

## DISTRIBUTION OF UNITS OF REAL QUADRATIC NUMBER FIELDS

YEN-MEI J. CHEN, YOSHIYUKI KITAOKA AND JING YU<sup>1</sup>

*Dedicated to the seventieth birthday of Professor Tomio Kubota*

**Abstract.** Let  $k$  be a real quadratic field and  $\mathfrak{o}_k$ ,  $E$  the ring of integers and the group of units in  $k$ . Denoting by  $E(\mathfrak{p})$  the subgroup represented by  $E$  of  $(\mathfrak{o}_k/\mathfrak{p})^\times$  for a prime ideal  $\mathfrak{p}$ , we show that prime ideals  $\mathfrak{p}$  for which the order of  $E(\mathfrak{p})$  is theoretically maximal have a positive density under the Generalized Riemann Hypothesis.

### §1. Statement of the result

Let  $k$  be a real quadratic number field with discriminant  $D_0$  and fundamental unit  $\epsilon (> 1)$ , and let  $\mathfrak{o}_k$  and  $E$  be the ring of integers in  $k$  and the set of units in  $k$ , respectively. For a prime ideal  $\mathfrak{p}$  of  $k$  we denote by  $E(\mathfrak{p})$  the subgroup of the unit group  $(\mathfrak{o}_k/\mathfrak{p})^\times$  of the residue class group modulo  $\mathfrak{p}$  consisting of classes represented by elements of  $E$  and set  $I_p := [(\mathfrak{o}_k/\mathfrak{p})^\times : E(\mathfrak{p})]$ , where  $p$  is the rational prime lying below  $\mathfrak{p}$ . It is obvious that  $I_p$  is independent of the choice of prime ideals lying above  $p$ . Set

$$\ell_p := \begin{cases} 1, & \text{if } p \text{ is decomposable or ramified in } k, \\ p - 1, & \text{if } p \text{ remains prime in } k \text{ and } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ (p - 1)/2, & \text{if } p \text{ remains prime in } k \text{ and } N_{k/\mathbf{Q}}(\epsilon) = -1, \end{cases}$$

where  $N_{k/\mathbf{Q}}$  stands for the norm from  $k$  to the rational number field  $\mathbf{Q}$ . In [IK] we have shown that  $\ell_p$  divides  $I_p$  and we observed that in each case the set of prime numbers satisfying  $I_p = \ell_p$  has a natural density. K. Masima found that the values in tables there, are connected with the Artin constant  $A := \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558 \dots$  and showed in [M] that the set of decomposable prime numbers satisfying  $I_p = \ell_p$  has a density under the

---

Received October 7, 1999.

1991 *Mathematics Subject Classification*: 11R45

<sup>1</sup>Research partially supported by National Science Council, Rep. of China.

Generalized Riemann Hypothesis (GRH) following [H]. In this paper, we treat the case where prime numbers remain prime in  $k$  following [H], [M]. However, instead of counting prime ideals which are completely decomposable, we use the Chebotarev Density Theorem by [LO], [S] under the GRH. Our main result is the following.

**THEOREM.** *Let  $\mathbb{P}(x)$  be the set of odd prime numbers  $p \leq x$  which remain prime in  $k$  and let  $N(x)$  be the subset of  $p \in \mathbb{P}(x)$  satisfying  $I_p = \ell_p$ . Then we have*

$$\#N(x) = c_0 \text{Li}(x) + O(x \log \log x / (\log x)^2)$$

for a positive constant  $c_0$  under the GRH.

Here fields where the GRH is involved are  $k(\zeta_{2n}, \sqrt[t]{\epsilon})$  for square-free natural numbers  $n$  and  $t = n$  or  $2n$ , where  $\zeta_m$  stands for a primitive  $m$ -th root of unity. The function  $\text{Li}(x)$  stands for  $\int_2^x dt / \log t$  as usual.

**§2. Algebraic preparation**

Throughout this paper, we keep the notation in Section 1. The main results in this section are Theorems 1 and 2.

**LEMMA 1.** *Let  $n$  be a square-free integer ( $\geq 1$ ) and suppose that  $k \not\subset \mathbf{Q}(\zeta_{2n})$  and suppose  $\sqrt[2n]{\epsilon} \in \mathbf{R}$ . Set*

$$K := \begin{cases} k(\zeta_{2n}, \sqrt[2n]{\epsilon}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ k(\zeta_{2n}, \sqrt[n]{\epsilon}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1, \end{cases}$$

and let  $N := [K : k(\zeta_{2n})]$  be the extension degree of fields. Then we have

$$\begin{aligned} N &= [K : \mathbf{Q}] / 2\varphi(2n) \\ &= \begin{cases} n, & \text{either if } N_{k/\mathbf{Q}}(\epsilon) = 1 \text{ and } \sqrt{\epsilon} \in k(\zeta_{2n}), \\ & \text{or if } N_{k/\mathbf{Q}}(\epsilon) = -1 \text{ and } 2 \nmid n, \\ 2n, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1 \text{ and } \sqrt{\epsilon} \notin k(\zeta_{2n}), \end{cases} \end{aligned}$$

where  $\varphi(m)$  is the Euler function.

*Proof.* Let us recall that

for an integer  $m$ , and an element  $a$  in a field  $F$  ( $\text{ch}(F) \neq 2$ ) which is not contained in  $F^p$  for every prime divisor  $p$  of  $m$ , a polynomial  $x^m - a$  is irreducible either if  $4 \nmid m$ , or if  $4 \mid m$  and  $-4a \notin F^4$ .

Let  $q$  be an odd prime or 4 and suppose  $q|2n$ . We show  $\sqrt[q]{\epsilon} \notin k(\zeta_{2n})$  first. Suppose  $\sqrt[q]{\epsilon} \in k(\zeta_{2n})$ ; then  $\mathbf{Q}(\sqrt[q]{\epsilon}) = \mathbf{Q}((\sqrt[q]{\epsilon})^{2n/q}) \subset \mathbf{R}$  is a subfield of an abelian field  $k(\zeta_{2n})$ . Hence any conjugate element of  $\sqrt[q]{\epsilon}$  should be real. This is a contradiction. Hence  $\sqrt[q]{\epsilon}$  is not in  $k(\zeta_{2n})$ .

Let us show that  $x^{2n} - \epsilon$  is irreducible over  $k(\zeta_{2n})$  if  $\sqrt{\epsilon} \notin k(\zeta_{2n})$ . We have only to consider the case of  $2|n$ . Suppose that  $2|n$ ,  $\sqrt[4]{-4\epsilon} \in k(\zeta_{2n})$  and  $\sqrt{\epsilon} \notin k(\zeta_{2n})$ ; then  $\sqrt{-4\epsilon} \in k(\zeta_{2n})$  and  $\sqrt{-1}\sqrt{\epsilon} \in k(\zeta_{2n})$  hold. This contradicts that  $\sqrt{\epsilon} \notin k(\zeta_{2n})$  since  $\sqrt{-1} \in k(\zeta_{2n})$  holds by  $2|n$ . Thus the above criterion yields that a polynomial  $x^{2n} - \epsilon$  is irreducible over  $k(\zeta_{2n})$  if  $\sqrt{\epsilon} \notin k(\zeta_{2n})$ . Then we have  $N = [k(\zeta_{2n}, \sqrt[2n]{\epsilon}) : k(\zeta_{2n})] = 2n$ . If, next  $\sqrt{\epsilon} \in k(\zeta_{2n})$ , then a polynomial  $x^n - \sqrt{\epsilon}$  is irreducible over  $k(\zeta_{2n})$  and then we have  $N = [k(\zeta_{2n}, (\sqrt{\epsilon})^{1/n}) : k(\zeta_{2n})] = n$ . Similarly,  $x^n - \epsilon$  is irreducible over  $k(\zeta_{2n})$  if  $N_{k/\mathbf{Q}}(\epsilon) = -1$  and  $2 \nmid n$ . □

*Remark.* In Lemma 1, a rational prime  $p$  is unramified in  $K$  if  $p \nmid 2nD_0$ .

