EUCLID'S ALGORITHM IN CUBIC FIELDS WITH COMPLEX CONJUGATES

ELIZABETH MARY TAYLOR

ROYAL HOLLOWAY COLLEGE, LONDON

SUPERVISOR: PROFESSOR H.J. GODWIN

ABSTRACT

This thesis investigates the existence of a Euclidean Algorithm in cubic fields with complex conjugates. This investigation is made using the following methods.

The first method is a modification of a result of Cassels which states that no field of discriminant less than $-\left(\frac{81(5+3\sqrt{3})}{2}\right)^2 = -(412.944..)^2$ possesses a Euclidean Algorithm. By using the modification it is possible to show that some fields of discriminant greater than the above bound, but close to it, also do not possess a Euclidean Algorithm.

A second method is to choose an algebraic integer β which is a divisor of $1 \pm \epsilon^n$, where ϵ is the fundamental unit of the field in question and n is a rational integer. We then determine whether there are any residue classes modulo β which do not contain an integer of norm of absolute value less than the absolute value of the norm of β.

The next method is an adaptation of a method of Barnes and Swinnerton-Dyer for the real quadratic fields, modified here for the fields in question. This method aims to isolate the points with minimum at least 1.

An indirect method, which is used as the final step of the last method described, is to determine the minimum of numbers of the form $\frac{\alpha}{1-\epsilon^n}$, where α is an integer of the field in question and n is a positive rational integer.

In addition to existing results, 37 fields have been shown

to possess a Euclidean Algorithm and it has been established that there is no Euclidean Algorithm in 289 fields. For some fields the inhomogeneous minimum has been determined.

The numerical results obtained are given in the last chapter of this work. The listings of the computer programs used for the above methods are in the appendix to this thesis.

ACKNOWLEDGEMENTS

I wish to express my thanks to my supervisor, Professor H.J. Godwin, for his invaluable advice and encouragement and for his assistance with calculations particularly while the methods were being developed.

My thanks are also due to Dr. I.O. Angell for his assistance with some computing details and the adaptations of his routines for use in the methods of this thesis; and who, together with Professor Godwin, provided details of the fields of discriminants -160087 and -169271.

I am grateful to members of the department of Statistics and Computer Science at Royal Holloway College for assistance with the compilation and running of the programs; and on whose link to the University of London's CDC 6600 computer the programs were run.

Finally, I wish to acknowledge the financial support of the Science Research Council.

CONTENTS

The Appendix volume to this thesis contains listings of all routines used.

INTRODUCTION

I.1 If there are algebraic integers β, ξ in K such that $\beta \neq 0$ and

$$|N(\xi - \gamma\beta)| \geqslant |N(\beta)| \qquad (I.1)$$

for every algebraic integer γ in K, where N represents the norm of the algebraic number, there is said to be no Euclidean Algorithm in the field.

I.2 Let $L_1, \ldots, L_n$ be n linear forms in the real variables $x_1, \ldots, x_n$ of determinant Δ. Let $(x_1, \ldots, x_n)$ be the co-ordinates of the point P in n-dimensional space, then, if $y_1, \ldots, y_n$ are real numbers and $(y_1, \ldots, y_n)$ are the co-ordinates of the point P_o, we say

$$P \equiv P_o \pmod 1 \text{ if } x_1 \equiv y_1, \ldots, x_n \equiv y_n \pmod 1.$$

We define

$$M(L_1, \ldots, L_n; P_o) = \min_{P \equiv P_o} |L_1 \ldots L_n|$$

and $$M(L_1, \ldots, L_n) = \max_{P_o} M(L_1, \ldots, L_n; P_o).$$

$M(L_1, \ldots, L_n)$ is then said to be the inhomogeneous minimum of the linear forms $L_1, \ldots, L_n$.

I.3 If $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are rational and $\alpha = \alpha^{(1)}$ is the value of L_1 for $(x_1, \ldots, x_n) = (\alpha_1, \ldots, \alpha_n)$, α is an algebraic number and $\alpha^{(2)}, \ldots, \alpha^{(n)}$, the corresponding values of $L_2, \ldots, L_n$, are its algebraic conjugates; we also have

$$N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)},$$

and the set of values of L_1 over all rational values of $(x_1, \ldots, x_n)$ constitute an algebraic number field K of discriminant D where $D = \Delta^2$.

