MATHEMATICS OF COMPUTATION
Volume 65, Number 216
October 1996, Pages 1675–1679

NON-GALOIS CUBIC FIELDS WHICH ARE EUCLIDEAN BUT NOT NORM-EUCLIDEAN

DAVID A. CLARK

ABSTRACT. Weinberger in 1973 has shown that under the Generalized Riemann Hypothesis for Dedekind zeta functions, an algebraic number field with infinite unit group is Euclidean if and only if it is a principal ideal domain. Using a method recently introduced by us, we give two examples of cubic fields which are Euclidean but not norm–Euclidean.

Let R be the ring of integers of an algebraic number field K. A Euclidean algorithm on R is a map $\phi : R \to \mathbb{N}$ 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, that is, $\phi(ab) = \phi(a)\phi(b)$, then ϕ can be extended to a completely multiplicative function on K. The Euclidean property can be expressed as follows: for every $x \in K$ there is $\gamma \in R$ such that $\phi(x - \gamma) < 1$. The problem which has been studied most often is the determination of those number fields for which the absolute value of the norm is a Euclidean algorithm. We refer to this function simply as the norm and denote it by N. We call a field norm–Euclidean when the norm is a Euclidean algorithm for the field.

Weinberger [9] showed that, under the assumption of the Generalized Riemann Hypothesis for Dedekind zeta functions, if there are infinitely many units in R, then R is a Euclidean domain if and only if it is a principal ideal domain. The assumption of the Generalized Riemann Hypothesis was removed in [2] and [4] for totally real Galois extensions K of $\mathbb{Q}$ with degree greater than or equal to 3, with the requirement to find sufficiently many nonassociate prime elements $\pi_1, \dots, \pi_n$ of R such that the unit group of the ring of integers maps onto $(R/(\pi_1\pi_2 \cdots \pi_n)^2)^*$ via the reduction map. In [3], the ring of integers of $\mathbb{Q}(\sqrt{69})$ was shown to be Euclidean but not norm–Euclidean. This paper may be viewed as an extension of the ideas in [3] to cubic fields. We will show that the cubic fields with discriminants -327 and 1929 are Euclidean but not norm–Euclidean. Taylor [8] and Smith [7], respectively, showed that these fields are not norm–Euclidean.

We outline the method for defining our Euclidean algorithm. First, we determine the set B of elements modulo which there exists a coprime residue class which does not contain elements of smaller norm. Equivalently, we determine the elements x of K such that $\min_{\gamma \in R} N(x - \gamma) \geq 1$. Now we try to define a new completely multiplicative Euclidean algorithm on the ring of integers by setting it equal to the norm for primes not dividing elements of B and increasing the value at primes which do divide the elements of B.

Received by the editor February 18, 1994 and, in revised form, April 15, 1994, August 11, 1994, and February 22, 1995.

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

We consider the field of discriminant 1929 which is generated by a root α of the polynomial $x^3 - x^2 - 10x + 13$. The integral basis is the power basis, so the ring of integers is $\mathbb{Z}[\alpha]$. The elements $\varepsilon_1 = -3 + \alpha$ and $\varepsilon_2 = 5 - 5\alpha + \alpha^2$ are a pair of fundamental units of the field.

Lemma 1. *The only coprime residue classes of* $\mathbb{Z}[\alpha]$ *that do not contain any elements which have norm smaller than the norm of the modulus and which are not divisible by* $9 - \alpha^2$ *are* $\pm(6 - 3\alpha + \alpha^2)$ *modulo the ideal* $(-4 + \alpha)$.

Assuming the lemma, we can carry out the details of the outline mentioned above. The element $-4 + \alpha$ has norm 21 and is divisible by $9 - \alpha^2$ of norm 7. The residue class $6 - 3\alpha + \alpha^2$ modulo $-4 + \alpha$ contains the element $6 - 7\alpha + 2\alpha^2$ of norm 21 but contains no element of smaller norm. This shows that K is not norm–Euclidean. Define a completely multiplicative function ϕ on the prime elements π of $\mathbb{Z}[\alpha]$ by

$$\phi(\pi) = \begin{cases} 8 & \text{if } \pi \text{ is associate to } 9 - \alpha^2, \\ N(\pi) & \text{otherwise.} \end{cases}$$

Lemma 1 implies that every coprime residue class modulo any element of $\mathbb{Z}[\alpha]$ contains an element with smaller ϕ-value than the ϕ-value of the modulus. In particular, $\phi(-4 + \alpha) = 24$ and $\phi(6 - 7\alpha + 2\alpha^2) = 21$. In addition, $\phi(0) = 0$ and $\phi(u) = 1$ for u a unit. Hence, because ϕ is completely multiplicative, ϕ is a Euclidean algorithm.

