MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 145
JANUARY 1979, PAGES 389–398

The Euclidean Condition in Pure Cubic and Complex Quartic Fields

By Vincent G. Cioffari

Abstract. In this paper we prove that a field $Q(\sqrt[3]{d})$ is euclidean with respect to the ordinary norm if and only if $d = 2$, 3 or 10. We also prove that certain fields of the form $Q(\sqrt[4]{-d})$, $d > 0$, are or are not euclidean.

The purpose of this research is to determine which pure cubic fields are euclidean with respect to the ordinary norm, and partially to determine the same for fields $Q(\sqrt[4]{-d})$, $d > 0$. More precisely, a field is said to be euclidean for the ordinary norm (just euclidean, for short) if its ring of integers R has the following property:

$$\forall a,\ b \in R \quad \exists p,\ r \in R \text{ s.t. } a = pb + r, \quad |N(r)| < |N(b)|.$$

We prove the following:

THEOREM A. *$Q(\sqrt[3]{d})$ is euclidean if and only if $d = 2$, 3 or 10.*

THEOREM B. *If $d = 2$, 3 or 7, then $Q(\sqrt[4]{-d})$ is euclidean. If $d \neq 12$, 44, 67 or the preceding values, and if neither d nor $2d$ is a perfect square, then $Q(\sqrt[4]{-d})$ is not euclidean, $d > 0$.*

Pure Cubic Fields

By a pure cubic field we mean a cubic field of the form $Q(\sqrt[3]{d})$, $d \in Z$. Any such field has one real embedding and a pair of conjugate complex embeddings and, hence, has one fundamental unit and negative discriminant. The three fields proven to be euclidean are the pure cubics of smallest discriminant (in absolute value).

Cassels [1] proved that a cubic field of negative discriminant D cannot be euclidean if $-D > 420^2 = 176{,}400$. This result reduces our problem to a finite number of cases, a number which is reduced much further by the necessity of unique factorization.

Notation. We consider fields $Q(\sqrt[3]{d})$: d will always be used in this context.
R: the ring of integers of $Q(\sqrt[3]{d})$,
ϵ: the fundamental unit of $Q(\sqrt[3]{d})$,
D: the discriminant of $Q(\sqrt[3]{d})$,
θ: $\sqrt[3]{d}$,
(b): the ideal bR, for $b \in Q(\sqrt[3]{d})$,
$N(b)$ (resp. $N(\mathfrak{p})$): the norm of the element b (resp. of the ideal $\mathfrak{p}$),
$\overline{b}(c)$: the residue class of b mod c, for $b,\ c \in R$.

Received June 14, 1977; revised December 2, 1977.
AMS (MOS) subject classifications (1970). Primary 12A30.

Latin letters refer to field elements and German letters to ideals. Note: in a field $Q(\sqrt[3]{d})$,

$$N(a + b\sqrt[3]{d} + c\sqrt[3]{d^2}) = a^3 + b^3d + c^3d^2 - 3abcd.$$

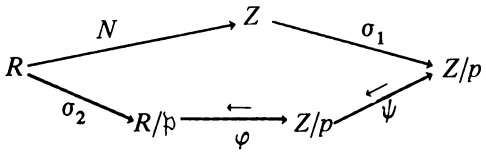
I. **Preliminary Results.**

(a) *Class Number.* We determine criteria for a field to have class number one, a necessary condition for the euclidean property.

The following lemma will be used again later to prove that certain fields are not euclidean.

LEMMA. *Let K be a field of odd prime degree q. Let p be a prime totally ramified in K, $p \not\equiv 1\ (q)$, and let $(p) = \mathfrak{p}^q$ denote the prime ideal factorization of (p). Let $u \in R$, the ring of integers of K. Then $u \equiv b \bmod \mathfrak{p}$, where b is the unique integer in the set $\{0, 1, \ldots, p-1\}$ such that $b^q \equiv N(u) \bmod p$.*

Proof.



In this diagram, σ_1 and σ_2 are the canonical maps; N is the norm map; φ is the map which associates to each class in $R/\mathfrak{p}$ the unique integer mod p which belongs to that class; ψ is the map which sends each element to its qth power. All the maps are multiplicative homomorphisms, and φ and ψ are isomorphisms.

