[28] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York 1973.

[29] E. C. Titchmarsh, *The theory of functions*, second ed., Clarendon Press, Oxford 1939.

[30] — *The theory of the Riemann zeta-function*, Clarendon Press, Oxford 1951.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS 61801
U.S.A.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA AT SAN DIEGO
LA JOLLA, CALIFORNIA 92093
U.S.A.

Received on 25. 10. 1984
and in revised form on 29. 4. 1985 (1465)

ACTA ARITHMETICA
XLVII (1986)

Some euclidean properties for real quadratic fields

by

Daniel B. Shapiro* (Columbus, Ohio),
Raj K. Markanda (Merida, Venezuela) and Ezra Brown (Blacksburg, Va.)

The goal of this work is the determination of all the real quadratic number fields which are euclidean in a strong sense. The new requirement is that in every division the remainder can be taken to be positive.

To be more precise, let $\mathcal{O}$ be the ring of integers in an algebraic number field K (a finite algebraic extension of the field $\boldsymbol{Q}$ of rational numbers). Let $\mathscr{U}$ be a set of orderings (real primes) of K. If $\alpha, \beta \in K$, the statement "$\alpha < \beta$ (relative to $\mathscr{U}$)" means that $\beta - \alpha$ is positive with respect to each of the orderings in $\mathscr{U}$. We write $N\alpha$ as an abbreviation of $N_{K/\boldsymbol{Q}}(\alpha)$, the absolute norm.

Definition 1. K is *euclidean* mod $\mathscr{U}$ if for every $\alpha, \beta \in \mathcal{O}$ with $\alpha \geqslant \beta > 0$ (relative to $\mathscr{U}$), there exist $\varkappa, \varrho \in \mathcal{O}$ satisfying $\alpha = \beta\varkappa + \varrho$, $|N\varrho| < |N\beta|$, and $\varrho \geqslant 0$ (relative to $\mathscr{U}$).

This notion was introduced by Eichler [3] in 1938 and was considered recently in [7]. We have not found any further investigations of it in the literature. If $\mathscr{U}$ is empty then K is euclidean mod $\mathscr{U}$ exactly when K is euclidean in the classical sense.

One can show that if K is euclidean mod $\mathscr{U}$ for some set $\mathscr{U}$, then K must be euclidean. When $K = \boldsymbol{Q}(\sqrt{d})$ is a real quadratic field it is known exactly when the euclidean property holds. There are 16 cases.

Theorem 2. *Suppose* $K = \boldsymbol{Q}(\sqrt{d})$ *where* $d > 1$ *is a square-free integer. Then* K *is euclidean if and only if* $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57,$ *or* 73.

The proof of this theorem is rather difficult, and many mathematicians have contributed to the final result. Davenport [2] used reduction theory of binary quadratic forms to show that if $\boldsymbol{Q}(\sqrt{d})$ is euclidean then d is bounded. Careful calculations are then needed to classify the remaining cases. See [1] and the discussions in [4] and [5].

* Supported in part by the NSF.

The orderings of a number field K are given by the different embedding homomorphisms into the reals, $i\colon K \to \mathbf{R}$. If $K = \mathbf{Q}(\theta)$ is viewed as a subfield of $\mathbf{C}$, then there is exactly one ordering of K for each conjugate of θ which is real. When $K = \mathbf{Q}(\sqrt{d})$ is real quadratic there are two orderings. One is given by the inclusion map $j\colon K \to \mathbf{R}$ and the other comes from the conjugate $\bar{j}$. The relevant sets of orderings here are $\mathscr{U} = \{j\}$ and $\mathscr{U} = \{j, \bar{j}\}$. (The properties "euclidean mod $\mathscr{U}$" for $\mathscr{U} = \{j\}$ and $\mathscr{U} = \{\bar{j}\}$ coincide since j and $\bar{j}$ differ only by an automorphism.) Here is the main result of this paper.

THEOREM 3. *Let $K = \mathbf{Q}(\sqrt{d})$ where $d > 1$ is a square-free integer.*

(a) *K is euclidean* mod $\{j\}$ *if and only if $d = 2$, 3 or 5.*

(b) *K is euclidean* mod $\{j, \bar{j}\}$ *if and only if $d = 5$.*

One should recall here that $\mathbf{Q}(\sqrt{5})$ is the real quadratic field with smallest discriminant, and $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ have the next smallest discriminants.

