Article ID:0253-2778(2015)08-0623-04

Ramification in relative quadratic extensions and fundamental units of real quadratic fields

WANG Bing[1], ZHANG Zhe[2]

(1. School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China;
2. School of Mathematics and Statistics, Xidian University, Xi'an 710126, China)

Abstract: Let $F=\mathbb{Q}(\sqrt{d})$ be a real quadratic field and $\varepsilon=x+y\sqrt{d}$ the fundamental unit of F satisfying $N_{F/\mathbb{Q}}(\varepsilon)=1$. Some connections between the ramification properties for dyadic prime ideals in quadratic extension $F(\sqrt{\varepsilon})/F$ and congruence properties of x, y were established. As a corollary, some congruence properties about x, y were given when $d=p_1\cdots p_r$ or $2p_1\cdots p_r$ with $p_1\equiv\cdots\equiv p_r\equiv 1 \bmod 4$ being distinct prime numbers.

Key words: real quadratic field; fundamental unit; dyadic prime ideal; ramification

CLC number: O156.2 **Document code**: A doi: 10.3969/j.issn.0253-2778.2015.08.001

2010 Mathematics Subject Classification: 11R27

Citation: Wang Bing, Zhang Zhe. Ramification in relative quadratic extensions and fundamental units of real quadratic fields[J]. Journal of University of Science and Technology of China, 2015,45(8):623-626.

相对二次扩张的分歧性与实二次域的基本单位

王 兵[1],张 哲[2]

(1.中国科学技术大学数学科学学院,安徽合肥 230026;2.西安电子科技大学数学与统计学院,陕西西安 710126)

摘要:设 $F=\mathbb{Q}(\sqrt{d})$为实二次域,$\varepsilon=x+y\sqrt{d}$为 F 的基本单位,并且 ε 满足 $N_{F/\mathbb{Q}}(\varepsilon)=1$. 建立起二次扩张 $F(\sqrt{\varepsilon})/F$的二进素理想的分歧性质和 x, y 的同余性质之间的联系. 并在 $d=p_1\cdots p_r$ 或 $2p_1\cdots p_r$ 的情形下,给出 x, y 的一些同余性质,其中,$p_1,\cdots,p_r$ 为模 4 余 1 的不同素数.

关键词:实二次域;基本单位;二进素理想;分歧性质

0 Introduction

Let d be a square-free positive integer and $F=\mathbb{Q}(\sqrt{d})$ a real quadratic field. Let $\varepsilon=x+y\sqrt{d}>1$ be the fundamental unit of F. We assume that $N_{F/\mathbb{Q}}(\varepsilon)=1$. In this paper, we establish some connections between ramification properties for dyadic prime ideals in the relative quadratic extension $F(\sqrt{\varepsilon})/F$ and congruence properties of x, y. As a corollary, we give some congruence

Received: 2014-11-10; **Revised**: 2015-07-07

Foundation item: Supported by National Key Basic Research Program of China (2013CB834202), National Natural Science Foundation of China (11171317,11501429) and Fundamental Research Funds for the Central Universities (JB150706).

Biography: WANG Bing, male, born in 1982, PhD candidate. Research field: algebraic number theory. E-mail: wangbinx@mail.ustc.edu.cn

Corresponding author: ZHANG Zhe, PhD/lecturer. E-mail: zhangz@xidian.edu.cn

properties about x, y in certain cases.

It is well known that if $d\equiv 1 \bmod 8$ or $d\equiv 2,3 \bmod 4$, then x, y are integers, and if $d\equiv 5 \bmod 8$, it can happen that x, y are not integers, if so, then ε^3 does have integral coefficients. To avoid fractions, we will temporarily let $\varepsilon = x + y\sqrt{d}$, where the positive integer pair (x, y) is the fundamental integer solution to the Diophantine equation

$$x^2 - dy^2 = 1 \tag{1}$$

and we shall refer to ε as the fundamental integral unit of $F=\mathbb{Q}(\sqrt{d})$ (cf. Ref. [1, p. 273]). Thus, if $d\equiv 1 \bmod 8$ or $d\equiv 2,3 \bmod 4$, the fundamental unit of F is the fundamental integral unit. If $d\equiv 5 \bmod 8$ and the fundamental unit of F is not the fundamental integral unit, then its third power is the fundamental integral unit of F.

