MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 173
JANUARY 1986, PAGES 295–299

Use of a Computer Scan to Prove $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ and $\mathbf{Q}(\sqrt{3+\sqrt{2}})$ are Euclidean

By Harvey Cohn* and Jesse Deutsch

Abstract. The fields in the title are shown to be norm-Euclidean by a computer scan of the unit 4-cube representing coordinates of a field element translated by integers. The method is to subdivide this cube into sufficiently many small boxes so the norm is less than unity in each box, when referred to an appropriate "neighboring" integer.

Let K be a number field, $N_{\mathbf{Q}}^{K}$ the norm from K to $\mathbf{Q}$, and $\mathcal{O}_K$ the algebraic integers in K. Then K is a Euclidean field for the norm if for all $\alpha \in K$ there exists $\xi \in \mathcal{O}_K$ such that for some constant δ,

$$\left|N_{\mathbf{Q}}^{K}(\xi - \alpha)\right| \leqslant \delta < 1.$$

A computer scan is used to demonstrate that $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ and $\mathbf{Q}(\sqrt{3+\sqrt{2}})$ are Euclidean for the norm. Lenstra's tables (see [6] and [7]) show that there are just nine known totally real Euclidean fields of degree four over $\mathbf{Q}$, while Godwin (see [4] and [5]) provides the proof. The two fields of the title were not previously known to be Euclidean for the norm. Apparently, totally real fields are somewhat more difficult to prove to be Euclidean than those with some complex embeddings. For further information on Euclidean fields including tables of those known to have this property, see Lenstra ([6] and [7]).

For a fixed $\alpha \in K$ and a variable $\xi \in \mathcal{O}_K$, we define

$$M(\alpha) = \min\left|N_{\mathbf{Q}}^{K}(\xi - \alpha)\right|.$$

Then the Euclidean property of the field K is

$$M(\alpha) \leqslant \delta < 1.$$

Since the estimates found here might be of interest for other fields, we write the general α as

$$\alpha = a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}, \qquad a, b, c, d \in \mathbf{Q}.$$

We also use a special submodule of $\mathcal{O}$, namely $\mathcal{M}$, defined by

$$\xi = x + y\sqrt{m} + (z + w\sqrt{m})\sqrt{n + \sqrt{m}}, \qquad x, y, z, w \in \mathbf{Z}.$$

Here ξ is also written for convenience as (x, y, z, w). We can restrict $a, b, c, d \in [-\frac{1}{2}, \frac{1}{2}]$ because any other values can be reached by using ξ as a suitable "translation vector". It might have been hoped that $\xi = 0$ suffices (as in corresponding Euclidean cases such as $\mathbf{Q}(\sqrt{2})$ where $\alpha = a + b\sqrt{2}$). This is not the case here, and the translation vectors ξ required for α are of some intrinsic interest.

Received December 12, 1984.
1980 *Mathematics Subject Classification.* Primary 12A30, 12A50.
Key words and phrases. Euclidean algorithm.
*Research supported by NSF Grant MCS 82-01717 and PSC-CUNY Award 665266.

0025-5718/86 $1.00 + $.25 per page

The numerical evidence supports the following results:

CONJECTURE I. For $K = \mathbf{Q}(\sqrt{2+\sqrt{2}})$:

(a) $M(\alpha) \leqslant \frac{1}{2}$ and the only translation vectors ξ used are

$$0 = (0,0,0,0), \quad \pm 1 = (\pm 1,0,0,0), \quad \pm\sqrt{2} = (0,\pm 1,0,0),$$
$$\sqrt{2+\sqrt{2}} = (0,0,\pm 1,0), \qquad \pm\sqrt{2}\sqrt{2+\sqrt{2}} = (0,0,0,\pm 1).$$

(b) If $\alpha \neq \frac{1}{2}\sqrt{2}\cdot\sqrt{2+\sqrt{2}} + \xi$, $\xi \in \mathcal{O}_K$, then $M(\alpha) \leqslant \frac{1}{4}$.

(c) If α is not of the form $\frac{1}{2}\sqrt{2}\cdot\sqrt{2+\sqrt{2}} + \xi$, $\frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{2}\sqrt{2+\sqrt{2}} + \xi$, $\frac{1}{2}\sqrt{2} + \xi$, $\xi \in \mathcal{O}_K$, then $M(\alpha) < \frac{1}{4}$.

