113. *Construction of Certain Real Quadratic Fields*

By Tsuyoshi UEHARA
Department of Mathematics, Saga University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1983)

Let n be a given natural number. In this note we shall construct real quadratic fields whose fundamental units are congruent to ± 1 modulo n. We also give a new proof of the existence of infinitely many real quadratic fields each with class number divisible by n (cf. Weinberger [3], Yamamoto [4]).

Let Z, Q be the ring of rational integers, the field of rational numbers respectively. For a rational integer $m \neq 0$ and a prime p we denote by $\mathrm{ord}_p\, m$ the greatest nonnegative rational integer f such that $m \equiv 0 \pmod{p^f}$.

Lemma. *Let α, β be integers of a quadratic field K such that $\alpha = \pm\beta^n$ for some $n>1$ in Z. We write $\alpha=(a+b\sqrt{d})/2$, $\beta=(s+t\sqrt{d})/2$ with a, b, s, t in Z, where d is the discriminant of K. If p is a prime dividing d such that $\mathrm{ord}_p\, a = \mathrm{ord}_p\, 2$, then we have*

$$\mathrm{ord}_p\, t = \mathrm{ord}_p\, b - \mathrm{ord}_p\, n$$

except in the following two cases: (i) $p=2$, $\mathrm{ord}_2\, d=2$ *and* $n \equiv 0 \pmod 2$, (ii) $p=3$, $d \equiv 6 \pmod 9$ *and* $n \equiv 0 \pmod 3$.

Proof. First assume that $\mathrm{ord}_p\, d = \mathrm{ord}_p(4p)$. Then $\mathrm{ord}_p\, a = \mathrm{ord}_p\, 2$ implies $\mathrm{ord}_p\, s = \mathrm{ord}_p\, 2$. If $5 \leqq k \leqq n$, we have $\mathrm{ord}_p \binom{n}{k} \geqq \mathrm{ord}_p\, n - \mathrm{ord}_p\, k \geqq \mathrm{ord}_p\, n + 1 - k/2$. Hence

$$b \equiv \pm nt(s/2)^{n-3}\{(s/2)^2+(n-1)(n-2)t^2d/24\} \pmod{p^{g+1}}$$

with $g=\mathrm{ord}_p(nt)$. Thus $\mathrm{ord}_p\, b = g$ holds except in the case (ii). Next let $p=2$, $\mathrm{ord}_2\, d=2$ and $(n,2)=1$. Then $\beta^2 \equiv 0$ or $1 \pmod 2$ according as $s/2 \equiv t$ or $t+1 \pmod 2$. Since $\mathrm{ord}_2\, a=1$, $\alpha \equiv \beta \pmod 2$ and $s/2 \equiv t+1 \equiv 1 \pmod 2$. Hence $b \equiv \pm nt(s/2)^{n-1} \pmod{2t}$. Thus the lemma follows.

Theorem. *Let n be a given natural number and let $k>1$ be a square free rational integer such that $k \equiv 0 \pmod p$ for any prime p dividing n. We put*

$$\varepsilon = (kn^2 \pm 2 + n\sqrt{m})/2 \quad \textit{with} \quad m = k(kn^2 \pm 4),$$

and assume that $kn^2 \pm 4 \neq c^2$, $2c^2$ for any c in Z and that $m \equiv 3 \pmod 9$ if 3 divides n. Then $\varepsilon>1$ is the fundamental unit of $K=Q(\sqrt{m})$.

Proof. It is easy to see that $\varepsilon>1$ is a unit of K with norm 1. We write $kn^2 \pm 4 = c^2u$ with c in Z and a square free rational integer $u>0$. From the assumption we have $u \geqq 3$. Since $(u,k)=1$ or 2, the discriminant d of K is ku if n is odd, and is $4ku$ if n is even. Note that

$d\equiv 3 \pmod 9$ if 3 divides n.

