Functiones et Approximatio
XXXVII.2 (2007), 337–340

EUCLIDEAN ALGORITHM IN SMALL ABELIAN FIELDS

Władysław Narkiewicz

To Jean-Marc Deshouillers
on his 60-th birthday

Abstract: It is shown that a small change in the argument of Harper and Murty implies that there are at most two real quadratic fields with class-number one and without Euclidean algorithm.

Keywords: Euclidean algorithm, real quadratic fields, Abelian cubic fields.

It has been proved by M.Harper ([H]) that if K is a real quadratic field of class-number one and discriminant not exceeding 100, then there is a Euclidean algorithm in K, i.e., K is Euclidean, and it has been established by M.Harper and M.Ram Murty ([HRM]) that the same happens if K is a normal extension of the rationals with class-number one and unit rank $\geqslant 4$. The aim of this note is to point out that a small modification of the arguments in these papers leads to the same assertion for real quadratic and normal cubic fields with at most two exceptions:

Theorem. (i) *If K is a real quadratic field with class-number one, then K is Euclidean, except for at most two fields.*

(ii) *If K is a normal cubic extensions of the rationals with class-number one, then K is Euclidean, except for at most one field.*

Note that a result of P.J.Weinberger ([W]) implies that the existence of exceptions in these theorems would contradict the General Riemann Hypothesis.

Proof. In [H] and [HRM] Dirichlet's theorem has been invoked at some point, however actually another result should be used here, which we state as a lemma. It is a simple consequence of Hecke's theorem on prime ideals in ideal classes.

Lemma 1. *Let K be an algebraic number field of class-number one, and let Z_K be its ring of integers. If $\alpha, \beta \in Z_K$ generate co-prime ideals, then denote by*

2000 Mathematics Subject Classification: primary: 11R11; secondary: 11R20, 13F07.

$\pi_{\alpha,\beta}(x)$ the number of principal prime ideals I of K with $N(I) \leqslant x$, which have a generator θ, satisfying $\theta \equiv \alpha \pmod{\beta}$. Then for x tending to infinity one has

$$\pi_{\alpha,\beta}(x) = \left(\frac{1}{h_f} + o(1)\right)\frac{x}{\log x},$$

where f is the ideal generated by β, and h_f is the class-number mod f.

Proof. Observe that the set of all ideals θZ_K with $\theta \equiv \alpha \pmod{\beta}$ forms an ideal class in the class-group mod βZ_K, and apply Hecke's theorem (see e.g. [N1], corollary 4 to proposition 7.17). ∎

Let B_0 be the unit group of K and denote for $n = 1, 2, \ldots$, following [H], by B_n be the set of all primes π of the ring Z_K of integers of K such that every non-zero residue class mod π contains an element of B_{n-1}. Denote by $B_n(x)$ the number of distinct ideals generated by elements of B_n, which have their norms bounded by x. Lemma 2 of [H] shows that if $B_1(x) \gg x/\log^2 x$, then K is Euclidean. The next lemma weakens slightly the assumption, without changing its proof:

Lemma 2. *If for a sequence $1 < x_1 < x_2 < \ldots$ tending to infinity one has*

$$B_1(x_n) \geqslant c\frac{x_n}{\log^2 x_n} \tag{1}$$

with a positive constant c, then K is Euclidean.

Proof. The sieve argument given in [H] (pp.62–63) shows that (1) implies

$$B_2(\sqrt{x_n}) = (1 + o(1))\frac{\sqrt{x_n}}{\log(\sqrt{x_n})}. \tag{2}$$

Indeed, assume that (1) holds, and put $y_n = \sqrt{x_n}$. Let A be the set of representatives of $B_1(x_n) = B_1(y_n^2)$,

$$Z = \#A = \#B_1(x_n) \gg \frac{x_n}{\log^2 x_n},$$

and let $\mathcal{P}$ be the set of prime ideals of norm $\leqslant y_n$ which do not lie in $B_2(y_n)$.