The proof of this theorem separates naturally into two parts. The positive results for $\mathbf{Q}(\sqrt{d})$ where $d = 2$, 3, 5 are done geometrically by explicitly covering a fundamental domain by "good" translates. For the negative results, each of the remaining 15 cases listed in Theorem 2 is eliminated by applying elementary congruence methods. The full proof of Theorem 3 is obtained by combining Propositions 5, 6, 7, 8 and 9 below. We have been unable to find a more unified proof for these negative results.

It is a pleasure to thank W. McWorter for his help in preparing the drawings.

1. Geometric methods.

Before specializing to real quadratic fields we mention a few equivalent formulations of our euclidean property.

PROPOSITION 4. *Let K be a number field with ring of integers $\mathcal{O}$. Let $\mathscr{U}$ be a set of orderings of K. The following statements are equivalent.*

(1) *K is euclidean* mod $\mathscr{U}$.

(2) *For every $\alpha, \beta \in \mathcal{O}$ with $\beta \neq 0$, there exist $\varkappa, \varrho \in \mathcal{O}$ with $\alpha = \beta\varkappa + \varrho$, $|N\varrho| < |N\beta|$ and $\varrho\beta \geqslant 0$ (relative to $\mathscr{U}$).*

(3) *For every $\alpha \in \mathcal{O}$ and $m \in \mathbf{Z}$ with $m > 0$, there exist $\varkappa, \varrho \in \mathcal{O}$ with $\alpha = m\varkappa + \varrho$, $|N\varrho| < |Nm|$ and $\varrho \geqslant 0$ (relative to $\mathscr{U}$).*

(4) *For every $\xi \in K$ there exists $\varkappa \in \mathcal{O}$ with $|N(\xi - \varkappa)| < 1$ and $\xi - \varkappa \geqslant 0$ (relative to $\mathscr{U}$).*

Proof. We show $(1) \to (3) \to (4) \to (2) \to (1)$. First note that $(2) \to (1)$ is trivial. $(1) \to (3)$: Let $\alpha \in \mathcal{O}$ and $m \in \mathbf{Z}$ with $m > 0$ be given. Since $\mathbf{Q}$ is dense in K relative to each ordering, we can choose $k \in \mathbf{Z}$ so that $\alpha + km > 0$ for every ordering. Let $\alpha' = \alpha + (k+1)m$. Then $\alpha' \geqslant m$ (relative to $\mathscr{U}$) and from (1) we find $\varkappa'$, ϱ with $\alpha' = m\varkappa' + \varrho$ where $|N\varrho| < |Nm|$ and $\varrho \geqslant 0$ (relative to $\mathscr{U}$). With $\varkappa = \varkappa' - (k+1)$ we find $\alpha = m\varkappa + \varrho$ as required.

$(3) \to (4)$. Given $\xi \in K$ we can express $\xi = \alpha/m$ where $\alpha \in \mathcal{O}$ and $m \in \mathbf{Z}$, $m > 0$. Let $\varkappa, \varrho \in \mathcal{O}$ be the values given in (3). Then $\xi - \varkappa = \varrho/m$ fulfils the conditions.

$(4) \to (2)$. Given $\alpha, \beta \in \mathcal{O}$ let $\varkappa \in \mathcal{O}$ be the value given in (4) using $\xi = \alpha/\beta$. Setting $\varrho = \alpha - \beta\varkappa$ the conditions are satisfied. ■

Consequently, if $\mathscr{V} \subseteq \mathscr{U}$ are sets of orderings of K, and K is euclidean mod $\mathscr{U}$, then K must also be euclidean mod $\mathscr{V}$. In particular, if K is euclidean mod $\mathscr{U}$ for some $\mathscr{U}$, then K is euclidean in the classical sense.

Let us now restrict attention to the case $K = \mathbf{Q}(\sqrt{d})$. As usual we take $d > 1$ to be a square-free integer. The ring of integers $\mathcal{O}$ has a $\mathbf{Z}$-basis $\{1, \theta\}$ where

$$\theta = \begin{cases} \sqrt{d} & \text{if} \quad d \not\equiv 1 \pmod 4, \\ (1+\sqrt{d})/2 & \text{if} \quad d \equiv 1 \pmod 4. \end{cases}$$

The standard embedding of K into the real plane $\mathbf{R}^2$ is provided by sending $\alpha \in K$ to $(\alpha, \bar{\alpha}) \in \mathbf{R}^2$. Then K becomes a dense subset of $\mathbf{R}^2$ and the ring $\mathcal{O}$ becomes the $\mathbf{Z}$-lattice generated by the vectors $(1, 1)$ and $(\theta, \bar{\theta})$. The norm function N on K extends to $N\colon \mathbf{R}^2 \to \mathbf{R}$ by setting $N((x, y)) = xy$.

