TOKYO J. MATH.
VOL. 2, No. 2, 1979

Euclid's Algorithm in Pure Quartic Fields

Shigeki EGAMI

Keio University

(Communicated by T. Saito)

A finite algebraic number field K is said to be euclidean if, for any integers α and $\beta(\neq 0)$ of K, there is an integer γ of K such that $|N_K(\alpha-\beta\gamma)|<|N_K\beta|$. It is well-known that there are exactly 21 quadratic euclidean fields (see E. S. Bernes and H. P. F. Swinnerton-Dyer [1]). As for cubic fields H. Davenport [4] showed that there are only a finite number of euclidean fields which are not totally real. There are several finiteness theorems like this. H. Heilbronn [2], [3], showed that, if p is a prime then the number of cyclic euclidean fields of degree p is finite. H. Davenport [5] (cf. J. W. S. Cassels [6]) also proved the finiteness of the number of totally imaginary quartic euclidean fields.

In this paper we shall prove the following

THEOREM. *There exist only a finite number of quartic euclidean fields of the form $Q(\sqrt[4]{m})$, where m is a* 4th *power-free rational integer not expressible as* $2p^2$ *with a prime* $p\equiv 3 \pmod 8$.

In proving Theorem we can restrict our consideration to some special forms of quartic fields. Indeed for the fields $Q(\sqrt[4]{-m})$, where m is a positive integer, the finiteness follows from the result of Davenport mentioned above. Further C. J. Parry [7] proved that the class number of the field $Q(\sqrt[4]{m})$ with a positive integer m is even except those of the following forms

(I) $Q(\sqrt[4]{p})$ $p\equiv 5 \pmod 8$, $Q(\sqrt[4]{4p})$ $p\equiv 5 \pmod 8$,

(II) $Q(\sqrt[4]{p})$ $p\equiv 3 \pmod 8$, $Q(\sqrt[4]{2p})$ $p\equiv 3 \pmod 8$,
$Q(\sqrt[4]{4p})$ $p\equiv 3, 7 \pmod 8$, $Q(\sqrt[4]{8p})$ $p\equiv 3 \pmod 8$,

(III) $Q(\sqrt[4]{2p^2})$ $p\equiv 3 \pmod 8$, $Q(\sqrt[4]{2})$,

where p is a rational prime. Thus our theorem is reduced to the statement that the number of euclidean fields of the form (I) or (II) is finite, since an algebraic number field of class number greater than one is not

Received September 18, 1978
Revised September 1, 1979

euclidean. (As for the remaining case (III) the problem is still open. Our method, which is similar to that of Heilbronn [2], [3], can not be available for this case; see Remark of Lemma 2.)

For the proof we prepare two lemmas.

LEMMA 1. *If d is a sufficiently large positive integer of one of the following forms*

(i) $d=p$, $p\equiv 1 \pmod 4$,

(ii) $d=4p$ *or* $8p$, $p\equiv 3 \pmod 4$,

where p is a prime, then there exist two rational primes $q_1=q_1(d)$, $q_2=q_2(d)$ satisfying

$$\left(\frac{d}{q_1}\right)=\left(\frac{d}{q_2}\right)=-1\ ,$$

were $\left(\frac{d}{q}\right)$ denotes the Kronecker symbol, and

$$(1)\qquad \begin{aligned} &7\leqq q_1<q_2<p^{1/6}\ , \quad \text{if } d \text{ is of the form (i)}\ ,\\ &3\leqq q_1<q_2<p^{1/3}\ , \quad \text{if } d \text{ is of the form (ii)}\ . \end{aligned}$$

To prove this lemma we need an estimate for character sums obtained by D. A. Burgess [8]: For any $\varepsilon>0$ there exists a $\delta>0$ such that if χ is a non-principal character to a (sufficiently large) prime modulus p, and if H is an integer satisfying $H>p^{1/4+\varepsilon}$, then

$$(2)\qquad \left|\sum_{m=N+1}^{N+H}\chi(m)\right|<Hp^{-\delta}$$

for every N.

