then $\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d} \in R_d$. Moreover, since $\alpha_4 = (\frac{1}{2} + \frac{1}{2}\sqrt{d}) + 2(\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d})$, we obtain that α_4 belongs to the equivalence class $[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$. If k_1 and k_2 are not of the same parity, then $\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d} \in R_d$. Furthermore, $\alpha_4 = (\frac{1}{2} - \frac{1}{2}\sqrt{d}) + 2(\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d})$. Thus, α_4 belongs to the equivalence class $[\frac{1}{2} - \frac{1}{2}\sqrt{d}]$.

Finally, we show that the classes of (5) (a) are distinct. Clearly

$$[0] \neq [1] \neq [\frac{1}{2} \pm \frac{1}{2}\sqrt{d}] \neq [0].$$

If $[\frac{1}{2} + \frac{1}{2}\sqrt{d}] = [\frac{1}{2} - \frac{1}{2}\sqrt{d}]$, then there exits $\gamma = \frac{x_1}{2} + \frac{x_2}{2}\sqrt{d} \in R_d$, where $x_1, x_2 \in \mathbb{Z}$ are of the same parity, such that

$$\frac{1}{2} + \frac{1}{2}\sqrt{d} = (\frac{1}{2} - \frac{1}{2}\sqrt{d}) + 2(\frac{x_1}{2} + \frac{x_2}{2}\sqrt{d}).$$

Clearly, the above equation holds if and only if $x_1 = 0$ and $x_2 = 1$, which is impossible, since $x_1, x_2 \in \mathbb{Z}$ must be of the same parity. Hence, we conclude that $[\frac{1}{2} + \frac{1}{2}\sqrt{d}] \neq [\frac{1}{2} - \frac{1}{2}\sqrt{d}]$. Therefore, the classes of (5) (a) are distinct.

(b) Now, let $n \geqslant 2$. We determine the structure of the quotient ring $R_d/\langle 2^n \rangle$. Suppose $\beta_1 = a_1 + a_2\sqrt{d} \in R_d$, where $a_1, a_2 \in \mathbb{Z}$. Let $a_i = 2^{n-1}k_i + r_i$, $k_i, r_i \in \mathbb{Z}$, and $0 \leqslant r_i \leqslant 2^{n-1} - 1$ for $i = 1, 2$. First, if k_1 and k_2 are of the same parity, then $\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d} \in R_d$. Moreover, since $\beta_1 = (r_1 + r_2\sqrt{d}) + 2^n(\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d})$, we conclude that β_1 and $r_1 + r_2\sqrt{d}$ belong to the same equivalence class in the quotient ring $R_d/\langle 2^n \rangle$. Secondly, if k_1 and k_2 are not of the same parity, then $\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d} \in R_d$. Since $\beta_1 = [r_1 - (2^{n-1} - r_2)\sqrt{d}] + 2^n(\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d})$, we obtain that β_1 and $r_1 - (2^{n-1} - r_2)\sqrt{d}$ belong to the same equivalence class. Furthermore, since $0 \leqslant r_2 \leqslant 2^{n-1} - 1$, we derive that $1 \leqslant 2^{n-1} - r_2 \leqslant 2^{n-1}$. So in the second case, i.e., k_1 and k_2 are not of the same parity, we get that β_1 and $r_1 - {r'}_2\sqrt{d}$ belong to the same equivalence class, where $1 \leqslant {r'}_2 \leqslant 2^{n-1}$ and ${r'}_2 = 2^{n-1} - r_2$.

Next, suppose that $\beta_2 = \frac{b_1}{2} + \frac{b_2}{2}\sqrt{d}$, where b_1 and b_2 are odd integers. Let $b_i = 2^n k_i + r_i$, where $k_i, r_i \in \mathbb{Z}$, $1 \leqslant r_i \leqslant 2^n - 1$ and $2 \nmid r_i$ for $i = 1, 2$. First, if k_1 and k_2 are of the same parity, then $\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d} \in R_d$. Moreover, since $\beta_2 = (\frac{r_1}{2} + \frac{r_2}{2}\sqrt{d}) + 2^n(\frac{k_1}{2} + \frac{k_2}{2}\sqrt{d})$, we obtain that β_2 and $\frac{r_1}{2} + \frac{r_2}{2}\sqrt{d}$ belong to the same equivalence class. Secondly, if k_1 and k_2 are not of the same parity, then $\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d} \in R_d$. Since $\beta_2 = (\frac{r_1}{2} - \frac{2^n - r_2}{2}\sqrt{d}) + 2^n(\frac{k_1}{2} + \frac{k_2+1}{2}\sqrt{d})$, it follows that β_2 and $\frac{r_1}{2} - \frac{2^n - r_2}{2}\sqrt{d}$ belong to the same equivalence class. Furthermore, according to $1 \leqslant r_2 \leqslant 2^n - 1$, we have $1 \leqslant 2^n - r_2 \leqslant 2^n - 1$. So, in the second case, i.e., k_1 and k_2 are not of the same parity, we obtain that β_2 and $\frac{r_1}{2} - \frac{{r'}_2}{2}\sqrt{d}$ belong to the same equivalence class, where $1 \leqslant {r'}_2 \leqslant 2^n - 1$ and ${r'}_2 = 2^n - r_2$.

Finally, we claim that the classes of (5) (b) are distinct. We only show that

$$[\frac{r_1}{2} + \frac{r_2}{2}\sqrt{d}] \neq [\frac{x_1}{2} - \frac{x_2}{2}\sqrt{d}],$$

where $r_i, x_i \in \{1, 3, \cdots, 2^n-1\}$ with $2 \nmid r_i x_i$ for $i = 1, 2$. Indeed, if $[\frac{r_1}{2}+\frac{r_2}{2}\sqrt{d}\,] = [\frac{x_1}{2}-\frac{x_2}{2}\sqrt{d}\,]$, then there exit $t_1, t_2 \in \mathbb{Z}$ of the same parity such that

$$\frac{r_1}{2}+\frac{r_2}{2}\sqrt{d} = (\frac{x_1}{2}-\frac{x_2}{2}\sqrt{d}) + 2^n(\frac{t_1}{2}+\frac{t_2}{2}\sqrt{d}).$$

So we obtain $r_1 = x_1 + 2^n t_1$ and $r_2 = -x_2 + 2^n t_2$. It is easy to show that $t_1 = 0$ and $t_2 = 1$, which is a contradiction.

Example 2.4 To illustrate the case $d = -19$, $q = 23 = \pi\overline{\pi}$ and $n = 2$, let $\gamma = \frac{1}{2}(b_1 + b_2\sqrt{-19}) \in R_d$, where $b_1 = 3$ and $b_2 = 1$. We give the equivalence class in $R_d/\langle\pi^2\rangle$ which γ belongs to. Since $\pi = 2 - \sqrt{-19}$ is a proper factor of q in R_d, $\pi^2 = -15 - 4\sqrt{-19} = \frac{-30}{2} - \frac{8}{2}\sqrt{-19}$. Denoted by $s = -30$, $t = -8$. Substituting the values for s, t, b_1, b_2, d, q and n into congruence (2.6), we get that $a = 198$ is a solution to congruence (2.6). Moreover, substituting the values for a, s, t, b_1, b_2 and d into equations (2.1) and (2.2), we have $x = 11$ and $y = -3$. Therefore,

$$\gamma = \frac{3}{2} + \frac{1}{2}\sqrt{-19} = 198 + \pi^2(\frac{11}{2} - \frac{3}{2}\sqrt{-19}),$$

which implies that γ belongs to the class [198].

As an easy consequence of Theorem 2.1 (5), we have

Corollary 2.5 Suppose that 2 is prime in R_d. Let $\alpha = [a + b\sqrt{d}] \in R_d/\langle 2^n\rangle$, where $0 \leqslant a, b \leqslant 2^{n-1} - 1$, $a, b \in \mathbb{Z}$. Then

(1) $\alpha = [1]$ if and only if $a = 2^{n-1}k_1 + 1$, $b = 2^{n-1}k_2$, where $k_1, k_2 \in \mathbb{Z}$ are of the same parity.

(2) If $a = 2^n k_1 + 1$, $b = 2^n k_2$, $k_1, k_2 \in \mathbb{Z}$, then $\alpha = [1]$.

Now, we determine the structure of unit groups of $R_d/\langle\vartheta^n\rangle$ for an arbitrary prime ϑ of R_d. First of all, we consider the case of $\vartheta = \delta = \sqrt{d}$. Let $\overline{R} = R_d/\langle\delta^n\rangle$. For $\alpha = [a + b\sqrt{d}\,] \in \overline{R}$, it is easy to show that $\alpha \in U(\overline{R})$ if and only if $d \nmid (a^2 - db^2)$, if and only if $d \nmid a$, if and only if $D \nmid a$.

