# Note on distribution of units of real quadratic number fields

By Norisato KATAOKA

Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya, 464-8602

(Communicated by Heisuke HIRONAKA, M. J. A., Dec. 12, 2001)

**Abstract:** Let $k$ be a real quadratic number field and $\mathfrak{o}_k$, $E$ the ring of integers and the group of units in $k$. Denote by $E_\mathfrak{p}$ a subgroup represented by $E$ of $(\mathfrak{o}_k/\mathfrak{p})^\times$ for a prime ideal $\mathfrak{p}$ in $k$. We report that for a given positive integer $a$, the set of prime ideals of degree 1 for which the residual index of $E_\mathfrak{p}$ is equal to $a$ has a density under the Generalized Riemann Hypothesis.

**Key words:** Number theory; quadratic field; density.

**1. Introduction.** Let $k$ be an algebraic number field and $\mathfrak{o}_k$, $E$ the ring of integers and the group of units in $k$, respectively. For an integral ideal $\mathfrak{m}$ of $k$ we denote by $E_\mathfrak{m}$ a subgroup of the residue class group $(\mathfrak{o}_k/\mathfrak{m})^\times$ consisting of classes represented by elements of $E$. By the class field theory the extension degree of the ray class field over $k$ with respect to $\mathfrak{m}$ is a product of the absolute class number of $k$ and the index $((\mathfrak{o}_k/\mathfrak{m})^\times : E_\mathfrak{m})$. The former is well studied, but $((\mathfrak{o}_k/\mathfrak{m})^\times : E_\mathfrak{m})$ is not well known. We consider a real quadratic number field as $k$. If $\mathfrak{m}$ is a prime ideal $\mathfrak{p}$ of $k$, then $I_p := ((\mathfrak{o}_k/\mathfrak{p})^\times : E_\mathfrak{p})$ depends only on the prime number $p$ lying below $\mathfrak{p}$. Set $\ell_p = 1$, $p-1$, $(p-1)/2$ if $p$ decomposes, inerts with $N_{k/\mathbf{Q}}(\varepsilon) = 1$, or inerts with $N_{k/\mathbf{Q}}(\varepsilon) = -1$ in $k$, respectively, where $N_{k/\mathbf{Q}}$ stands for the norm from $k$ to the rational number field $\mathbf{Q}$ and $\varepsilon$ $(> 1)$ stands for a fundamental unit of $k$. Then it has been shown that $\ell_p$ divides $I_p$ for any $p$ in [3]. Moreover in [1, 5–7] it is shown that the set of prime numbers satisfies $I_p = \ell_p$ has a natural density under the Generalized Riemann Hypothesis (GRH). These problems concern the Artin conjecture on the primitive roots. In [2] Hooley proved this problem under the GRH. Later in [5] Lenstra Jr. has considered the generalized Artin conjecture. In this paper, we report that for a given positive integer $a$, the set of rational primes $p$ decomposed in $k$ for which satisfies $I_p = a$ has a natural density under the GRH, which is also the generality of [6]. The proof will be published elsewhere. Hereafter we denote the discriminant of $k$ by $D$. The letter $q$ denotes a prime number, and $p$ is an odd prime number. We put

$$\mathbf{P}(x) = \{p \le x;\ p \text{ is decomposable in } k\}$$

and a rational integer $e = \nu_q(t)$ is defined by $q^e \parallel t$ for $t \in \mathbf{Q}^\times$. For a given positive integer $a$, we denote by $N_a(x)$ the number of $p \in \mathbf{P}(x)$ satisfies $I_p = a$. We apply the Chebotarev Density Theorem (CDT) by [4, 8] to estimate $N_a(x)$ under the GRH.

**Proposition** (CDT [4, 8])**.** *Let $L/F$ be a Galois extension of algebraic number fields, and $C$ a conjugacy class of* $\mathrm{Gal}(L/F)$*. For a prime ideal $\mathfrak{p}$ of $F$, we denote by $[(L/F)/\mathfrak{p}]$ a conjugacy class which includes the Frobenius automorphism with respect to a prime ideal of $L$ dividing $\mathfrak{p}$, and $\pi_C(x, L/F)$ the number of unramified prime ideals $\mathfrak{p}$ of $F$ which satisfy $C = [(L/F)/\mathfrak{p}]$ and $N_{F/\mathbf{Q}}\mathfrak{p} \le x$. Suppose that the GRH holds for $L$.*

$$\left|\pi_C(x, L/F) - \frac{\sharp C}{[L:F]} Li(x)\right| < c'\left(\frac{\sharp C}{[L:F]}\sqrt{x}\log(d(L)x^{[L:\mathbf{Q}]})\right)$$

*where $c'$ is a positive absolute constant. Here we denote the absolute discriminant of $L$ by $d(L)$, and the function $Li(x)$ denotes $\int_2^x (\log t)^{-1}dt$ as usual.*

We put $K_n := k(\zeta_{2an}, \sqrt[an]{\varepsilon})$ for a natural number $n$ where $\zeta_m$ stands for a primitive $m$-th root of unity. Applying CDT to $K_n/\mathbf{Q}$, $C = \{\mathrm{id}_{K_n}\}$, we get the following main result.