CONJECTURE II. For $K = \mathbf{Q}(\sqrt{3+\sqrt{2}})$:

(a) $M(\alpha) \leqslant \frac{1}{2}$ and here we use the larger set of translation vectors ξ, namely

$$0 = (0,0,0,0), \quad \pm 1 = (\pm 1,0,0,0), \quad \pm\sqrt{2} = (0,\pm 1,0,0),$$
$$\pm\sqrt{3+\sqrt{2}} = (0,0,\pm 1,0), \quad \pm\sqrt{2}\sqrt{3+\sqrt{2}} = (0,0,0,\pm 1)$$

and, in addition,

$$\pm 1 \pm \sqrt{2} = (\pm 1,\pm 1,0,0), \quad \pm 1 + \sqrt{3+\sqrt{2}} = (\pm 1,0,\pm 1,0),$$
$$\pm 1 \pm \sqrt{2}\sqrt{3+\sqrt{2}} = (\pm 1,0,0,\pm 1), \quad \pm\sqrt{2} \pm \sqrt{3+\sqrt{2}} = (0,\pm 1,\pm 1,0)$$
$$\pm\sqrt{2} \pm \sqrt{2}\sqrt{3+\sqrt{2}} = (0,\pm 1,0,\pm 1),$$
$$\pm\sqrt{3+\sqrt{2}} \pm \sqrt{2}\sqrt{3+\sqrt{2}} = (0,0,\pm 1,\pm 1),$$

a total of 33 vectors, using independent $\pm$ signs.

(b) If $\alpha \neq \frac{1}{2}\sqrt{2}(1+\sqrt{3+\sqrt{2}}) + \xi$, $\xi \in \mathcal{O}_K$, then $M(\alpha) \leqslant 7/16$.

(c) If α is not of the form $\frac{1}{2}\sqrt{2}(1+\sqrt{3+\sqrt{2}}) + \xi$, $\frac{1}{2} + \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{2}\sqrt{3+\sqrt{2}} + \xi$, $\xi \in \mathcal{O}_K$, then $M(\alpha) < 7/16$.

In both cases we have the computational result that $M(\alpha) \leqslant .99$ with sufficient accuracy to guarantee $M(\alpha) \leqslant \delta < 1$. A preliminary evaluation at a grid of points of the form

$$a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n+\sqrt{m}},$$

where $a, b, c, d \in \{-.5, -.4, \ldots, .4, .5\}$, seems to confirm parts (b) and (c) of the conjectures.

In proving the Euclidean character, we automatically demonstrate that the module $\mathcal{M}$ forms a unique factorization domain. Therefore $\mathcal{M} = \mathcal{O}_K$, the ring of integers in K (see Cohn [3]).

The idea is to cut the four-dimensional cube into subboxes and demonstrate that the norm is $\leqslant \delta < 1$ on each box or on some algebraic integer translate of each box. It would be most agreeable if the maximum norm for each box (by "convexity") would occur at the corners only. This is not true, so we must find suitable functions to majorize the norm so the maximum can be tested principally at the corners. If the bound is not verified on a particular subbox, we cut it into 16 equal size subboxes and attempt to verify the bound again. Define for $a, b, c, d \in \mathbf{Q}$

$$N(a,b,c,d) = N_{\mathbf{Q}}^{K}\left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n+\sqrt{m}}\right).$$

We put a bound for $|N|$ on each box by elementary inequalities only. Set $k = \mathbf{Q}(\sqrt{m})$ and note

$$\begin{aligned} N(a,b,c,d) &= N_{\mathbf{Q}}^{k} N_{k}^{K}\left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right) \\ &= N_{\mathbf{Q}}^{k}\left(a^2 + mb^2 - nc^2 - nmd^2 - 2ncd + \sqrt{m}\,(2ab - c^2 - 2ncd - md^2)\right) \\ &= L^2 - mR^2, \end{aligned}$$

where

$$L = a^2 + mb^2 - nc^2 - nmd^2 - 2mcd, \qquad R = 2ab - c^2 - 2ncd - md^2.$$

To find a bound for the minimum and maximum of N over the cube

$$[A_1, A_2] \times [B_1, B_2] \times [C_1, C_2] \times [D_1, D_2]$$

we will put upper and lower bounds on $a^2 + mb^2$, $2ab$, $nc^2 + nmd^2 + 2mcd$, $c^2 + 2ncd + md^2$ individually and then bring them together as follows: Suppose

$$M_1 \leqslant a^2 + mb^2 \leqslant M_2, \qquad M_3 \leqslant nc^2 + nmd^2 + 2mcd \leqslant M_4,$$

$$M_1 - M_4 \leqslant a^2 + mb^2 - nc^2 - nmd^2 - 2mcd \leqslant M_2 - M_3,$$

$$L^2 \leqslant \max\left((M_2 - M_3)^2, (M_1 - M_4)^2\right).$$

If $M_1 - M_4$ and $M_2 - M_3$ have opposite sign, then the minimum for L^2 is zero. Otherwise,

$$L^2 \geqslant \min\left((M_2 - M_3)^2, (M_1 - M_4)^2\right).$$

Bounds for R and N are obtained in a similar fashion.