The aim of this paper is to prove the following theorem.

Theorem 0.1 Let d be a square-free positive integer and $F=\mathbb{Q}(\sqrt{d})$ a real quadratic field. Let ε be the fundamental integral unit of F. Assume that $N_{F/\mathbb{Q}}(\varepsilon)=1$, we have

① Suppose $d\equiv 1 \bmod 4$. Then $F(\sqrt{\varepsilon})/F$ is unramified at the dyadic prime ideal(s) of F if and only if $x\equiv 1 \bmod 32$, $y\equiv 0 \bmod 8$ or $x\equiv 9 \bmod 32$, $y\equiv 4 \bmod 8$. $F(\sqrt{\varepsilon})/F$ is ramified at the dyadic prime ideal(s) of F if and only if $x\equiv 31 \bmod 32$, $y\equiv 0 \bmod 8$ or $x\equiv 23 \bmod 32$, $y\equiv 4 \bmod 8$.

② Suppose $d\equiv 2 \bmod 8$. Then $F(\sqrt{\varepsilon})/F$ is unramified at the dyadic prime ideal of F if and only if $x\equiv 1 \bmod 16$, $y\equiv 0 \bmod 4$ or $x\equiv 3 \bmod 16$, $y\equiv 2 \bmod 4$. $F(\sqrt{\varepsilon})/F$ is ramified at the dyadic prime ideal of F if and only if $x\equiv 15 \bmod 16$, $y\equiv 0 \bmod 4$ or $x\equiv 13 \bmod 16$, $y\equiv 2 \bmod 4$.

③ Suppose $d\equiv 6 \bmod 8$. Then $F(\sqrt{\varepsilon})/F$ is unramified at the dyadic prime ideal of F if and only if $x\equiv 1 \bmod 16$, $y\equiv 0 \bmod 4$ or $x\equiv 11 \bmod 16$, $y\equiv 2 \bmod 4$. $F(\sqrt{\varepsilon})/F$ is ramified at the dyadic prime ideal of F if and only if $x\equiv 15 \bmod 16$, $y\equiv 0 \bmod 4$ or $x\equiv 5 \bmod 16$, $y\equiv 2 \bmod 4$.

④ Suppose $d\equiv 5 \bmod 8$. If $\eta=\dfrac{x+y\sqrt{d}}{2}>1$, $x\equiv y\equiv 1 \bmod 2$ is the fundamental unit of F, then $F(\sqrt{\eta})/F$ is unramified at the dyadic prime ideal of F if and only if $x\equiv 3 \bmod 4$; $F(\sqrt{\eta})/F$ is ramified at the dyadic prime ideal of F if and only if $x\equiv 1 \bmod 4$.

We use σ to denote the dyadic prime ideal of F (i.e., prime ideal of F lying above 2). Let F_σ be the completion of F at σ and $\mathcal{O}_{F_\sigma}$ the ring of integers of F_σ. Then $F(\sqrt{\varepsilon})/F$ is unramified at σ if $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is an unramified extension. The proof of Theorem 0.1 is given in Section 1.

Before proving our theorem, we give a corollary.

Corollary 0.2 Let $F=\mathbb{Q}(\sqrt{d})$ be a real quadratic field and ε the fundamental integral unit of F. Assume that $N_{F/\mathbb{Q}}(\varepsilon)=1$, then we have

① If $d=p_1\cdots p_r$ with $p_1\equiv\cdots\equiv p_r\equiv 1 \bmod 4$ primes, then $x\equiv 1 \bmod 32$, $y\equiv 0 \bmod 8$ or $x\equiv 9 \bmod 32$, $y\equiv 4 \bmod 8$.