Now suppose that $\varepsilon=\eta^p$ for some unit $\eta=(s+t\sqrt{d})/2$ with s, t in Z and for some prime p. When p is odd, one sees $s>t\sqrt{d}>0$ and so $kn^2\pm 2>(t\sqrt{d})^p$. On the other hand, applying Lemma to ε, η and the primes dividing n, we get $t\equiv 0 \pmod n$ if $(n,p)=1$ and $t\equiv 0 \pmod{n/p}$ if $n\equiv 0 \pmod p$. In the case $n\equiv 0 \pmod p$, using $kn^2\geqq p^3$ we have

$$(t\sqrt{d})^p\geqq (kn^2)^{p/2}u^{p/2}p^{-p}\geqq kn^2(u^p p^{p-6})^{1/2}>2kn^2.$$

Here notice that $u\geqq 5$ if 3 divides n. It is obvious that $(t\sqrt{d})^p>kn^2u$ if $(n,p)=1$. Thus in both the cases we obtain $(t\sqrt{d})^p>kn^2\pm 2$, which is contrary to the above. When $p=2$, we derive from Lemma that $t^2d\equiv 0 \pmod{kn^2u}$ and $s^2t^2d\geqq (t^2d-1)t^2d>n^2m$. This is a contradiction. Thus the proof is complete.

Our result is similar to that of Morikawa [1]. A part of the units described as in Theorem have been considered in our previous paper [2] to find imaginary abelian fields whose relative class numbers are divisible by a given odd prime.

Proposition. *Let n' be a natural number and put $n=n'$ if n' is odd and $n=2n'$ if n' is even. For a rational integer $q>1$ and a divisor $e>0$ of q^n-1 we assume that* (i) $\mathrm{ord}_p\, e$ *is odd for every odd prime p dividing q^n-1,* (ii) $\mathrm{ord}_p\, e=1$ *for every odd prime p dividing n,* (iii) $e\equiv 2, 3 \pmod 4$ or $e\equiv 4 \pmod{16}$, (iv) $e\equiv 6 \pmod 9$ *if* 3 *divides n,* (v) $(2e-1,q)=1$, *and* (vi) $f=(q^n-1)/4e$ *is a natural number satisfying $f\equiv 0 \pmod p$ for every prime p dividing $2n$. Then the class number $h(K)$ of the real quadratic field $K=Q(\sqrt{m})$ is divisible by n' and any prime dividing q^n-1 is ramified in K, where*

$$m=\{1-2e+(q^n-1)/2\}^2-q^n.$$

Proof. We compute $m=4e\{e(f-1)^2-1\}$ and write $m=c^2d$, where c, d are natural numbers and d is square free. Then $d\equiv 2 \pmod 4$ if $e\equiv 2, 3 \pmod 4$ and $d\equiv 3 \pmod 4$ if $e\equiv 4 \pmod{16}$. Hence the discriminant of K is $4d$. From (i) we see that d is divisible by every odd prime dividing q^n-1. Thus the second assertion follows. Note that $4d\equiv m\equiv 3 \pmod 9$ if 3 divides n.

We define $a=2ef(f-1)-1$ and $b=2e(f-1)+1$. One sees by simple calculation that

$$\eta=(a+f\sqrt{m})/(b-\sqrt{m})=2e(f-1)^2-1+(f-1)\sqrt{m}$$

is a unit of K and $b^2-m=q^n$. From (v) we have $(b,q)=1$. This implies that $(a+f\sqrt{m})=(b-\sqrt{m})=I^n$ for some ideal I in K.

We now suppose that $h(K)$ is not divisible by p^k with $k=\mathrm{ord}_p\, n'$ for some prime p dividing n'. Then $a+f\sqrt{m}=\beta^{p'}\zeta$ holds with a unit ζ and an integer β of K, where $p'=p$ if $p>2$ and $p'=4$ if $p=2$. We denote by $\varepsilon=x+y\sqrt{d}>1$ the fundamental unit of K with x, y in Z. Then $\eta=\varepsilon^i$, $\zeta=\varepsilon^j$ for some i, $j>0$. First assume that p is odd. Then