We now define

$$M(K,\alpha) = \min_{\gamma} |N(\alpha - \gamma)|$$

where the minimum is over all algebraic integers γ in K, and

$$M(K) = \max_{\alpha} M(K,\alpha) \tag{I.2}$$
$$= \max_{\alpha} \min_{\gamma} |N(\alpha - \gamma)|$$

where the maximum is over all algebraic numbers α in K. We then say $M(K)$ is the inhomogeneous minimum of the field K. We have

$$M(K,\alpha) = M(L_1, \ldots, L_n; \tilde{\alpha})$$

and $\qquad M(K) \leq M(L_1, \ldots, L_n)$

with equality in the latter relationship when $M(L_1, \ldots, L_n)$ is attained at a rational point.

I.4 Since the quotient of any two numbers of K is itself a number in K, for all algebraic integers ξ, β in K we have

$$\left|N\left(\frac{\xi}{\beta} - \gamma\right)\right| \leq M(K)$$

for some algebraic integer γ in K; so that

$$|N(\xi - \beta\gamma)| \leq M(K)|N(\beta)|.$$

Hence, if $M(K) < 1$, the field has a Euclidean Algorithm.

Conversely, if $M(K) \geq 1$ there exists an algebraic number $\alpha = \frac{\xi}{\beta}$ in K, where ξ, β are algebraic integers of K, so that

$$\left|N\left(\frac{\xi}{\beta} - \gamma\right)\right| \geq 1$$

for every algebraic integer γ in K, since every algebraic number in K may be expressed as the quotient of two algebraic integers in K; thus

$$|N(\zeta - \beta\gamma)| \geqslant |N(\beta)|$$

for every algebraic integer γ in K. Hence, if $M(K) \geqslant 1$, the field has no Euclidean Algorithm.

Thus

K has a Euclidean Algorithm if and only if $M(K) < 1$ (I.3)

We see that a sufficient condition for the existence of a Euclidean Algorithm is

$$M(L_1, \ldots, L_n) < 1.$$

If $M(K, \alpha) \geqslant 1$ for some algebraic number α in K, immediately $M(K) \geqslant 1$; thus the non-existence of a Euclidean Algorithm in an algebraic number field may be established by finding a single algebraic number α in K for which $M(K, \alpha) \geqslant 1$.

I.5 The question of a Euclidean Algorithm in complex quadratic fields was relatively easily answered, a proof is given in (22) of the fact that the complex quadratic field $K(\sqrt{m})$ has a Euclidean Algorithm only when $m = -1, -2, -3, -7, -11$.

For the real quadratic fields, the fact that the field $K(\sqrt{d})$ of discriminant $d > 0$ does not have a Euclidean Algorithm if d is sufficiently large was first established by a combination of several results, notably those of Berg (3), Behrbohm and Rédei (4), Erdös and Ko (15) and Heilbronn (24). Davenport (8) gave an independent proof of this result; the underlying principles of the method employed are given in (9). Davenport's method is based on a consideration of the corresponding binary quadratic forms, the more general result given is that: if $f(x,y) = ax^2 + bxy + cy^2$ is an indefinite binary quadratic form with real coefficients and discriminant $d = b^2 - 4ac > 0$, and $f(x,y)$ does not represent 0 for any integral values of x,y other than $0,0$, there exist real numbers ξ, η with the property that

$$|f(x+\xi, y+\eta)| > \kappa^2\sqrt{d}.$$

The proof is based on the construction of the point (ξ,η) from an infinite chain of reduced forms all equivalent to the original form. In (8) the reduction due to Hurwitz is used and leads to a specific constant, 2^{-7}, in place of κ^2. Davenport then goes on to show that, when a, b, c are rational integers, ξ and η, when constructed as above, are rational, thus there is no Euclidean Algorithm if $\sqrt{d} > 2^7$. Since there are only a finite number of real quadratic fields with bounded discriminant there are only a finite number of real quadratic fields with a Euclidean Algorithm.

Davenport used this basic method to show that there is a Euclidean Algorithm in only a finite number of cubic fields with complex conjugate fields (11), and in only a finite number of complex quartic fields whose conjugate fields are also complex (12).