② If $d=2p_1\cdots p_r$ with $p_1\equiv\cdots\equiv p_r\equiv 1 \bmod 4$ primes, then $x\equiv 1 \bmod 16$, $y\equiv 0 \bmod 4$ or $x\equiv 3 \bmod 16$, $y\equiv 2 \bmod 4$.

③ If $d=p_1\cdots p_r\equiv 5 \bmod 8$ with $p_1\equiv\cdots\equiv p_r\equiv 1 \bmod 4$ primes and $\eta=\dfrac{x+y\sqrt{d}}{2}>1$, $x\equiv y\equiv 1 \bmod 2$, is the fundamental unit of F, then $x\equiv 3 \bmod 4$.

④ If $d=p_1p_2\equiv 5 \bmod 8$ with $p_1\equiv p_2\equiv 3 \bmod 4$ primes and $\eta=\dfrac{x+y\sqrt{d}}{2}>1$, $x\equiv y\equiv 1 \bmod 2$, is the fundamental unit of F, then $x\equiv 1 \bmod 4$.

In order to prove this corollary, we need a lemma:

Lemma 0.3[2, Lemma 2.3] Let F be a real quadratic number field with the fundamental unit ε and discriminant d_F. Suppose $N_{F/\mathbb{Q}}(\varepsilon)=1$, then there exists a positive square-free integer m dividing d_F such that $m\varepsilon$ is a square in F.

Proof of Corollary 0.2 According to Theorem 0.1, it suffices to show that $F(\sqrt{\varepsilon})/F$ is unramified at every dyadic prime ideal of F in cases ①, ②, ③ and ramified in case ④. From Lemma 0.3, in cases ①, ②, ③, we have that $F(\sqrt{\varepsilon})=F(\sqrt{m})=\mathbb{Q}(\sqrt{d}, \sqrt{m})$, where $m\mid p_1\cdots p_r$ if $d=p_1\cdots p_r$ and $m\mid 8p_1\cdots p_r$ if $d=2p_1\cdots p_r$. Since $p_1\equiv\cdots\equiv p_r\equiv 1 \bmod 4$, $F(\sqrt{\varepsilon})/F$ is unramified at any dyadic prime ideal of F. In case ④, $m|p_1p_2$, thus $m=p_1$ or p_2 (see also Ref. [3, Lemma 3.2]). Since $p_1\equiv p_2\equiv 3 \bmod 4$, $F(\sqrt{\varepsilon})/F$ is ramified at the dyadic prime ideal of F. This completes the proof.

Remark 0.4 As Ref. [4] proved, Corollary 0.2 can also be proved using the method given in Ref. [5].

For other results of congruences for fundamental units of real quadratic field, the reader is referred to Ref. [6].

1 Proof of the theorem

In order to prove the theorem, we need three lemmas.

Lemma 1.1[3, Lemma 2.3] Suppose $F=\mathbb{Q}_2(\sqrt{2n})$ where n is an odd integer. Then $\pi=\sqrt{2n}$ a uniformizer of F and

(1) $U_F^{(5)}=(U_F^{(3)})^2$ and $U_F^2=U_F^{(5)}\cup(1+\pi^2+\pi^3)U_F^{(5)}$;

(2) $F(\sqrt{1+\pi^2+\pi^3+\pi^4})=F(\sqrt{1+\pi^4})=F(\sqrt{5})$ is unramified over F.