Define the subsets $V_2 \subseteq V_1 \subseteq V \subseteq \mathbf{R}^2$ as follows:

$$V = \{(x, y) \in \mathbf{R}^2\colon |xy| < 1\},$$

$$V_1 = \{(x, y) \in \mathbf{R}^2\colon |xy| < 1 \text{ and } x \geqslant 0\},$$

$$V_2 = \{(x, y) \in \mathbf{R}^2\colon |xy| < 1, x \geqslant 0 \text{ and } y \geqslant 0\}.$$

Then V is bounded by the hyperbolas $xy = 1$ and $xy = -1$, V_1 is the right half of V and V_2 is the upper half of V_1. We often identify K with its image in $\mathbf{R}^2$, and simply write α rather than $(\alpha, \bar{\alpha})$. For instance if $\varrho \in \mathcal{O}$ we write $\varrho \in V_2$ to mean that $|N\varrho| < 1$, $\varrho \geqslant 0$ and $\bar{\varrho} \geqslant 0$.

Property (4) of Proposition 4 furnishes geometric criteria which imply our euclidean properties. For example, K is euclidean mod $\{j\}$ if the translates $\varkappa + V_1$ for $\varkappa \in \mathcal{O}$ cover the whole plane $\mathbf{R}^2$. (It is not clear that the converse holds. Compare [6], pp. 74–75.) In order to see that a given $\xi \in \mathbf{R}^2$ lies in one of these translates, we may freely add elements of $\mathcal{O}$ to ξ. So we may assume ξ lies in a fundamental domain, like

$$D = \{r(1, 1) + s(\theta, \bar{\theta}) \in \mathbf{R}^2\colon 0 \leqslant r < 1 \text{ and } 0 \leqslant s < 1\}.$$

The next result is a simple illustration of these ideas.

PROPOSITION 5. *$\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{5})$ are euclidean* mod $\{j\}$.

Proof. The easier case $\mathbf{Q}(\sqrt{5})$ is left as an exercise. A stronger result is proved in Proposition 6. For $\mathbf{Q}(\sqrt{2})$ see Figure 1. In this picture, the points of $\mathcal{O}$ are the intersection points of the two systems of parallel lines. The region V_1 is shaded.

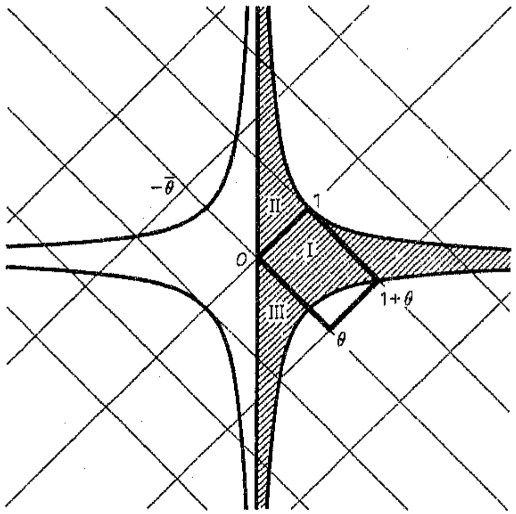

Fig. 1

The fundamental domain D (outlined in the figure) is essentially the rectangle spanned by 1 and θ, but some care should be taken with the boundary points. A short calculation shows that the regions labelled I, II, III cover D, after translation. That is, $D \subseteq V_1 \cup (1+V_1) \cup (\theta+V_1)$.

Remark. In each of these two cases one can find a connected fundamental domain (with either smooth or polygonal boundary) which is entirely contained within the region V_1. Is there a convex fundamental domain in V_1?

The next two propositions use the same ideas but are more difficult since infinitely many translates are involved.

PROPOSITION 6. *$\boldsymbol{Q}(\sqrt{5})$ is euclidean* mod $\{j, \bar{j}\}$.