**PROPOSITION 1.** *Let  $n, K, N$  be those in Lemma 1. Let  $\eta \in \text{Gal}(k(\zeta_{2n})/\mathbf{Q})$  be an automorphism such that  $\eta(\zeta_{2n}) = \zeta_{2n}^{-1}$  and  $\eta$  induces the non-trivial automorphism of  $\text{Gal}(k/\mathbf{Q})$ .*

(I) *The case of  $N_{k/\mathbf{Q}}(\epsilon) = 1$ . There exists an automorphism  $\rho$  of order 2 in  $\text{Gal}(K/\mathbf{Q})$  such that  $\rho = \eta$  on  $k(\zeta_{2n})$  if and only if (i)  $N = 2n$ , (ii)  $N = n$  is odd, or (iii)  $N = n$  is even and  $\eta(\sqrt{\epsilon})\sqrt{\epsilon} = 1$ . When  $\rho$  exists, it is in the center of  $\text{Gal}(K/\mathbf{Q})$  and satisfies  $\rho(\sqrt[2n]{\epsilon}) = \pm \sqrt[2n]{\epsilon}^{-1}$  and both signs  $\pm$  are possible if and only if  $N$  is even.*

(II) *The case of  $N_{k/\mathbf{Q}}(\epsilon) = -1$ . If  $n$  is odd, then there exists a unique automorphism  $\rho$  of order 2 in  $\text{Gal}(K/\mathbf{Q})$  such that  $\rho = \eta$  on  $k(\zeta_{2n})$ . It is in the center of  $\text{Gal}(K/\mathbf{Q})$  and  $\rho(\sqrt[n]{\epsilon}) = -\sqrt[n]{\epsilon}^{-1}$ . If  $n$  is even, then there is no such automorphism.*

*Proof.* Set  $t = 2n$  or  $n$  according to  $N_{k/\mathbf{Q}}(\epsilon) = 1$  or  $-1$ , respectively. If  $\rho \in \text{Gal}(K/\mathbf{Q})$  is an extension of  $\eta$  and  $\rho^2 = \text{id.}$ , then setting  $\rho(\sqrt[t]{\epsilon}) = \delta \sqrt[t]{\epsilon}^{-1}$  for some  $\delta \in K$ , we have  $\delta^{2n} = 1$  and hence  $\delta$  is a  $2n$ -th root of unity and hence  $\rho(\delta) = \eta(\delta) = \delta^{-1}$  and  $\sqrt[t]{\epsilon} = \rho^2(\sqrt[t]{\epsilon}) = \rho(\delta \sqrt[t]{\epsilon}^{-1}) = \delta^{-1}(\delta \sqrt[t]{\epsilon}^{-1})^{-1} = \delta^{-2} \sqrt[t]{\epsilon}$ . Thus we have  $\delta = \pm 1$ .

Proof of the case (I).

Suppose  $N_{k/\mathbf{Q}}(\epsilon) = 1$ . Assume that either  $N = 2n$ , or  $N = n$  is odd, first. We define  $\xi_n = \pm 1$  by

$$\xi_n := \begin{cases} 1, & \text{if } N = 2n, \\ \eta(\sqrt{\epsilon})\sqrt{\epsilon}, & \text{if } N = n, \end{cases}$$

where if  $N = n$ ,  $\sqrt[n]{\epsilon} \in k(\zeta_{2n})$  holds by virtue of Lemma 1, and  $\eta$  can act on  $\sqrt[n]{\epsilon}$ .

Let  $\eta' \in \text{Gal}(K/\mathbf{Q})$  be an extension of  $\eta \in \text{Gal}(k(\zeta_{2n})/\mathbf{Q})$ ; then we have

$$(\eta'({}^{2n}\sqrt{\epsilon}) {}^{2n}\sqrt{\epsilon} \xi_n)^N = \eta(\epsilon)\epsilon = 1$$

and hence  $\eta'({}^{2n}\sqrt{\epsilon}) = \zeta_N^r \xi_n {}^{2n}\sqrt{\epsilon}^{-1}$  for some integer  $r$  and a primitive  $N$ -th root  $\zeta_N$  of unity. Since  $K = k(\zeta_{2n})({}^{2n}\sqrt{\epsilon})$  and  $N = [K : k(\zeta_{2n})]$ , there exists an automorphism  $\alpha \in \text{Gal}(K/k(\zeta_{2n}))$  such that  $\alpha({}^{2n}\sqrt{\epsilon}) = \zeta_N^r {}^{2n}\sqrt{\epsilon}$ . Thus an automorphism  $\rho := \alpha\eta'$  is an extension of  $\eta$  and satisfies  $\rho({}^{2n}\sqrt{\epsilon}) = \xi_n {}^{2n}\sqrt{\epsilon}^{-1}$  and the order of  $\rho$  is equal to 2.

Secondly, we consider the case where  $N = n$  is even. By Lemma 1, we have  $\sqrt[n]{\epsilon} \in k(\zeta_{2n})$ . Take any extension  $\eta'$  in  $\text{Gal}(K/\mathbf{Q})$  of  $\eta$ . Since  $(\eta'({}^{2n}\sqrt{\epsilon}) {}^{2n}\sqrt{\epsilon})^{2n} = \eta(\epsilon)\epsilon = 1$ , we have  $\eta'((\sqrt[n]{\epsilon})^{1/n}) = \zeta_{2n}^t (\sqrt[n]{\epsilon})^{-1/n}$  for some integer  $t$ , and

$$\eta(\sqrt[n]{\epsilon}) = \zeta_{2n}^{tn} \sqrt[n]{\epsilon}^{-1}.$$

If, hence  $\eta(\sqrt[n]{\epsilon})\sqrt[n]{\epsilon} = 1$ , then  $t$  is even and since  $[K : k(\zeta_{2n})] = n$  and  $\sqrt[n]{\epsilon} \in k(\zeta_{2n})$ , we can take  $\alpha \in \text{Gal}(K/k(\zeta_{2n}))$  so that  $\alpha({}^{2n}\sqrt{\epsilon}) = \zeta_{2n}^t {}^{2n}\sqrt{\epsilon}$ , and therefore  $\rho := \alpha\eta'$  is what we want. If  $\eta(\sqrt[n]{\epsilon})\sqrt[n]{\epsilon} = -1$ , then  $t$  is odd and the order of  $\eta'$  is not equal 2, since  $\eta'^2({}^{2n}\sqrt{\epsilon}) = \zeta_n^{-t} {}^{2n}\sqrt{\epsilon} \neq {}^{2n}\sqrt{\epsilon}$ . Thus we have completed the proof of the first assertion. Next, we show that if  $\rho_{\pm} \in \text{Gal}(K/\mathbf{Q})$  is an extension of  $\eta$  such that  $\rho_{\pm}({}^{2n}\sqrt{\epsilon}) = \pm {}^{2n}\sqrt{\epsilon}^{-1}$ , then  $\rho_{\pm}$  is in the center of  $\text{Gal}(K/\mathbf{Q})$ . Take an element  $u \in \text{Gal}(K/\mathbf{Q})$ ; then  $u({}^{2n}\sqrt{\epsilon}) = \zeta_{2n}^r {}^{2n}\sqrt{\epsilon}$  or  $\zeta_{2n}^r {}^{2n}\sqrt{\epsilon}^{-1}$  for some integer  $r$ . If  $u({}^{2n}\sqrt{\epsilon}) = \zeta_{2n}^r {}^{2n}\sqrt{\epsilon}$ , then  $\rho_{\pm}u({}^{2n}\sqrt{\epsilon}) = \pm \zeta_{2n}^{-r} {}^{2n}\sqrt{\epsilon}^{-1}$  and  $u\rho_{\pm}({}^{2n}\sqrt{\epsilon}) = u(\pm {}^{2n}\sqrt{\epsilon}^{-1}) = \pm \zeta_{2n}^{-r} {}^{2n}\sqrt{\epsilon}^{-1}$  and hence  $\rho_{\pm}u = u\rho_{\pm}$ . The case of  $u({}^{2n}\sqrt{\epsilon}) = \zeta_{2n}^r {}^{2n}\sqrt{\epsilon}^{-1}$  is similar and then  $\rho_{\pm}$  is in the center of  $\text{Gal}(K/\mathbf{Q})$ . Lastly, suppose that  $N$  is even; then there is an automorphism  $\kappa \in \text{Gal}(K/k(\zeta_{2n}))$  such that  $\kappa({}^{2n}\sqrt{\epsilon}) = -{}^{2n}\sqrt{\epsilon}$  and hence both signs  $\pm$  are possible. Conversely, if there exist automorphisms  $\rho_{\pm} \in \text{Gal}(K/\mathbf{Q})$  such that  $\rho_{\pm} = \eta$  on  $k(\zeta_{2n})$  and  $\rho_{\pm}({}^{2n}\sqrt{\epsilon}) = \pm {}^{2n}\sqrt{\epsilon}^{-1}$ , then  $\rho_{-}\rho_{+}$  is the identity on  $k(\zeta_{2n})$  and  $\rho_{-}\rho_{+}({}^{2n}\sqrt{\epsilon}) = -{}^{2n}\sqrt{\epsilon}$  and hence the order of  $\rho_{-}\rho_{+} \in \text{Gal}(K/k(\zeta_{2n}))$  is two and it yields that  $N = [K : k(\zeta_{2n})]$  is even. Thus we have completed the proof of the case (I).