I.6 Cassels (5) establishes the same general results as Davenport but with the following specific constants

For the real quadratic fields $M(K) > \frac{\Delta}{45.2}$

For the cubic fields with complex conjugate fields $M(K) > \frac{|\Delta|}{420}$

For the complex quartic fields whose conjugate fields are also complex $M(K) > \frac{|\Delta|}{5300}$

Cassels in fact establishes these results for the minima of the corresponding linear forms and uses the same basic method in each case. A further consideration and extension of the case of the cubic fields with complex conjugate fields is made in chapter 2 of this thesis.

I.7 Chatland (7) gives a summary of the results concerning the real quadratic fields and investigates those fields of discriminant less than 2^{14}, Davenport's bound. He states that there is no Euclidean Algorithm in $K(\sqrt{m})$ unless

$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$

except possibly when $m = 193, 241, 313, 337, 457, 601$. For these last six cases Chatland and Davenport (6) show that there is no Euclidean Algorithm by a modification of Davenport's general method of (8). Inkeri (25) used a method based on that of Erdös and Ko (15) to give an independent proof of these results.

The statement that $K(\sqrt{97})$ has a Euclidean Algorithm was shown to be false by Barnes and Swinnerton-Dyer (2). In (2) the inhomogeneous minima of the norm forms f_m of the fields $K(\sqrt{m})$ for $m \leq 101$, except for $m = 46, 57, 67, 71, 73, 86, 94$, are obtained; for these last seven forms an upper bound for $M(f_m)$ is given. Godwin (20) modified the method of Barnes and Swinnerton-Dyer to give $M(f_m)$ for these seven forms which are the norm forms of those fields with a large fundamental unit.

The basis of the method of (2) is to choose a value M' slightly less than $M(f_m)$ and to show that for (x_1,y_1) in all but a small sub-region R of a fundamental region modulo 1 in the (x,y)-plane there is an integer point (x_0,y_0) such that

$$|f_m(x_1-x_0,y_1-y_0)| \leqslant M'.$$

Having found such a region R, any point $P^* = (x^*,y^*)$ at which $M(f_m,P^*) > M'$ must lie in R and also in its transform by the fundamental automorph E of $f_m(x,y)$; hence points at which $M(f_m)$ is taken must lie in the set R_0 which is common to $E^n(R)$, reduced modulo 1, for all integral values of n. This method is extended to the case of the cubic fields with complex conjugate fields in chapter 4 of this thesis.

I.8 Ennola (14) used a modification of Davenport's method of (8) to obtain the result that for the real quadratic fields $M(K) > \frac{\Delta}{16 + 6\sqrt{6}} > \frac{\Delta}{30.69}$. In this paper Ennola supplies a proof of the results concerning the existence of the Euclidean Algorithm in real quadratic fields which are stated above.

I.9 The results outlined so far are concerned with those fields which possess only one fundamental unit; there are no corresponding general results for other fields. Heilbronn (23) proves that Euclid's Algorithm holds in only a finite number of cyclic cubic fields. Godwin (16) obtains an upper bound for the inhomogeneous minimum of some totally real cubic norm forms, which gives rise to the fact that there is a Euclidean Algorithm in those fields of discriminant 49, 81, 148, 169, 229, 257, 316, and 361; an upper bound is also supplied for the inhomogeneous minimum of the field of discriminant 321 which was shown to possess a Euclidean Algorithm by Smith, the result being quoted in (16). Samet (26) extends the method of Barnes and Swinnerton-Dyer (2) to a special set of linear forms, those corresponding to the field of discriminant 148, and shows that the inhomogeneous minimum is $\frac{1}{2}$ so that the field has a Euclidean Algorithm. In (27) Samet considers the family of fields defined by

$$\theta^3 - a\theta^2 - 2\theta - a = 0 \qquad \text{I.4}$$

where a is a large positive integer; $\theta + 1$, $\theta - 1$ are units with norms -1 and $+1$ respectively and the discriminant is $\Delta^2 = 4a^4 + 13a^2 + 32$. He assumes that $1, \theta, \theta^2$ is a basis for the field, which is the case if Δ^2 has no squared factor other than 4 and $a \equiv 1, 2, 3 \pmod 4$. Then, if ξ, η, ζ are the forms

$$\xi = x + y\theta + z\theta^2$$
$$\eta = x + y\phi + z\phi^2$$
$$\zeta = x + y\psi + z\psi^2$$

where θ, ϕ, ψ are the roots of I.4, by using a modification of the method of Barnes and Swinnerton-Dyer, Samet shows that for all sufficiently large a