Proof. In the embedding of $\boldsymbol{Q}(\sqrt{5})$ into $\boldsymbol{R}^2$, the ring $\mathcal{O}$ goes to the $\boldsymbol{Z}$-lattice spanned by 1 and θ, where $\theta = (1+\sqrt{5})/2$. In order to exploit the symmetry, we use the fundamental domain D' based on the vectors θ and $\bar{\theta}$. See Figure 2 for a picture, where the region V_2 is shaded. Both D' and V_2 are symmetric about the line $y = x$.

Now consider the portion of D' covered by the three translates V_2, $-\theta+V_2$ and $-2\theta+V_2$. This portion is the shaded area in Figure 3.

By symmetry we need only cover the half of D' lying above the line $y = x$. So we still need to cover the triangular region OAB in Figure 3. Here the edge OA is included in the region, but edges AB and OB are not (since they are already covered).

Since θ is the fundamental unit of $\mathcal{O}$ we see that the points θ^{2m} for $m \in \boldsymbol{Z}$

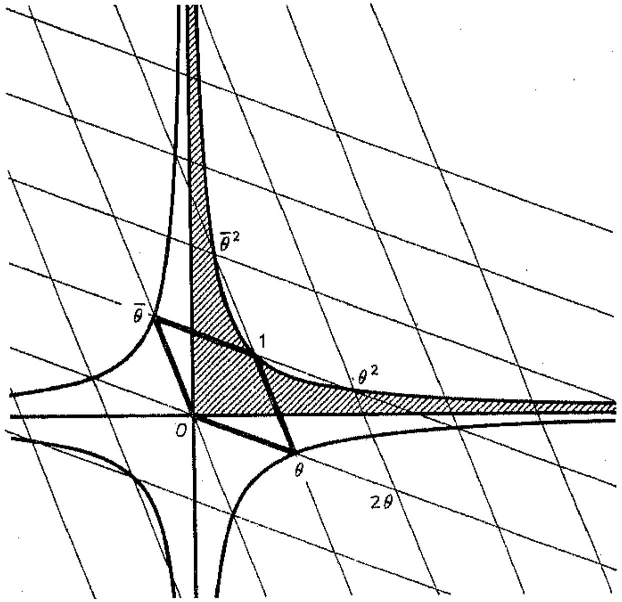

Fig. 2

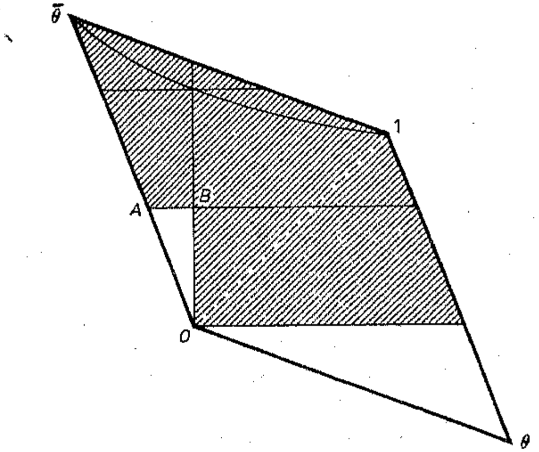

Fig. 3

lie on the hyperbola $xy = 1$ and are in the first quadrant. The Proposition will be proved once we establish the following:

CLAIM. *The union of all $-\theta^{-2m}+V_2$ for $m = 0, 1, 2, \ldots$ covers the region OAB.*

For given m, consider the region $D' \cap (-\theta^{-2m}+V_2)$, which is shaded in

Figure 4. This shaded region is bounded by the vertical line $x = -\theta^{-2m}$ and the hyperbola $(x+\theta^{-2m})(y+\bar{\theta}^{-2m}) = 1$. Let G_m and H_m be the intersections of the line AB with this bounding line and hyperbola, respectively.