(ii) and (vi) imply $e\equiv f\equiv 0 \pmod{p}$. Thus $a+f\sqrt{m}\equiv -1 \pmod{p}$ and $\beta^p\equiv v \pmod{p}$ for some v in Z, prime to p. So $\zeta\equiv -v \pmod{p}$. We derive from Lemma that if $(j,p)=1$ then $y\equiv 0 \pmod{p}$. However $\eta\equiv -(1+c\sqrt{d}) \pmod{p}$ and $(c,p)=1$. Hence p divides j. We can write $a+f\sqrt{m}=(s+t\sqrt{d})^p$ with s, t in Z. Since $a>f\sqrt{m}>0$, we see $s>t\sqrt{d}>0$ and $2a>(2t\sqrt{d})^p$. From (i) any prime divisor of ef divides d. Applying Lemma we get $t^2d\equiv 0 \pmod{4ef^2/p^2}$. Because $ef^2\geqq p^3$ it follows that

$$(2t\sqrt{d})^p\geqq 4^p e^{p/2} f^p p^{-p}>4ef^2>2a.$$

This is a contradiction. Next assume $p=2$. Let $g=2$ if $d\equiv 2 \pmod 4$ and $g=3$ if $d\equiv 3 \pmod 4$. By computation we can see that $\alpha^4\equiv 1 \pmod{2^g}$ for any integer α of K, prime to 2. Since $\mathrm{ord}_2 c=g-1$, $a+f\sqrt{m}\equiv\zeta\equiv -1 \pmod{2^g}$. When $(j,2)=1$, by Lemma one has $y\equiv 0 \pmod{2^g}$. But $\eta\not\equiv v \pmod{2^g}$ for any v in Z. Hence $\mathrm{ord}_2 j=1$ and so $\zeta\equiv\varepsilon^2\equiv -1 \pmod{2^g}$. The last congruence implies $(i,2)=1$. Using Lemma again we get $y\equiv 0 \pmod 2$. This shows $\varepsilon^2\not\equiv -1 \pmod 4$, which gives a contradiction. Consequently $h(K)$ is divisible by n'.

Let K_i $(i=1,\cdots,s)$ be a finite number of quadratic fields. To prove the theorem of Weinberger and Yamamoto, it suffices to find a real quadratic field, different from any K_i, with class number divisible by a given natural number n'. Take a prime l unramified in any K_i and a natural number r prime to $2n'$. Let q be a prime such that $q-1$ is divisible by l, r^3 and every odd prime dividing n', and further by 32 if n' is odd, by 8 if n' is even. Let n be as in Proposition. Then q^n-1 is divisible by l and by p^2 for any prime p dividing n'. Denote by e_1 the product of all distinct primes dividing q^n-1. If $e_1\not\equiv 3 \pmod 9$, we put $e_2=e_1$. When $e_1\equiv 3 \pmod 9$, let $e_2=2e_1$ if $e_1\equiv 2 \pmod 8$ and $e_2=e_1/2$ if $e_1\equiv 6 \pmod 8$. Since $(r^2-1, q)=1$, either $2e_2-1$ or $2e_2r^2-1$ is prime to q. Thus putting $e=e_2$ or e_2r^2 we get a divisor e of q^n-1 satisfying from (i) to (vi). By means of Proposition we find a real quadratic field K with $h(K)\equiv 0 \pmod{n'}$ such that l is ramified in K and hence $K\neq K_i$ for any i, $1\leqq i\leqq s$.

References

[1] R. Morikawa: On units of real quadratic number fields. J. Math. Soc. Japan, 31, 245–250 (1979).
[2] T. Uehara: On some congruences for generalized Bernoulli numbers. Rep. Fac. Sci. Engrg. Saga Univ. Math., 10, 1–8 (1982).
[3] P. J. Weinberger: Real quadratic fields with class numbers divisible by n. J. Number Theory, 5, 237–241 (1973).
[4] Y. Yamamoto: On unramified Galois extensions of quadratic number fields. Osaka J. Math., 7, 57–76 (1970).