PROOF OF LEMMA 1. Let d be of the form (i). Then the Kronecker symbol is a non-principal character $\chi(n)$ modulo p. Assume that the number of primes l satisfying $\chi(l)=-1$ and $7\leqq l<p^{1/6}$ is at most one. Put

$$x=p^{1/4+0.01},\ R=R(p)=\prod_{q<p^{1/6},\,\chi(q)=-1} q\ .$$

Note that R is a product of at most 2, 3, 5, and a prime l. First we observe

$$(3)\qquad \sum_{\substack{(n,R)=1\\ n\leqq x}}\chi(n)=\sum_{r\mid R}\mu(r)\sum_{\substack{r\mid n\\ n\leqq x}}\chi(n)=o(x)\ ,$$

where $\mu(r)$ denotes Mobius function. In fact for $r\leqq p^{0.005}$ we have by (2) with $\varepsilon=0.005$

$$\sum_{\substack{r|n \\ n\leq x}} \chi(n)=\chi(r)\sum_{n\leq x/r}\chi(n)=O(p^{1/4+0\cdot 01-\delta}) .$$

And for $r>p^{0\cdot 005}$,

$$\left|\sum_{\substack{r|n \\ n\leq x}} \chi(n)\right| \leqq \sum_{\substack{r|n \\ n\leq x}} 1=O(p^{1/4+0\cdot 005}) ,$$

which proves (3). On the other hand,

$$\begin{aligned}\sum_{\substack{(n,R)=1 \\ n\leq x}} \chi(n) &= \sum_{\substack{(n,R)=1 \\ n\leq x}} 1-2\sum_{\substack{(n,R)=1 \\ \chi(n)=-1 \\ n\leq x}} 1 \\ &=\sum_{r|R}\mu(r)\left[\frac{x}{r}\right]-2\sum_{\substack{p^{1/6}\leqq q<x \\ \chi(q)=-1 \\ q\nmid R}}\ \sum_{\substack{(n,R)=1 \\ q|n \\ n\leqq x}} 1\end{aligned}$$

since $p^{2/6}>p^{1/4+0\cdot 01}=x$ and $\chi(q)=1$ for every prime $q\nmid R$ less than $p^{1/6}$. Here

$$\sum_{\substack{(n,R)=1 \\ q|n \\ n\leqq x}} 1=\sum_{r|R}\mu(r)\frac{x}{qr}+O(1)$$

so that

$$\sum_{\substack{(n,R)=1 \\ n\leqq x}} \chi(n)=\left\{x+O(1)-2x\sum_{\substack{p^{1/6}\leqq q\leqq x \\ \chi(q)=-1 \\ q\nmid R}}\frac{1}{q}+O(\pi(x))\right\}\sum_{r|R}\frac{\mu(r)}{r}$$

where $\pi(x)$ denotes as usual the number of primes not exceeding x. Combining this with (3) we obtain

$$\sum_{\substack{p^{1/6}<q\leqq x \\ \chi(q)=-1 \\ q\nmid R}}\frac{1}{q}=\frac{1}{2}+o(1) \tag{4}$$

as $p\to\infty$ since

$$\begin{aligned}\sum_{r|R}\frac{\mu(r)}{r} &\geqq \prod_{q|R}\left(1-\frac{1}{q}\right) \\ &\geqq\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\end{aligned}$$

and

$$\pi(x)=O\left(\frac{x}{\log x}\right) .$$

But from Mertens' theorem

$$\sum_{q\leq x}\frac{1}{q}=\log\log x+C+O\Big(\frac{1}{\log x}\Big)\,,$$

where C is an absolute constant, we have

$$\sum_{p^{1/6}\leq q\leq x}\frac{1}{q}=\log\Big(\frac{\log x}{\log p^{1/6}}\Big)+o(1)$$
$$=\log 1.56+o(1)=0.44\cdots+o(1)\,;$$

which contradicts to (4).

For d of the form (ii) the proof is similar but easier. In this case we can do in place of Burgess' estimate with the weaker one obtained by Polya and Vinogradov;

$$\sum_{m=N+1}^{N+H}\chi(m)=O(\sqrt{M}\log M) \tag{5}$$

where N, H are arbitrary integers and χ is a non-principal character to a (not nesessary prime) modulus M.

Next we give a criterion for non-euclidean fields.