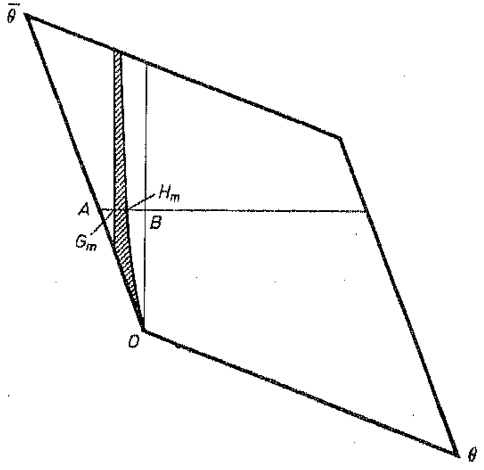

Fig. 4

The points A, G_m, H_m, B all have y-coordinate $-1+\theta$. Let the x-coordinates be a, g_m, h_m, 0, respectively. A calculation shows that $g_m < g_{m+1} < h_m < h_{m+1}$ for every $m \geqslant 0$. Also $g_0 < a$ and $\lim g_m = \lim h_m = 0$ as $m \to \infty$. These facts show that the shaded regions do overlap appropriately. In other words, every point in the region OAB does lie in one of the translates $-\theta^{-2m} + V_2$, proving the claim. ■

Proposition 7. *$\boldsymbol{Q}(\sqrt{3})$ is euclidean* mod $\{j\}$.

Proof. Embedding into $\boldsymbol{R}^2$ as usual, the ring $\mathcal{O}$ becomes the $\boldsymbol{Z}$-lattice spanned by 1 and θ where $\theta = \sqrt{3}$. It is convenient to use the fundamental domain D' based on the vectors 1 and $\bar{\theta} = -\theta$, as indicated in Figure 5.

Now consider the portion of D' covered by the three translates V_1, $-\theta+V_1$ and $-(1+\theta)+V_1$. This portion appears as the shaded region in Figure 6.

There remain two uncovered pieces. The region PQR in the figure can be covered by the translate $-(4+3\theta)+V_1$. To see this, first compute the coordinates

$$P = ((1+\sqrt{5}-2\sqrt{3})/2,\ (1-\sqrt{5}+2\sqrt{3})/2),$$
$$Q = (0,\ 2\sqrt{3}/3),$$
$$R = (0,\ 3(-1+\sqrt{3})/2).$$

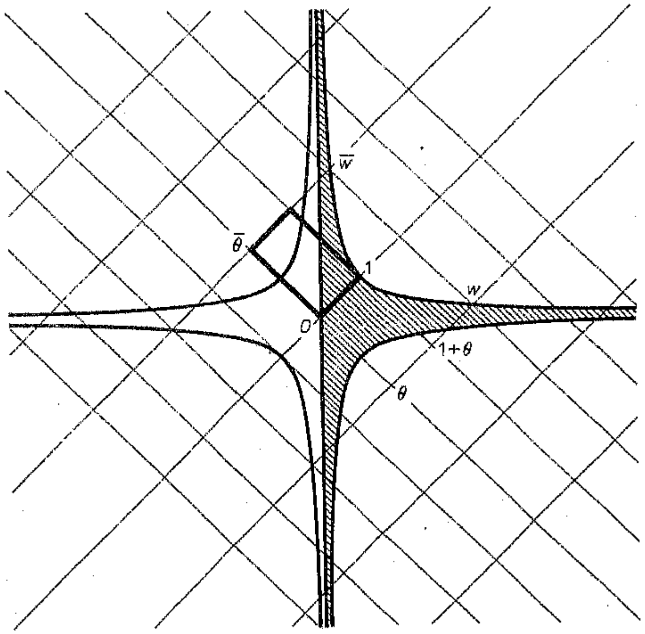

Fig. 5

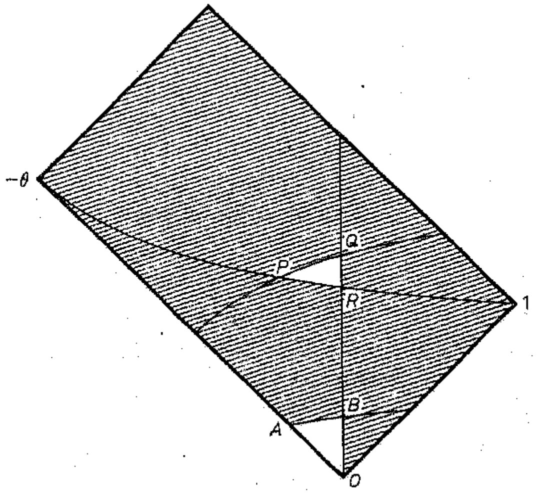

Fig. 6

Evaluating $f(x, y) = (x+4+3\sqrt{3})(y+4-3\sqrt{3})$ at P, Q, R shows that these three points do lie between the hyperbolas $f(x, y) = \pm 1$.