To see that the diagram commutes, let $u \equiv c \bmod \mathfrak{p}$, where $c \in \{0, 1, \ldots, p-1\}$. Then $u - c \in \mathfrak{p}$, so by the Eisenstein criterion the characteristic polynomial of $u - c$ is of the form

$$x^q + d_{q-1}x^{q-1} + \cdots + d_1x + d_0, \quad p \mid d_i \qquad \forall i.$$

Hence, u satisfies the polynomial

$$(x-c)^q + d_{q-1}(x-c)^{q-1} + \cdots + d_1(x-c) + d_0,$$

so $N(u) \equiv c^q \bmod p$. Q.E.D.

PROPOSITION 1. *Let $K = Q(\sqrt[q]{r})$, with q an odd prime and r free of qth powers. If r is divisible by a prime congruent to 1 mod q, then $q \mid h(K)$.*

This well-known result follows from the lemma. We omit the details of the proof.

PROPOSITION 2. *Let K be a field of prime degree q with r fundamental units. If at least $r + 2$ primes are totally ramified in K, then $q \mid h(K)$.*

Proof. Let $\epsilon_1, \ldots, \epsilon_r$ be the fundamental units. Let $p_1, \ldots, p_{r+2}$ be totally ramified primes, and let $(p_i) = \mathfrak{p}_i^q$ denote their prime ideal factorizations. If q is totally ramified, let $p_1 = q$.

Suppose $h = 1$. Then $\forall i\ \exists b \in r$ s.t. $(b_i) = \mathfrak{p}_i$, and

$$b_i^q = p_i\epsilon_1^{k_{i1}} \cdots \epsilon_r^{k_{ir}}, \qquad i = 1, \ldots, r+2,\ k_{ij} \in Z.$$

It can be deduced that some qth power-free rational integer s, divisible by some p_i's but not by p_{r+2}, is a qth power in K. This implies that $K = Q(\sqrt[q]{s})$. We have a contradiction; hence, $h \neq 1$. It is easily deduced that $q|h$. Q.E.D.

There are forty-two fields satisfying Cassels' bound which are not excluded by these propositions. Consulting class number lists [2], we find that the following thirty-one actually have class number one: 2, 3, 5, 6, 10, 12, 17, 23, 29, 33, 41, 44, 45, 46, 53, 55, 59, 69, 71, 82, 99, 107, 116, 145, 179, 188, 197, 226, 332, 404 and 575.

(b) *Standard Form for d.* In view of Proposition 2, we will always assume d to be of one of the following forms:

(i) $d = p$, a prime,

(ii) $d = p_1p_2$, the product of two primes,

(iii) $d = p_1p_2^2$, $p_1 > p_2$.

Subject to these conditions, no two values of d generate the same field.

(c) *Basis and Discriminant.* We state without proof the following well-known results:

	Z-basis of R	D
$d \not\equiv \pm 1$ (9)		
$d = p$ or p_1p_2	$1, \theta, \theta^2$	$-27d^2$
$d = p_1p_2^2$	$1, \theta, \theta^2/p_2$	$-27p_1^2p_2^2$
$d \equiv \pm 1$ (9)		
$d = p$ or p_1p_2	$1, \theta, \frac{1 \pm \theta + \theta^2}{3}$	$-3d^2$
$d = p_1p_2^2$	$1, \theta, \frac{1 \pm \theta \pm \theta^2/p_2}{3}$	$-3p_1^2p_2^2$

(d) *Decomposition of Primes.* Any prime dividing d is totally ramified. The discriminant reveals that $(3) = \mathfrak{p}^3$ if $d \not\equiv \pm 1$ (9) and $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ if $d \equiv \pm 1$ (9).

All other primes are unramified. Using Hensel's lemma, if $p \equiv 2$ (3), then $(p) = \mathfrak{p}\mathfrak{p}'$, where $N(\mathfrak{p}) = p$ and $N(\mathfrak{p}') = p^2$; if $p \equiv 1$ (3), then (p) splits completely if d is a cubic residue mod p, and (p) remains prime otherwise.