Theorem 2.6 Let $\overline{R} = R_d/\langle(\sqrt{d})^n\rangle$, n is an arbitrary positive integer. Let $D = -d$. Then the unit groups $U(\overline{R})$ of $\overline{R}$ are as the follows:

(1) Let $n = 1$. Then $U(\overline{R}) \cong \mathbb{Z}_{D-1}$.

(2) Let $n = 2$. Then $U(\overline{R}) \cong \mathbb{Z}_{D-1} \times \mathbb{Z}_D$.

(3) Let $n = 2m$ with $m \geqslant 2$.

(a) If $d \neq -3$, then $U(\overline{R}) \cong \mathbb{Z}_{D-1} \times \mathbb{Z}_{D^{m-1}} \times \mathbb{Z}_{D^m}$;

(b) If $d = -3$, then $U(\overline{R}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_{3^{m-1}}$.

(4) If $n = 2m + 1$ with $m \geqslant 1$, then $U(\overline{R}) \cong \mathbb{Z}_{D-1} \times \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^m}$.

Proof (1) If $n = 1$, by Theorem 2.1 (2), $\overline{R}$ is a field of order $D = -d$, so $|U(\overline{R})| = D - 1$. Therefore, $U(\overline{R})$ is a cyclic group of order $D - 1$ and hence $U(\overline{R}) \cong \mathbb{Z}_{D-1}$.

(2) If $n = 2$, then $|U(\overline{R})| = -d(-d-1) = D(D-1)$. Note that D is a prime, moreover D and $D - 1$ are relatively prime, we get that $U(\overline{R}) \cong H \times \mathbb{Z}_D$, where H is a subgroup of order $D - 1$. Moreover, we can easily show that $D - 1$ is square-free for $D = 3, 7, 11, 43$ and 67.

On the other hand, if $D=19$, then $D-1=2\times 3^2$, clearly $[4]\in U(\overline{R})$ is of order 3^2. If $D=163$, then $D-1=2\times 3^4$, clearly $[4]\in U(\overline{R})$ is of order 3^4. Therefore $H\cong \mathbb{Z}_{D-1}$. So $U(\overline{R})\cong \mathbb{Z}_{D-1}\times\mathbb{Z}_D$.

(3) (a) Suppose that $d\neq -3$. Let $n=2m$ with $m\geqslant 2$. Let $\alpha=[a+b\sqrt{d}\,]\in\overline{R}$, where $a,b\in\{0,1,\cdots,D^m-1\}$. Since $\alpha\in U(\overline{R})$ if and only if $D\nmid a$, $|U(\overline{R})|=(D-1)D^{2m-1}$, and we can write $U(\overline{R})=P\times H$, where P, H are finite groups, and $|P|=D-1$, $|H|=D^{2m-1}$.

We determine the structure of H. Let $\alpha=[a+b\sqrt{d}\,]\in\overline{R}$ with $D\nmid a$. By Theorem 2.1 (1), for an arbitrary odd integer $W>1$, α^W equals to the equivalence class [1], i.e., $\alpha^W=[1]$ if and only if the following congruences hold

$$a^W+d\binom{W}{2}a^{W-2}b^2+\cdots+d^{\frac{W-1}{2}}\binom{W}{W-1}ab^{W-1}\equiv 1 \pmod{D^m}, \tag{2.7}$$
$$\binom{W}{1}a^{W-1}b+d\binom{W}{3}a^{W-3}b^3+\cdots+d^{\frac{W-1}{2}}b^W\equiv 0 \pmod{D^m}. \tag{2.8}$$

First, we claim that for any $\alpha\in H$, $\alpha^{D^m}=[1]$. Let $W=D^m$. Since $d^m\mid d^j\binom{W}{2j}$ for $j\geqslant 1$, the congruence (2.7) is equivalent to $a^{D^m}\equiv 1 \pmod{D^m}$. It is well known that the unit group of the ring $\mathbb{Z}/\langle D^m\rangle$ is isomorphic to $\mathbb{Z}_{D^{m-1}}\times\mathbb{Z}_{D-1}$. Hence, we obtain that $a^{D^m}\equiv 1 \pmod{D^m}$ if and only if $a\in\mathbb{Z}_{D^{m-1}}$. So in the set $\{0,1,\cdots,D^m-1\}$, there are precisely D^{m-1} elements a such that $a^{D^m}\equiv 1 \pmod{D^m}$.

On the other hand, since $d^m\mid d^j\binom{W}{2j+1}$ for $j\geqslant 0$, congruence (2.8) holds for any positive integer b. Therefore, we can conclude that $\alpha^W=[1]$ if and only if $a\in\mathbb{Z}_{D^{m-1}}$ and $b\in\{0,1,\cdots,D^m-1\}$. Hence, the number of $\alpha\in U(\overline{R})$ satisfying $\alpha^{D^m}=[1]$ is

$$D^{m-1}\times D^m=D^{2m-1}.$$

Recall that $U(\overline{R})=P\times H$ with $|P|=D-1$ and $|H|=D^{2m-1}$, we get that $\alpha^{D^m}=[1]$ for $\alpha\in H$.

Second, we consider the number of $\alpha\in U(\overline{R})$ satisfying $\alpha^{D^{m-1}}=[1]$. Let $W=D^{m-1}$. Since $d^m\mid d^j\binom{W}{2j}$ for $j\geqslant 1$, congruence (2.7) holds if and only if $a^{D^{m-1}}\equiv 1 \pmod{D^m}$, if and only if $a\in\mathbb{Z}_{D^{m-1}}$.

On the other hand, note that $d\neq -3$ and $d^m\mid d^j\binom{W}{2j+1}$ for $1\leqslant j\leqslant\frac{W-1}{2}$, congruence (2.8) is equivalent to $D^{m-1}a^{D^{m-1}-1}b\equiv 0 \pmod{D^m}$. That is, $D^{m-1}b\equiv 0 \pmod{D^m}$, since $D\nmid a$. Hence, we obtain $d\mid b$. So the solutions to congruence (2.8) are $b=D\cdot l$ with $l=0,1,\cdots,D^{m-1}-1$. Thus the number of $\alpha\in U(\overline{R})$ satisfying $\alpha^{D^{m-1}}=[1]$ is $D^{m-1}\times D^{m-1}=D^{2m-2}$. Then the number of elements of order D^m in $U(\overline{R})$ is

$$D^{2m-1}-D^{2m-2}=d^{\,2m-2}(-d-1).$$

Finally, let we calculate the number of $\alpha\in H$ satisfying $\alpha^{D^{m-2}}\equiv 1 \pmod{D^m}$. Let $W=D^{m-2}$. Since $d^m\mid d^j\binom{W}{2j+1}$ for $2\leqslant j\leqslant\frac{W-1}{2}$, congruence (2.8) holds if and only if

$$Wa^{W-3}b\,[6a^2+d(W-1)(W-2)b^2\,]\equiv 0 \pmod{D^m}. \tag{2.9}$$

Since $D\nmid a$ and $d\neq -3$, we derive that $D\nmid[6a^2+d(W-1)(W-2)b^2]$. So congruence (2.9) holds if and only if $d^2\mid b$, i.e., congruence (2.8) holds if and only if $d^2\mid b$. Furthermore, in the case of $d^2 \mid b$, we have $d^m \mid d^j \binom{W}{2j} b^{2j}$ for $j \geqslant 1$. Hence, in the case of $d^2 \mid b$ congruence (2.7) holds if and only if $a^W \equiv 1 \pmod{D^m}$. Clearly, the number of solutions of the last congruence is D^{m-2}. Thus the number of $\alpha \in H$ such that $\alpha^{D^{m-2}} = 1$ is $D^{m-2} \times D^{m-2} = d^{\,2m-4}$. So we derive that the number of elements of order D^{m-1} in $U(\overline{R})$ is

$$D^{2m-2} - D^{2m-4} = d^{\,2m-4}(d^2 - 1). \tag{2.10}$$

Now, let $\beta = [1 + \sqrt{d}\,] \in \overline{R}$. Then by the above argument, we know that β is of order D^m. Since $m \geqslant 2$, clearly $\beta \in H$. Therefore $\mathbb{Z}_{D^m}$ is a subgroup of H and we can suppose $H \cong \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^{l_1}} \times \cdots \times \mathbb{Z}_{D^{l_h}}$, where $l_1 + \cdots + l_h = m - 1$. If $h \geqslant 2$, then $1 \leqslant l_i \leqslant m-2$ for $i = 1, \cdots, h$ and hence there are exactly $(D-1) \cdot D^{2m-3}$ elements in H of order D^{m-1}, which contradicts the above result (2.10). If $h = 1$, then $H \cong \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^{m-1}}$. Therefore, the number of elements of order D^{m-1} in H is $D^{m-1} \times D^{m-1} - D^{m-2} \times D^{m-2} = d^{\,2m-4}(d^2-1)$, which is the same as (2.10). So we can conclude that $h = 1$ and $H \cong \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^{m-1}}$.

