MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 201
JANUARY 1993, PAGES 421–423

ON THE EUCLIDEAN NATURE OF FOUR CYCLIC CUBIC FIELDS

H. J. GODWIN AND J. R. SMITH

ABSTRACT. It is shown that the cyclic cubic fields with discriminants 103^2, 109^2, 127^2, and 157^2 are Euclidean

1. INTRODUCTION

If a cyclic cubic field is Euclidean, then it necessarily has class number one, and so its discriminant is either 81 or d^2, where d (here and below) denotes a prime such that $d \equiv 1 \pmod 6$. Over the years it has been established that only finitely many d are possible (Heilbronn [2]), that d cannot lie between 157 and 10000 (Smith [5]), and that the only uncertain values of d below 10000 are 103, 109, 127, and 157 (Smith [5]). In the present paper we show that these last four values do in fact give Euclidean fields.

2. NOTATION

We can represent d uniquely as $(v^2 + 27w^2)/4$ with $v \equiv 2 \pmod 3$ and $w > 0$. It is easy to verify that $r = (d-1)/3$, $s = (vd - 3d + 1)/27$, $t = -(v + 3w + 4)/6$, and $u = (v + 2 + 9w - 4d)/18$ are all rational integers. The field can be defined by the equation $x^3 - x^2 - rx - s = 0$ and, if θ is one root, the others are $\varphi = (\theta^2 + t\theta + u)/w$ and $\psi = (\varphi^2 + t\varphi + u)/w$. An integral basis for the field is $(1, \theta, \varphi)$.

Let $x_1 = a + b\theta + c\varphi$, $y_1 = a + b\varphi + c\psi$, $z_1 = a + b\psi + c\theta$, with a, b, c rational integers; we denote the region $|(x - x_1)(y - y_1)(z - z_1)| \le K$ by $H(a, b, c)$, where K is some real number. If we can cover a fundamental region of the lattice of integers of the field by regions $H(a, b, c)$, with $K < 1$, then the field is Euclidean. Since the lattice may be reflected in the origin, and the values θ, φ, and ψ may be permuted cyclically without altering the lattice, it is in fact sufficient to cover one-sixth of the fundamental region, and we chose to cover $0 \le \alpha, \beta, \gamma \le 1$, $\alpha + \beta \le 1$, $\gamma \le \beta$, where $x = \alpha + \beta\theta + \gamma\varphi$, etc.; we denote this region by S.

3. SCHEME OF CALCULATION

For brevity we call a rectangular parallelepiped, with faces parallel to the coordinate planes, a box, which can be divided into subboxes by planes parallel

Received by the editor October 8, 1991.
1991 *Mathematics Subject Classification.* Primary 11R16, 11Y40.

to the faces of the box. We embed S in a set of boxes with unit sides, checking that the volumes of the portions of S in each box add up to the correct total. We then deal with each box in turn. A list of useful sets (a, b, c) is started by taking $b = c = 0$ and a equal to one of the coordinates of a vertex of the box. If the box is not covered by any $H(a, b, c)$ on the list, the box is subdivided by choosing the number of subdivisions of each coordinate, and the subboxes dealt with in turn (having first checked that the subbox lies wholly or partly in S). If we still fail to get a covering, a search is made for suitable centers a, b, c by spiralling outwards from the origin in the b, c plane, up to a specified bound on $|b|, |c|$. If a center is found that covers a subbox, $H(a, b, c)$ is added to the list and used for later subboxes. If only a portion of the unit cube is covered after a time, the process can be repeated with a box, smaller than the unit cube, containing the uncovered region.

It is undesirable for b and c to be too large, because of rounding errors, and so in some cases use was made of automorphic transformations. (See [1] for the use of these in connection with quadratic fields, and [3, 4, 5] for their use with cubic fields.) We multiply x, y, and z by the components of the fundamental unit of the field: this leaves the integral lattice unchanged and transforms a subbox σ into one with dimensions expanded in some directions and contracted in others. By a shift with integral values of the coordinates, this is equivalent to a congruent region in S, and if this has already been covered, then σ must be covered also.

The original intention was to run the program interactively on a VAX system and so the choices of subdivision could be made at the time. When covering took too long for the VAX, the work was completed in batch mode on a CYBER 840, which was faster and had a 48-bit mantissa. The CYBER was also used to check all the work.

To guard against round-off error, K was taken to be 0.9999, and the inequalities defining S were required to be satisfied with a difference of at least 10^{-4} (on the VAX) or 10^{-10} (on the CYBER).

In this way we have succeeded in covering with $K < 1$ in each case.

4. The difficulty with 157

The cases $d = 103, 109$, and 127 were dealt with fairly easily, but $d = 157$ required many hours of CYBER time before a covering was obtained, and we have tried to find a reason for this. There seem a priori to be two possibilities:

(i) that a slightly smaller value of K would be unable to produce a covering, and

(ii) that the size of at least one of the components of the fundamental unit is large, so that the subbox has to have at least one very small dimension before an automorphic transformation can be used.

We denote the lower bound of values of K that could provide a covering by $M(d)$ (this is the inhomogeneous minimum of the norm-form). From Heilbronn's method [2] we can find a lower bound for $M(d)$ as follows. Partition the cubic residues of d in $(1, d-1)$ into two sets: C^* consisting of residues that are the product of two coprime nonresidues, and C the remainder. If we can find p and $d - p \in C^*$, then the field is non-Euclidean. Otherwise, let p be the least member of C^* such that $d - p \in C$. Then $M(d) \geq (d-p)/d$. In many cases this bound is sharp, but not, for example, for $d = 73$.

For the four fields considered in this paper we find:

$$M(103) \geq 93/103 = 0.902\ldots, \qquad M(109) \geq 76/109 = 0.697\ldots,$$
$$M(127) \geq 94/127 = 0.740\ldots, \qquad M(157) \geq 118/157 = 0.751\ldots.$$

The components of the fundamental units of the four fields have the following approximate values:

103	40.957	−5.95	−0.0041
109	−1338.2	1.203	−0.00063
127	426.4	−115.4	−0.000020
157	−9142	0.000036	−3.01

We have been unable to improve the Heilbronn bound on $M(157)$, and so cannot support reason (i). Since 109 gave somewhat more difficulty than 103 and 127, reason (ii) appears to be the likely one, though we are still surprised at the extent to which the difficulty was magnified.

Bibliography

1. E. S. Barnes and H. P. F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms*, Acta Math. **87** (1952), 259–322.
2. H. Heilbronn, *On Euclid's algorithm in cubic self-conjugate fields*, Proc. Cambridge Philos. Soc. **46** (1950), 377–382.
3. P. A. Samet, *The product of non-homogeneous linear forms*. I, Proc. Cambridge Philos. Soc. **50** (1954), 372–379.
4. ____, *The product of non-homogeneous linear forms*. II, Proc. Cambridge Philos. Soc. **50** (1954), 380–390.
5. J. R. Smith, *On Euclid's algorithm in some cyclic cubic fields*, J. London Math. Soc. **44** (1969), 577–582.

Department of Computer Science, Royal Holloway and Bedford New College, Egham Hill, Egham, Surrey TW20 0EX, England

Department of Computing and Mathematics, Royal Naval Engineering College, Manadon, Plymouth, PL5 3AQ, England