Corollary 1.2 Let n be an odd integer and $F=\mathbb{Q}(\sqrt{2n})$ a quadratic number field. Let σ be the dyadic prime ideal of F and $\alpha\in\mathcal{O}_F\setminus\sigma$ an algebraic integer. Then $F(\sqrt{\alpha})/F$ is unramified at σ if and only if

$$\alpha\equiv 1,5,3+2\sqrt{2n} \text{ or } 7+2\sqrt{2n} \bmod \sigma^5.$$

Moreover, if $\alpha=a+b\sqrt{2n}$ and $2|b$, then if $b\equiv 0 \bmod 4$, $F_\sigma(\sqrt{\alpha})/F_\sigma$ is unramified if and only if $a\equiv 1 \bmod 4$. If $b\equiv 2 \bmod 4$, then $F_\sigma(\sqrt{\alpha})/F_\sigma$ is unramified if and only if $a\equiv 3 \bmod 4$. Thus, if $2|b$, then $F_\sigma(\sqrt{\alpha})/F_\sigma$ is unramified if and only if $a+b\equiv 1 \bmod 4$.

Proof This follows directly from Lemma 1.1. □

Lemma 1.3 Suppose $d\equiv 5 \bmod 8$, then

(1) If $d\equiv 13 \bmod 16$, then in the field $\mathbb{Q}_2(\sqrt{-3})$, $\sqrt{d}\equiv\sqrt{-3} \bmod 8$.

(2) If $d\equiv 5 \bmod 16$, then in the field $\mathbb{Q}_2(\sqrt{-3})$, $\sqrt{d}\equiv\sqrt{-3}+4 \bmod 8$.

Proof The proof is similar to Ref. [7, Lemma 2.5]. □

Lemma 1.4 Let $F=\mathbb{Q}_2(\sqrt{-3})$ and $\omega=\frac{-1+\sqrt{-3}}{2}$. Then $F(\sqrt{1+4\omega})=F(\sqrt{1+4\omega^2})$ is an unramified extension of F.

Proof It is clear that F is unramified over $\mathbb{Q}_2$ and the residue field of F is $\mathbb{F}_4$. Consider the separable polynomial $f(x)=x^2-x-\bar{\omega}$ over $\mathbb{F}_4$. Since $\mathrm{Trace}_{\mathbb{F}_4/\mathbb{F}_2}(\bar{\omega})=\bar{1}\neq 0$, $f(x)$ is irreducible over $\mathbb{F}_4$ (see Ref. [8, Corollary 3.79]). Since $x^2-x-\omega$ is a lifting of $f(x)$, the roots $(1\pm\sqrt{1+4\omega})/2$ of $x^2-x-\omega$ give an unramified extension. □

Now we prove Theorem 0.1.

Proof of Theorem 0.1 ① Let $\varepsilon=x+y\sqrt{d}$ be the fundamental unit of $F=\mathbb{Q}(\sqrt{d})$, then $x^2-dy^2=1$. Since $d\equiv 1 \bmod 4$, we must have that $4|y$. Moreover, if $8|y$, then $x\equiv\pm 1 \bmod 32$; if $y\equiv 4 \bmod 8$, then $x\equiv\pm 9 \bmod 32$. Now we prove that $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is unramified if and only if $x\equiv 1 \bmod 4$; $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is ramified if and only if $x\equiv 3 \bmod 4$. In fact,

$$\varepsilon=x+y\sqrt{d}=x+y+\frac{-1+\sqrt{d}}{2}\cdot 2y\equiv x+y \bmod 8\mathcal{O}_F.$$

Thus, $F_\sigma\cong\mathbb{Q}_2(\sqrt{d})$, $F_\sigma(\sqrt{\varepsilon})\cong\mathbb{Q}_2(\sqrt{d},\sqrt{x+y})$. Since $d\equiv 1 \bmod 4$, $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is unramified if and only if $x+y\equiv 1 \bmod 4$, if and only if $x\equiv 1 \bmod 4$, because $y\equiv 0 \bmod 4$. Similarly, $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is ramified if and only if $x\equiv 3 \bmod 4$. Therefore, $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is unramified if and only if $x\equiv 1 \bmod 32$, $y\equiv 0 \bmod 8$ or $x\equiv 9 \bmod 32$, $y\equiv 4 \bmod 8$. $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is ramified if and only if $x\equiv 31 \bmod 32$, $y\equiv 0 \bmod 8$ or $x\equiv 23 \bmod 32$, $y\equiv 4 \bmod 8$.