In the following, we determine the structure of the subgroup P of $U(\overline{R})$, where $|P| = -d-1$. Clearly, $-d-1$ is square-free for $d = -7, -11, -43, -67$ and hence $P \cong \mathbb{Z}_{D-1}$ in these cases. If $d = -19$, then $|P| = 18 = 2 \times 3^2$.

On the other hand, let $a < 19^m$ be a positive integer. If $a^{19^t} \equiv 1 \pmod{19^m}$ for some integers $t > 1$, then clearly $a = 1 + 19x$ for some non-negative integers x. Hence, $4^{19^t} \not\equiv 1 \pmod{19^m}$ and $(4^3)^{19^t} \not\equiv 1 \pmod{19^m}$ for any $t > 1$. Furthermore, we have

$$\begin{aligned} 4^{9\times 19^{m-1}} &= 262144^{19^{m-1}} \\ &= (19 \times 13797 + 1)^{19^{m-1}} \\ &= 19^{19^{m-1}} \times 13797^{19^{m-1}} + \cdots + 19^{m-1} \times 19 \times 13797 + 1 \\ &\equiv 1 \pmod{19^m}. \end{aligned}$$

Thus, if $d = -19$, the class $[4] \in \overline{R}$ is of order $3^2 \cdot 19^{m-1}$, so $P \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \cong \mathbb{Z}_{18}$. Analogously, if $d = -163$, we have

$$\begin{aligned} 4^{81\times 163^{m-1}} &= (4^{81} - 1 + 1)^{163^{m-1}} \\ &= (4^{81}-1)^{163^{m-1}} + 163^{m-1}(4^{81}-1)^{163^{m-1}-1} + \cdots + 163^{m-1}(4^{81}-1) + 1 \\ &\equiv 1 \pmod{163^m}. \end{aligned}$$

Since $163 \parallel (4^{81} - 1)$, the element $[4] \in \overline{R}$ in the case of $d = -163$ is of order $3^4 \times 163^{m-1}$, so $P \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^4} \cong \mathbb{Z}_{162}$. Therefore, we can conclude that $P \cong \mathbb{Z}_{D-1}$ for $d = -7, -11, -19, -43, -67, -163$. Accordingly, $U(\overline{R}) \cong P \times H \cong \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^{m-1}} \times \mathbb{Z}_{D-1}$, as desired.

(b) Suppose that $d = -3$, $n = 2m$, $m \geqslant 1$. Let $\alpha = [a + b\sqrt{d}\,] \in U(\overline{R})$, where $a, b \in \{0, 1, \cdots, 3^m - 1\}$ and $3 \nmid a$. Since $|U(\overline{R})| = 2 \times 3^{2m-1}$, we can write $U(\overline{R}) \cong \mathbb{Z}_2 \times Q$, where $|Q| = 3^{2m-1}$. We claim that $\alpha^{3^{m-1}} = [1]$ for $\alpha \in Q$. Let $W = 3^{m-1}$. Since $3^m \mid 3^j \binom{W}{2j}$ for $j \geqslant 1$, congruence (2.7) holds if and only if $a^{3^{m-1}} \equiv 1 \pmod{3^m}$, if and only if $a \in \mathbb{Z}_{3^{m-1}}$.

On the other hand, note that $3^m \mid 3^j \binom{W}{2j+1}$ for $2 \leqslant j \leqslant \frac{W-1}{2}$, congruence (2.8) is equivalent to

$$b\left[a^2 - \frac{(3^{m-1}-1)(3^{m-1}-2)}{2}b^2\right] \equiv 0 \pmod 3. \tag{2.11}$$

If $3 \mid b$, then clearly congruence (2.11) holds. If $3 \nmid b$, we show that congruence (2.11) holds, too. Indeed, since $3 \nmid b$, it follows from congruence (2.11) that

$$2a^2 - (3^{m-1}-1)(3^{m-1}-2)b^2 \equiv 0 \pmod 3. \tag{2.12}$$

Moreover, we have $2a^2 \equiv 2 \pmod 3$ for $3 \nmid a$. Thus congruence (2.12) reduces to $2 - 2b^2 \equiv 0 \pmod 3$. The last congruence holds for $3 \nmid b$. Hence, congruence (2.12) holds for any integers b. So we can conclude that $\alpha^{3^{m-1}} = [1]$ if and only if

$$a \in \mathbb{Z}_{3^{m-1}}, \quad b \in \{0, 1, \cdots, 3^m - 1\}. \tag{2.13}$$

Thus there are precisely $3^{m-1} \times 3^m = 3^{2m-1}$ elements $\alpha \in U(\overline{R})$ such that $\alpha^{3^{m-1}} = [1]$. Recall that $|Q| = 3^{2m-1}$, we obtain $\alpha^{3^{m-1}} = [1]$ for $\alpha \in Q$.

Next, we show that there exist elements in Q with order 3^{m-1}. Indeed, putting $W = 3^{m-2}$. Substituting the value for W into congruence (2.7). Note that $3^m \mid 3^j \binom{3^{m-2}}{2j}$ for $j \geqslant 2$, we derive that congruence (2.7) holds if and only if

$$2a^{3^{m-2}} - 3^{m-1}(3^{m-2}-1)a^{3^{m-2}-2}b^2 \equiv 2 \pmod{3^m}. \tag{2.14}$$

If we substitute $a = b = 1$ into congruence (2.14), we have $3^{m-1}(3^{m-2}-1) \equiv 0 \pmod{3^m}$, which is impossible for $m \geqslant 2$. Accordingly, congruence (2.7) does not hold for $a = b = 1$, which implies that $(1+\sqrt{-3}\,)^{3^{m-2}} \neq [1]$. Moreover, by the condition (2.13), $(1+\sqrt{-3}\,)^{3^{m-1}} = [1]$. So $\beta = [1 + \sqrt{-3}\,] \in Q$. Hence β is of order 3^{m-1}. So $\langle 1 + \sqrt{-3}\rangle \cong \mathbb{Z}_{3^{m-1}}$. Thus $Q \cong \mathbb{Z}_{3^{m-1}} \times J$, where J is a subgroup of Q with order 3^m.

Now, we claim that there are elements in J with order 3^{m-1}. We first note that $(1 + \sqrt{-3})^3 = -8$, thus $(1 + \sqrt{-3})^{3t} \in \mathbb{Z}$ for $t \geqslant 1$. Moreover, since $(1 + \sqrt{-3})^2 = -2 + 2\sqrt{-3}$, we conclude that $(1 + \sqrt{-3})^s = x + y\sqrt{-3}$, where $3 \nmid y$ and $3 \nmid s$. Let $\gamma = [1 + 3\sqrt{-3}\,]$. By condition (2.13), $\gamma \in Q$. Thus $\gamma^{3^{m-1}} = [1]$ but $\gamma \notin \langle 1 + \sqrt{-3}\,\rangle$. Hence, $\gamma \in J$. Substituting $a = 1$, $b = 3$ and $W = 3^{m-2}$ into congruence (2.8), and note that $3^m \mid 3^j \binom{3^{m-2}}{2j+1}$ for $j \geqslant 2$, we derive that congruence (2.8) holds if and only if

$$3^{m-1} - \frac{3^{m+1}(3^{m-2}-1)(3^{m-2}-2)}{2} \equiv 0 \pmod{3^m}.$$

The above congruence does not hold for $m \geqslant 2$. It follows that $(1+3\sqrt{-3}\,)^{3^{m-2}} \neq [1]$. Thus, $\gamma \in J$ is of order 3^{m-1}. Hence, $\mathbb{Z}_{3^{m-1}}$ is a subgroup of J, and $J \cong \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3$. Accordingly, if $d = -3$, then $U(\overline{R}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_{3^{m-1}}$, as desired.