II. Proving That Fields Are Not Euclidean.

(a) *Totally Ramified Primes.*

PROPOSITION 3. *Let p be a prime totally ramified in a field K of odd prime degree q, $p \not\equiv 1$ (q). If there exists a positive integer $e < p$ such that neither e nor $p - e$ is a norm from R, then K is not euclidean.*

Proof. Since $p \not\equiv 1$ (q), there exists a unique $c \in \{0, 1, \ldots, p-1\}$ such that $c^q \equiv e \bmod p$. Suppose there exists $u \in R$ such that $u \equiv c \bmod \mathfrak{p}$ and $|N(u)| < N(\mathfrak{p}) = p$. By the lemma in Section 1, $N(u) \equiv c^q \equiv e \bmod p$, so either $N(u) = e$ or $N(u) = -p + e$, and in the latter case, $N(-u) = p - e$. Thus, we have a contradiction.

Letting $b \in R$ be a generator of $\mathfrak{p}$, it follows that

$$\forall r \equiv c(b), \quad |N(r)| \geqslant |N(b)| = p.$$

Therefore, K is not euclidean. Q.E.D.

To find a suitable value of e, we must determine which rational primes generate prime ideals in R; this was done in Section I(d).

COROLLARY. *If* $d = 59, 71, 82, 107, 179, 197, 226, 332$ *or* 404, *then* $Q(\sqrt[3]{d})$ *is not euclidean.*

Proof. In the following list, we give values of e which satisfy the hypotheses of Proposition 3.

d	p	e	$p - e$
59	59	7	52
71	71	19	52
82	41	13	28
107	107	14	91
179	179	7	172
197	197	39	158
226	113	37	76
332	83	7	76
404	101	28	73

Q.E.D.

PROPOSITION 4. *Let* p_1 *and* p_2 *be totally ramified in a cubic field* K, $p_1 \not\equiv 1\ (3)$, $p_2 \not\equiv 1\ (3)$. *If there exists a positive integer* $e < p_1 p_2$ *such that neither* e *nor* $p_1 p_2 - e$ *are norms from* R, *then* K *is not euclidean.*

Proof. Let $(p_1) = \mathfrak{p}_1^3$, $(p_2) = \mathfrak{p}_2^3$; then $R/\mathfrak{p}_1\mathfrak{p}_2 \sim R/\mathfrak{p}_1 \times R/\mathfrak{p}_2 \sim Z/p_1 \times Z/p_2$. The proof then follows from Proposition 3; we omit the details. Q.E.D.

COROLLARY. *If* $d = 23, 29, 33, 41, 46, 69, 116, 145, 188$ *or* 575, *then* $Q(\sqrt[3]{d})$ *is not euclidean.*

Proof.

d	p_1	p_2	e	$p_1 p_2 - e$
23	3	23	13	56
29	3	29	26	61
33	3	11	7	26
41	3	41	19	104
46	2	23	7	39
69	3	23	26	43
116	2	29	21	37
145	5	29	26	119
188	2	47	37	57
575	5	23	37	78

Q.E.D.

PROPOSITION 5. *$Q(\sqrt[3]{53})$ is not euclidean.*

Proof. Let $\mathfrak{p}$ be the unique ideal of norm 53, and let $\mathfrak{q}$ be the unique ideal of norm 2. Let $u \in R$ be such that $u \equiv 1 \bmod \mathfrak{q}$ and $u \equiv -25 \bmod \mathfrak{p}$; then $N(u) \equiv (-25)^3 \equiv -10 \bmod 53$.

Suppose $|N(u)| < 106$; then $N(u) = -10, 43, -63$ or 96. But 43 and -63 are not norms from R, and any element of norm -10 or 96 is in $\mathfrak{q}$. Hence, $|N(u)| \geqslant 106$.

Let $(b) = \mathfrak{q}\mathfrak{p}$. We have proven that $a \equiv u \bmod b$ implies $|N(a)| \geqslant |N(b)| = 106$. Hence, $Q(\sqrt[3]{53})$ is not euclidean. Q.E.D.