**Theorem 1.** *In the above notation we assume GRH in $K_n$ for square free positive integers $n$. Then we have*

$$N_a(x) = c \cdot Li(x) + O\left(\frac{x\log\log x}{\log^2 x}\right)$$

$$\text{where } c = \sum_{n\ge 1}\frac{\mu(n)}{[K_n:\mathbf{Q}]},$$

2000 Mathematics Subject Classification. 11R45.

*and the infinite series $c$ is absolutely convergent. Here $\mu(n)$ denotes the Möbius function.*

**Remark 1.** We note that $c$ is not necessarily positive. We state the explicit formula and the positivity of $c$ in next section.

**2. The formulation and the positivity of $c$.** We set $N := 2aD$. For a square free positive integer $n$, we write $n = lm$ with $(m, lN) = 1$, $l|N$. We have the following lemma.

**Lemma.** *In the above notation we put $K_{m,1} := k(\zeta_m, \sqrt[m]{\varepsilon})$. Then we have $[K_n : k] = [K_l : k] \cdot [K_{m,1} : k]$ and $[K_{m,1} : k] = m\varphi(m)$ where $\varphi(m)$ denotes the Euler function.*

By this lemma, we have

$$(1)\quad c = \frac{1}{[k:\mathbf{Q}]} \cdot \sum_{l|N} \frac{\mu(l)}{[K_l : k]} \cdot \sum_{(m,N)=1} \frac{\mu(m)}{[K_{m,1} : k]}$$
$$= A \cdot \prod_{q|N} \frac{q(q-1)}{q^2-q-1} \cdot \sum_{l|N} \frac{\mu(l)}{[K_l : \mathbf{Q}]},$$

where $A$ is the Artin constant $\prod_q \{1 - 1/(q(q-1))\}$. Now we denote by $c_0$ the finite sum $\sum_{l|N} \mu(l)/([K_l : \mathbf{Q}])$. We give a sum $c_0$ more explicitly. For a positive integer $t$ we put

$$\lambda(t) = \begin{cases} 1 & (\text{if } q \mid t \text{ for any divisor } q \text{ of } N) \\ \displaystyle\prod_{\substack{q|N \\ q\nmid t}} q & (\text{otherwise}) \end{cases}$$

$$E(t) = \begin{cases} 1 & (\text{if } \lambda(t) = 1) \\ \displaystyle\prod_{q|\lambda(t)} \frac{q^2-q-1}{q(q-1)} & (\text{if } \lambda(t) \neq 1) \end{cases}$$

$$v(t) = \begin{cases} 1 & (\text{if } t = 1) \\ \displaystyle\frac{1}{t^2} \prod_{q|t} \frac{q+1}{q} & (\text{if } t \neq 1). \end{cases}$$

If $N_{k/\mathbf{Q}}(\varepsilon) = 1$, then putting $\varepsilon = (t + u\sqrt{D})/2$ where $t$, $u$ are rational integers with $t > 0$, we have $k(\sqrt{\varepsilon}) = \mathbf{Q}(\sqrt{t+2}, \sqrt{t-2})$. Then we put $k_0 = k$, $k_1 = \mathbf{Q}(\sqrt{t+2})$, $k_2 = \mathbf{Q}(\sqrt{t-2})$, and denote their discriminants by $D = D_0$, $D_1$, $D_2$. Moreover we put

$$D_i^* := \frac{D_i}{2^{\nu_2(D_i)} \cdot (a_0, D_i)} \quad (1 \le i \le 3)$$

where $a_0 := a/2^{\nu_2(a)}$ and $(a, b)$ is the greatest common divisor for rational integers $a$, $b$. Then note that $(2a_0, D_i^*) = 1$ and $D_i^*$'s are square free odd positive integers. We set for $i = 0, 1, 2$

$$R_a(D_i) := \begin{cases} 0 & (\text{if } D_i^* \nmid D_0^*) \\ \dfrac{\mu(D_i^*)}{D_i^* \varphi(D_i^*)} \cdot v(a_0) \cdot E(2a_0 D_i^*) & \\ & (\text{if } D_i^* \mid D_0^*) \end{cases}$$

$$r_i(a) = \begin{cases} 0 & (\text{if } 8 \| D_i, 2 \nmid a) \\ -\dfrac{1}{2^{2\nu_2(a)+3}} & \begin{pmatrix} \text{if } 2 \nmid D_i, 2 \nmid a, \\ i = 1, 2, \\ \text{if } 4 \| D_i, 2 \nmid a, \text{ or} \\ \text{if } 8 \| D_i, 2 \| a \end{pmatrix} \\ \dfrac{3}{2^{2\nu_2(a)+3}} & (\text{otherwise}). \end{cases}$$