(4) (a) Suppose that $d \neq -3$. Let $n = 2m + 1$ with $m \geqslant 1$. For $\alpha = [a + b\sqrt{d}\,] \in \overline{R}$, we know that $\alpha \in U(\overline{R})$ if and only if $D \nmid a$. Then, for $n = 2m+1$, we have $|U(\overline{R})| = (D-1)\cdot D^{2m}$. So $U(\overline{R}) = K \times G$, where K, G are finite groups, and $|K| = D - 1$, $|G| = D^{2m}$.

We now determine the structure of G. Consider the polynomial expansions of α^X, where X is an arbitrary integer. By Theorem 2.1 (2), α^X equals to the equivalence class [1] if and only if the following congruences hold

$$a^X + d\binom{X}{2}a^{X-2}b^2 + \cdots + d^{\frac{X-1}{2}}\binom{X}{X-1}ab^{X-1} \equiv 1 \pmod{D^{m+1}}, \tag{2.15}$$

$$\binom{X}{1}a^{X-1}b + d\binom{X}{3}a^{X-3}b^3 + \cdots + d^{\frac{X-1}{2}}b^X \equiv 0 \pmod{D^m}. \tag{2.16}$$

Firstly, putting $X = D^m$, and noting that $D^{m+1} \mid d^j\binom{D^m}{2j}$ for $j \geqslant 1$, we derive that congruence (2.15) holds if and only if $a^{D^m} \equiv 1 \pmod{D^{m+1}}$, if and only if $a \in \{1, 2, \cdots, D^{m+1}-1\}$ with $a \in \mathbb{Z}_{D^m}$. Therefore, congruence $a^{D^m} \equiv 1 \pmod{D^{m+1}}$ has precisely D^m solutions.

On the other hand, congruence (2.16) holds for $b \in \{1, 2, \cdots, D^m - 1\}$. Hence, the number of elements in $U(\overline{R})$ satisfying $\alpha^{D^m} = [1]$ is $D^m \times D^m = D^{2m}$. Recall that $|G| = D^{2m}$, we derive that $\alpha^{D^m} = [1]$ if and only if $\alpha \in G$.

Secondly, substituting $X = D^{m-1}$ into congruence (2.16). If $\alpha^{D^{m-1}} = [1]$, clearly $\alpha \in G$. Since $d \neq -3$, we have $D^m \mid d^j\binom{D^{m-1}}{2j+1}$ for $j \geqslant 1$. Therefore, congruence (2.16) holds if and only if $D \mid b$. In the case of $D \mid b$, congruence (2.15) holds if and only $a^{D^{m-1}} \equiv 1 \pmod{D^{m+1}}$, if and only if $a \in \mathbb{Z}_{D^{m-1}}$. Therefore, the number of elements in G satisfying $\alpha^{D^{m-1}} = [1]$ is $D^{m-1} \times D^{m-1} = D^{2m-2}$. Hence, there are precisely

$$D^{2m} - D^{2m-2} = (d^2 - 1) \cdot d^{2m-2} \tag{2.17}$$

elements of order D^m in $\overline{R}$.

Now, let $\beta = [1+\sqrt{d}\,]$. Then $\beta^{D^m} = [1]$. However, by the above argument, we know that $\beta^{D^{m-1}} \neq [1]$. So the order of β is D^m. Therefore $\mathbb{Z}_{D^m}$ is a subgroup of G, and $G \cong \mathbb{Z}_{D^m} \times G_2$, where $\langle 1 + \sqrt{d}\,\rangle \cong \mathbb{Z}_{D^m}$ and $|G_2| = D^m$.

Suppose $G_2 \cong \mathbb{Z}_{D^{s_1}} \times \cdots \times \mathbb{Z}_{D^{s_h}}$, where $s_1 + \cdots + s_h = m$. If $h \geqslant 2$, then $1 \leqslant s_j \leqslant m-1$ for $j = 1, \cdots, h$. Hence, there are precisely $(D-1) \cdot D^{2m-1}$ elements of order D^m in $\overline{R}$, which contradicts the above result (2.17). If $h = 1$, then $G_2 \cong \mathbb{Z}_{D^m}$ and hence $G \cong \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^m}$. Thus the number of elements in $\overline{R}$ of order D^m is $(d^2 - 1) \cdot d^{2m-2}$, which is the same as (2.17). Hence, we conclude that $h = 1$ and $G_2 \cong \mathbb{Z}_{D^m}$. Therefore, if $n = 2m+1$ with $m \geqslant 1$, then $U(\overline{R}) \cong K \times \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^m}$.

Finally, we determine the structure of the subgroup K for each case. Recall that $|K| = D - 1$. If $d = -7$, then $|K| = 6 = 2 \times 3$, we have $K \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_{D-1}$. If $d = -11$, then $|K| = 10 = 2 \times 5$, thus $K \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{D-1}$. If $d = -19$, then $|K| = 18 = 2 \times 3^2$, and by the similar argument to (3) above, the element $[4] \in \overline{R}$ is of order $3^2 \times 19^m$. So $K \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \cong \mathbb{Z}_{D-1}$. If $d = -43$, then $|K| = 42 = 6 \times 7$, so $K \cong \mathbb{Z}_6 \times \mathbb{Z}_7 \cong \mathbb{Z}_{D-1}$. If $d = -67$, then $|K| = 66 = 6 \times 11$, thus $K \cong \mathbb{Z}_6 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{D-1}$. If $d = -163$, then $|K| = 162 = 2 \times 3^4$, and by the similar argument to (3) above, the element $[4] \in \overline{R}$ is of order $3^4 \times 163^m$. So $K \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^4} \cong \mathbb{Z}_{D-1}$. Hence $K \cong \mathbb{Z}_{D-1}$ for each case. Thus $U(\overline{R}) \cong \mathbb{Z}_{D-1} \times \mathbb{Z}_{D^m} \times \mathbb{Z}_{D^m}$, as desired.

(b) Suppose $d = -3$. Let $\alpha = [a + b\sqrt{-3}\,] \in \overline{R}$, where $3 \nmid a$. Then $|U(\overline{R})| = 2 \times 3^{2m}$. So $U(\overline{R}) = \mathbb{Z}_2 \times G$, where $|G| = 3^{2m}$. Applying the similar argument of above (a) for the case

$d \neq -3$, we get that $\alpha^{D^m} = [1]$ if and only if $a \in \mathbb{Z}_{3^m}$ and $b \in \{0, 1, \cdots, 3^m - 1\}$, if and only if $\alpha \in G$.

Now, substituting $X = 3^{m-1}$ into congruence (2.16). We obtain that congruence (2.16) holds if and only if $2a^2b - (3^{m-1} - 1)(3^{m-1} - 2)b^3 \equiv 0 \pmod 3$. We can verify that the last congruence holds for any integers b.

On the other hand, congruence (2.15) holds if and only if

$$2a^{3^{m-1}} - 3^m(3^{m-1} - 1)a^{3^{m-1}-2}b^2 \equiv 2 \pmod{3^{m+1}}. \tag{2.18}$$

Clearly, the above congruence (2.18) does not hold, if $a = b = 1$. So $(1 + \sqrt{-3}\,)^{3^m} = [1]$, but $(1 + \sqrt{-3}\,)^{3^{m-1}} \neq [1]$. Hence, $\beta = [1 + \sqrt{-3}\,] \in G$ is of order 3^m. Then $G \cong \mathbb{Z}_{3^m} \times E$, where $\langle 1 + \sqrt{-3}\,\rangle \cong \mathbb{Z}_{3^m}$, $|E| = 3^m$.

Furthermore, if we substitute $a = 2$, $b = 3$ into above congruence (2.18), we have

$$2^{3^{m-1}} - 1 \equiv 0 \pmod{3^{m+1}}. \tag{2.19}$$

However,

$$\begin{aligned} 2^{3^{m-1}} - 1 &= (3-1)^{3^{m-1}} - 1 \\ &= 3^{3^{m-1}} - \binom{3^{m-1}}{1} 3^{3^{m-1}-1} + \cdots - \binom{3^{m-1}}{2} \times 3^2 + \binom{3^{m-1}}{1} \times 3 - 2 \\ &\equiv 3^m - 2 \pmod{3^{m+1}}. \end{aligned}$$

Therefore, congruence (2.19) does not hold for $m \geqslant 1$. Hence, if we let $\gamma = [2 + 3\sqrt{-3}\,]$, then by the above argument, we have $\gamma^{3^m} = [1]$, but $\gamma^{3^{m-1}} \neq [1]$. Thus, γ is of order 3^m. It leads to $\gamma \in G$. Moreover, $(1 + \sqrt{-3})^{3t} \in \mathbb{Z}$ for $t \geqslant 1$, $(1 + \sqrt{-3})^s = x + y\sqrt{-3}$, where $3 \nmid y$ and $3 \nmid s$. So we get that $\gamma \notin \langle 1 + \sqrt{-3}\,\rangle$, which implies that $\gamma \in E$. Recall that $|E| = 3^m$, therefore we have $E \cong \langle 2 + 3\sqrt{-3}\,\rangle \cong \mathbb{Z}_{3^m}$.