(b) *Residue Classes* mod 2. If d is odd, then $\{0, 1, \theta, \theta^2, 1 + \theta, 1 + \theta^2, \theta + \theta^2, 1 + \theta + \theta^2\}$ is a complete set of residue class representatives mod 2. Elements congruent to 1, θ or θ^2 are of odd norm and other elements are of even norm.

PROPOSITION 6. *Assume d is in standard form as described in Section 1b. If $2 \nmid d$, $h = 1$ and if there exists a totally ramified odd prime p not equal to d, then $\epsilon \equiv 1$ (2) (for any choice of ϵ).*

Proof. As before, let $(p) = \mathfrak{p}^3$. Since $h = 1$, there exists an element $c \in R$ such that $(c) = \mathfrak{p}$; clearly, c can be chosen so that $c^3 = p\epsilon^n$, where $n = 0$, 1 or -1. Since $Q(\sqrt[3]{p}) \neq Q(\sqrt[3]{d})$, we have $n \neq 0$, and by choice of ϵ we can assume that $n = 1$.

Then $c^3 = p\epsilon \equiv \epsilon$ (2). Since c is of odd norm, $c \equiv 1$, θ or θ^2 (2). In any of these cases it follows that $\epsilon \equiv 1$ (2). Then $-\epsilon$, ϵ^{-1} and $-\epsilon^{-1}$ are all congruent to 1 mod 2 also. Q.E.D.

Letting p equal 3 or some prime dividing d, Proposition 6 applies when $d = 5$, 45, 55 or 99. Since $\epsilon \equiv 1$ (2), elements generating the same ideal belong to the same residue class mod 2. In the proof of Proposition 7, we will express this relation by saying that the ideal itself belongs to a particular residue class mod 2.

PROPOSITION 7. *$Q(\sqrt[3]{5})$, $Q(\sqrt[3]{45})$, $Q(\sqrt[3]{55})$ and $Q(\sqrt[3]{99})$ are not euclidean.*

Proof. $Q(\sqrt[3]{5})$ and $Q(\sqrt[3]{45})$.

We denote prime factorizations as follows: $(2) = \mathfrak{p}\mathfrak{p}'$, $N(\mathfrak{p}) = 2$, $N(\mathfrak{p}') = 4$, $(3) = \mathfrak{q}^3$, $(5) = \mathfrak{r}^3$. In both fields (7) is prime. Thus, there are six nonzero proper ideals of norm less than 8: $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{p}^2$, $\mathfrak{r}$ and $\mathfrak{q}\mathfrak{p}$. In $Q(\sqrt[3]{5})$, none of these ideals belongs to $\overline{\theta}$ (2); hence $a \equiv \theta$ (2) implies $|N(a)| \geqslant 8$, so $Q(\sqrt[3]{5})$ is not euclidean. In $Q(\sqrt[3]{45})$ none of the six ideals belongs to $\overline{1 + \theta}$ (2), so $Q(\sqrt[3]{45})$ is not euclidean either. Q.E.D.

The proofs for $Q(\sqrt[3]{55})$ and $Q(\sqrt[3]{99})$ are similar.

PROPOSITION 8. *$Q(\sqrt[3]{6})$ is not euclidean.*

Proof. The fundamental unit ϵ is $1 - 6\theta + 3\theta^2$, so $\epsilon \equiv 1 + \theta^2$ (2). Since $R = Z[\theta]$, the set $\{0, 1, \theta, \theta^2, 1 + \theta, 1 + \theta^2, \theta + \theta^2, 1 + \theta + \theta^2\}$ is a complete set of residue class representatives mod 2.

Every element of norm ± 2 is of the form $\pm(2 - \theta)\epsilon^n$, $n \in Z$, and, therefore, congruent to θ mod 2. Every element of norm ± 6 is of the form $\pm\theta\epsilon^n$, $n \in Z$, and, therefore, congruent to θ mod 2, also.

Suppose $a \equiv \theta + \theta^2$ (2). It is easily shown that $N(a) \equiv 2$ (4), and since $|N(a)| \neq 2$ or 6 it follows that $|N(a)| > N(2) = 8$. Therefore, $Q(\sqrt[3]{6})$ is not euclidean. Q.E.D.