The remaining part OAB can be covered by an infinite union of translates by units. The fundamental unit here is $w = 2+\theta$, which has norm 1.

Claim. *The union of all* $-w^{-m}+V_1$ *for* $m = 0, 1, 2, \ldots$ *covers the region* OAB.

The proof of this claim is similar to the argument given for the previous proposition, and is left to the reader. ■

Surprisingly, in the two propositions above an infinite number of translates $\varkappa+V_i$ is required. Here is a proof for the case $K = \boldsymbol{Q}(\sqrt{5})$. Suppose D' is covered by some finite union of translates $\varkappa+V_2$ for $\varkappa \in \mathcal{O}$. Then there must be one $\lambda+V_2$ which contains an infinite number of the points $P_n = (-1/n^2, 1/n)$. The point $(0, 0)$ must then lie in the closure of $\lambda+V_2$, so that $-\lambda$ is in the closure of V_2. The only integers in the closure of V_2 are 0 and the units θ^{2k} for $k \in \boldsymbol{Z}$. Certainly $\lambda \neq 0$ since V_2 does not contain any of the points P_n. Therefore $-\lambda = \theta^{2k}$ for some k and $-\theta^{2k}+V_2$ contains infinitely many P_n. This is easily seen to be false. (See Figure 4 for the case $k < 0$.)

2. Congruence methods. By applying congruence arguments we can prove that certain real quadratic fields are not euclidean mod $\mathcal{U}$. By the classical Theorem 2 we need only investigate those fields already known to be euclidean.

Proposition 8. $\boldsymbol{Q}(\sqrt{2})$ *and* $\boldsymbol{Q}(\sqrt{3})$ *are not euclidean* mod $\{j, \bar{j}\}$.

Proof. Suppose $\boldsymbol{Q}(\sqrt{2})$ is euclidean mod $\{j, \bar{j}\}$. Letting $\theta = \sqrt{2}$ we divide $1+\theta$ by 2 to get $1+\theta = 2\varkappa+\varrho$, where $|N\varrho| < 4$, $\varrho \geqslant 0$ and $\bar{\varrho} \geqslant 0$. Expressing $\varrho = r+s\theta$ we see that $r \equiv s \equiv 1 \pmod 2$. Then $r^2 \equiv s^2 \equiv 1 \pmod 8$ and therefore $N\varrho = r^2-2s^2 \equiv 7 \pmod 8$. Since $-4 < N\varrho < 4$ this forces $N\varrho = -1$, but $N\varrho = \varrho\bar{\varrho} \geqslant 0$. Contradiction.

Suppose $\boldsymbol{Q}(\sqrt{3})$ is euclidean mod $\{j, \bar{j}\}$ and set $\theta = \sqrt{3}$. Again dividing $1+\theta$ by 2 we arrive at a similar contradiction. ■

The same technique is used in the remaining cases but the details are harder. We use the fact that $K = \boldsymbol{Q}(\sqrt{d})$ has a fundamental unit w. Every unit of $\mathcal{O}$ equals $\pm w^n$ for some $n \in \boldsymbol{Z}$. Also in all our cases $\mathcal{O}$ has unique factorization (since K is euclidean). Then for a given $k \in \boldsymbol{Z}$ we can list explicitly all $\alpha \in \mathcal{O}$ with $N\alpha = k$.

Proposition 9. *Suppose* $d = 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ *or* 73. *Then* $\boldsymbol{Q}(\sqrt{d})$ *is not euclidean* mod $\{j\}$.

Proof. By Proposition 4(3), if the euclidean property fails then there is a counterexample where the divisor is some rational integer $m > 1$. In each case we provide an example of $\alpha \in \mathcal{O}$ divided by m which contradicts the property "euclidean mod $\{j\}$". The divisor m is chosen to be the smallest positive rational integer which gives a counterexample. This minimal divisor m is often related to the fundamental unit w: usually $w \equiv 1$ or $w^2 \equiv 1 \pmod m$. The following table lists the relevant cases.

d	w	m	α
6	$5+2\theta$	4	$2+3\theta$
7	$8+3\theta$	7	4θ
11	$10+3\theta$	3	$2+2\theta$
13	$1+\theta$	3	$1+2\theta$
17	$3+2\theta$	4	$2+3\theta$
19	$170+39\theta$	13	10θ
21	$2+\theta$	3	$2+2\theta$
29	$2+\theta$	5	$2+4\theta$
33	$19+8\theta$	11	$2+7\theta$
37	$5+2\theta$	3	2θ
41	$27+10\theta$	4	$2+3\theta$
57	$131+4\theta$	5	$2+3\theta$
73	$943+250\theta$	6	$2+3\theta$

For illustration we indicate the steps in two typical cases, $d = 19$ and $d = 41$.