Hence, if $d = -3$, then $U(\overline{R}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^m} \times \mathbb{Z}_{3^m}$, as desired.

Theorem 2.7 Let $p \in \mathbb{Z}$ be an odd prime satisfying the Legendre symbol $(\frac{p}{-d}) = -1$. Let $\overline{R} = R_d/\langle p^n \rangle$, $n \geqslant 1$. Then $U(\overline{R}) \cong \mathbb{Z}_{p^2-1} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}}$.

Proof For $\alpha = [a + b\sqrt{d}\,] \in R_d/\langle p^n \rangle$, where $0 \leqslant a, b \leqslant p^n - 1$, it is easy to prove that α is a unit of $\overline{R}$ if and only if $p \nmid (a^2 - db^2)$. So $|U(\overline{R})| = (p^2 - 1)p^{2n-2}$.

If $n = 1$, as p is prime in $\overline{R}$, then $R_d/\langle p \rangle$ is a field with p^2 elements. Therefore $U(\overline{R}) \cong \mathbb{Z}_{p^2-1}$.

If $n \geqslant 2$, then $U(\overline{R}) \cong G_1 \times G_2$, where G_1 and G_2 are finite groups, and $|G_1| = p^2 - 1$, $|G_2| = p^{2n-2}$. First, we prove that $G_1 \cong \mathbb{Z}_{p^2-1}$. Clearly, there is an epimorphism of rings

$$\phi: \quad R_d/\langle p^n \rangle \to R_d/\langle p \rangle.$$

So there exists an epimorphism of groups

$$\varphi: U(R_d/\langle p^n \rangle) \to U(R_d/\langle p \rangle).$$

That is $\varphi:\ U(\overline{R}) \to\ \mathbb{Z}_{p^2-1}$. Clearly, the kernel $\ker(\varphi)$ of φ is G_2. If $\mathbb{Z}_{p^2-1} = \langle\eta\rangle$, then there exists $\theta \in U(\overline{R})$ such that $\varphi(\theta) = \eta$. Suppose the order of $\theta \in U(\overline{R})$ is t, then $\varphi(\theta^t) = 1$. Since the order of $\eta \in \mathbb{Z}_{p^2-1}$ is p^2-1, we have $\varphi(\theta^{p^2-1}) = \eta^{p^2-1} = 1$. Therefore, $\varphi(\theta^t) = \varphi(\theta^{p^2-1})$, i.e., $\eta^t = \eta^{p^2-1} = 1$. Thus we easily find that $(p^2-1)\,|\,t$, that is $(p^2-1)\,|\,o(\theta)$. Recall that $\ker(\varphi) = G_2$, and $\varphi(\theta) = \eta \neq 1$, so $\theta \notin \ker(\varphi) = G_2$. Thus $\theta \in G_1$, and $o(\theta)\,|\,(p^2-1)$. Therefore, $o(\theta) = p^2-1$. So we may conclude that $G_1 \cong \mathbb{Z}_{p^2-1}$.

In the following, we investigate the structure of G_2. For $\alpha = [a + b\sqrt{d}\,] \in G_2$. It is obvious that either $p \nmid a$ or $p \nmid b$. Consider the polynomial expansions of α^N, where $N > 1$ is an arbitrary odd integer. It is evident that $\alpha^N = [1]$ if and only if the following congruences hold

$$a^N + d\binom{N}{2}a^{N-2}b^2 + \cdots + d^{\frac{N-1}{2}}\binom{N}{N-1}ab^{N-1} \equiv 1 \pmod{p^n}, \tag{2.20}$$

$$\binom{N}{1}a^{N-1}b + d\binom{N}{3}a^{N-3}b^3 + \cdots + d^{\frac{N-1}{2}}b^N \equiv 0 \pmod{p^n}. \tag{2.21}$$

By the similar argument to Theorem 2.6 (3), we know that $\alpha^{p^{n-1}} = 1$ for all $\alpha \in G_2$, and there are precisely p^{2n-4} elements $\gamma \in G_2$ satisfying $\gamma^{p^{n-2}} = [1]$.

Moreover, let $\beta = [c + e\sqrt{d}\,] \in G_2$ with $p \nmid c$ and $p \parallel e$. By the polynomial expansions of $\beta^{p^{n-2}}$, we know that $\beta^{p^{n-2}} \neq 1$, which implies $o(\beta) = p^{n-1}$. So $G_2 \cong H \times P$, where $H = \langle\beta\rangle \cong \mathbb{Z}_{p^{n-1}}$ and $|P| = p^{n-1}$.

Suppose $G_2 \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{h_1}} \times \cdots \times \mathbb{Z}_{p^{h_r}}$, where $h_1 + \cdots + h_r = n-1$. If $r \geqslant 2$, then $1 \leqslant h_i \leqslant n-2$ for $i = 1, \cdots, r$. Thus there are $p^{n-2}p^{h_1}\cdots p^{h_r} = p^{2n-3}$ elements $\gamma \in G_2$ satisfying $\gamma^{p^{n-2}} = [1]$, which contradicts the above result. If $r = 1$, then $G_2 \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}}$. So there are exactly $p^{n-2}p^{n-2} = p^{2n-4}$ elements $\gamma \in G_2$ satisfying $\gamma^{p^{n-2}} = [1]$, which is the same as above result. So we derive that $r = 1$ and this leads to $G_2 \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}}$. This completes the proof.

Theorem 2.8 Let $q \in \mathbb{Z}$ be a prime satisfying the Legendre symbol $(\frac{q}{-d}) = 1$. Suppose that π is a proper factor of q. Let $\overline{R} = R_d/\langle\pi^n\rangle$, $n \geqslant 1$.

(1) Suppose $q = 2$. Then $U(\overline{R}) \cong \mathbb{Z}_1$ if $n = 1$, $U(\overline{R}) \cong \mathbb{Z}_2$ if $n = 2$, $U(\overline{R}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ if $n > 2$.

(2) Suppose $q \neq 2$. Then $U(\overline{R}) \cong \mathbb{Z}_{q^{n-1}} \times \mathbb{Z}_{q-1}$.

Proof Applying Theorem 2.1 (4), we derive that $\overline{R} \cong \mathbb{Z}/\langle q^n\rangle$. So the theorem follows.

We obtain from the proof of Theorem 1.2 that 2 is not a prime in R_d if $d = -7$. So we may assume $d \neq -7$ in the following theorems. We investigate the unit groups of $R_d/\langle 2^n\rangle$ for $d = -3,\ -11,\ -19,\ -43,\ -67,\ -163$.

Theorem 2.9 Suppose $d = -3, -11, -19, -43, -67, -163$. Let $\overline{R} = R_d/\langle 2^n\rangle$, $n \geqslant 2$. Then

(1) $U(\overline{R}) = \overline{R}_1 \cup \overline{R}_2 \cup \overline{R}_3$, where

$\overline{R}_1 = \left\{[r_1 + r_2\sqrt{d}\,]:\ 0 \leqslant r_1, r_2 \leqslant 2^{n-1}-1,\ r_1, r_2 \in \mathbb{Z} \text{ are not of the same parity}\right\}$,

$\overline{R}_2 = \left\{[r_1 - r_2\sqrt{d}\,]:\ 0 \leqslant r_1 \leqslant 2^{n-1}-1,\ 1 \leqslant r_2 \leqslant 2^{n-1}, r_1, r_2 \in \mathbb{Z} \text{ are not of the same parity}\right\}$,

$\overline{R}_3 = \left\{[\frac{r_1}{2} \pm \frac{r_2}{2}\sqrt{d}\,]:\ 1 \leqslant r_i \leqslant 2^n-1,\ r_i \in \mathbb{Z},\ 2 \nmid r_i,\ i = 1, 2\right\}$.

(2) Suppose $n \geqslant 4$. Then there are exactly 8 elements $\alpha \in \overline{R}_1 \cup \overline{R}_2$ satisfying $\alpha^2 = [1]$.

(3) Suppose $n \geqslant 5$. Then there are exactly 32 elements $\alpha \in \overline{R}_1 \cup \overline{R}_2$ satisfying $\alpha^4 = [1]$.