(c) *Use of Absolute Values.* The methods of sections (a) and (b) fail to prove that $Q(\sqrt[3]{d})$ is not euclidean when $d = 12$, 17 or 44. For these cases, we use the following equivalent definition of the euclidean property:

$$\forall x \in Q(\sqrt[3]{d}) \quad \exists\, p \in R \text{ s.t. } |N(x+p)| < 1.$$

If $x_1, x_2 \in Q(\sqrt[3]{d})$ and $x_1 - x_2 \in R$, we say that $x_1 \equiv x_2 \bmod R$, or that x_1 is an R-translate of x_2. Thus, to prove that $Q(\sqrt[3]{d})$ is not euclidean, we must find a suitable element x and prove that no R-translate of x has norm less than 1 in absolute value. As stated in the following propositions, it is sufficient to test a finite number of R-translates of x.

TABLE

d	θ	φ	a	b	c
12	$\sqrt[3]{12}$	$\sqrt[3]{18}$	40	6	7
17	$\sqrt[3]{17}$	$\dfrac{1-\theta+\theta^2}{3}$	105	17	15
44	$\sqrt[3]{44}$	$\dfrac{-1+\theta+\theta^2/2}{3}$	230	31	15

PROPOSITION 9. *Let d, θ, φ, a, b and c be as in the table. Let $x \in Q(\sqrt[3]{d})$. Suppose that*

(i) $x\epsilon \equiv \pm x \bmod R$,

(ii) $\exists\, y \equiv x \bmod R$ *s.t.* $|N(y)| < 1$. *Then there exists* $z = r + s\theta + t\varphi$, $r, s, t \in Q$, *such that*

(iii) $z \equiv \pm x \bmod R$,

(iv) $|N(z)| < 1$,

(v) $|r| < a$, $|s| < b$, $|t| < c$.

Proof. We note that $\{1, \theta, \varphi\}$ is a Z-basis for R. We give the proof for $d = 12$; $d = 17$ and 44 are similar.

The idea of the proof is to locate z such that $.006 < |z| < 1$ and $|N(z)| < 1$; the bounds on the coefficients r, s and t then follow. We identify any $u \in R$ with its real embedding, and let u' and u'' denote the conjugates that send $\sqrt[3]{12}$ to $\sqrt[3]{12}\omega$ and $\sqrt[3]{12}\omega^2$, respectively, where $\omega = (-1 + \sqrt{3}\,i)/2$.

Since $|\epsilon| > .006$, where ϵ is the fundamental unit $1 + 3\sqrt[3]{12} - 3\sqrt[3]{18}$, there exists n such that $.006 < |y\epsilon^n| < 1$. Let $z = y\epsilon^n$; then $z \equiv \pm y \equiv \pm x \bmod R$, by (i), and $|N(z)| = |N(y)| < 1$. Since $|N(z)| = |z|\,|z'|\,|z''| = |z|\,|z'|^2 < 1$ and $|z| > .006$, it follows that $|z'| < 14$. Therefore, $|z - z'| < 15$; letting r, s and t be the coefficients of z with respect to the basis $\{1, \theta, \varphi\}$, we have

$$|\mathrm{re}\, z - z'| = \left| \frac{3}{2}\sqrt[3]{12}s + \frac{3}{2}\sqrt[3]{18}t \right| < 15,$$

$$|\text{im } z - z'| = \left| -\frac{\sqrt{3}}{2}\sqrt[3]{12}s + \frac{\sqrt{3}}{2}\sqrt[3]{18}t \right| < 15.$$

Solving the inequalities shows that $|s| < 6$ and $|t| < 7$. Since $|z| < 1$, computation shows that $|r| < 40$. Q.E.D.

PROPOSITION 10. *$Q(\sqrt[3]{12})$, $Q(\sqrt[3]{17})$ and $Q(\sqrt[3]{44})$ are not euclidean.*

Proof. Let x be as follows:

d	x
12	$\frac{2}{3} + \frac{5}{6}\theta + \frac{4}{9}\varphi$
17	$-\frac{94}{257} + \frac{233}{514}\theta - \frac{19}{1028}\varphi$
44	$x = 12/c, \quad c = 5 + 2\theta + \varphi$

In each case we show by computer that no R-translate of x, within the bounds of (v) in Proposition 9, has norm less than 1 in absolute value. Therefore, by Proposition 9, no R-translate of x has norm less than 1 in absolute value.