If now for $P \in \mathcal{P}$ we denote by $\omega(P)$ the number of residue classes mod P which do not contain elements of A, then Lemma 9.1 of [H] implies

$$\sum_{P\in\mathcal{P}} \frac{\omega(P)}{NP} \ll \log^2 y_n.$$

Denote by $f(P)$ the number of residue classes mod P containing units. Since $\omega(P) \geqslant f(P)$, we get

$$\log^2 y_n \gg \sum_{P\in\mathcal{P}} \frac{f(P)}{N(P)} \geqslant \sum_{\substack{P\in\mathcal{P}\\ f(P)>N(P)^{1/4}}} \frac{f(P)}{N(P)}$$

$$\geqslant \sum_{\substack{P\in\mathcal{P}\\ f(P)>N(P)^{1/4}}} \frac{1}{N(P)^{3/4}} \geqslant \frac{\#\{P \in \mathcal{P} :\ f(P) \geqslant N(P)^{1/4}\}}{y_n^{3/4}},$$

hence

$$\#\{P \in \mathcal{P}:\ f(P) \geqslant N(P)^{1/4}\} \leqslant y_n^{3/4} \log^2 y_n. \tag{3}$$

On the other hand the Gupta-Murty bound implies

$$\#\{P:\ f(P) \leqslant Y\} \ll Y^2,$$

hence in particular

$$\#\{P:\ N(P) \leqslant y_n,\ f(P) \leqslant N(P)^{1/4}\} \ll \sqrt{y_n}, \tag{4}$$

and from (3) and (4) we get

$$\#\{P \in \mathcal{P}:\ N(P) \leqslant y_n\} \ll y_n^{3/4} \log^2 y_n,$$

showing that

$$\#B_2(y_n) = (1 + o(1))\frac{y_n}{\log y_n}. \tag{5}$$

To show that (5) implies that all primes lie in B_3 we repeat the argument of [H]: were $\pi \notin B_3$, then a residue class $\bmod\ \pi$ would have no representative from B_2, and the application of Lemma 1 would lead for large n to

$$\#B_2(y_n) \leqslant (1 - \delta)\frac{y_n}{\log y_n},$$

with a certain $\delta > 0$, contradicting (5). Our Lemma follows now from Lemma 1 of [H].

It follows from Theorem III of [N] that if K is a real Abelian field and $a_1, a_2, a_3 \in K^*$ are multiplicatively independent, then for some $i \in \{1, 2, 3\}$ either a_i or $-a_i$ is a primitive root $\bmod\ P$ for infinitely many splitting prime ideals P. The proof given in [N] shows that if $A(x)$ denotes the number of such P's with $N(P) \leqslant x$, then for a sequence x_i tending to infinity one has

$$A(x_i) \gg x_i / \log^2 x_i. \tag{3}$$

Let now $K_i = Q(\sqrt{d_i})$ $(i = 1, 2, 3)$ be distinct real quadratic fields, and denote by ϵ_i the fundamental unit of K_i. Moreover let $K = K_1K_2K_3$, and let $U(K)$ be its group of units. Observe now that the numbers $\epsilon_1, \epsilon_2, \epsilon_3$ are multiplicatively independent, hence at least one of the units $\pm\epsilon_i$ $(i = 1, 2, 3)$, say $\eta \in K_s$ generates $U(K) \bmod\ P$ for a set Ω of splitting prime ideals P of K, with

$$\#\{P \in \Omega:\ N(P) \leqslant x_i\} \geqslant c\frac{x_i}{\log^2 x_i}$$

for a sequence x_i tending to infinity and a certain $c > 0$. Put $p = P \cap K_s$, and $\Omega^* = \{p\}$. Since the map

$$Z_{K_s}/p \longrightarrow Z_K/P$$

is an isomorphism, η generates the group of units of K_s modulo p, and because of $N(P) = N(p)$ we get from (3) the inequality

$$\#\{p \in \Omega^* : \ N(p) \leqslant x_i\} \gg x_i / \log^2 x_i.$$

Since the generators of ideals lying in Ω^* belong to B_1, the application of Lemma 2 shows that K_s is Euclidean. Therefore from every triplet of real quadratic fields with class-number one at least one is Euclidean, so the number of exceptions is at most two.

The same argument works also in the case if there would be two normal cubic, hence Abelian, extensions of the rationals having class-number one, but not being Euclidean. ■

References

[1] M. Harper, $\mathbf{Z}[\sqrt{14}]$ *is Euclidean*, Canad. Math. J., **56**, 2004, 55–70.

[2] M. Harper, M.Ram Murty, *Euclidean rings of algebraic integers*, Canad. Math. J., **56**, 2004, 71–76.

[3] W. Narkiewicz, *Units in residue classes*, Arch. Math., **51**, 1988, 238–241.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer 2004.

[5] P.J. Weinberger, *On Euclidean rings of algebraic integers*, Proc. Symposia Pure Math., **24**, 1972, 321–332.

Address: Institute of Mathematics, Wrocław University
E-mail: narkiew@math.uni.wroc.pl

Received: 13 December 2006; **revised:** 27 June 2007