(i) $M = \frac{1}{8}a^2$ if $a \equiv 2 \pmod 4$

and this value is taken only at points $P \equiv (0, 0, \frac{1}{2})$

(ii) $M = \frac{1}{8}a^2\left(1 - \frac{1}{a}\right)^3$ if $a \equiv 1$ or $3 \pmod 4$

and this value is taken only at points $P \equiv \pm\left(\frac{1}{a}, 0, \frac{1}{2} - \frac{1}{2a}\right)$.

Smith (28) uses Heilbronn's method to show that the only cyclic cubic fields of discriminant $< 10^8$ which may possess a Euclidean Algorithm are those of discriminants 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2, 73^2, 103^2, 109^2, 127^2 and 157^2. He then goes on to use the method of Barnes and Swinnerton-Dyer (2), as extended by Samet (26), to give the values of the inhomogeneous minima of the fields of discriminants 13^2, 19^2, 31^2, 37^2, 43^2, and 73^2 and to show that the fields of discriminants 61^2 and 67^2 possess a Euclidean Algorithm. Davenport (10) had previously obtained the values of the inhomogeneous minima of the fields of discriminants 7^2 and 9^2, and in this way shown that they possess a Euclidean Algorithm, also, as stated above, Godwin (16) had shown that the fields of discriminants 13^2 (=169) and 19^2 (=361) are Euclidean. Smith shows that the inhomogeneous minima of the fields of discriminants 13^2, 19^2, 31^2, 37^2 and 43^2 are less than 1, and so the fields possess a Euclidean Algorithm; but that of the field of discriminant 73^2 is $\frac{9}{8}$, greater than 1, so that this field does not possess a Euclidean Algorithm.

For fields of higher degree, Godwin (17) has shown that the totally real quartic fields with discriminants 725, 1125, 1600, 1957, 2225, 2304, 2624, 2777 and 4205 possess a Euclidean Algorithm, as does the totally real quintic field $K(2\cos(2\pi/11))$, which is the totally real quintic field of least discriminant.

I.10 I now turn to the cubic fields with complex conjugate fields, which are the subject of this thesis. Godwin (18) adapted his method of (16) and (17) to show that the fields of discriminants

-23, -31, -44, -59, -76, -83, -87, -104, -107, -108, -116, -135, -139, -140, -152 possess a Euclidean Algorithm. The basis of this method is to show that, if a polynomial $P(x)$ has zeros which are not too far apart, the set of x for which $P(x) < 1$ contains a complete set of residues modulo 1. The fifteen fields shown to possess a Euclidean Algorithm are the first fifteen in the table of cubic fields with complex conjugate fields of Angell (1); the method yields no result for other fields, but by the methods described in this thesis I have shown that the next two fields in the table, those of discriminants -172 and -175, also possess a Euclidean Algorithm. The next, that of discriminant -199, has inhomogeneous minimum 1; thus, it is the first in the table which does not possess a Euclidean Algorithm.

I.11 In the following $(1,\theta,\lambda)$ is an integral basis for the cubic number field $K = K(\theta)$, where θ is the real zero of the polynomial $x^3 - ax^2 + bx - c$. The field has discriminant D where $D < 0$, and, if ℓ is the index of the polynomial over the field,

$$\lambda = \frac{\theta^2 + t\theta + s}{\ell} \qquad 0 \leq t,s < \ell$$

where t and s are rational integers.

ϵ is the fundamental unit of K satisfying $0 < \epsilon < 1$ and has algebraic conjugates $\epsilon', \epsilon'' = \bar{\epsilon}'$.

Let θ have algebraic conjugates $\phi, \bar{\phi}$; and λ have algebraic conjugates $\psi, \bar{\psi}$ then $\psi = \dfrac{\phi^2 + t\phi + s}{\ell}$.

Throughout the thesis, the terms number and integer without qualification mean cubic number and cubic integer. Only fields of class number 1 will be considered, since this is a necessary condition for the existence of a Euclidean Algorithm.