Proof (1) If $\alpha = [r_1 \pm r_2\sqrt{d}\,] \in \overline{R}$, where $r_1, r_2 \in \mathbb{Z}$, it is easy to show that $\alpha \in U(\overline{R})$ if and only if $2 \nmid N(\alpha)$, i.e., $2 \nmid (r_1^2 - dr_2^2)$, if and only if r_1 and r_2 are not of the same parity.

If $\alpha = [\frac{r_1}{2} \pm \frac{r_2}{2}\sqrt{d}\,] \in \overline{R}$, where $r_1, r_2 \in \mathbb{Z}$ with $2 \nmid r_1 r_2$, then $\alpha \in U(\overline{R})$ if and only if $2 \nmid N(\alpha)$, i.e., $2 \nmid \frac{1}{4}(r_1^2 - dr_2^2)$, if and only if $8 \nmid (r_1^2 - dr_2^2)$. Let $r_i = 2k_i + 1$, $i = 1, 2$. Then

$$r_1^2 - dr_2^2 = 4(k_1^2 + k_1 - dk_2^2 - dk_2) + (1 - d).$$

Clearly, $2 \,|\, (k_1^2 + k_1 - dk_2^2 - dk_2)$. However, $4 \parallel (1 - d)$ for $d = -3, -11, -19, -43, -67, -163$. Therefore, $8 \nmid (r_1^2 - dr_2^2)$. Hence, $\alpha \in U(\overline{R})$.

(2) First, let $\alpha = a \in \mathbb{Z}$, where $1 \leqslant a \leqslant 2^{n-1} - 1$. Then $\alpha \in U(\overline{R})$ if and only if $2 \nmid a$. By Corollary 2.5, $\alpha^2 = [1]$ if and only if $a^2 \equiv 1 \pmod{2^n}$. The last congruence has precisely 2 solutions.

Second, let $\alpha = \pm b\sqrt{d}$, where $1 \leqslant b \leqslant 2^{n-1} - 1$. Then $\alpha \in U(\overline{R})$ if and only if $2 \nmid b$. Let $b = 2k + 1$. By Corollary 2.5, $\alpha^2 = [1]$ if and only if $d(4k^2 + 4k + 1) \equiv 1 \pmod{2^n}$. Since $d - 1 = -4x$, where $x = 1, 3, 5, 11, 17, 41$, we obtain that $d(4k^2 + 4k + 1) - 1 = 4(k^2 d + kd - x)$. Note that $2 \nmid (k^2 d + kd - x)$, we derive that $d(4k^2 + 4k + 1) \not\equiv 1 \pmod{2^n}$. Therefore $\alpha^2 \neq [1]$.

Thirdly, let $\alpha = a + b\sqrt{d}$, where $1 \leqslant a, b \leqslant 2^{n-1} - 1$, $a, b \in \mathbb{Z}$ are not of the same parity. By Corollary 2.5, $\alpha^2 = [1]$ if and only if the following congruences hold

$$a^2 + b^2 d = 2^{n-1} k_1 + 1, \tag{2.22}$$

$$2ab = 2^{n-1} k_2, \tag{2.23}$$

where k_1 and k_2 are of the same parity. If $2 \nmid a$ while $2 \,|\, b$, then (2.23) reduces to $b \equiv 0 \pmod{2^{n-2}}$. Recall that $1 \leqslant b \leqslant 2^{n-1} - 1$, so the last congruence has exactly one solution $b = 2^{n-2}$. Hence, the left hand of (2.23) is $2ab = 2^{n-1} a$ with $2 \nmid a$. The left hand of (2.22) is $a^2 + b^2 d = a^2 + 2^{2n-4} d = a^2 + 2^{n-1} \times 2^{n-3} d$. Because $n \geqslant 4$, so 2^{n-3} is even. Then equality (2.22) holds for some odd integers k_1 if and only if $a^2 = 2^{n-1} k + 1$ for some odd integers k, if and only if $a = 2^{n-2} \pm 1$. So we can conclude that in the case of $2 \nmid a$ and $2 \,|\, b$, there are exactly 2 elements α satisfying $\alpha^2 = [1]$.

On the other hand, suppose that $2 \,|\, a$ while $2 \nmid b$. Then (2.23) reduces to $a \equiv 0 \pmod{2^{n-2}}$. Recall that $1 \leqslant a \leqslant 2^{n-1} - 1$, so the last congruence has exactly one solution $a = 2^{n-2}$. Hence, the left hand of (2.23) is $2ab = 2^{n-1} b$ with $2 \nmid b$. The left hand of (2.22) is $a^2 + b^2 d = 2^{2n-4} + b^2 d = 2^{n-1} \times 2^{n-3} + b^2 d$. So equality (2.22) holds for some odd integers k_1 if and only if $b^2 d = 2^{n-1} h + 1$ for some odd integers h. Putting $b = 2s + 1$, then $b^2 d - 1 = 4d(s^2 + s) + (d - 1)$. Because $s^2 + s$ is even and $4 \parallel (d - 1)$ for $d = -3, -11, -19, -43, -67, -163$, we obtain that $4 \parallel (b^2 d - 1)$. Therefore, for $n \geqslant 4$, $b^2 d \neq 2^{n-1} h + 1$ for any integers h. So we can conclude that in the case of $2 \,|\, a$ and $2 \nmid b$, there does not exist any element α satisfying $\alpha^2 = [1]$.

Finally, let $\alpha = a - b\sqrt{d}$, where $1 \leqslant a \leqslant 2^{n-1} - 1$, $1 \leqslant b \leqslant 2^{n-1}$, $a, b \in \mathbb{Z}$ are not of the same parity. If $2 \nmid a$ while $2 \,|\, b$, then (2.23) reduces to $b \equiv 0 \pmod{2^{n-2}}$. Thus $b = 2^{n-2}$ or 2^{n-1}. In the case of $b = 2^{n-2}$, applying the similar argument of above, we get that $\alpha^2 = [1]$ if and only if $a = 2^{n-2} \pm 1$. For the other case $b = 2^{n-1}$, equality (2.23) reduces to $2ab = 2^n a$, and the left hand of equality (2.22) is $a^2 + b^2 d = a^2 + 2^{2n-2} d$. By Corollary 2.5, $\alpha^2 = [1]$ if and only if $a^2 \equiv 1 \pmod{2^n}$, if and only if $a = 1, 2^{n-1} - 1$. Therefore, there are exactly 4 elements α satisfying $\alpha^2 = [1]$, if $2 \nmid a$ and $2 \mid b$.

On the other hand, if $2 \mid a$ while $2 \nmid b$, by the similar above argument, we obtain that $\alpha^2 \neq [1]$.

Thus, there are exactly 8 elements $\alpha \in \overline{R}_1 \cup \overline{R}_2$ satisfying $\alpha^2 = [1]$, as desired.

(3) Firstly, let $\alpha = a \in \mathbb{Z}$, where $1 \leqslant a \leqslant 2^{n-1} - 1$ with $2 \nmid a$, $a \in \mathbb{Z}$. By Corollary 2.5, $\alpha^4 = [1]$ if and only if $a^4 \equiv 1 \pmod{2^n}$. The last congruence has precisely 4 solutions.

Secondly, let $\alpha = \pm b\sqrt{d}$, where $1 \leqslant b \leqslant 2^{n-1} - 1$ with $2 \nmid b$, $b \in \mathbb{Z}$. Let $b = 2k + 1$. By Corollary 2.5, $\alpha^4 = [1]$ if and only if $b^4 d^2 - 1 \equiv 0 \pmod{2^n}$, i.e.,

$$8d^2(2k^4 + 4k^3 + 3k^2 + k) + (d^2 - 1) \equiv 0 \pmod{2^n}. \tag{2.24}$$

It is evident that $2^4 \nmid (d^2 - 1)$ for $d = -3, -11, -19, -43, -67, -163$. So $b^4 d^2 - 1 \not\equiv 0 \pmod{2^n}$ for $n \geqslant 5$. Thus, $\alpha^4 \neq [1]$.

Thirdly, let $\alpha = a + b\sqrt{d}$, where $1 \leqslant a, b \leqslant 2^{n-1} - 1$, a and b are not of the same parity. By Corollary 2.5, $\alpha^4 = [1]$ if and only if the following congruences hold

$$a^4 + b^2(6a^2 d + b^2 d^2) = 2^{n-1} k_1 + 1, \tag{2.25}$$

$$4b(a^3 + ab^2 d) = 2^{n-1} k_2, \tag{2.26}$$

where k_1 and k_2 are of the same parity. If $2 \nmid a$ while $2 \mid b$, then (2.26) reduces to $b \equiv 0 \pmod{2^{n-3}}$. The last congruence has exactly three solutions $b = 2^{n-3} x$, where $x = 1, 2, 3$. Suppose first that $b = 2^{n-3} x$, $x = 1, 3$. Then the left hand of equation (2.26) equals $4b(a^3 + ab^2 d) = 2^{n-1} k_2$, where $k_2 = x(a^3 + ab^2 d)$ is odd.