Proof of the case (II).

Suppose  $N_{k/\mathbf{Q}}(\epsilon) = -1$ . First we consider the case where  $n$  is odd; Since  $\eta(\epsilon) = -\epsilon^{-1}$ , taking an extension  $\eta' \in \text{Gal}(K/\mathbf{Q})$  of  $\eta \in \text{Gal}(k(\zeta_{2n})/\mathbf{Q})$ , we have  $\eta'(\sqrt[n]{\epsilon}) = -\zeta_n^r \sqrt[n]{\epsilon}^{-1}$  for some integer  $r$ . There exists an automorphism  $\alpha \in \text{Gal}(K/k(\zeta_{2n}))$  such that  $\alpha(\sqrt[n]{\epsilon}) = \zeta_n^r \sqrt[n]{\epsilon}$  since  $[K : k(\zeta_{2n})] = n$  is odd.

We have only to set  $\rho := \alpha\eta'$ .  $\rho$  is in the center of  $\text{Gal}(K/\mathbf{Q})$  as above. If there are two automorphisms  $\rho_{\pm}$  of order 2 such that  $\rho_{\pm}$  is  $\eta$  on  $k(\zeta_{2n})$ , then  $\rho_{\pm}(\sqrt[n]{\epsilon}) = \pm \sqrt[n]{\epsilon}$  should hold as at the beginning of the proof. As in the proof of the case (I), it implies the extension degree  $[K : k(\zeta_{2n})] = n$  is even, which is a contradiction. Lastly suppose that  $n$  is even and there is an automorphism  $\rho$  of order 2 in  $\text{Gal}(K/\mathbf{Q})$  such that  $\rho = \eta$  on  $k(\zeta_{2n})$ ; then  $\rho(\epsilon) = -\epsilon^{-1}$  implies  $\rho(\sqrt[n]{\epsilon}) = \zeta_{2n}^r \sqrt[n]{\epsilon}^{-1}$  for an odd integer  $r$ . Then  $\sqrt[n]{\epsilon} = \rho^2(\sqrt[n]{\epsilon}) = \zeta_{2n}^{-r} (\zeta_{2n}^r \sqrt[n]{\epsilon}^{-1})^{-1} = \zeta_{2n}^{-2r} \sqrt[n]{\epsilon}$  implies  $\zeta_n^r = \zeta_{2n}^{2r} = 1$ , which is a contradiction, since  $2|n$  and  $2 \nmid r$ . This completes the proof of the proposition.  $\square$

LEMMA 2. *Suppose  $N_{k/\mathbf{Q}}(\epsilon) = 1$  and let  $p$  be an odd prime which remains in  $k$ . Then for a square-free natural number  $n$ ,  $n(p-1)|I_p$  holds if and only if  $p+1 \equiv 0 \pmod{2n}$  and each prime ideal of  $k(\zeta_{2n})$  lying above  $p$  is completely decomposable at  $K = k(\zeta_{2n})(\sqrt[n]{\epsilon})$ .*

*Proof.* First note that  $p-1$  divides  $I_p$  as in the introduction. Let us show the “only if” part. Suppose that  $n(p-1)|I_p$  and set  $t = I_p/n(p-1) (\in \mathbf{Z})$ . Since  $p^2 - 1 = \sharp(\mathfrak{o}_k/(p))^\times = I_p \cdot \sharp E((p))$ , we have  $(p+1)/n = (p^2 - 1)/n(p-1) = I_p \cdot \sharp E((p))/n(p-1) = t \sharp E((p)) \equiv 0 \pmod{2}$  since  $\sharp E((p)) \equiv 0 \pmod{2}$  by  $\pm 1 \in E((p))$ . Hence we have  $p+1 \equiv 0 \pmod{2n}$ . Next we show the following

CLAIM. *The relative degree of  $p$  at  $k(\zeta_{2n})/\mathbf{Q}$  is 2.*

Let  $\mathfrak{p}$  be a prime ideal of  $k(\zeta_{2n})$  lying above  $p$ . In the local field  $k(\zeta_{2n})_{\mathfrak{p}}$ , the closure of  $k$  is an unramified extension of  $\mathbf{Q}_{\mathfrak{p}}$  of degree 2 and  $p \equiv -1 \pmod{2n}$  implies the closure of  $\mathbf{Q}(\zeta_{2n})$  has the same property, and the uniqueness of the unramified extension of degree 2 over  $\mathbf{Q}_{\mathfrak{p}}$  implies that  $k(\zeta_{2n})_{\mathfrak{p}}$  is the unramified extension of degree 2 over  $\mathbf{Q}_{\mathfrak{p}}$ . This completes the proof of the claim.

Let  $\alpha \in \mathfrak{o}_k$  be a generator of  $(\mathfrak{o}_k/(p))^\times$  and  $r$  the order of  $\epsilon$  in  $(\mathfrak{o}_k/(p))^\times$ , and define an integer  $u$  with  $(u, r) = 1$  by  $\epsilon \equiv \alpha^{u(p^2-1)/r} \pmod{(p)}$ . Since  $p^2 - 1 = I_p \cdot \sharp E((p)) \equiv 0 \pmod{n(p-1) \cdot r} \equiv 0 \pmod{2nr}$ , we have  $p^2 - 1 = 2nrw$  for some integer  $w$ . Then  $\epsilon \equiv (\alpha^{uw})^{2n} \pmod{(p)}$  implies that the equation  $x^{2n} = \epsilon$  has a solution in the local field  $k_{(p)}$  by successive approximation by Newton. Let  $\mathfrak{p}$  be a prime ideal of  $k(\zeta_{2n})$  lying above  $p$ ; then  $k(\zeta_{2n})_{\mathfrak{p}} \cong k_{(p)}$  follows from the Claim and hence the equation  $x^{2n} = \epsilon$  has a solution in  $k(\zeta_{2n})_{\mathfrak{p}}$ , hence  $\mathfrak{p}$  is completely decomposable in  $k(\zeta_{2n}, \sqrt[n]{\epsilon})$ .

Next let us show the “if” part. Let  $\mathfrak{P}, \mathfrak{p} (= \mathfrak{P} \cap k(\zeta_{2n}))$  be prime ideals of  $k(\zeta_{2n}, \sqrt[2n]{\epsilon}), k(\zeta_{2n})$  lying above  $p$ , respectively. By the assumption, the relative degree of  $\mathfrak{P}/\mathfrak{p}$  is one. Hence the equation  $x^{2n} - \epsilon = 0$  is soluble in the local field  $k(\zeta_{2n})_{\mathfrak{p}}$ . Since  $p+1 \equiv 0 \pmod{2n}$ ,  $p$  is unramified in  $\mathbf{Q}(\zeta_{2n})$  and the closure of  $\mathbf{Q}(\zeta_{2n})$  in  $k(\zeta_{2n})_{\mathfrak{p}}$  is  $\mathbf{Q}_p$  or its unramified quadratic extension. Thus  $k(\zeta_{2n})_{\mathfrak{p}}$  is the unramified quadratic extension of  $\mathbf{Q}_p$  and hence  $x^{2n} = \epsilon$  is soluble in  $k_{(p)} \cong k(\zeta_{2n})_{\mathfrak{p}}$ . Hence there exist a primitive root  $\alpha \in \mathfrak{o}_k$  and an integer  $u \in \mathbf{Z}$  such that

$$(\alpha^u)^{2n} \equiv \epsilon \pmod{(p)}.$$

(i) The case where  $E((p)) = \langle \pm 1, \epsilon \pmod{(p)} \rangle$  but  $E((p)) \neq \langle \epsilon \pmod{(p)} \rangle$ .