III. Proving That Fields Are Euclidean. We note that a theorem of Godwin [3] implies that $Q(\sqrt[3]{2})$ is euclidean, and E. M. Taylor [4] has recently shown that $Q(\sqrt[3]{3})$ and $Q(\sqrt[3]{10})$ are euclidean. This section verifies their results.

To prove that $Q(\sqrt[3]{2})$, $Q(\sqrt[3]{3})$ and $Q(\sqrt[3]{10})$ are euclidean requires the aid of a computer. We represent each field R with the correspondence

$$\sigma: \quad x + y\theta + z\varphi \longrightarrow (x, y, z).$$

For $d = 2$ or 3, the ring of integers R is then represented by the lattice of points with rational integer coordinates. For $d = 10$, R is generated by the vectors $(1, 0, 0)$, $(0, 1, 0)$ and $(1/3, 1/3, 1/3)$, and the definitions which follow must be modified accordingly.

For $d = 2$ or 3, we define the fundamental cube C to be the set of points (x, y, z) such that $0 \leqslant x, y, z < 1$. By the norm of a point we mean the norm of the element it represents. To prove that a field is euclidean, we must show that every point in C has an R-translate with $|N| < 1$. The obvious difficulty is the infinite number of points in C. Our approach, therefore, is to divide C into sufficiently small cubes, each of which has an R-translate in the region in R^3, where $|N| < 1$.

Given a set of points $S \subset R^3$ and $\xi \in R$, we call the set $\{(x, y, z) + \sigma(\xi) | (x, y, z) \in S\}$ the translate of S by ξ. The program first subdivides C into eight cubes through the planes $x, y, z = 1/2$. We then test 1500 R-translates of a given cube C'; if any one of these translates is found to lie entirely in the region $|N| < 1$, then C' is said to be covered. If C' is not shown to be covered, then C' is in turn divided into eight cubes. Each of these eight cubes is tested in the same way; if any one of 1500 R-translates lies in the region $|N| < 1$, the cube is said to be covered; if it is not covered it is subdivided, and so on. If we reach a stage where

every cube is covered, we have proven that every point in C has an R-translate with $|N| < 1$; hence the field is euclidean.

The precise number 1500 is of course arbitrary, and based on practicality. The following propositions supply sufficient conditions for a cube to be contained in the region $|N| < 1$.

For convenience we perform the following change of variables: let $u = x$, $v = \sqrt[3]{d}y$ and $w = \sqrt[3]{d^2}z$.

PROPOSITION 11. *Let* $\overline{N}(u, v, w) = u^3 + v^3 + w^3 - 3uvw$. *Let* E *be a region in* R^3 *bounded by the planes* $u = a_1$, $u = a_2$, $v = b_1$, $v = b_2$, $w = c_1$, *and* $w = c_2$; *let* E *lie entirely in one octant in* R^3. *If* $|\overline{N}| < 1$ *everywhere on the one-skeleton of* E, *then* $|\overline{N}| < 1$ *everywhere in* E.

Proof. Let S be the intersection of E with any plane parallel to the coordinate planes; as an example suppose that S is parallel to the uv-plane. For $\overline{N}(u, v)$ to have an extremum in the interior of S, it is necessary that $\delta\overline{N}/\delta u = \delta\overline{N}/\delta v = 0$. Since S lies entirely in one octant, this is only possible when $u = v = w \neq 0$, in which case $\overline{N} = 0$. Since the same reasoning applies when S is parallel to any coordinate plane, it follows that $|\overline{N}|$ cannot have a maximum in the interior of S. It follows that the maximum of $|\overline{N}|$ on E occurs on the one-skeleton of E. The theorem is immediate. Q.E.D.