On the other hand, the left hand of equation (2.25) equals $a^4 + 2^{n-1}(3 \times 2^{n-4} a^2 d + 2^{3n-11} d^2 x^2) x^2$. Since $n \geqslant 5$, we get that $(3 \times 2^{n-4} a^2 d + 2^{3n-11} d^2 x^2) x^2$ is even. Therefore, $\alpha^4 = [1]$ if and only if $a^4 = 2^{n-1} s + 1$ for some odd integers s. Since $1 \leqslant a \leqslant 2^{n-1} - 1$, clearly there are exactly 4 elements a satisfying $a^4 = 2^{n-1} s + 1$ for some odd integers s. Now suppose $b = 2^{n-3} x$, where $x = 2$. Then the left hand of equation (2.26) equals $4b(a^3 + ab^2 d) = 2^n (a^3 + ab^2 d)$. Therefore, by equation (2.25), we obtain that $\alpha^4 = [1]$ if and only if $a^4 \equiv 1 \pmod{2^n}$. The last congruence has exactly 4 solutions $a \in \{1, \cdots, 2^{n-1} - 1\}$. Hence, there are totally 12 elements α satisfying $\alpha^4 = [1]$, in the case of $2 \nmid a$ and $2 \mid b$. For another case of $2 \mid a$ and $2 \nmid b$, we reduce from equation (2.25) that $2^{n-3} \mid a$. Hence, $a = 2^{n-3} y$, where $y = 1, 2, 3$. Suppose $a = 2^{n-3} y$, where $y = 1, 3$. Then by equations (2.25) and (2.26), $\alpha^4 = [1]$ if and only if $b^4 d^2 = 2^{n-1} s + 1$ for some odd integers s. Let $b = 2k + 1$, then $b^4 d^2 - 1$ is equal to the left side of congruence (2.24). Since $2^4 \nmid (d^2 - 1)$ for $d = -3, -11, -19, -43, -67, -163$. So $b^4 d^2 - 1 \not\equiv 0 \pmod{2^{n-1}}$ for $n \geqslant 5$. Thus, $\alpha^4 \neq [1]$. Next, we assume that $a = 2^{n-3} y$, where $y = 2$. Then by equations (2.25) and (2.26), $\alpha^4 = [1]$ if and only if $b^4 d^2 \equiv 1 \pmod{2^n}$, if and only if congruence (2.24) holds for any integers k and n. However, this congruence does not hold for $n \geqslant 5$. Therefore, we can conclude that in the case of $2\,|\,a$ and $2\nmid b$, there does not exist any element α satisfying $\alpha^4=[1]$. Hence, there are totally 12 elements $\alpha=[a+b\sqrt{d}]\in\overline{R}_1$ satisfying $\alpha^4=[1]$, where $a\neq 0$ and $b\neq 0$.

Finally, let $\alpha=a-b\sqrt{d}$, where $1\leqslant a\leqslant 2^{n-1}-1$, $1\leqslant b\leqslant 2^{n-1}$, a and b are not of the same parity. If $2\nmid a$ while $2\,|\,b$, then (2.26) reduces to $b\equiv 0 \pmod{2^{n-3}}$. The last congruence has exactly four solutions, namely $b=2^{n-3}x$, where $x=1,2,3,4$. Applying the similar argument above, we obtain that there are exactly 16 elements $\alpha\in\overline{R}_2$ satisfying $\alpha^4=[1]$, where $a\neq 0$. On the other hand, if $2\,|\,a$ and $2\nmid b$, there does not exist any element $\alpha\in\overline{R}_2$ satisfying $\alpha^4=[1]$.

Thus, there are exactly 32 elements $\alpha\in\overline{R}_1\cup\overline{R}_2$ satisfying $\alpha^4=[1]$, as desired.

In the sequel, we assume that 2 is prime in the ring R_d. If $n=1$, by Theorem 2.1 (5) and Theorem 2.9, $R_d/\langle 2\rangle$ is a field with 4 elements. Therefore, $U(R_d/\langle 2^n\rangle)\cong\mathbb{Z}_3$.

If $n=2$, then $|U(R_d/\langle 2^n\rangle)|=3\times 2^2$. The unit group of $R_d/\langle 2^n\rangle$ is

$$\left\{1,\ \pm\sqrt{d},\ 1-2\sqrt{d},\ \frac{1}{2}\pm\frac{1}{2}\sqrt{d},\ \frac{1}{2}\pm\frac{3}{2}\sqrt{d},\ \frac{3}{2}\pm\frac{1}{2}\sqrt{d},\ \frac{3}{2}\pm\frac{3}{2}\sqrt{d}\right\}.$$

By calculation, we obtain that for $d=-3,-11,-19,-43,-67,-163$, $(\pm\sqrt{d})^2=4k+1$ for some integers k. So by Corollary 2.5, $\pm\sqrt{d}$ is of order 2. Similarly, $(\frac{3}{2}\pm\frac{3}{2}\sqrt{d})^3=-27=[1]$. So the order of $\frac{3}{2}\pm\frac{3}{2}\sqrt{d}$ is 3. Moreover, we show that $o(1-2\sqrt{d})=2$, $o(\frac{1}{2}\pm\frac{1}{2}\sqrt{d})=o(\frac{1}{2}\pm\frac{3}{2}\sqrt{d})=o(\frac{3}{2}\pm\frac{1}{2}\sqrt{d})=6$. Hence, $U(R_d/\langle 2^2\rangle)\cong\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2$.

Analogously, if $n=3$, then $|U(R_d/\langle 2^n\rangle)|=3\times 2^4$. The unit group of $R_d/\langle 2^n\rangle$ is

$$\begin{aligned}&\left\{1,\ 3,\ \pm\sqrt{d},\ \pm 3\sqrt{d},\ 1\pm 2\sqrt{d},\ 2\pm\sqrt{d},\ 2\pm 3\sqrt{d},\ 3\pm 2\sqrt{d},\ 1-4\sqrt{d},\ 3-4\sqrt{d}\right\}\\ \bigcup\ &\left\{\frac{a}{2}\pm\frac{b}{2}\sqrt{d}:\quad a,b=1,3,5,7\right\}.\end{aligned}$$

By calculation, we obtain that $o(3)=o(1\pm 2\sqrt{d})=o(3\pm 2\sqrt{d})=o(1-4\sqrt{d})=o(3-4\sqrt{d})=2$, and $o(\pm\sqrt{d})=o(\pm 3\sqrt{d})=o(2+\sqrt{d})=o(2+3\sqrt{d})=o(2-\sqrt{d})=o(2-3\sqrt{d})=4$. Moreover, $o(\frac{a}{2}\pm\frac{b}{2}\sqrt{d})\neq 2,4$ for $a,b=1,3,5,7$. Therefore, $U(R_d/\langle 2^3\rangle)\cong\mathbb{Z}_3\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2\times\mathbb{Z}_2$.

Theorem 2.10 Suppose that $d=-3$, -11, -19, -43, -67 or -163. Then

(1) $U(R_d/\langle 2\rangle)\cong\mathbb{Z}_3$.

(2) $U(R_d/\langle 2^n\rangle)\cong\mathbb{Z}_3\times\mathbb{Z}_{2^{n-1}}\times\mathbb{Z}_{2^{n-2}}\times\mathbb{Z}_2$ for $n\geqslant 2$.

Proof The unit groups for the cases of $n=1,2,3$ have been stated above. So we assume $n\geqslant 4$ in the following. By Theorem 2.9, we get $|U(R_d/\langle 2^n\rangle)|=3\times 2^{2n-2}$. Thus $U(R_d/\langle 2^n\rangle)\cong\mathbb{Z}_3\times H$, where H is a subgroup with order 2^{2n-2}.