Note that any integer greater than 7 could be used in place of 8 in the definition of ϕ. One of the referees states that Lenstra [6, p. 28] suggested this sort of function as a possible Euclidean algorithm in number fields.

Proof of Lemma 1. We consider R as a lattice in $\mathbb{R}^3$ under the embedding which sends $x + y\alpha + z\alpha^2$ to (x, y, z). This lattice has a fundamental domain consisting of (x_1, x_2, x_3) with $-1/2 < x_i \leq 1/2$. We call a point $x = a/b$, with $a, b \in \mathbb{Z}[\alpha]$, in the fundamental domain of the lattice of integers of the field "bad" if there exists no $\gamma \in \mathbb{Z}[\alpha]$ such that $N(x - \gamma) < 1$ and $9 - \alpha^2$ does not divide $a - b\gamma$. We verified by computer that the fundamental domain of the lattice of integers of the field can be cut into small cubes for which there are two integer translates of the small cubes such that the norm is less than one inside both of the translates of the cube and such that $9 - \alpha^2$ does not divide the difference of the integers by which the cubes are translated (with the exceptions noted below). If x is not one of the exceptional points and γ_1 and γ_2 are the two integer translates, then at least one of $a - b\gamma_1$ and $a - b\gamma_2$ is not divisible by $9 - \alpha^2$.

To make the verification, upper and lower bounds for the norm are computed in each small cube and its translates. The bounds can be given more generally for a ternary form $T(x, y, z) = \sum_\nu a_\nu x^{\nu_1} y^{\nu_2} z^{\nu_3}$, with multi-index $\nu = (\nu_1, \nu_2, \nu_3)$, by bounding each term separately in the sum defining $T(x, y, z)$.

These bounds are very poor for large values of x, y, z. Another way to give bounds on $T(x, y, z)$ is to check that the first partial derivatives of T are not equal to zero within the small cube. The method of the previous paragraph can be used for this verification. The upper and lower bounds of T then occur at vertices of the cube.

In the computer program, the fundamental domain was cut into cubes of side-length 1/20. The bounds for the norm were checked for translates of the cube by $(n_1, n_2, n_3) \in \mathbb{Z}^3$ with $-2 \le n_i \le 2$. If the norm could not be bounded less than 0.999 in two of the integer translates, the cube was cut into smaller cubes of sidelength 1/200. The bounds for the norm were then checked for translates of the cube with $-20 \le n_i \le 20$. The division of the cube stopped at sidelength 5×10^{-6} and translates with $-50 \le n_i \le 50$. The program was written in Fortran and took approximately 22 hours of CPU–time on an HP9000-712.

There are five small regions of the fundamental domain of the lattice of integers in which the two desired integer translates were not found; namely, R_1

$$\begin{gathered} -0.005 \le x \le 0.005 \\ -0.005 \le y \le 0.005 \\ -0.005 \le z \le 0.005, \end{gathered}$$

R_2,

$$\begin{gathered} -0.05 \le x \le -0.045 \\ 0.425 \le y \le 0.43 \\ 0.475 \le z \le 0.48, \end{gathered}$$

R_3,

$$\begin{gathered} 0.33 \le x \le 0.335 \\ -0.005 \le y \le 0.005 \\ -0.335 \le z \le -0.33, \end{gathered}$$

and the images of these regions under multiplication by -1.

To determine the bad points in R_2, we use a method similar to the one in Barnes and Swinnerton-Dyer [1]. As observed above, there is at least one bad point, $(-6+3\alpha-\alpha^2)/(-4+\alpha)$ in this region. Embed the field into the real numbers by sending α to the root which is approximately 1.36922. Under this embedding the points $x + y\alpha + z\alpha^2$ in R_2 satisfy the inequality

$$1.403 \le x + y\alpha + z\alpha^2 \le 1.466.$$

If the elements of R_2 are multiplied by the unit ε_1, then one can check that the only integer translate of the five regions found above which intersects the image $\varepsilon_1 R_2$ is the translate of R_2 by $-6+3\alpha-\alpha^2$. Suppose that the best bounds on the set B of bad points in R_2 under the embedding into the real numbers are

$$\lambda_1 \le x + y\alpha + z\alpha^2 \le \lambda_2.$$

The image of B under multiplication by ε_1 (which is negative under the embedding) must satisfy the translate of this inequality, so

$$-6+3\alpha-\alpha^2+\lambda_1 \le \varepsilon_1\lambda_2 \le \varepsilon_1\lambda_1 \le -6+3\alpha-\alpha^2+\lambda_2.$$