We note that the assumption yields  $\epsilon^t \not\equiv -1 \pmod{(p)}$  for any integer  $t$ . Let  $r$  be the order of  $\epsilon \pmod{(p)}$  in  $(\mathfrak{o}_k/(p))^\times$ . If  $r$  is even,  $(\epsilon^{r/2})^2 \equiv 1 \pmod{(p)}$  and hence  $\epsilon^{r/2} \equiv \pm 1 \pmod{(p)}$ . Since  $r$  is the order of  $\epsilon \pmod{(p)}$ , we have  $\epsilon^{r/2} \equiv -1 \pmod{(p)}$ . It contradicts the assumption. Hence  $r$  is odd and  $\sharp E((p)) = 2r$  implies  $p^2 - 1 = I_p \cdot 2r$ . Now we have  $1 \equiv \epsilon^r \equiv (\alpha^u)^{2nr} \pmod{(p)}$  and then we have  $2nr u \equiv 0 \pmod{p^2 - 1}$  and  $2ntu \not\equiv 0 \pmod{p^2 - 1}$  for any proper divisor  $t$  of  $r$ , since  $r$  is the order of  $\langle \epsilon \pmod{(p)} \rangle$ . Set  $2nr u = w(p^2 - 1)$  for an integer  $w$ . Then we have

$$(r, w) = 1 \quad \text{and} \quad ru = w(p - 1) \frac{p + 1}{2n}.$$

Let us show  $(r, p - 1) = 1$ . If a prime number  $q$  divides  $(r, p - 1)$ , then  $q$  is odd, since  $r$  is odd. On the other hand,  $\mathbf{Z} \ni I_p/(p - 1) = (p + 1)/2r$  and  $q|r$  imply  $q|(p + 1)$ . Therefore  $q$  divides  $p \pm 1$  and hence  $q = 2$ , which is the contradiction and hence  $(r, p - 1) = 1$ . Thus  $r$  divides  $(p + 1)/2n$  and hence  $I_p/n(p - 1) = 2rI_p/2rn(p - 1) = (p^2 - 1)/2rn(p - 1) = (p + 1)/2rn \in \mathbf{Z}$  which yields that  $n(p - 1)$  divides  $I_p$ .

(ii) The case where  $E((p)) = \langle \epsilon \pmod{(p)} \rangle$ .

Since  $1 \not\equiv -1 \pmod{(p)}$ , the order  $r$  of  $\epsilon \pmod{(p)}$  in  $(\mathfrak{o}_k/(p))^\times$  is even. As in the case (i), we have  $2nur \equiv 0 \pmod{p^2 - 1}$  and for any proper divisor  $t$ , we have  $2nut \not\equiv 0 \pmod{p^2 - 1}$ . Set  $2nur = w(p^2 - 1)$  ( $w \in \mathbf{Z}$ ); then  $(r, w) = 1$  follows and if a prime number  $q$  divides  $(r, p - 1)$ , then  $q|r$  and

$$\frac{p + 1}{r} = \frac{I_p}{p - 1} \in \mathbf{Z}$$

imply  $q|(p + 1)$  and hence  $q = 2$ . Set  $r = 2^t \cdot r'$  ( $r' : \text{odd}$ ); then we have shown  $(r', p - 1) = 1$  and  $2^t r' u = w(p - 1) \frac{p+1}{2n}$  implies

$$r' \mid \frac{p + 1}{2n}$$

by  $(r, w) = 1$  and  $(r', p - 1) = 1$ . Let us show  $nr|(p + 1)$ . If  $n$  is odd, then  $(p + 1)/r \in \mathbf{Z}$  implies  $2^t|(p + 1)$  and hence  $(p + 1)/2nr' \in \mathbf{Z}$  implies  $r = 2^t r' \mid \frac{p+1}{n}$ . If  $n$  is even, then  $p + 1 \equiv 0 \pmod{2n} \equiv 0 \pmod{4}$ , and hence  $(p - 1)/2$  is odd. Since  $2^t r' u = w \frac{p-1}{2} \frac{p+1}{n}$  and  $(r, w \frac{p-1}{2}) = 1$ , we have  $r \mid \frac{p+1}{n}$ . Thus we have  $I_p = (p^2 - 1)/r = \frac{p+1}{nr} \cdot (p - 1)n \equiv 0 \pmod{(p - 1)n}$  and hence we have completed the proof. □

**THEOREM 1.** *Suppose that  $N_{k/\mathbf{Q}}(\epsilon) = 1$  and  $p$  is an odd prime number which remains prime in  $k$ . Let  $n$  be a square-free integer ( $\geq 1$ ). Then  $n(p - 1)|I_p$  holds if and only if  $k \not\subset \mathbf{Q}(\zeta_{2n})$  and for a prime ideal  $\mathfrak{P}$  of  $K = k(\zeta_{2n}, \sqrt[n]{\epsilon})$  lying above  $p$ , the Frobenius automorphism  $\rho_0 = \left(\frac{K/\mathbf{Q}}{\mathfrak{P}}\right)$  is equal to an automorphism  $\rho$  given in Proposition 1.*

*Proof.* Suppose  $n(p - 1)|I_p$ ; then  $p + 1 \equiv 0 \pmod{2n}$  follows from Lemma 2 and hence  $\rho_0$  is the complex conjugation on  $\mathbf{Q}(\zeta_{2n})$  and then  $\rho_0$  fixes each element in  $k$  if  $k \subset \mathbf{Q}(\zeta_{2n})$ . On the other hand,  $p$  remains prime in  $k$  by the assumption and hence  $\rho_0$  is a non-trivial automorphism of  $k$ , which is a contradiction. Thus we have  $k \not\subset \mathbf{Q}(\zeta_{2n})$ . By Lemma 2, the relative degree of  $\mathfrak{P}$  is two and so  $\rho_0^2 = \text{id.}$  and hence we have  $\rho_0 = \rho$  given in Proposition 1.

Conversely suppose that  $k \not\subset \mathbf{Q}(\zeta_{2n})$  and  $\rho_0$  is an automorphism of order 2 and it is equal to  $\eta$  in Proposition 1 on  $k(\zeta_{2n})$ . Then  $\rho_0$  is the complex conjugation on  $\mathbf{Q}(\zeta_{2n})$  and then  $p + 1 \equiv 0 \pmod{2n}$ . Since the order of  $\rho_0$  is two, we have  $[K_{\mathfrak{P}} : \mathbf{Q}_p] = 2$  and  $[k_{(p)} : \mathbf{Q}_p] = 2$ , which yields that the relative degree of  $\mathfrak{P}$  at  $K/k$  and hence at  $K/k(\zeta_{2n})$  is one. Now Lemma 2 implies  $n(p - 1)|I_p$ . □

**LEMMA 3.** *Suppose  $N_{k/\mathbf{Q}}(\epsilon) = -1$  and let  $p$  be an odd prime which remains prime in  $k$ . Then for a square-free natural number  $n$ ,  $n \frac{p-1}{2}|I_p$  holds if and only if  $p + 1 \equiv 0 \pmod{2n}$  and each prime ideal of  $k(\zeta_{2n})$  lying above  $p$  is completely decomposable at  $K = k(\zeta_{2n})(\sqrt[n]{\epsilon})$ .*

*Proof.* We note that  $\frac{p-1}{2}|I_p$  as in the introduction ([IK]). Set  $r := \#E((p))$ . We claim  $r \equiv 0 \pmod{4}$ . Because of  $\epsilon^{p+1} \equiv -1 \pmod{(p)}$  ([IK]),

$E((p))$  is generated by  $\epsilon \pmod{(p)}$ .  $\pm 1 \in E((p))$  implies  $r \equiv 0 \pmod{2}$ . Suppose that  $r = 2t$  for some odd integer  $t$ ; then we have  $\epsilon^{(p+1)t} \equiv -1 \pmod{(p)}$  and on the other hand  $(p+1)t \equiv 0 \pmod{2t}$  implies  $\epsilon^{(p+1)t} \equiv 1 \pmod{(p)}$ , which is a contradiction. Therefore  $r \equiv 0 \pmod{4}$  and note  $p^2 - 1 = I_p \cdot r$ .