Now we have

$$c_0 = \begin{cases} v(2a) \cdot E(2a) + r_0(a) \cdot R_a(D_0) & \\ & (\text{if } N_{k/\mathbf{Q}}(\varepsilon) = -1) \\ v(2a) \cdot E(2a) + \displaystyle\sum_{i=0}^{2} r_i(a) \cdot R_a(D_i) & \\ & (\text{if } N_{k/\mathbf{Q}}(\varepsilon) = 1). \end{cases}$$

**Examples.** Suppose that $k_0 = \mathbf{Q}(\sqrt{39})$ and $a = 39$, or $k_0 = \mathbf{Q}(\sqrt{55})$ and $a = 55$. These are examples satisfying $c = 0$.

**Remark 2.** We can also see that if either $N_{k/\mathbf{Q}}(\varepsilon) = -1$ or both $N_{k/\mathbf{Q}}(\varepsilon) = 1$ and $D_0^* \neq 1$ (which is satisfied if $a = 1$), then a constant $c$ is positive.

Next we consider an algebraic necessary and sufficient condition to be $c > 0$. The following holds.

**Theorem 2.** *For the constant $c$ in Theorem 1, $c > 0$ holds if and only if there exists $\rho \in \mathrm{Gal}(K_N/\mathbf{Q})$ satisfying that $\rho|_{K_1} = \mathrm{id}_{K_1}$ and $\rho|_{K_q} \neq \mathrm{id}_{K_q}$ for any prime $q$ divides $N$.*

**Remark 3.** In [5] Lenstra Jr. has considered the following generalized Artin conjecture: Let $F$ be a finite Galois extension over a global field $K$, and let $C$ be a subset of $G = \mathrm{Gal}(F/K)$ which is a union of conjugacy classes, and let $W$ be a finitely generated subgroup of $K^\times$ which has rank $r \ge 1$ modulo the torsion subgroup, and let $a$ be a positive integer. Then he considered the set $M(K, F, C, W, a)$ of prime ideals of $K$ which satisfy the following:

(i) $(\mathfrak{p}, F/K) \subset C$ where $(\mathfrak{p}, F/K)$ denotes the Frobenius symbol
(ii) $\mathrm{ord}_\mathfrak{p}(w) = 0$ for all $w \in W$ where $\mathrm{ord}_\mathfrak{p}$ denotes the normalized valuation
(iii) if $\psi : W \to \bar{K}_\mathfrak{p}^\times$ where $\bar{K}_\mathfrak{p}$ is the residue class field at $\mathfrak{p}$ is the natural map, then the index of $\psi(W)$ in $\bar{K}_\mathfrak{p}^\times$ divides $a$.

He has proved that $M$ has a density under GRH, and also has given a necessary and sufficient condition to

be non-zero for this density. Our density formula (1) follows from his fomula in principal, by using the Möbius inversion formula. But even in our case, his formula is not explisit and the condition for the positiveness of the density is another problem.

## References

[ 1 ] Chen, Y.-M., Kitaoka, Y., and Yu, J.: Distribution of units of real quadratic number fields. Nagoya Math. J., **158**, 167–184 (2000).

[ 2 ] Hooley, C.: On Artin's conjecture. J. Reine Angew. Math., **225**, 209–220 (1967).

[ 3 ] Ishikawa, M., and Kitaoka, Y.: On the distribution of units modulo prime ideals in real quadratic fields. J. Reine Angew. Math., **494**, 65–72 (1998).

[ 4 ] Lagarias, J. C., and Odlyzko, A. M.: Effective version of the Chebotarev density theorem. Algebraic Number Fields (ed. Frölich, A.). Academic Press, London-New York, pp. 409–464 (1977).

[ 5 ] Lenstra Jr., H. W.: On Artin's conjecture and Euclid' algorithm in global fields. Invent. Math., **42**, 201–224 (1977).

[ 6 ] Mashima, K.: On the distribution of units modulo prime ideal and Artin conjecture. RIMS Kokyuroku, no. 1026, pp. 156–166 (1998) (in Japanese).

[ 7 ] Roskam, H.: A quadratic analogue of Artin conjecture on primitive root. J. Number Theory, **81**, 93–109 (2000).

[ 8 ] Serre, J. P.: Quelques applications du théorème de densité de Chebotarev. I.H.E.S., **54**, 323–401 (1981).