LEMMA 2. *Let K be an algebraic number field of degree n. If there exist a rational prime p which is totally ramified in K and positive integers a, b with $a+b=p$ such that a is a nth power residue* mod p *and both a and $-b$ are not norms of integers of K, then K is not euclidean.*

PROOF. Suppose that K is euclidean. Since the ring of all integers in K is a principal ideal domain, there is a prime π of K such that $(p)=(\pi)^n$. Choose a rational integer u satisfying

$$u^n\equiv a \pmod p\,. \tag{6}$$

Applying the euclidean algorithm in K to u and π, we have

$$u\equiv\alpha \pmod \pi\,,\qquad |N_K\alpha|<|N_K\pi| \tag{7}$$

for some integer α of K. Let $\bar{K}$ be the Galois closure of K over Q, and denote by φ an arbitrary conjugate map of K into $\bar{K}$, and by $(\bar{\beta})$ a principal ideal of $\bar{K}$ generated by β. $(\bar{\pi})^n=(\bar{p})=(\overline{\varphi(\pi)})^n$, so that $(\bar{\pi})=(\overline{\varphi(\pi)})$, we have $u\equiv\varphi(\alpha)$ (mod $(\bar{\pi})$) in $\bar{K}$. Multiplying over all the conjugate maps φ, we get $u^n\equiv\prod_\varphi\varphi(\alpha)=N_K\alpha(\text{mod }(\bar{\pi}))$, so that $u^n\equiv N_K\alpha(\text{mod }p)$. Hence we have by (6) $N_K\alpha=a+rp$ for some rational integer r. It follows therefore from (7) that $|a+rp|=|N_K\alpha|<|N_K\pi|=p$. Hence r must be 0 or -1, which yields $a=N_K\alpha$ or $-b=N_K\alpha$; a contradiction.

REMARK. Lemma 2 is not applicable to a field of the form (III), since 2 is the only rational prime which is totally ramified in K/Q.

PROOF OF THEOREM. As have already pointed out we can restrict our argument to the fields of the form (I) and (II). Our proof is to give a decomposition $p=a+b$ in Lemma 2 for all sufficiently large p.

We consider first the case (II). But to avoid the complexities of notations we shall prove here the finiteness only for the fields of the form $Q(\sqrt[4]{p})$, $p\equiv 3 (\mathrm{mod}\, 8)$. The following arguments are also valid for the remaining cases in (II).

Now according to Lemma 1, there exist two primes q_1, q_2 satisfying

$$\left(\frac{4p}{q_1}\right)=\left(\frac{4p}{q_2}\right)=-1\,, \qquad 3\leqq q_1<q_2<p^{1/3}\,,$$

for sufficiently large p. Choose rational integers s, t such that

$$p=sq_1+tq_2\,, \qquad 0<t<q_1 \tag{8}$$

so that $s>0$ since $tq_2<p^{2/3}$. If $(q_1, s)=1$, sq_1 is not a norm of an ideal of K, since q_1 is not a norm of an ideal of the quadratic subfield $Q(\sqrt{p})$ of K. Similarly for tq_2. Otherwise i.e., $(q_1, s)\neq 1$, we write

$$p=s'q_1+t'q_2 \tag{9}$$

where $s'=s-tq_2$, $t'=t(q_1+1)$. Then $s'q_1$, $t'q_2$ are positive since $0<t'q_2<q_1^2q_2<p$. Furthermore $(q_1, s')=(q_1, s-q_2t)=1$ and $(q_2, t')=(q_2, t(q_1+1))=1$ since $q_1\neq 2$, and so both $s'q_1$ and $t'q_2$ are not norms of ideals of K as in the previous case. Thus we have a decomposition $p=a+b$ defined by (8) or (9). In order to apply Lemma 2 we have only to show that either a or b is a 4th power residue mod p. But this follows immediately from the relations

$$\left(\frac{a}{p}\right)=\left(\frac{-b}{p}\right)=(-1)^{(p-1)/2}\left(\frac{b}{p}\right)$$

and $p\equiv 3 (\mathrm{mod}\, 4)$. Therefore K is not euclidean.