Part I describes the theory of the methods of investigation. Chapter 1 gives a summary of the properties of relative minima, since these will be required in later chapters. Chapter 2 gives an extension of a result of Cassels. Chapter 3 considers the fact: if there is no integer of K of norm of absolute value less than $|N(\beta)|$, congruent to ξ modulo β for two integers β and ξ in K, where β is non-zero, there is no Euclidean Algorithm in K; it is shown how this fact may be formulated into a practicable method to show that a field does not possess a Euclidean Algorithm. Chapter 4 shows how the method of Barnes and Swinnerton-Dyer may be adapted to show that a field possesses a Euclidean Algorithm. Chapter 5 shows how the minimum of a point of the form $\frac{\alpha}{1-\epsilon^n}$, where α is an integer of K, may be computed. Chapter 6 uses one particular field to demonstrate each of the methods employed, and describes the limitations of each of these methods.

Part II gives descriptions of the actual programs used, and contains a table showing the results obtained.

PART I

THE THEORY OF THE METHODS OF INVESTIGATION.

CHAPTER 1

RELATIVE MINIMA AND IDEALS WHOSE NORM IS A RATIONAL PRIME.

1.1 We give a short summary of certain properties of relative minima, in particular in the context of fields K which consist of elements $x + y\theta + z\theta^2$ where x, y, z are rational numbers and θ is the real root of a cubic equation of negative discriminant; relative minima will be used in some later chapters.

Consider the space B with general point $(x, y + iz)$, where x, y, z are elements of the real number field. We define the space A to be the set of points $\hat{\alpha} = (\delta(\theta), \delta(\phi))$ where $\alpha = \delta(\theta) = d_1\theta^2 + d_2\theta + d_3$ is in K, and d_1, d_2, d_3 are rational real numbers; the isomorphism $\alpha \leftrightarrow \hat{\alpha}$ then establishes an isomorphism $K \leftrightarrow A$. We have $B \supset A$ and addition, subtraction, multiplication and division are defined component-wise in B and in A.

1.2 If $\hat{\omega} = (x, y + iz)$ is in B, the directional parameters ρ_1, ρ_2 are defined by

$$\rho_1(\hat{\omega}) = |x|$$

$$\rho_2(\hat{\omega}) = y^2 + z^2.$$

From their definitions ρ_1 and ρ_2 are multiplicative.

The normed body of a point $\hat{\alpha}$ in A is defined to be the region $V \subset B$ given by

$$V = \{\hat{\omega}: \hat{\omega} \in B, \ \rho_j(\hat{\omega}) < \rho_j(\hat{\alpha}); \quad j = 1,2\}.$$

1.3 If $\mathfrak{J}$ is an ideal of K and has typical element α, $\hat{\mathfrak{J}}$ is the ideal lattice in A with typical point $\hat{\alpha}$. Multiplicative lattices $\hat{\mathfrak{J}}$ in A are those lattices for which the product of any two points of $\hat{\mathfrak{J}}$ also belongs to $\hat{\mathfrak{J}}$. The ideal lattices are multiplicative.

If $\hat{\alpha}$ is in $\hat{\mathfrak{J}}$, $\hat{\mathfrak{J}}' = \{\hat{\alpha}\hat{\gamma} : \hat{\gamma} \in \hat{\mathfrak{J}}\}$ is also in $\hat{\mathfrak{J}}$ and is a multiplicative lattice; point-lattice multiplication is defined by

$$\hat{\mathfrak{J}}' = \hat{\alpha}\hat{\mathfrak{J}}.$$

If there exists a multiplicative lattice $\hat{\mathfrak{J}}''$ such that $\hat{\mathfrak{J}} = \hat{\alpha}\hat{\mathfrak{J}}''$, point-lattice division is defined by

$$\hat{\mathfrak{J}}'' = \frac{1}{\hat{\alpha}}\hat{\mathfrak{J}}.$$

1.4 A point of an ideal lattice $\hat{\mathfrak{J}}$ in A is called a relative minimum of $\hat{\mathfrak{J}}$ if its normed body contains no other point of $\hat{\mathfrak{J}}$ except the origin.