First suppose  $n \frac{p-1}{2} | I_p$  and set  $I_p = n \frac{p-1}{2} \cdot t$  for an integer  $t$ . Then we have  $(p+1)/n = (p^2 - 1)/n(p-1) = I_p r/n(p-1) = tr/2 \in 2\mathbf{Z}$  and then

$$p + 1 \equiv 0 \pmod{2n}.$$

Since the order of  $\epsilon$  in  $(\mathfrak{o}_k/(p))^\times$  is  $r$ , we can take a generator  $\alpha \in \mathfrak{o}_k$  of  $(\mathfrak{o}_k/(p))^\times$  so that  $\epsilon \equiv \alpha^{u(p^2-1)/r} \pmod{(p)}$  for an integer  $u$  with  $(u, r) = 1$ . Then we have  $\epsilon \equiv (\alpha^{u(p^2-1)/nr})^n \pmod{(p)}$ , where  $(p^2 - 1)/nr = I_p/n$  is an integer. Hence  $x^n \equiv \epsilon \pmod{(p)}$  is soluble in  $\mathfrak{o}_k$  and  $x^n = \epsilon$  has a solution in the local field  $k_{(p)}$ . Let  $\mathfrak{P}$  be a prime ideal of  $K = k(\zeta_{2n}, \sqrt[n]{\epsilon})$  lying above  $p$  and set  $\mathfrak{p} = \mathfrak{P} \cap k(\zeta_{2n})$ ; then  $p + 1 \equiv 0 \pmod{2n}$  implies that the closure of  $\mathbf{Q}(\zeta_{2n})$  in  $k(\zeta_{2n})_{\mathfrak{p}}$  is an unramified extension of degree 2, at most over  $\mathbf{Q}_p$  and therefore  $k(\zeta_{2n})_{\mathfrak{p}} = k_{(p)}$ . Hence the solubility of the equation  $x^n = \epsilon$  in  $k_{(p)} = k(\zeta_{2n})_{\mathfrak{p}}$  yields that  $\mathfrak{p}$  is completely decomposable at  $K/k(\zeta_{2n})$ .

Conversely, we suppose  $p + 1 \equiv 0 \pmod{2n}$  and each prime ideal of  $k(\zeta_{2n})$  lying above  $p$  is completely decomposable at  $K$ . Let  $\mathfrak{P}$  be a prime ideal of  $K$  lying above  $p$ , and set  $\mathfrak{p} = \mathfrak{P} \cap k(\zeta_{2n})$ . Since  $p \equiv -1 \pmod{2n}$ , the closure of  $\mathbf{Q}(\zeta_{2n})$  in  $K_{\mathfrak{p}}$  is an unramified extension of degree 2 over  $\mathbf{Q}_p$  and so is the closure of  $k$ . Hence by the assumption,  $K_{\mathfrak{p}} = k(\zeta_{2n})_{\mathfrak{p}}$  holds where  $\mathfrak{p} = \mathfrak{P} \cap k(\zeta_{2n})$ , and the equation  $x^n = \epsilon$  is completely soluble over  $k(\zeta_{2n})_{\mathfrak{p}} = k_{(p)}$ . Take a generator  $\alpha \in \mathfrak{o}_k$  of  $(\mathfrak{o}_k/(p))^\times$  and an integer  $u$  such that  $(\alpha^u)^n \equiv \epsilon \pmod{(p)}$ .  $1 \equiv \epsilon^r \equiv \alpha^{run} \pmod{(p)}$  implies  $run \equiv 0 \pmod{p^2 - 1}$  and for any proper divisor  $t$  of  $r$ ,  $tun \not\equiv 0 \pmod{p^2 - 1}$  holds from the definition of  $r$ . Set  $run = w(p^2 - 1)$  ( $w \in \mathbf{Z}$ ); then  $(r, w) = 1$  holds. If a prime number  $q$  divides  $(r, p - 1)$ , then  $\frac{2(p+1)}{r} = \frac{I_p}{(p-1)/2} \in \mathbf{Z}$  implies  $q|2(p+1)$  by  $q|r$  and hence  $q = 2$  because of  $q|(p-1)$ . Set  $r = 2^t \cdot r'$  ( $r' : \text{odd}$ ); then we have shown  $(r', p-1) = 1$  and then  $ru = 2^t \cdot r'u = w(p-1) \frac{p+1}{nr}$  and  $(r, w) = 1 = (r', p-1)$  imply  $(r', w(p-1)) = 1$  and  $2^t u = w(p-1) \frac{p+1}{nr'}$  and

$$nr' | (p + 1).$$

To show  $n \frac{p-1}{2} | I_p$ , i.e.,  $\frac{I_p}{n(p-1)/2} = \frac{2(p+1)}{nr} \in \mathbf{Z}$ , we have only to show  $\text{ord}_2 \frac{2(p+1)}{nr} \geq 0$ , where  $a := \text{ord}_2(b)$  is defined by  $2^a || b$ . At the beginning of the proof, we showed  $4|r$  and then  $t \geq 2$ .  $(r, w) = 1$  implies that  $w$  is odd.



If  $n$  is odd, then  $\frac{2(p+1)}{r} = \frac{I_p}{(p-1)/2} \in \mathbf{Z}$  yields  $\text{ord}_2 \frac{2(p+1)}{nr} = \text{ord}_2 \frac{2(p+1)}{r} \geq 0$ .  
 If  $n$  is even, then  $p + 1 \equiv 0 \pmod 4$  implies  $0 \leq \text{ord}_2 u = \text{ord}_2 \frac{w(p^2-1)}{nr} = \text{ord}_2 \frac{p+1}{nr} + \text{ord}_2(p-1) = \text{ord}_2 \frac{p+1}{nr} + 1 = \text{ord}_2 \frac{2(p+1)}{nr}$ . Thus we have shown  $\text{ord}_2 \frac{2(p+1)}{nr} \geq 0$  and then  $\frac{I_p}{n(p-1)/2} = \frac{2(p+1)}{nr}$  is an integer and hence we have completed the proof of Lemma 3. □

**THEOREM 2.** *Suppose that  $N_{k/\mathbf{Q}}(\epsilon) = -1$  and  $p$  is an odd prime number which remains prime in  $k$ . Let  $n$  be a square-free natural number. Then  $n \frac{p-1}{2} | I_p$  holds if and only if  $k \not\subset \mathbf{Q}(\zeta_{2n})$ ,  $n$  is odd and for each prime ideal  $\mathfrak{P}$  of  $K = k(\zeta_{2n}, \sqrt[n]{\epsilon})$  lying above  $p$ , the Frobenius automorphism  $\rho_0 = \left(\frac{K/\mathbf{Q}}{\mathfrak{P}}\right)$  is equal to  $\rho$  given in Proposition 1.*

*Proof.* Suppose  $n \frac{p-1}{2} | I_p$ ; then by Lemma 3,  $\rho_0$  induces the complex conjugation on  $\mathbf{Q}(\zeta_{2n})$  and the order of  $\rho_0$  is two, since  $K_{\mathfrak{P}}$  is a quadratic unramified extension of  $\mathbf{Q}_p$ . If  $k \subset \mathbf{Q}(\zeta_{2n})$ , then  $\rho_0$  induces the trivial automorphism on  $k$ , which is a contradiction. Hence  $k \not\subset \mathbf{Q}(\zeta_{2n})$  holds and then Proposition 1 implies that  $n$  is odd and the uniqueness implies  $\rho_0 = \rho$ .

Now let us show the converse. Since  $\rho_0 = \rho$  and  $\rho$  induces the complex conjugation on  $\mathbf{Q}(\zeta_{2n})$ ,  $p + 1 \equiv 0 \pmod{2n}$  holds. Since the order of  $\rho_0 = 2$ , and the closure of  $k$  in  $K_{\mathfrak{P}}$  is a quadratic unramified extension of  $\mathbf{Q}_p$ , the relative degree of  $\mathfrak{P}$  at  $K/k$  and hence  $K/k(\zeta_{2n})$  is one and then Lemma 3 implies  $n \frac{p-1}{2} | I_p$ . □

**§3. Analytic part of the proof of the theorem**

Hereafter  $q$  denotes a prime number and  $p$  denotes an odd prime number which remains prime in the real quadratic field  $k$ . We set  $\tilde{\ell}_p := I_p/\ell_p$ , which is an integer ([IK]). As in the Section 1, we denote by  $\mathbb{P}(x)$  the set of odd prime numbers  $p \leq x$  which remains prime in  $k$ . Set for  $x \geq 3$ ,

$$\begin{aligned} N(x) &:= \#\{p \in \mathbb{P}(x) \mid \tilde{\ell}_p = 1\}, \\ N(x, \eta) &:= \#\{p \in \mathbb{P}(x) \mid q \nmid \tilde{\ell}_p \text{ for } \forall q \leq \eta\}, \\ M(x, \eta_1, \eta_2) &:= \#\{p \in \mathbb{P}(x) \mid q \mid \tilde{\ell}_p \text{ for } \eta_1 < \exists q \leq \eta_2\}, \\ P(x, n) &:= \#\{p \in \mathbb{P}(x) \mid n \mid \tilde{\ell}_p\}, \\ \xi_1 &:= 6^{-1} \log x, \quad \xi_2 := \sqrt{x}(\log x)^{-2}, \quad \xi_3 := \sqrt{x} \log x. \end{aligned}$$

Then it is easy to see  $N(x, \xi_1) - M(x, \xi_1, \xi_2) - M(x, \xi_2, \xi_3) - M(x, \xi_3, x-1) \leq N(x) = N(x, x-1) \leq N(x, \xi_1)$ .