Now let K be a field of the form (I) with p sufficiently large. According to Lemma 1, there exist two primes q_1, q_2 satisfying

$$\left(\frac{p}{q_1}\right)=\left(\frac{p}{q_2}\right)=-1\,, \qquad 7\leqq q_1<q_2<p^{1/6}\,.$$

Choose positive integers s, t such that $p=sq_1+tq_2$, $0<t<q_1$. Let S denote the set of all the non-negative integers n not exceeding $x=(p/q_1q_2)-(t/q_1)$ such that $q_1(s-nq_2)$ is a 4th power residue $\bmod p$ and satisfying $(q_1, s-nq_2)=1$, $(q_2, t+nq_1)=1$. Since, as in the previous case, q_1, q_2 are not norms of ideals of K, p, $a=q_1(s-nq_2)$, and $b=q_2(t+nq_1)$ with $n\in S$ satisfy all the conditions required in Lemma 2. Therefore it is sufficient to show that S is not empty. It is easy to see that

$$|S|=\sum_{\substack{(q_1,s-nq_2)=1\\(q_2,t+nq_1)=1\\0\leqq n\leqq x}}\frac{1}{4}\sum_{\chi^4=1}\chi(q_1(s-nq_2))\ ,$$

where $|S|$ is the cardinality of S and $\sum_{\chi^4=1}$ denotes the sum ranging over all the characters $\bmod p$ of order 4. Thus

$$\begin{aligned}|S|&=\sum_{0\leqq n\leqq x}\frac{1}{4}\sum_{\chi^4=1}\chi(q_1(s-nq_2))\\&\quad-\sum_{\substack{q_1|s-nq_2\\ \text{or } q_2|t+nq_1\\0\leqq n\leqq x}}\frac{1}{4}\sum_{\chi^4=1}\chi(q_1(s-nq_2))\\&\geqq\frac{x}{4}-\frac{1}{4}\Big|\sum_{\substack{\chi^4=1\\ \chi\neq 1}}\sum_{0\leqq n\leqq x}\chi(q_1(s-nq_2))\Big|\\&\quad-\sum_{\substack{q_1|s-nq_2\\0\leqq n\leqq x}}1-\sum_{\substack{q_2|t+nq_1\\0\leqq n\leqq x}}1-O(1)\ .\end{aligned}$$

Noticing that $q_1\geqq 7$, $q_2\geqq 11$ and using Polya-Vinogradov's estimate (5), we obtain

$$\begin{aligned}|S|&\geqq x\Big(\frac{1}{4}-\frac{1}{7}-\frac{1}{11}\Big)-O(\sqrt{p}\log p)\\&\geqq\frac{5}{308}p^{2/3}-O(\sqrt{p}\log p)\end{aligned}$$

and hence $|S|>0$ if p is sufficiently large. This proves the theorem for the case (I).

References

[1] E. S. BERNES and H. P. F. SWINNERTON-DYER, The inhomogeneous minima of binary quadratic forms I, Acta Math., **87** (1952), 259-323.

[2] H. HEILBRONN, On Euclid's algorithm in cubic self conjugated fields, Math. Proc. Cambridge Philos. Soc., **46** (1950), 377-382.

[3] H. HEILBRONN, On Euclid's algorithm in cyclic fields, Canad. J. Math., **3** (1951), 257-268.

[4] H. DAVENPORT, Euclid's algorithm in cubic fields of negative discriminants, Acta Math., **84** (1950), 159-179.

[5] H. DAVENPORT, Euclid's algorithm in certain quartic fields, Trans. Amer. Math. Soc., **68** (1950), 508–532.

[6] J. W. S. CASSELS, The imhomogeneous minima of binary quadratic, ternary cubic and quarternary quartic forms, Math. Proc. Cambridge Philos. Soc., **48** (1952), 72–86.

[7] C. J. PARRY, Pure quartic fields whose class numbers are even, J. Reine Angew. Math., **272** (1975), 102–112.

[8] D. A. BURGESS, On character sums and primitive roots, Proc. London Math. Soc., **12** (1962), 179–192.

Present Address:
DEPARTMENT OF MATHEMATICS
KEIO UNIVERSITY
HIYOSHI-CHO, KOHOKU-KU
YOKOHAMA 223