PROPOSITION 12. *Let* $\overline{N}$ *and* E *be as in Proposition* 11. *Assume that* $|\overline{N}| < 1$ *on all eight vertices of* E, *and that the following are all nonnegative*:

$$\underline{(a_1 - b_i c_j)(a_2 - b_i c_j), \quad i, j = 1, 2,}$$

$$\underline{(b_1 - a_i c_j)(b_2 - a_i c_j), \quad i, j = 1, 2,}$$

$$\underline{(c_1 - a_i b_j)(c_2 - a_i b_j), \quad i, j = 1, 2.}$$

Then $|\overline{N}| < 1$ *everywhere on* E.

The last set of conditions ensures that, on each segment of the one-skeleton, the appropriate partial derivative is nonzero so $\overline{N}$ has no local maxima or minima on the one-skeleton other than the vertices.

Thus, we have the following result.

PROPOSITION 13. $Q(\sqrt[3]{2})$, $Q(\sqrt[3]{3})$ *and* $Q(\sqrt[3]{10})$ *are euclidean.*

With this result, the proof of Theorem A is complete.

FIELDS OF THE FORM $Q(\sqrt[4]{-d})$, $d > 0$

IV. Proving Fields $Q(\sqrt[4]{-d})$ Are Not Euclidean. We use the following notation: Let $K = Q(\sqrt[4]{-d})$, where $d = sr^2$, and s and r are square-free positive integers, $s \neq 1$; let $k = Q(\sqrt{-s})$, the unique quadratic subfield of K; let A and B be the rings of integers of k and K, respectively; let ϵ be the fundamental unit of B. Chevalley [5] showed that $h(K) = 1$ only if $h(k) = 1$. Therefore, we can assume that $s = 2, 3, 7, 11, 19, 43, 67$ or 163. With the added assumption that $s \neq r$ we ensure that different values of d generate different fields K.

The list of possible fields of class number one is further narrowed by the following proposition.

PROPOSITION 14. *If there exist three primes in K which ramify in K, then* $h(K) \neq 1$.

Proof. Let $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ be primes in k, $\mathfrak{p}_i = \mathfrak{r}_i^2$ in K, $i = 1, 2, 3$; we can assume that $\mathfrak{p}_1 = \sqrt{-s}A$. Suppose $h(K) = 1$; let $\mathfrak{p}_i = a_i A$ and $\mathfrak{r}_i = b_i B$, where $a_i \in A$ and $b_i \in B$, $i = 2, 3$. We can choose the b_i's such that either $b_2^2 = a_2$ or $b_3^2 = a_3$ or $(b_2 b_3)^2 = a_2 a_3$; this would imply that $K = k(\sqrt{a_2})$, $K = K(\sqrt{a_3})$ or $K = k(\sqrt{a_2 a_3})$, respectively—all impossibilities. Hence $h(K) \neq 1$. Q.E.D.

By the proposition, it is possible that $h(K) = 1$ only if either $s = 2$ or $d = 3, 7, 11, 19, 43, 67, 163, 12, 44, 76, 172, 268$ or 652. While we will not attempt to determine which of these actually have class number one, we will show that many cannot be euclidean in any case.

PROPOSITION 15. *If* $s \equiv 3$ (4), *and if there exists a prime* $p < s$ *such that* $p \equiv 1$ (4) *and* $-d$ *is a quadratic, but not a quartic, residue* mod p, *then K is not euclidean.*

Proof. We can assume that $h(K) = 1$, and, hence, that s is prime; let $(s) = \mathfrak{q}^4$ in K. Since $(-d/p) = 1$, we can deduce by quadratic reciprocity that $(p/s) = 1$. Since $s \equiv 3$ (4) it follows that p is a quartic residue mod s also; hence, there exists $b \in Z$ such that $b^4 \equiv p$ (s).

Let $u \in B$, $u \equiv b$ mod $\mathfrak{q}$ and suppose $N(u) < s$. Since $N(u) \equiv b^4 \equiv p(s)$ (see the proof of Lemma 1), it follows that $N(u) = p$, so there would exist an ideal $\mathfrak{p}$ of norm p. Then there would exist $n \in Z$ such that $\sqrt[4]{-d} + n \in \mathfrak{p}$, so $p | N(\sqrt[4]{-d} + n) = d + n^4$, so $n^4 \equiv -d(p)$; but this is impossible, since $-d$ is not a quartic residue mod p.