We split $[-\frac{1}{2}, \frac{1}{2}]^4$ into subcubes of sidelength $1/q$, q even, so that $[A_1, A_2] \times [B_1, B_2]$ is contained in a single quadrant of the AB plane. Hence to obtain the maximum and minimum of $a^2 + mb^2$ and $2ab$ we just evaluate the corner points of $[A_1, A_2] \times [B_1, B_2]$ nearest to and furthest from the orgin.

Now consider the function

$$g(c,d) = c^2 + md^2 + 2ncd \quad \text{on } [C_1, C_2] \times [D_1, D_2],$$

$$\partial g/\partial c = 2c + 2nd, \qquad \partial g/\partial d = 2nc + 2md,$$

$$\Delta = \begin{vmatrix} 2 & 2n \\ 2n & 2m \end{vmatrix} = 4(m - n^2) \neq 0,$$

so the only extreme point not on the boundary is $(0,0)$. However, we have rigged the boundary so that $(0,0)$ must in fact be one of the four corners of our square in CD space if it is in this square. For maxima and minima on the boundary of the square fix $d = D_1$ or D_2. Then $\partial g/\partial c = 0$ implies $c = -nd$, but $(-nD_1, D_1)$, $(-nD_2, D_2)$ are corner points of $[C_1, C_2] \times [D_1, D_2]$ if they are in this box. Fix $c = C_1$ or C_2; then $\partial g/\partial d = 0$ implies $d = (-n/m)c$. Note $g(c, -nc/m) = c^2(1 - n^2/m)$. The points $(C_1, -nC_1/m)$, $(C_2, -nC_2/m)$ may be in $[C_1, C_2] \times [D_1, D_2]$ but are not necessarily corner points. Hence for $g(c,d)$ we must evaluate four corner points and at most two additional points.

A similar argument for $f(c,d) = nc^2 + 2mcd + nmd^2$ shows we must check the four corner points and the following if they are in the box;

$$(C_1, -C_1/n), (C_2, -C_2/n), (-mD_1/n, D_1), (-mD_2/n, D_2).$$

Note $f(c, -c/n) = c^2(n - m/n)$, $f(-md/n, d) = d^2(nm - m^2/n)$.

Another technique based on the same general idea of scanning subcubes is to use the inequality of arithmetic and geometric means,

$$|AB| \leqslant \tfrac{1}{2}(A^2 + B^2), \qquad A, B \in \mathbf{R}.$$

Let $K = \mathbf{Q}(\sqrt{n + \sqrt{m}})$, and $k = \mathbf{Q}(\sqrt{m})$; then

$$\begin{aligned} N(a,b,c,d) &= \prod_{\sigma \in \mathrm{Gal}(K/\mathbf{Q})} \left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right) \\ &= N_k^K\left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right) \\ &\quad \cdot N_k^K\left(a - b\sqrt{m} + (c - d\sqrt{m})\sqrt{n - \sqrt{m}}\right), \end{aligned}$$

$$\begin{aligned} &\left|N_k^K\left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right)\right| \\ &\quad = \left|\left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right)\left(a + b\sqrt{m} - (c + d\sqrt{m})\sqrt{n + \sqrt{m}}\right)\right| \\ &\quad \leqslant a^2 + mb^2 + nc^2 + nmd^2 + 2mcd + \sqrt{m}\,(2ab + 2ncd + c^2 + md^2). \end{aligned}$$

Similarly,

$$\begin{aligned} \left|N_k^K\left(a - b\sqrt{m} + (c - d\sqrt{m})\sqrt{n - \sqrt{m}}\right)\right| &\leqslant a^2 + mb^2 + nc^2 + nmd^2 + 2mcd \\ &\quad - \sqrt{m}\,(2ab + 2ncd + c^2 + md^2). \end{aligned}$$

Hence $|N| \leqslant L'^2 - mR'^2$, where

$$\begin{aligned} L' &= a^2 + mb^2 + nc^2 + nmd^2 + 2mcd, \\ R' &= 2ab + 2ncd + c^2 + md^2. \end{aligned}$$

Hence

$$\max|N| \leqslant \max L'^2 - m \min R'^2,$$

where the maxima and minima are taken over the box in question. As $\partial^2 L'/\partial a^2$, $\partial^2 L'/\partial b^2$, $\partial^2 L'/\partial c^2$, $\partial^2 L'/\partial d^2$ are greater than or equal to zero we conclude by convexity that the maximum of L' must occur at a corner of the four-dimensional box. Note $f(c,d)$ is positive semidefinite. The minimum for R' can be obtained in a fashion similar to the previous technique.