For a relative minimum $\hat{\Omega}$ of $\hat{\mathfrak{J}}$ we define the region $V(\hat{\Omega}, d)$ by

$$V(\hat{\Omega}, d) = \left\{ \begin{array}{l} \hat{\alpha} : \rho_{j_1}(\hat{\alpha}) < \rho_{j_1}(\hat{\Omega}) \quad j_1 = 1, 2, \\ \quad : \rho_{j_2}(\hat{\alpha}) \leq \rho_{j_2}(\hat{\Omega}) + d \\ \quad\quad d \text{ a real non-negative number, } j_2 = 1, 2, \ j_2 \neq j_1 \end{array} \right\}$$

From Minkowski's convex body theorem there is a lattice point $\hat{\Omega}_1$ which lies in $V(\hat{\Omega}, d)$ for some $d > 0$; and if $\hat{\Omega}_1$ is the first such point obtained by increasing d from 0, $\hat{\Omega}_1$ is also a relative minimum of $\hat{\mathfrak{J}}$. If the point $\hat{\gamma}$ satisfies the conditions stated above for $\hat{\Omega}_1$, $-\hat{\gamma}$ also satisfies them. $\hat{\gamma}' = (x, y + iz)$ is chosen to be $\hat{\gamma}$ or $-\hat{\gamma}$ so that

$$x > 0 \qquad \text{if } j_1 = 2,\ j_2 = 1$$

$$-\frac{\pi}{2} < \arg(y + iz) \leq \frac{\pi}{2} \qquad \text{if } j_1 = 1,\ j_2 = 2;$$

in this way $\hat{\Omega}_1 = \hat{\gamma}'$ is uniquely defined, and will be said to be the relative minimum adjacent to $\hat{\Omega}$ in the ρ_{j_2} direction.

By this means a two-way chain of relative minima $\ldots \hat{\Omega}_{-1}, \hat{\Omega}_0, \hat{\Omega}_1, \hat{\Omega}_2 \ldots$ may be defined. If $\hat{\Omega}_1, \hat{\Omega}_2, \ldots$ are relative minima of $\hat{\mathfrak{J}}$, $\Omega_1, \Omega_2, \ldots$ are said to be relative minima of $\mathfrak{J}$.

A more detailed account of relative minima may be found in (13).

1.5 From now on, in this chapter, we restrict the consideration to the case when K is a cubic field of negative discriminant. In this case, if α is in K, so that $\hat{\alpha}$ is in A, and $N(\hat{\alpha})$ is defined by

$$N(\hat{\alpha}) = \rho_1(\hat{\alpha})\rho_2(\hat{\alpha}),$$

we have $\qquad N(\hat{\alpha}) = |N(\alpha)|.$

LEMMA 1.1

Given an ideal $\mathfrak{J}$, if $\Omega_1, \Omega_2, \ldots, \Omega_j, \ldots$ are successive relative minima of $\mathfrak{J}$, and $\mathfrak{J}$ is divided by these relative minima to give the ideals

$$\mathfrak{J}_1 = \frac{\mathfrak{J}}{\Omega_1};\quad \mathfrak{J}_2 = \frac{\mathfrak{J}}{\Omega_2};\ \ldots\ldots;\quad \mathfrak{J}_j = \frac{\mathfrak{J}}{\Omega_j};\ \ldots\ldots,$$

for some k, $\mathfrak{J}_k$ is the unit ideal $(1, \theta, \lambda)$ and Ω_k produces $\mathfrak{J}$.

PROOF OF LEMMA 1.1

As stated in the introduction, this thesis considers only cubic fields of negative discriminant with class number 1; thus there exists an integer α_1 for which $\mathfrak{J} = (\alpha_1)$.

We suppose, first of all, that α_1 is not a relative minimum of $\mathfrak{J}$, we may find α_2, a relative minimum of $\mathfrak{J}$, such that

$$\rho_{j_1}(\hat{\alpha}_2) < \rho_{j_1}(\hat{\alpha}_1)$$

and
$$\rho_{j_2}(\hat{\alpha}_2) < \rho_{j_2}(\hat{\alpha}_1)$$

which implies

$$|N(\alpha_2)| = N(\hat{\alpha}_2) = \rho_{j_1}(\hat{\alpha}_2)\rho_{j_2}(\hat{\alpha}_2) < \rho_{j_1}(\hat{\alpha}_1)\rho_{j_2}(\hat{\alpha}_1) = N(\hat{\alpha}_1) = |N(\alpha_1)|,$$

this contradicts the choice of α_1 as an integer which produces $\mathfrak{J}$.