When $d = 19$ then $\mathcal{O} = \boldsymbol{Z}+\boldsymbol{Z}\theta$ where $\theta = \sqrt{19}$. Suppose $\boldsymbol{Q}(\theta)$ is euclidean mod $\{j\}$. Then there exist $\varkappa, \varrho \in \mathcal{O}$ with $10\theta = 13\varkappa+\varrho$ where $|N\varrho| < 169$ and $\varrho \geqslant 0$. Suppose $\varrho = r+s\theta$. Then $N\varrho \equiv N(10\theta) \equiv 11 \pmod{13}$. For each of the 26 possibilities $k \equiv 11 \pmod{13}$ with $-169 < k < 169$, consider the equation $N\varrho = r^2-19s^2 = k$. Some cases are quickly eliminated by working locally (i.e., examining the equation over the p-adic completions for various primes p). The remaining cases are: $k = -67, -15, -2, 24, 102$. Each of these is eliminated using the unique factorization in $\mathcal{O}$.

For example suppose $N\varrho = 24$. Factoring 2 and 3 in $\mathcal{O}$ we find $2 = -\sigma\bar{\sigma}$ where $\sigma = 13+3\theta$, and $3 = -\tau\bar{\tau}$ where $\tau = 4+\theta$. Here 2 is ramified since $\bar{\sigma} = (\text{unit})\cdot\sigma$. Because $N\varrho = 2^3\cdot 3$, unique factorization implies that either $\varrho = (\text{unit})\cdot\sigma^3\tau = (\text{unit})\cdot 2\sigma\tau$ or $\varrho = (\text{unit})\cdot\sigma^3\bar{\tau} = (\text{unit})\cdot 2\sigma\bar{\tau}$. Every unit is some $\pm w^n$ and the sign is determined since $\varrho \geqslant 0$: either $\varrho = w^n\cdot 2\sigma\tau$ or $\varrho = -w^n\cdot 2\sigma\bar{\tau}$, for some $n \in \boldsymbol{Z}$. Since $w \equiv 1 \pmod{13}$ it follows that $\varrho \equiv 2\sigma\tau$ or $-2\sigma\bar{\tau} \pmod{13}$. Multiplying these out we find that neither possibility agrees with the hypothesis that $\varrho \equiv 10\theta \pmod{13}$.

Let us move on to the case $d = 41$ and $\mathcal{O} = \boldsymbol{Z}+\boldsymbol{Z}\theta$ where now $\theta = (1+\sqrt{41})/2$. If $\boldsymbol{Q}(\theta)$ is euclidean mod $\{j\}$ there must exist $\varkappa, \varrho \in \mathcal{O}$ with $2+3\theta = 4\varkappa+\varrho$ where $|N\varrho| < 16$ and $\varrho \geqslant 0$. Suppose $\varrho = r+s\theta$. Then $N\varrho = r^2+rs-10s^2 \equiv N(2+3\theta) \equiv 0 \pmod 4$. For each of the 7 possible k with $k \equiv 0 \pmod 4$ and $-16 < k < 16$, we examine the equation $r^2+rs-10s^2 = k$. After checking the local conditions, we are left with the possibilities $N\varrho = \pm 4, \pm 8$.

Suppose for example that $N\varrho = \pm 4$. Since $2 = \pi\bar{\pi}$ where $\pi = 3+\theta$, unique factorization implies that up to a unit factor, ϱ must equal π^2, $\pi\bar{\pi}$ or $\bar{\pi}^2$. Since $\varrho > 0$ this unit factor is w^n for some $n \in \boldsymbol{Z}$. Now $w = 27+10\theta$ so that $w^2 \equiv 1 \pmod 4$. Hence, $\varrho \equiv \pi^2$, $\pi\bar{\pi}$, $\bar{\pi}^2$, $w\pi^2$, $w\pi\bar{\pi}$, or $w\bar{\pi}^2 \pmod 4$. Multiplying these out we find that none of them is compatible with the hypothesis $\varrho \equiv 2+3\theta \pmod 4$.