Our algorithm checked to see if a box of sidelength $1/10$ satisfied $|N| \leqslant \delta < 1$. If not, it was shifted by the translates listed in the conjectures to see if $|N| \leqslant \delta < 1$ on the translated box. Boxes that failed the initial pass were cut into cubes of sidelength $1/20$ and checked. The algorithm stopped at sidelength $1/80$ for both $\mathbf{Q}(\sqrt{2 + \sqrt{2}})$ and $\mathbf{Q}(\sqrt{3 + \sqrt{2}})$.

The programs used for proving $M(\alpha) \leqslant \delta < 1$ were written in the WATFIV variant of FORTRAN and run on an IBM 3081 and 3033. For $\mathbf{Q}(\sqrt{3 + \sqrt{2}})$ total run time was 12.9 seconds to prove $\delta = .99$ held as a bound. For $\mathbf{Q}(\sqrt{2 + \sqrt{2}})$ it took 1.28 seconds to show that all but one box of size $(1/20)^4$ satisfied $\delta = .99$. The exception was $[.45, .5] \times [.45, .5] \times [.45, .5] \times [.35, .4]$. Further calculations showed that the norm in the last case was less than .81. If the 33 translations similar to those in Conjecture II were used for the case $\mathbf{Q}(\sqrt{2 + \sqrt{2}})$, 1.62 seconds sufficed to demonstrate the bound $\delta = .99$ with boxes of size $(1/10)^4$.

The numerical evidence for the critical points of parts (b) and (c) of Conjectures I and II were produced by programs written in SNOBOL and run on the same computer system as the previous programs. For $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ the program took over 14 seconds and for $\mathbf{Q}(\sqrt{3+\sqrt{2}})$ it took almost 17 seconds to calculate the norms of

$$a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{n + \sqrt{m}}, \qquad a, b, c, d \in \{-.5, -.4, \ldots, .5\}.$$

Actually it is very easily verified that our fields have class number one by Minkowski bounds. It is more difficult to do this for the next maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_{2^t})$, namely

$$\hat{K} = \mathbf{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$$

(see Bauer [1]). Even so, numerical evidence (see Cohn [2]), however incomplete, seems to confirm the hypothesis that the sequence of fields $\mathbf{Q}(\cos(2\pi/2^t))$ has class number either equal to one or fantastically high. One expects the critical point for $\hat{K}$ analogous to Conjecture I(b) to be $\frac{1}{2}\sqrt{2}\cdot\sqrt{2+\sqrt{2}}\cdot\sqrt{2+\sqrt{2+\sqrt{2}}}$. Therefore, there is reason to believe other cyclotomic fields, particularly $\hat{K}$, may be Euclidean, but a corresponding scan seems to require a disproportionate effort in computer time and numerical analysis.

Department of Mathematics
City College (C.U.N.Y.)
New York, New York 10031

Mathematics Program
City University of New York
New York, New York 10036

1. H. Bauer, "Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper," *J. Number Theory*, v. 1, 1969, pp. 161–162.

2. H. Cohn, "A numerical study of Weber's real class number calculation I," *Numer. Math.*, v. 2, 1960, pp. 374–362.

3. H. Cohn, *A Classical Introduction to Algebraic Numbers and Class Fields*, Springer-Verlag, Berlin and New York, 1978, p. 9.

4. H. Godwin, "Real quartic fields with small discriminant," *J. London Math. Soc.*, v. 31, 1956, pp. 478–485.

5. H. Godwin, "On Euclid's algorithm in some quartic and quintic fields," *J. London Math. Soc.*, v. 40, 1965, pp. 699–704.

6. H. Lenstra, Jr., "Euclidean number fields of large degree," *Invent. Math.*, v. 38, 1977, pp. 237–254.

7. H. Lenstra, Jr., "Euclidean number fields 2," *Math. Intelligencer*, v. 2, 1980, pp. 73–83.

8. J. Masley, "Class numbers of real cyclic number fields with small conductor," *Compositio Math.*, v. 37, 1978, pp. 297–319.