LEMMA 1.  $M(x, \xi_2, \xi_3) = O((x \log(\log x))/(\log x)^2)$ .

*Proof.* Since  $\tilde{\ell}_p = I_p/\ell_p$  divides  $2I_p/(p-1)$  and  $I_p$  divides  $p^2-1$ ,  $\tilde{\ell}_p$  divides  $2(p+1)$ . For a prime number  $q$  with  $\xi_2 < q \leq \xi_3$ ,  $q|\tilde{\ell}_p$  implies  $q|2(p+1)$  and then  $p \equiv -1 \pmod q$ . Thus we have

$$\begin{aligned} M(x, \xi_2, \xi_3) &\leq \sum_{\xi_2 < q \leq \xi_3} \#\{p \in \mathbb{P}(x) \mid p \equiv -1 \pmod q\} \\ &= O((x \log(\log x))/(\log x)^2), \end{aligned}$$

as is shown in [H]. □

LEMMA 2.  $M(x, \xi_3, x-1) = O(x(\log x)^{-2})$ .

*Proof.* For a prime number  $p \in \mathbb{P}(x)$ , suppose that a prime number  $q$  with  $\xi_3 < q \leq x-1$  satisfies  $q|\tilde{\ell}_p$ . Set

$$\delta = \begin{cases} 1, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ 2, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1. \end{cases}$$

Then  $\delta\ell_p = p-1$  and  $\frac{2(p+1)}{q\#\mathbb{E}((p))} = \frac{2(p+1)I_p}{q\#\mathbb{E}((p))I_p} = \frac{2(p+1)\ell_p\tilde{\ell}_p}{q(p^2-1)} = \frac{2\tilde{\ell}_p}{\delta q}$  is an integer. Hence  $\#\mathbb{E}((p))$  divides  $2(p+1)/q$ , where we note that  $2(p+1)/q$  is an even integer. Thus  $\epsilon^{2(p+1)/q} \equiv 1 \pmod (p)$  holds and then  $N_{k/\mathbf{Q}}(\epsilon^{2(p+1)/q} - 1) \equiv 0 \pmod{p^2}$ . Here  $2(p+1)/q < 2(x+1)/\sqrt{x} \log x \ll \sqrt{x}/\log x$ . Thus  $p^2$  divides  $\prod_{m \ll \sqrt{x}/\log x, m:\text{even}} N_{k/\mathbf{Q}}(\epsilon^m - 1)$ . Denote by  $\epsilon_1$  the conjugate of  $\epsilon$ ; then  $|\epsilon_1| < 1$  and for an even integer  $m$ , we have  $|N_{k/\mathbf{Q}}(\epsilon^m - 1)| = |\epsilon^m - 1||\epsilon_1^m - 1| < \epsilon^m - 1 < \epsilon^m$ , and then we have

$$2^{2M(x, \xi_3, x-1)} \leq \prod_p p^2 \leq \prod_{m \ll \sqrt{x}/\log x} \epsilon^m,$$

where  $p$  runs over the set which defines  $M(x, \xi_3, x-1)$ . Therefore we have  $M(x, \xi_3, x-1) \ll \sum_{m < \sqrt{x}/\log x} m \ll x/(\log x)^2$ . □

LEMMA 3.  $M(x, \xi_1, \xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P(x, q)$ .

*Proof.* It is obvious. □

LEMMA 4. Set  $Q(\xi_1) := \prod_{q \leq \xi_1} q$ ; then we have  $N(x, \xi_1) = \sum_{n|Q(\xi_1)} \mu(n)P(x, n)$ , where  $\mu(n)$  is the Möbius function.

*Proof.*  $N(x, \xi_1)$  is equal to

$$\begin{aligned} \#\{p \in \mathbb{P}(x) \mid (Q(\xi_1), \tilde{\ell}_p) = 1\} &= \sum_{p \in \mathbb{P}(x)} \sum_{n \mid (Q(\xi_1), \tilde{\ell}_p)} \mu(n) \\ &= \sum_{n \mid Q(\xi_1)} \mu(n) \sum_{p \in \mathbb{P}(x), n \mid \tilde{\ell}_p} 1 = \sum_{n \mid Q(\xi_1)} \mu(n) P(x, n). \quad \square \end{aligned}$$

Thus we have

$$N(x) = \sum_{n \mid Q(\xi_1)} \mu(n) P(x, n) + O\left(\sum_{\xi_1 < q \leq \xi_2} P(x, q)\right) + O(x \log(\log x) / (\log x)^2).$$

Now let  $n$  be a square-free natural number, and set

$$K_n := \begin{cases} k(\zeta_{2n}, \sqrt[2n]{\epsilon}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ k(\zeta_{2n}, \sqrt[n]{\epsilon}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1. \end{cases}$$

Then from Lemma 1 in the Section 2 follows that under the condition  $k \not\subset \mathbf{Q}(\zeta_{2n})$

$$[K_n : \mathbf{Q}] = \begin{cases} 4n\varphi(2n), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1 \text{ and } \sqrt{\epsilon} \notin k(\zeta_{2n}), \\ 2n\varphi(2n), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1 \text{ and } \sqrt{\epsilon} \in k(\zeta_{2n}), \\ 2n\varphi(n), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1 \text{ and } 2 \nmid n. \end{cases}$$

Let  $C$  be a union of conjugacy classes consisting of automorphisms  $\rho$  in  $\text{Gal}(K_n/\mathbf{Q})$  in Proposition 1 of the Section 2; then we have under the condition  $k \not\subset \mathbf{Q}(\zeta_{2n})$

$$\#(C) = \begin{cases} 2, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \text{ and} \\ & \text{either } 2 \mid n, \sqrt{\epsilon} \in k(\zeta_{2n}) \text{ and } \eta(\sqrt{\epsilon})\sqrt{\epsilon} = 1, \text{ or } \sqrt{\epsilon} \notin k(\zeta_{2n}), \\ 1, & \text{either if } N_{k/\mathbf{Q}}(\epsilon) = 1, 2 \nmid n, \text{ and } \sqrt{\epsilon} \in k(\zeta_{2n}), \\ & \text{or if } N_{k/\mathbf{Q}}(\epsilon) = -1 \text{ and } 2 \nmid n, \\ 0, & \text{otherwise,} \end{cases}$$

where  $\eta$  is an automorphism such that it is the complex conjugation on  $\mathbf{Q}(\zeta_{2n})$  and is the non-trivial automorphism on  $k$ , and note that the equality  $[K_n : k(\zeta_{2n})] = n$  implies  $\sqrt{\epsilon} \in k(\zeta_{2n})$  by Lemma 1 in the Section 2 when  $N_{k/\mathbf{Q}}(\epsilon) = 1$ . Moreover Theorems 1 and 2 imply that

$$P(x, n) = \begin{cases} \#\left\{p \in \mathbb{P}(x) \mid k \not\subset \mathbf{Q}(\zeta_{2n}), \left(\frac{K_n/\mathbf{Q}}{\mathfrak{P}}\right) \in C\right\}, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ \#\left\{p \in \mathbb{P}(x) \mid k \not\subset \mathbf{Q}(\zeta_{2n}), n:\text{odd}, \left(\frac{K_n/\mathbf{Q}}{\mathfrak{P}}\right) \in C\right\}, & \\ & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1, \end{cases}$$

where  $\mathfrak{P}$  is any prime ideal of  $K_n$  lying above a prime ideal  $p$ . We apply the Chebotarev density theorem under the GRH ([LO], Théorème 4 in [S]):

**CHEBOTAREV DENSITY THEOREM.** *Suppose that the GRH holds for  $K_n$ . Let  $C$  be the union of conjugacy classes of  $\text{Gal}(K_n/\mathbf{Q})$  defined above. Denote by  $\pi_C(x, K_n)$  the number of unramified prime number  $p$  such that  $\left(\frac{K_n/\mathbf{Q}}{\mathfrak{P}}\right) \in C$  and  $p \leq x$ , where  $\mathfrak{P}$  is a prime ideal of  $K_n$  lying above  $p$ . Then we have*

$$\left| \pi_C(x, K_n) - \frac{\#(C)}{[K_n : \mathbf{Q}]} \text{Li}(x) \right| < c \left( \frac{\#(C)}{[K_n : \mathbf{Q}]} \sqrt{x} \log(dK_n x^{[K_n:\mathbf{Q}]}) \right),$$

where  $c$  is an absolute constant and  $dK_n$  stands for the absolute discriminant of  $K_n$ .