The rest of the cases in this proposition are settled by similar calculations. ■

References

[1] H. Chatland and H. Davenport, *Euclid's algorithm in real quadratic fields*, Canadian J. Math. 2 (1950), pp. 289–296.

[2] H. Davenport, *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Proc. London. Math. Soc. (2) 53 (1951), pp. 65–82.

[3] M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörper und ihre L-Reihen*, J. Reine Angew. Math. 179 (1938), pp. 227–251. See especially pp. 240–241.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford Univ. Press, 1960. See especially § 14.8 and § 14.9.

[5] C. G. Lekkerkerker, *Geometry of Numbers*, Walters-Noordhoff and North-Holland, 1969. See especially § 47.5 and § 48.3.

[6] H. W. Lenstra, Jr., *Euclidean number fields* 2, Math. Intelligencer 2 (1980), pp. 73–77.

[7] R. K. Markanda and V. S. Albis-Gonzales, *Euclidean algorithm in principal arithmetic algebras*, Tamkang J. Math. (to appear).

DEPARTMENT OF MATHEMATICS
THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO 43210

DEPARTAMENTO DE MATEMATICAS
UNIVERSIDAD DE OS ANDES
MERIDA, VENEZUELA

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF IOWA
IOWA CITY, IOWA 52242

DEPARTMENT OF MATHEMATICS
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
BLACKSBURG, VIRGINIA 24061

Received on 20. 12. 1984
and in revised form on 11. 4. 1985 (1481)

ACTA ARITHMETICA
XLVII (1986)

On the l-rank of ideal class groups of certain number fields

by

Kiyoaki Iimura (Tokyo)

Introduction. Throughout this paper we shall fix an odd prime number l. Let $\boldsymbol{Z}$ and $\boldsymbol{Z}_l$ denote the ring of rational integers and of l-adic integers respectively. Let K be a nonabelian Galois extension of the rational numbers $\boldsymbol{Q}$ satisfying the following conditions.

(a) The degree $(K:\boldsymbol{Q})$ is nl with $n \mid l-1$, $n \neq 1$.

(b) The Galois group G of K over $\boldsymbol{Q}$ is generated by two elements σ and τ with the relations

$$\sigma^l = 1, \quad \tau^n = 1, \quad \tau\sigma\tau^{-1} = \sigma^r,$$

where r is a rational integer of order n in the multiplicative group $(\boldsymbol{Z}/l\boldsymbol{Z})^{\times}$.

Let T (resp. S) be the subgroup of G generated by τ (resp. σ), and let L (resp. k) be the fixed field of T (resp. S). Then $k/\boldsymbol{Q}$ is a cyclic extension of degree n, whose Galois group is generated by the restriction of τ to k. Also $L/\boldsymbol{Q}$ is a non-Galois extension of degree l, with Galois closure K. An important example of this situation is $L = \boldsymbol{Q}(\sqrt[l]{m})$, $k = \boldsymbol{Q}(\zeta)$, and $K = L\cdot k$, where ζ is a primitive lth root of unity and m is an lth power-free rational integer; such a field is called a *pure field of degree l.*

Let $H(L)$ denote the l-class group of L, i.e., the Sylow l-subgroup of the ideal class group of L. The *l-rank of $H(L)$* is defined to be the number of invariants of $H(L)$ divisible by l, which we call *rank $H(L)$*. The main purpose of the paper is to establish lower bounds for rank $H(L)$ (see Theorem 2.3 in § 2) by making use of the genus number formula found by Jaulent ([11], Theorem 3). In particular in the pure field case $L = \boldsymbol{Q}(\sqrt[l]{m})$, $l \neq 3$, one of our lower bounds in the corollary to Theorem 2.3 is equal to the number of distinct prime factors $\equiv \pm 1 \pmod{l}$ of m; this is an extension of one of the results in [1] which was a consequence of rational genus theory. Also we shall illustrate this Theorem 2.3 with some examples in Section 4, one of which says that if $p = (c_0^l + c_1^l)/(c_0 + c_1)$ with $l \geqslant 5$ and c_0,