Firstly, we claim that $\alpha^{2^{n-1}}=[1]$ for $\alpha\in\overline{R}_1\cup\overline{R}_2$, where $\overline{R}_1$ and $\overline{R}_2$ are stated in Theorem 2.9. Indeed, if we put $\alpha=a+b\sqrt{d}\in\overline{R}_1$, $\alpha^M=A+B\sqrt{d}$, M is even, then

$$\begin{aligned}A&=a^M+d\binom{M}{2}a^{M-2}b^2+d^2\binom{M}{4}a^{M-4}b^4+\cdots+d^{\frac{M-2}{2}}\binom{M}{M-2}a^2b^{M-2}+d^{\frac{M}{2}}b^M,\\ B&=\binom{M}{1}a^{M-1}b+d\binom{M}{3}a^{M-3}b^3+\cdots+d^{\frac{M-4}{2}}\binom{M}{M-3}a^3b^{M-3}+d^{\frac{M-2}{2}}\binom{M}{M-1}ab^{M-1}.\end{aligned}$$

Let $M=2^{n-1}$. If $2\nmid a$ while $2\,|\,b$, then $2^n\,|\,\binom{2^{n-1}}{s}b^s$ for $1\leqslant s\leqslant 2^{n-1}$. So we derive $2^n\,|\,(A-a^{2^{n-1}})$ and $2^n\,|\,B$. Hence, $A=2^nt+a^{2^{n-1}}$ and $B=2^nk$ for some integers t,k. By

Corollary 2.5, $\alpha^{2^{n-1}} = [1]$ if and only if $a^{2^{n-1}} \equiv 1 \pmod{2^n}$. Because $U(\mathbb{Z}/\langle 2^n\rangle) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ for $n \geqslant 3$, we derive that $a^{2^{n-1}} \equiv 1 \pmod{2^n}$ for $2 \nmid a$ and $n \geqslant 3$. Thus $\alpha^{2^{n-1}} = [1]$ in the case of $2 \nmid a$ and $2 \mid b$.

On the other hand, suppose $2 \mid a$ while $2 \nmid b$. Since $2^n \mid \binom{2^{n-1}}{s} a^{2^{n-1}-s}$ for $0 \leqslant s \leqslant 2^{n-1}-1$, it is obvious that $2^n \mid (A - d^{2^{n-2}} b^{2^{n-1}})$ and $2^n \mid B$. Since $d, b \in U(\mathbb{Z}/\langle 2^n\rangle)$, we must have $d^{2^{n-2}} \equiv 1 \pmod{2^n}$ and $b^{2^{n-1}} \equiv 1 \pmod{2^n}$. Hence, $d^{2^{n-2}} b^{2^{n-1}} \equiv 1 \pmod{2^n}$. Therefore, $\alpha^{2^{n-1}} = [1]$ in the case of $2 \mid a$ and $2 \nmid b$. So we conclude that $\alpha^{2^{n-1}} = [1]$ for $\alpha \in \overline{R}_1$. Similarly, we have $\alpha^{2^{n-1}} = [1]$ for $\alpha \in \overline{R}_2$. Thus, our claim follows.

Secondly, we prove that $\mathbb{Z}_{2^{n-1}}$ is a subgroup of H. Since the number of the set $\overline{R}_1 \cup \overline{R}_2$ is precisely 2^{2n-2} and note that the subgroup H is of order 2^{2n-2}, we can conclude that $\alpha \in H$ if and only if $\alpha \in \overline{R}_1 \cup \overline{R}_2$. So $H = \overline{R}_1 \cup \overline{R}_2$. Furthermore, let $\alpha_0 = [2 + \sqrt{d}] \in H$. We prove that $\alpha_0^{2^{n-2}} \neq [1]$. Setting $a = 2, b = 1, M = 2^{n-2}$. Substituting these values into the expressions for A and B. Since $2^n \mid \binom{2^{n-2}}{s} a^s$ for $3 \leqslant s \leqslant 2^{n-2}$, and $2^{n-1} \parallel \binom{2^{n-2}}{s} a^s$ for $s = 1, 2$, we derive that $2^{n-1} \parallel (A - d^{2^{n-3}})$ and $2^{n-1} \parallel B$. So $A = 2^{n-1}k + d^{2^{n-3}}$ for some odd integers k. Moreover, owing to Corollary 2.5, $\alpha_0^{2^{n-2}} = [1]$ if and only if $A = 2^{n-1}t + 1$ for some odd integers t, i.e., $A = 2^{n-1}k + d^{2^{n-3}} = 2^{n-1}t + 1$, if and only if $d^{2^{n-3}} = 2^{n-1}(t-k) + 1$. Since $2 \nmid kt$, we have $t - k$ is even. Therefore, $\alpha_0^{2^{n-2}} = [1]$ if and only if $d^{2^{n-3}} \equiv 1 \pmod{2^n}$. In the following, we show that $d^{2^{n-3}} \not\equiv 1 \pmod{2^n}$ for $d = -3, -11, -19, -43, -67$ or -163. Indeed, we have $-d = 4e - 1$ for some odd integers e. Then

$$d^{2^{n-3}} - 1 = (4e-1)^{2^{n-3}} - 1 = (4e)^{2^{n-3}} - \binom{2^{n-3}}{1}(4e)^{2^{n-3}-1} + \cdots + \binom{2^{n-3}}{2}(4e)^2 - \binom{2^{n-3}}{1}4e.$$

It is evident that $2^n \mid \binom{2^{n-3}}{s}(4e)^s$ for $2 \leqslant s \leqslant 2^{n-3}$. However, $\binom{2^{n-3}}{1}4e = 2^{n-1}e$ is not divisible by 2^n. Thus $d^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Hence, $\alpha_0^{2^{n-2}} \neq [1]$, which implies that α_0 is of order 2^{n-1}. Therefore, $\mathbb{Z}_{2^{n-1}}$ is a subgroup of H, as desired.

Now, owing to Theorem 2.9 (2), we obtain that $H \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^i} \times \mathbb{Z}_{2^j}$, where $i, j \geqslant 1$ and $i + j = n - 1$. If $n = 4$, then $i + j = 3$. Hence, $H \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2$ for the case $n = 4$. Next, we assume that $n > 4$. If $i, j \geqslant 2$, then there are precisely 64 elements $\alpha \in \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^i} \times \mathbb{Z}_{2^j}$ satisfying $\alpha^4 = [1]$, which contradicts Theorem 2.9 (3). If $i = n - 2$ and $j = 1$, then there are precisely 32 elements $\alpha \in \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$ satisfying $\alpha^4 = [1]$, which is the same as Theorem 2.9 (3). Therefore, we conclude that $H \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$. This completes the proof of the theorem.

References

[1] Pezda T. Cycles of polynomial mappings in two variables over rings of integers in quadratic fields [J]. Central Eur. J. Math., 2004, 2(2): 294–331.

[2] Pezda T. Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals II [J]. Monatsh. Math., 2005, 145: 321–331.

[3] Stark H M. A complete determination of the complex quadratic fields of class-number one [J]. Michigan Math. J., 1967, 14(1): 1–27.

[4] Cross J T. The Euler ϕ-function in the Gaussian integers [J]. Amer. Math. Monthly, 1983, 90: 518–528.

[5] Tang Gaohua, Su Hudong, Yi Zhong. The unit groups of $\mathbb{Z}_n[i]$ [J]. J. Guangxi Normal Univ., 2010, 28(2): 38–41.

[6] Wei Yangjiang, Su Huadong, Tang Gaohua. The unit groups of the quotient rings of the complex quadratic rings [J]. Front. Math. China, 2016, 11(4): 1037–1056.

[7] Wei Yangjiang, Tang Gaohua. The square mapping graphs of the ring $\mathbb{Z}_n[i]$ [J]. J. Math., 2016, 36(4): 676–682.

[8] Karpilovsky G. Units groups of classical rings [M]. New York: Oxford University Press, 1988.

[9] Niven I, Zuckerman H S. An introduction to the theory of numbers [M]. New York: John Wiley Sons, 1980.

虚二次环的商环的单位群

韦扬江, 苏磊磊, 唐高华

(广西师范学院数学与统计科学学院, 广西 南宁 530023)

摘 要: 本文研究了有理数域 $\mathbb{Q}$ 的二次扩域$\mathbb{Q}(\sqrt{d})$ 的整数环 R_d 的商环的单位群. 利用二项式分解以及有限交换群的结构性质, 获得了 $d=-3$, -7, -11, -19, -43, -67, -163 时 $R_d/\langle\vartheta^n\rangle$ 的单位群结构, 其中 ϑ 是 R_d 的素元, n 是任意正整数. 所得的结果推广了由 J. T. Cross (1983), G. H. Tang 与 H. D. Su (2010) 对 $d=-1$, 以及 Y. J. Wei (2016) 对 $d=-2$ 时关于 $R_d/\langle\vartheta^n\rangle$ 的单位群的研究.

关键词: 虚二次环; 商环; 单位群; 二次扩域

MR(2010)**主题分类号**: 11R04; 20K01 **中图分类号**: O152.1; O156.1