② Let $\varepsilon=x+y\sqrt{d}$ be the fundamental unit of $F=\mathbb{Q}(\sqrt{d})$, then $x^2-dy^2=1$. Since $d\equiv 2 \bmod 8$, $y\equiv 0$ or $2 \bmod 4$ according to $x\equiv\pm 1$ or $\pm 3 \bmod 8$. Moreover, if $4|y$, then $32|x^2-1$, thus $x\equiv\pm 1 \bmod 16$; if $y\equiv 2 \bmod 4$, then $x^2-1\equiv 8 \bmod 32$, thus $x\equiv\pm 3 \bmod 16$. Since $2|y$, by Corollary 1.2, $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is unramified if and only if $x+y\equiv 1 \bmod 4$. Therefore, if $y\equiv 0 \bmod 4$, then $x\equiv 1 \bmod 16$; if $y\equiv 2 \bmod 4$, then $x\equiv 3 \bmod 16$. Similarly, $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is ramified if and only if $x+y\equiv$

3 mod 4. Therefore, if $y\equiv 0$ mod 4, then $x\equiv$ 15 mod 16; if $y\equiv 2$ mod 4, then $x\equiv 13$ mod 16.

③ The proof of ③ is similar to that of ②.

④ Let $\eta=\frac{x+y\sqrt{d}}{2}$ be the fundamental unit of F with x, y odd integers. We see that $F_\sigma\cong\mathbb{Q}_2(\sqrt{-3})$ and every element $\alpha\in\mathcal{O}_{F_\sigma}$ can be written uniquely as $\alpha=a_0+a_1 2+a_2 2^2+a_3 2^3+\cdots$, $a_i\in\{0,1,\omega,\omega^2\}$, where $\omega=\frac{-1+\sqrt{-3}}{2}$.

We first show that in the local field F_σ,

$$\eta\equiv\omega(-x) \text{ or } \omega^2(-x) \bmod 4\mathcal{O}_{F_\sigma}.$$

Suppose first that $d\equiv 13$ mod 16, then by Lemma 1.3, $\sqrt{d}-\sqrt{-3}\equiv 0$ mod 8. Hence

$$\eta-wy=\frac{x+\sqrt{d}y}{2}-\frac{-1+\sqrt{-3}}{2}\cdot y=$$
$$\frac{x+y}{2}+\frac{\sqrt{d}-\sqrt{-3}}{2}y\equiv\frac{x+y}{2} \bmod 4.$$

Since $x^2-dy^2=4$ and $d\equiv 13$ mod 16, $x^2\equiv 13y^2+4\equiv y^2+(12y^2+4)\equiv y^2$ mod 16. If $x\equiv -y$ mod 8, then $\frac{x+y}{2}\equiv 0$ mod 4 and $\eta\equiv wy\equiv w(-x)$ mod 4; if $x\equiv y$ mod 8, then $\frac{x+y}{2}\equiv y$ mod 4 and $\eta\equiv(1+w)y=w^2(-y)\equiv w^2(-x)$ mod 4.

Suppose that $d\equiv 5$ mod 16. Then by Lemma 1.3, $\sqrt{d}-\sqrt{-3}\equiv 4$ mod 8. Hence

$$\eta-wy=\frac{x+y}{2}+\frac{\sqrt{d}-\sqrt{-3}}{2}\cdot y\equiv$$
$$\frac{x+y}{2}+2y\equiv\frac{x+y}{2}+2 \bmod 4,$$

because y is odd. Since $x^2-dy^2=4$ and $d\equiv$ 5 mod 16, $x^2\equiv 5y^2+4=y^2+4(y^2+1)\equiv y^2+$ 8 mod 16. If $x\equiv -y+4$ mod 8, then $\frac{x+y}{2}\equiv 2$ mod 4 and $\eta\equiv wy\equiv w(-x)$ mod 4; if $x\equiv y+4$ mod 8, then $\frac{x+y}{2}\equiv y+2$ mod 4 and $\eta\equiv(1+w)y=w^2(-y)\equiv w^2(-x)$ mod 4.