Hereafter we apply this theorem assuming the GRH. Now set  $d(n) := \#(C)[K_n : \mathbf{Q}]^{-1}$ ; then we have

$$d(n) = \begin{cases} (2n\varphi(n))^{-1}, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1, n \text{ is odd and } k \not\subset \mathbf{Q}(\zeta_n), \\ (n\varphi(2n))^{-1}, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, n \text{ is even, } \sqrt{\epsilon} \in k(\zeta_{2n}), \\ & \eta(\sqrt{\epsilon})\sqrt{\epsilon} = 1 \text{ and } k \not\subset \mathbf{Q}(\zeta_{2n}), \\ (2n\varphi(n))^{-1}, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, n \text{ is odd, } \sqrt{\epsilon} \in k(\zeta_{2n}) \text{ and} \\ & k \not\subset \mathbf{Q}(\zeta_{2n}), \\ (2n\varphi(2n))^{-1}, & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \sqrt{\epsilon} \notin k(\zeta_{2n}) \text{ and } k \not\subset \mathbf{Q}(\zeta_{2n}), \\ 0, & \text{otherwise.} \end{cases}$$

Note that  $d(n) = 0$  if  $k \subset \mathbf{Q}(\zeta_{2n})$ . By the theory of algebraic number fields, it is easy to see

$$dK_n | (2n)^{8n\varphi(2n)} D_0^{2n\varphi(2n)},$$

where  $D_0$  is the discriminant of  $k$  as in the introduction. Theorems 1 and 2 in the Section 2 imply  $\pi_C(x, K_n) = P(x, n)$  under the following condition  $c(n)$ :

$$\begin{cases} k \not\subset \mathbf{Q}(\zeta_{2n}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = 1, \\ n : \text{odd and } k \not\subset \mathbf{Q}(\zeta_{2n}), & \text{if } N_{k/\mathbf{Q}}(\epsilon) = -1. \end{cases}$$

Note that if the condition  $c(n)$  is not satisfied, then  $d(n) = 0$  holds. Hence we have

$$\begin{aligned} N(x) = & \sum_{\substack{n|Q(\xi_1) \\ c(n)}} \mu(n)\pi_C(x, K_n) + O\left( \sum_{\substack{\xi_1 < q \leq \xi_2 \\ c(q)}} \pi_C(x, K_q) \right) \\ & + O(x \log(\log x) / (\log x)^2). \end{aligned}$$

LEMMA 5.  $\sum_{\xi_1 < q \leq \xi_2, c(q)} \pi_C(x, K_q) = O(x \log(\log x) / (\log x)^2)$ .

*Proof.* It is easy to see that

$$\begin{aligned} & \sum_{\substack{\xi_1 < q \leq \xi_2 \\ c(q)}} \pi_C(x, K_q) \\ &= \sum_{\xi_1 < q \leq \xi_2} d(q) \text{Li}(x) + O\left(\sum_{\xi_1 < q \leq \xi_2} d(q) \sqrt{x} \log(dK_q x^{[K_q : \mathbf{Q}]})\right). \end{aligned}$$

Now we have

$$\sum_{\xi_1 < q \leq \xi_2} d(q) \ll \sum_{q > 6^{-1} \log x} q^{-2} \ll 1 / \log x,$$

and

$$\sum_{\xi_1 < q \leq \xi_2} d(q) \log dK_q \ll \sum_{\xi_1 < q \leq \xi_2} (\log q + 1) \ll \sqrt{x} (\log x)^{-2} < \sqrt{x} \frac{\log \log x}{(\log x)^2},$$

and lastly

$$\begin{aligned} \sum_{\xi_1 < q \leq \xi_2} d(q) [K_q : \mathbf{Q}] \log x &\ll \pi(\xi_2) \log x \ll \sqrt{x} (\log x)^{-2} \\ &\ll \sqrt{x} \log \log x / (\log x)^2. \end{aligned}$$

From these follows the assertion. □

LEMMA 6.

$$\sum_{\substack{n|Q(\xi_1) \\ c(n)}} \mu(n) \pi_C(x, K_n) = \left(\sum_{n=1}^{\infty} \mu(n) d(n)\right) \text{Li}(x) + O(x \log \log x / (\log x)^2).$$

*Proof.* By using the Chebotarev density theorem under the GRH, we have

the left-hand side

$$\begin{aligned} &= \sum_{n|Q(\xi_1)} \mu(n) \{d(n) \text{Li}(x) + O(d(n) \sqrt{x} \log(dK_n x^{[K_n : \mathbf{Q}]})\}) \\ &= \left(\sum_{n|Q(\xi_1)} \mu(n) d(n)\right) \text{Li}(x) + \sqrt{x} \log x O\left(\sum_{n|Q(\xi_1)} d(n) [K_n : \mathbf{Q}]\right) \\ &\quad + \sqrt{x} O\left(\sum_{n|Q(\xi_1)} d(n) \log dK_n\right). \end{aligned}$$

The first term is equal to

$$\sum_{n \geq 1} \mu(n)d(n) + O\left(\sum_n^* (n\varphi(n))^{-1}\right),$$

where  $\sum_n^*$  means that the sum on  $n$  which has a prime divisor larger than  $\xi_1 = 6^{-1} \log x$ , and it is easy to see

$$\begin{aligned} \sum_n^* (n\varphi(n))^{-1} &< \sum_{n > \xi_1} \frac{1}{n^2} \frac{n}{\varphi(n)} \\ &\ll \sum_{n > \xi_1} n^{-2} \sum_{d|n} 1/d = \sum_{d=1}^\infty 1/d \sum_{m > \xi_1/d}^\infty (md)^{-2} \\ &\ll \sum_{d=1}^\infty 1/d^3 \cdot \frac{1}{\xi_1/d} \ll 1/\xi_1 \ll 1/\log x. \end{aligned}$$

We note that  $\log Q(\xi_1)/(6^{-1} \log x) = \sum_{q \leq 6^{-1} \log x} \log q/(6^{-1} \log x) < 1.1$  and then  $Q(\xi_1) < x^{1.1/6}$  if  $x$  is large. The second term is

$$\begin{aligned} \sqrt{x} \log x O\left(\sum_{n|Q(\xi_1)} 1\right) &= \sqrt{x} \log x O(Q(\xi_1)^\delta) \\ &= O(x \log \log x / (\log x)^2) \end{aligned}$$

where  $\delta$  is an arbitrary small positive number. The third term is

$$\begin{aligned} \sqrt{x} O\left(\sum_{n|Q(\xi_1)} \left(\frac{n\varphi(n)}{n\varphi(n)} \log n + 1\right)\right) &= \sqrt{x} O\left(\sum_{n < Q(\xi_1)} (\log n + 1)\right) \\ &= O(\sqrt{x} Q(\xi_1) \log Q(\xi_1)) = \sqrt{x} O(x^{1.1/6} \log x^{1.1/6}) \\ &= O(x \log \log x / (\log x)^2). \quad \square \end{aligned}$$

Thus we have

$$N(x) = \left(\sum_{n=1}^\infty \mu(n)d(n)\right) \text{Li}(x) + O(x \log(\log x) / (\log x)^2)$$

and we have only to show that the infinite series  $\sum_{n=1}^\infty \mu(n)d(n)$  is a positive constant to complete the proof of the main theorem. The absolute convergence follows from  $\varphi(n) \gg n/\log \log n$  and then  $|\sum_{n=1}^\infty \mu(n)d(n)| \ll \sum_{n=1}^\infty (\log \log n)/n^2 < \infty$ . Set  $c_0 := \sum_{n=1}^\infty \mu(n)d(n)$ .

(I) The case of  $N_{k/\mathbf{Q}}(\epsilon) = -1$ .

In this case, we have  $c_0 = \sum_{n=1, n:\text{odd}, D_0 \nmid n}^{\infty} \mu(n)d(n)$ , where  $D_0$  is the discriminant of  $k$ .

(I.1) The case of  $D_0 \equiv 0 \pmod 2$ .

We have

$$c_0 = \sum_{\substack{n=1 \\ n:\text{odd}}}^{\infty} \frac{\mu(n)}{2n\varphi(n)} = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = A > 0,$$

where  $q$  runs over the set of all prime numbers.

(I.2) The case of  $D_0 \equiv 1 \pmod 2$ .