This yields

$$-6+3\alpha-\alpha^2 \le \varepsilon_1\lambda_2-\lambda_1 \le \varepsilon_1\lambda_1-\lambda_2 \le -6+3\alpha-\alpha^2$$

since $\varepsilon_1 + 1$ is also negative under the embedding. Thus,

$$\lambda_1 = \lambda_2 = \frac{-6+3\alpha-\alpha^2}{-4+\alpha}.$$

In the same way one can show that the only possible bad point in R_3 is

$$\lambda = \frac{-4+3\alpha}{1-\alpha}.$$

Since $\lambda - \alpha = (-4+2\alpha+\alpha^2)/(1-\alpha)$ has norm less than one and $-4+2\alpha+\alpha^2$ is not divisible by $9-\alpha^2$, this point is not bad. One can also show that the only bad point in R_1 is 0.

Thus, each coprime residue class, except those mentioned in the lemma, contains an integer translate not divisible by $9-\alpha^2$ with norm less than the modulus, which proves the lemma.

Another example. Now we consider the cubic field K with discriminant -327. This field is generated by a root β of the polynomial x^3+x^2-2x+3 and has fundamental unit $\varepsilon = 1-2\beta-\beta^2$ which is positive under the only embedding of the field into the real numbers. The ring of integers is $\mathbb{Z}[\beta]$.

Lemma 2. *The only coprime residue classes modulo any element of* $\mathbb{Z}[\beta]$ *which do not contain any elements of smaller norm and which are not divisible by* $\varepsilon+1$ *are* $\pm(2\varepsilon-3)$ *and* $\pm(3\varepsilon-2)$ *modulo the ideal* (ε^2-1).

Note that ε^2-1 has norm 99 and $\varepsilon+1$ has norm 11. The proof of this lemma is omitted since it is similar to that given for Lemma 1. The proof that this field is Euclidean now follows the proof given above for the field with discriminant 1929.

Using the methods of this paper, Lemmermeyer [5] has shown that the complex cubic fields with discriminants –199 and –351 are Euclidean.

Real cubic norm-Euclidean fields. Using a method similar to that described in the proof of Lemma 1, the author found 31 new examples of real cubic fields which are norm–Euclidean. The fields have discriminants 2024, 2057, 2089, 2101, 2177, 2213, 2228, 2241, 2292, 2296, 2300, 2429, 2505, 2557, 2589, 2636, 2673, 2677, 2700, 2708, 2713, 2804, 2808, 2917, 2920, 3124, 3132, 3144, 3221, 3229, 3261. In addition, the author has shown that the real cubic fields with discriminants 2597, 2777, 2836, 2857, 3305, and 3889 are not norm–Euclidean.

Independently, Lemmermeyer [5] has determined all of the real cubic norm–Euclidean fields with discriminant less than 4692 and has found several other examples with larger discriminants.

Acknowledgements

I would like to thank the referee for his helpful comments and for pointing out an error in the program used for verifying Lemma 1.

References

1. E.S. Barnes and H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms*, Acta Math. **87** (1952), 259–323. MR **14:**730a
2. D.A. Clark, *The Euclidean algorithm for Galois extensions of the rational numbers*, McGill University, Montréal, 1992.
3. ———, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math. **83** (1994), 327–330. MR **95f:**11086
4. D.A. Clark and M.R. Murty, *The Euclidean algorithm in Galois extensions of* $\mathbb{Q}$, J. Reine Angew. Math. **459** (1995), 151–162. CMP 95:09
5. F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Exposition. Math. **13** (1995), 385–416. CMP 96:04
6. H.W. Lenstra, *Lectures on Euclidean rings*, Bielefeld, 1974.

7. J.R. Smith, *The inhomogeneous minima of some totally real cubic fields*, Computers in Number Theory (A.O.L. Atkin and B.J. Birch, eds.), Academic Press, New York, 1971, pp. 223–224.

8. E.M. Taylor, *Euclid's algorithm in cubic fields with complex conjugates*, J. London Math. Soc. **14** (1976), 49–54. MR **54:**7420

9. P. Weinberger, *On Euclidean rings of algebraic integers*, Proc. Symp. Pure Math. **24** (1973), 321–332. MR **49:**2671

Department of Mathematics, Brigham Young University, Provo, Utah 84602
E-mail address: clark@math.byu.edu