From Voronoi, as described in (13), there are only a finite number of distinct ideals among $\mathfrak{J}_1, \mathfrak{J}_2, \ldots, \mathfrak{J}_j, \ldots$; so we have, for some rational integer f,

$$\mathfrak{J}_i = \mathfrak{J}_{i+f}, \quad \mathfrak{J}_i \neq \mathfrak{J}_{i+j} \qquad \text{for } 0 < j \leq f - 1$$

so that $\frac{\mathfrak{J}}{\Omega_i} = \frac{\mathfrak{J}}{\Omega_{i+f}}$

which gives $\frac{\Omega_{i+f}}{\Omega_i} = \epsilon$.

Since α_1 is a relative minimum of $\mathfrak{J}$, for some rational integers k, k_1 we have

$$\Omega_k = \epsilon^{k_1}\alpha_1$$

so that Ω_k produces $\mathfrak{J}$.

Also, if $\mathfrak{J}_k = \frac{\mathfrak{J}}{\Omega_k}$

$$N(\mathfrak{J}_k) = N\left(\frac{\mathfrak{J}}{\Omega_k}\right) = 1,$$

where the norm of an ideal is the norm of any integer which produces it, thus $\mathfrak{J}_k$ is the unit ideal.

1.6 We now turn to a description of the method used for computing, for any rational prime p, the ideals of norm p, the relative minima of each of these ideals and the integers which produce the ideals. The method described follows that used by Angell (1) for finding the ideals and corresponding relative minima for rational integers which are not necessarily prime.

Any ideal of norm p may be represented in the form

$$\mathfrak{J} = (i_1, i_2\theta + i_3, i_4\lambda + i_5\theta + i_6)$$

where $i_1, i_2, i_3, i_4, i_5, i_6$ are positive rational integers, $i_1 . i_2 . i_4 = p$ and from the additive property of ideals $0 \leq i_2 < i_1$, $0 \leq i_4 < i_1$, $0 \leq i_5 < i_2$, $0 \leq i_3 < i_1$, $0 \leq i_6 < i_1$. Since p is prime we have $i_1 = p$, $i_2 = 1$, $i_4 = 1$, $i_5 = 0$, so the ideal may be represented in the form

$$\mathfrak{J} = (p, \theta + i_3, \lambda + i_6) \qquad \text{where } 0 \leq i_3 < p,\ 0 \leq i_6 < p.$$

Thus, given p, for each pair of values, i_3, i_6, in the given range, a test is made for

$$\mathfrak{J} = (p, \theta + i_3, \lambda + i_6)$$

being an ideal. Automatically the additive property of ideals is held by $\mathfrak{J}$, now it remains to show that all the linear combinations of p, $\theta + i_3$, $\lambda + i_6$, when multiplied by an integer of the field, are in $\mathfrak{J}$. This is done by checking that $p\theta$, $p\lambda$, $\theta^2 + i_3\theta$, $\theta\lambda + i_3\lambda$, $\lambda\theta + i_6\theta$, $\lambda^2 + i_6\lambda$ all belong to $\mathfrak{J}$. If all the conditions are satisfied then $\mathfrak{J}$ is an ideal of norm p. We note that, since $N(p) = p^3$, there are at most three distinct ideal factors of (p), other than the unit ideal, and so at most three distinct ideals of norm p.

1.7 The method of determination of the relative minima of the ideals follows the steps of Voronoi's algorithm as enumerated in (13). We have the ideal $\mathfrak{J} = (p, \theta + i_3, \lambda + i_6)$, for application of the algorithm we consider the ideal $\frac{\mathfrak{J}}{p} = (1, \frac{\theta + i_3}{p}, \frac{\lambda + i_6}{p})$ which under the transformation $\zeta = 3\theta - a$, so that $\zeta^3 = q\zeta + n$ for some rational integers q and n, becomes

$$(1, \frac{m_1 + m_2\zeta + m_3\zeta^2}{i_9}, \frac{n_1 + n_2\zeta + n_3\zeta^2}{i_9})$$

for some rational integers $m_1, m_2, m_3, n_1, n_2, n_3, i_g$. Following the steps of the algorithm we obtain a basis $(1, \theta_g, \theta_h)$ for $\frac{\mathfrak{J}}{p}$, where θ_g is the relative minimum of $\frac{\mathfrak{J}}{p}$ adjacent to 1 in the ρ_2 direction; this basis is said to be the reduced basis of the lattice. The ideal $\frac{\mathfrak{J}}{p}$ is divided by θ_g to give the ideal with basis $(1, \frac{\theta_h}{\theta_g}, \frac{1}{\theta_g})$ and the process is repeated to obtain a reduced basis for this ideal.