In this case, we have

$$\begin{aligned} c_0 &= \sum_{\substack{n=1, n:\text{odd} \\ D_0 \nmid n}}^{\infty} \frac{\mu(n)}{2n\varphi(n)} = \sum_{n=1, n:\text{odd}}^{\infty} \frac{\mu(n)}{2n\varphi(n)} - \sum_{\substack{n=1, n:\text{odd} \\ D_0 \mid n}}^{\infty} \frac{\mu(n)}{2n\varphi(n)} \\ &= A - \sum_{\substack{m=1, m:\text{odd} \\ (m, D_0)=1}}^{\infty} \frac{\mu(D_0)\mu(m)}{2D_0m\varphi(D_0m)} \\ &= A - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \sum_{\substack{m=1, m:\text{odd} \\ (m, D_0)=1}}^{\infty} \frac{\mu(m)}{m\varphi(m)} \\ &= A - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \prod_{q \mid 2D_0} \left(1 - \frac{1}{q(q-1)}\right) \\ &= A \left\{1 - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \prod_{q \mid 2D_0} \frac{q(q-1)}{q^2 - q - 1}\right\} \\ &= A \left(1 - \mu(D_0) \prod_{q \mid D_0} \frac{1}{q^2 - q - 1}\right) > 0. \end{aligned}$$

(II) The case of  $N_{k/\mathbf{Q}}(\epsilon) = 1$ .

We note some facts.

- Suppose that  $m$  is odd square-free.  $k \subset \mathbf{Q}(\zeta_{2m}) = \mathbf{Q}(\zeta_m)$  if and only if  $D_0 \mid m$ .  $k \subset \mathbf{Q}(\zeta_{4m})$  if and only if  $D_0 \mid 4m$ .
- $\sum_{m=1, m:\text{odd}}^{\infty} \mu(m)/m\varphi(m) = 2A$ .

- $\sum_{m:\text{odd, square-free}} 1/m\varphi(m) = \prod_{2 \nmid p} (1 + \frac{1}{p(p-1)}) = 1.2957 \dots$

Now we have

$$\begin{aligned}
 c_0 &= \sum_{n=1}^{\infty} \mu(n)d(n) \\
 &= \sum_{\substack{n:\text{even} \geq 1 \\ \sqrt{\epsilon} \in k(\zeta_{2n}), \eta(\sqrt{\epsilon})\sqrt{\epsilon}=1 \\ k \nmid \mathbf{Q}(\zeta_{2n})}} \frac{\mu(n)}{n\varphi(2n)} + \sum_{\substack{n:\text{odd} \geq 1 \\ \sqrt{\epsilon} \in k(\zeta_{2n}) \\ k \nmid \mathbf{Q}(\zeta_{2n})}} \frac{\mu(n)}{2n\varphi(n)} + \sum_{\substack{n \geq 1 \\ \sqrt{\epsilon} \notin k(\zeta_{2n}) \\ k \nmid \mathbf{Q}(\zeta_{2n})}} \frac{\mu(n)}{2n\varphi(2n)} \\
 &= -\frac{1}{4} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \in k(\zeta_{4m}), \eta(\sqrt{\epsilon})\sqrt{\epsilon}=1 \\ k \nmid \mathbf{Q}(\zeta_{4m})}} \frac{\mu(m)}{m\varphi(m)} + \frac{1}{2} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \in k(\zeta_{2m}) \\ k \nmid \mathbf{Q}(\zeta_{2m})}} \frac{\mu(m)}{m\varphi(m)} \\
 &\quad + \frac{1}{2} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \notin k(\zeta_{2m}) \\ k \nmid \mathbf{Q}(\zeta_{2m})}} \frac{\mu(m)}{m\varphi(m)} - \frac{1}{8} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \notin k(\zeta_{4m}) \\ k \nmid \mathbf{Q}(\zeta_{4m})}} \frac{\mu(m)}{m\varphi(m)} \\
 &= \frac{1}{2} \sum_{\substack{m:\text{odd} \geq 1 \\ k \nmid \mathbf{Q}(\zeta_m)}} \frac{\mu(m)}{m\varphi(m)} - \frac{1}{4} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \in k(\zeta_{4m}), \eta(\sqrt{\epsilon})\sqrt{\epsilon}=1 \\ k \nmid \mathbf{Q}(\zeta_{4m})}} \frac{\mu(m)}{m\varphi(m)} \\
 &\quad - \frac{1}{8} \sum_{\substack{m:\text{odd} \geq 1 \\ \sqrt{\epsilon} \notin k(\zeta_{4m}) \\ k \nmid \mathbf{Q}(\zeta_{4m})}} \frac{\mu(m)}{m\varphi(m)}.
 \end{aligned}$$

The absolute value of the sum of the second and third terms is less than

$$\begin{aligned}
 &\frac{1}{4} \sum_{\substack{m:\text{odd, square-free} \\ \sqrt{\epsilon} \in k(\zeta_{4m})}} \frac{1}{m\varphi(m)} + \frac{1}{8} \sum_{\substack{m:\text{odd, square-free} \\ \sqrt{\epsilon} \notin k(\zeta_{4m})}} \frac{1}{m\varphi(m)} \\
 &= \frac{1}{8} \sum_{\substack{m:\text{odd, square-free} \\ \sqrt{\epsilon} \in k(\zeta_{4m})}} \frac{1}{m\varphi(m)} + \frac{1}{8} \sum_{\substack{m:\text{odd, square-free}}} \frac{1}{m\varphi(m)} \\
 &\leq \frac{1}{4} \sum_{\substack{m:\text{odd, square-free}}} \frac{1}{m\varphi(m)} - \frac{1}{8} \\
 &= 0.1989 \dots,
 \end{aligned}$$

where the last inequality follows from  $\sqrt{\epsilon} \notin k(\zeta_4)$ .



If  $4|D_0$ , then the first term is equal to

$$\frac{1}{2} \sum_{m:\text{odd}} \frac{\mu(m)}{m\varphi(m)} = A = 0.3739\dots$$

and hence  $c_0 > 0$  holds.

If  $D_0$  is odd, then the first term is

$$\begin{aligned} \frac{1}{2} \sum_{\substack{m:\text{odd} \\ D_0 \nmid m}} \frac{\mu(m)}{m\varphi(m)} &= \frac{1}{2} \sum_{m:\text{odd}} \frac{\mu(m)}{m\varphi(m)} - \frac{1}{2} \sum_{\substack{m:\text{odd} \\ D_0|m}} \frac{\mu(m)}{m\varphi(m)} \\ &= A - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \sum_{\substack{n:\text{odd} \\ (n,D_0)=1}} \frac{\mu(n)}{n\varphi(n)} \\ &= A - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \prod_{q \nmid 2D_0} \left(1 - \frac{1}{q(q-1)}\right) \\ &= A \left(1 - \frac{\mu(D_0)}{2D_0\varphi(D_0)} \prod_{q|2D_0} \frac{q(q-1)}{q^2 - q - 1}\right) \\ &= A \left(1 - \mu(D_0) \prod_{q|2D_0} \frac{1}{q^2 - q - 1}\right) \\ &\geq A(1 - 1/19) = 0.3542\dots, \end{aligned}$$

where the inequality follows from the fact that  $D_0$  is divisible by a prime  $\geq 5$  and hence we have  $c_0 > 0$ . Thus we have completed the proof of the main theorem.

REFERENCES

[H] C. Hooley, *On Artin’s conjecture*, J. reine angew. Math., **225** (1967), 209–220.  
 [IK] M. Ishikawa and Y. Kitaoka, *On the distribution of units modulo prime ideals in real quadratic fields*, J. reine angew. Math., **494** (1998), 65–72.  
 [LO] J. C. Lagarias and A. M. Odlyzko, *Effective version of the Chebotarev density theorem*, Algebraic Number Fields (Fröhlich, ed.), Academic Press (1977), 409–464.  
 [M] K. Masima, *On the distribution of units in the residue class field of real quadratic fields and Artin’s conjecture (in Japanese)*, RIMS Kokyuroku, **1026** (1998), 156–166.  
 [S] J. P. Serre, *Quelques applications du théorème de densité de Chebotarev*, I.H.E.S., **54** (1981), 323–401.

Yen-Mei J. Chen  
*Dept. of Math.*  
*Tamkang University*  
*Tamshui, Taipei*  
*Taiwan*  
ymjchen@mail.tku.edu.tw

Yoshiyuki Kitaoka  
*Dept. of Math.*  
*Meijo University*  
*Tenpaku-ku*  
*Nagoya, 468-8502*  
*Japan*  
kitaoka@meijo-u.ac.jp

Jing Yu  
*Institute of Math.*  
*Academia Sinica*  
*Nakang, Taipei*  
*Taiwan*  
*and National Center for Theoretical Science*  
*Hsinchu*  
*Taiwan*  
yu@math.sinica.edu.tw