manuscripta math. 83, 327 - 330 (1994)

manuscripta mathematica
©Springer-Verlag 1994

A QUADRATIC FIELD WHICH IS EUCLIDEAN BUT NOT NORM-EUCLIDEAN

DAVID A. CLARK

Institut für Experimentelle Mathematik
Universität GHS Essen
and
Brigham Young University

The classification of rings of algebraic integers which are Euclidean (not necessarily for the norm function) is a major unsolved problem. Assuming the Generalized Riemann Hypothesis, Weinberger [7] showed in 1973 that for algebraic number fields containing infinitely many units the ring of integers R is a Euclidean domain if and only if it is a principal ideal domain. Since there are principal ideal domains which are not norm-Euclidean, there should exist examples of rings of algebraic integers which are Euclidean but not norm-Euclidean. In this paper, we give the first example for quadratic fields, the ring of integers of $\mathbb{Q}(\sqrt{69})$.

Introduction

Let R be the ring of integers of an algebraic number field K. A Euclidean algorithm on R is a map $\phi : R \rightarrow \mathbb{N}$ such that $\phi(r) \neq 0$ for $r \neq 0$ and for all $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and $\phi(r) < \phi(b)$. If ϕ is completely multiplicative, namely $\phi(ab) = \phi(a)\phi(b)$, then ϕ can be

1991 *Mathematics Subject Classification.* Primary 11A05; Secondary 11R16.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

extended to a completely multiplicative function on K. Thus, the Euclidean property for •ompletely multiplicative Euclidean algorithms can be expressed as follows: for every $x \in K$ there is $\gamma \in R$ such that $\phi(x-\gamma) < 1$. The completely multiplicative Euclidean algorithm that has most often been studied in algebraic number fields is the absolute value of the norm. We will refer to such fields as being norm-Euclidean. It is easy to show that an integral domain equipped with a Euclidean algorithm is a principal ideal domain; therefore, we will consider only principal ideal domains.

In the Supplement XI to Dirichlet's *Vorlesungen über Zahlentheorie* [5], Dedekind showed that $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean for

$$d = -1, -2, -3, -7, -11, 2, 3, 5, 13.$$

In 1927 Dickson [4] claimed that this list of norm-Euclidean quadratic fields is complete. Perron [6] observed that Dickson's argument was valid only for imaginary quadratic fields. Perron gave additional examples. Over the next twenty years the quadratic fields which are Euclidean for the norm were completely characterized, namely for the additional values

$$d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

For references and a correction, see Barnes and Swinnerton-Dyer [1].

Weinberger [7] showed that, assuming the Generalized Riemann Hypothesis for Dedekind zeta functions, if the ring of integers of an algebraic number field contains infinitely many units, then the ring is Euclidean if and only if it is a principal ideal domain. Note that the algorithm need not be the absolute value of the norm. Since there are examples of such principal ideal domains which are not norm-Euclidean (see below), he showed, conjecturally, that there exist Euclidean fields which are not norm-Euclidean. In [2] and [3] the first examples of such fields were given. However, the method developed in these papers is restricted to totally real Galois extensions of $\mathbb{Q}$ of degree greater than or equal to three.

In this paper we verify that the ring of integers, $\mathbb{Z}[\alpha]$, of $\mathbb{Q}(\sqrt{69})$ is Euclidean, where $\alpha = (1+\sqrt{69})/2$. In the course of the proof, we will see that this ring is not norm-Euclidean. See also Barnes and Swinnerton-Dyer [1].

Lemma 1. *The only coprime residue classes modulo any element of $\mathbb{Z}[\alpha]$ which do not contain an element of smaller norm are $\pm(16+4\alpha)$ modulo $(10+3\alpha)$.*

Lemma 2. *The only coprime residue classes modulo any element of $\mathbb{Z}[\alpha]$ which do not contain an element of smaller norm not divisible by $10+3\alpha$ are $\pm(16+4\alpha)$ modulo $(10+3\alpha)$.*

If we assume these two lemmas, then the proof that $\mathbb{Z}[\alpha]$ is Euclidean is almost immediate. Define a completely multiplicative Euclidean algorithm ϕ on the prime elements by

$$\phi(\pi) = \begin{cases} N(\pi), & \text{if } \pi \neq 10+3\alpha \\ 26, & \text{if } \pi = 10+3\alpha, \end{cases}$$

where N is the absolute value of the norm. Since $N(16+4\alpha) = 25$, Lemma 2 implies that every coprime residue class contains an element with lower ϕ-value. Hence, because ϕ is completely multiplicative, ϕ is a Euclidean algorithm.

Note that Lemma 2 implies that any integer greater than 25 could be used in place of 26 in the definition of ϕ.

Proofs of the Lemmas

To prove Lemma 1, we verified by computer that the fundamental domain of the lattice of integers of the field can be cut into small squares such that there is a translate of each small square by an element of the ring of integers with the norm less than 1 in the translate. We are left with two small squares containing the "bad" points mentioned in the lemma. Next, we use the method of "automorphs" (see Barnes and Swinnerton-Dyer [1]) to verify that there is only one bad point in each of the squares that remain. The method consists of multiplying the bad squares by units of the field and observing that this must map the set of actual bad points into itself. Multiplication of the bad squares increases the size of the squares, so a fixed point argument shows there is only one bad point in each of the squares.

Lemma 2 is a stronger result than Lemma 1. The proof is similar except that we must find (again using a computer) two translations of each small square such that the norm is less than one in each translate and the difference of the two integers used for the translations is not divisible by $10+3\alpha$. We are left with 3 small bad squares. Two contain the "bad" points mentioned in the lemma and a third contains the origin. The method of automorphs shows that there can be at most one bad point in each square. The possible "bad" point in the third square is 0, which certainly satisfies the condition of the lemma. To see that this proves the lemma, consider any coprime residue class a modulo an element b with $b \neq 10+3\alpha$. We have found two elements r_1, r_2 of $\mathbb{Z}[\alpha]$ such that $N(a/b+r_i) < 1$ for $i = 1, 2$. At least one of the elements $a + r_i b$ is not divisible by $10+3\alpha$, which proves the lemma.

Acknowledgements.
I would like to thank the referees of this and an earlier manuscript for their careful comments and criticisms.

References

1. E.S. Barnes and H.P.F. Swinnerton-Dyer, *The Inhomogeneous Minima of Binary Quadratic Forms*, Acta Math. **87** (1952), 259–323
2. D.A. Clark, *The Euclidean Algorithm for Galois Extensions of the Rational Numbers*, Ph.D. Thesis, McGill University, Montréal, 1992
3. D.A. Clark and M.R. Murty, *The Euclidean Algorithm in Galois Extensions of* $\mathbb{Q}$, (to appear)
4. L.E. Dickson, *Algebren und ihre Zahlentheorie*, Orell Füssli Verlag, Zürich und Leipzig, 1927
5. P.G. Lejeune Dirichlet (ed. R. Dedekind), *Vorlesungen über Zahlentheorie*, Vieweg, Braunschweig, 1893
6. O. Perron, *Quadratische Zahlkörpern mit Euklidischem Algorithmus*, Math. Ann. **107** (1932), 489–495
7. P. Weinberger, *On Euclidean Rings of Algebraic Integers*, Proc. Symp. Pure Math. **24** (1973), 321–332

Department of Mathematics, Brigham Young University, Provo,
Utah, 84602, USA

(Received October 26, 1993;
in revised form April 7, 1994)