Since $\eta\equiv\omega^i(-x)$ mod $4\mathcal{O}_{F_\sigma}$, $i=1,2$, $\frac{\eta}{\omega^i}\equiv -x$ mod $4\mathcal{O}_{F_\sigma}$. Thus we have

$$\frac{\eta}{\omega^i}\equiv\begin{cases}1 \text{ or } 5 \text{ or } 1+4\omega \text{ or } 1+4\omega^2 \bmod 8\mathcal{O}_{F_\sigma}, \\ \quad \text{if } x\equiv 3 \bmod 4; \\ 3 \bmod 4\mathcal{O}_{F_\sigma}, \text{ if } x\equiv 1 \bmod 4.\end{cases}$$

By Lemma 1.4, we see that $F_\sigma(\sqrt{1+4\omega})=F_\sigma(\sqrt{1+4\omega^2})$ is the unique unramified extension of F_σ of degree two. Thus if $x\equiv 3$ mod 4, $F_\sigma(\sqrt{\eta})=F_\sigma(\sqrt{\eta/\omega^i})=F_\sigma$ or $F_\sigma(\sqrt{1+4\omega})$, which is unramified over F_σ. If $x\equiv 1$ mod 4, let $\eta/\omega^i=3+4\delta$, $\delta\in\mathcal{O}_{F_\sigma}$. Consider the polynomial $f(x)=x^2-(3+4\delta)$, it is evident that $f(x+1)=x^2+2x-(2+4\delta)$ is an Eisenstein polynomial. Thus $F_\sigma(\sqrt{\eta})=F_\sigma(\sqrt{\eta/\omega^i})$ is a totally ramified extension of F_σ. Thus, $F(\sqrt{\eta})/F$ is unramified at σ if and only if $x\equiv 3$ mod 4, $F(\sqrt{\eta})/F$ is ramified at σ if and only if $x\equiv 1$ mod 4. □

Remark 1.5 For $d\equiv 3$ mod 4 a square-free positive integer, we can also prove that $F_\sigma(\sqrt{\varepsilon})/F_\sigma$ is ramified if and only if $y\equiv 0$ mod 4, where ε is the fundamental unit of $F=\mathbb{Q}(\sqrt{d})$.

Acknowledgement The authors would like to thank Prof. Ouyang Yi and Prof. Yue Qin for their helpful comments.

References

[1] Brandler J A. Residuacity properties of real quadratic units[J]. J Number Theory, 1973, 5: 271-286.

[2] Mouhib A. On the parity of the class number of multiquadratic number fields[J]. Journal of Number Theory, 2009, 129: 1 205-1 211.

[3] Zhang Z, Yue Q. Fundamental units of real quadratic fields of odd class number[J]. Journal of Number Theory, 2014, 137: 122-129.

[4] Williams K S. Historical remark on a theorem of Zhang and Yue[J]. Journal of Number Theory, 2015, 147: 691-693.

[5] Dirichlet P G L. Einige neue Sätze über unbestimmte Gleichungen, Abh Königlich Preussischen Akad Wiss, 1834: 649-664; Werke[M]. New York: Chelsea Pub Co, 1969: 219-236.

[6] Shanks D, Sime P, Washington L. Zeros of 2-adic L-functions and congruences for class numbers and fundamental units[J]. Math Comp, 1999, 68: 1 243-1 255.

[7] Bae S, Yue Q. Hilbert genus fields of real biquadratic fields[J]. Ramanujan J, 2011, 24: 161-181.

[8] Lidl R, Niederreiter H. Finite Fields[M]. Cambridge: Cambridge University Press, 1997.