Therefore, $u \equiv b$ mod $\mathfrak{q}$ implies that $N(u) > N(\mathfrak{p}) = s$, so K is not euclidean. Q.E.D.

PROPOSITION 16. *The field K is not euclidean when* $d = 11, 19, 43, 76, 172$ *or* 268.

Proof. The values of p that satisfy Proposition 15 are given below.

d	p	d	s	p
11	5	76	19	5
19	17	172	43	13
43	17	268	67	29

Q.E.D.

Remark. Cassels [1] proved that K cannot be euclidean if $D_{K/Q} > 5300^2$; hence $Q(\sqrt[4]{-163})$ are $Q(\sqrt[4]{652})$ are not euclidean.

V. Proving That Fields $Q(\sqrt[4]{-d})$ Are Euclidean. In this section we prove that $Q(\sqrt[4]{-2})$ and $Q(\sqrt[4]{-7})$ are euclidean. The method and notation are analogous to Section III.

We represent these fields in R^4 under the correspondence

$$\sigma: \; w + x\theta + y\theta^2 + z\theta^3 \longrightarrow (w, x, y, z),$$

where $\theta = \sqrt[4]{-d}$ and $w, x, y, z \in Q$. Focusing on $Q(\sqrt[4]{-2})$, the ring of integers B is represented by the lattice of points with rational integer coefficients, and the fundamental four-cube C consists of points such that $0 \leqslant w, x, y, z < 1$. The four-cube C is divided into sixteen four-cubes by the hyperplanes $w, x, y, z = 1/2$; if a given four-cube C' has a translate contained in the region $N_{K/Q} < 1$, then C' is said to be covered; if it is not shown to be covered, it is subdivided, and so on as explained in Section III. The criteria for a four-cube to be contained in the region $N_{K/Q} < 1$ are given by the following proposition.

PROPOSITION 17. *Let S be a four-cube bounded by hyperplanes parallel to the coordinate hyperplanes, and such that the interior of S does not intersect the coordinate hyperplanes. Let $N1(w, x, y, z) = w^2 - dy^2 + 2dxz$ and let $N2(w, x, y, z) = -x^2 + dz^2 + 2wy$. If there exists a positive constant $\lambda < 1$ such that $|N1| < \sqrt{\lambda}$ and $|N2| < \sqrt{(1-\lambda)/d}$ on all sixteen vertices of S, then $N_{K/Q} < 1$ everywhere in S.*

Proof. Partial derivatives show that either $N1$ nor $N2$ has local extrema on the one-skeleton of S, hence on the two-skeleton, the three-skeleton and the entire four-cube. Since $N_{K/Q} = N1^2 + dN2^2$, the result is immediate. Q.E.D.

Using Proposition 17, we prove, with the aid of a computer, that $Q(\sqrt[4]{-2})$ and $Q(\sqrt[4]{-7})$ are euclidean. We note that Lakein [6] has shown that K is euclidean when $d = 3$. Theorem B summarizes all these results.

Because of the large discriminants it seems highly unlikely that $Q(\sqrt[4]{-44})$ or $Q(\sqrt[4]{-67})$ is euclidean.

Division of Mathematics
Assumption College
Worcester, Massachusetts 01609

1. J. W. S. CASSELS, "The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms," *Proc. Cambridge Philos. Soc.*, v. 48, 1952, pp. 72–86.

2. H. C. WILLIAMS, From a computer print-out, done recently at the University of Manitoba.

3. H. J. GODWIN, "On Euclid's algorithm in some cubic fields with signature one," *Quart. J. Math. Oxford Ser.* (2), v. 18, 1967, pp. 333–338.

4. E. M. TAYLOR, "Euclid's algorithm in cubic fields with complex conjugates," *J. London Math. Soc.* (2), v. 14, 1976, pp. 49–54.

5. C. CHEVALLEY, *C. R. Acad. Sci. Paris*, v. 192, 1931, pp. 257–258.

6. R. B. LAKEIN, "Euclid's algorithm in complex quartic fields," *Acta Math.*, v. 20, 1972.