In this way we obtain a sequence of ideals $\mathfrak{J}_1 = \frac{\mathfrak{J}}{p}$, $\mathfrak{J}_2 = \frac{\mathfrak{J}_1}{\theta_g^{(1)}}$, . . . , $\mathfrak{J}_{k+1} = \frac{\mathfrak{J}_k}{\theta_g^{(k)}}$ with reduced bases $(1, \theta_g^{(1)}, \theta_h^{(1)}) = (1, \theta_g, \theta_h)$, $(1, \theta_g^{(2)}, \theta_h^{(2)})$, . . . , $(1, \theta_g^{(k+1)}, \theta_h^{(k+1)})$ respectively, where $\mathfrak{J}_{k+1}$ is the unit ideal. The reduced basis of the unit ideal is previously found by applying one cycle of Voronoi's algorithm to the ideal $(1, \theta, \lambda)$.

From this we see that

$$\mathfrak{J} = (p \prod_{i=1}^{k} \theta_g^{(i)})$$

and, when $p = 1$, the relative minima of the field are given by

$$1, \theta_g^{(1)}, \theta_g^{(1)}\theta_g^{(2)}, \theta_g^{(1)}\theta_g^{(2)}\theta_g^{(3)}, \ldots\ldots,$$

so that $\mathfrak{J}$ is the integral lattice of the field; in this case

$$\prod_{i=1}^{k} \theta_g^{(i)} = \epsilon \quad \text{the fundamental unit of the field.}$$

CHAPTER 2

AN ADAPTATION OF A RESULT OF CASSELS.

2.1 Let $K(\theta)$ be the cubic field of discriminant $D = -\Delta^2$, if θ is a zero of the polynomial $P(x)$ let ℓ be the index of P over the field. Define the space $\mathfrak{a}$ to consist of points (ξ, η, ζ) where $\zeta \in K(\theta)$ and $\xi \pm i\eta$ are the algebraic conjugates of ζ; let (ξ, η, ζ) be said to be an integer point of $\mathfrak{a}$ when ζ is an integer of $K(\theta)$, then the integer points of $\mathfrak{a}$ form a lattice $\mathfrak{K}_\theta$.

Cassels (5) shows that there exists a point (ξ, η, ζ) of $\mathfrak{a}$ such that

$$\min|\zeta_0(\xi_0^2 + \eta_0^2)| > \frac{2|\Delta|}{81(5 + 3\sqrt{3})} = \frac{|\Delta|}{412.944\ldots} \qquad 2.1$$

where the minimum is over all points $(\xi_0, \eta_0, \zeta_0) \equiv (\xi, \eta, \zeta) \pmod 1$.

In the following it will be shown that, for any field for which $\ell = 1$, a value M, which depends on the relative minima of the field, may be found such that there exists a point (ξ, η, ζ) of $\mathfrak{a}$ such that

$$\min|\zeta_0(\xi_0^2 + \eta_0^2)| > \frac{2|D|}{81(9 + 5\sqrt{3})M} = \frac{|D|}{715.24\ldots M} \qquad 2.2$$

where the minimum is over all points $(\xi_0, \eta_0, \zeta_0) \equiv (\xi, \eta, \zeta) \pmod 1$.
For any such field

$$\frac{2|D|}{81(9 + 5\sqrt{3})M} \geqslant \frac{2|\Delta|}{81(5 + 3\sqrt{3})} \qquad 2.3$$

we note that

$$81(9 + 5\sqrt{3}) = \sqrt{3}.81(5 + 3\sqrt{3}).$$

Using this result I have investigated two fields of discriminant such that no result concerning the Euclidean Algorithm can be obtained using Cassels' result; both of these fields were shown to possess no Euclidean Algorithm.

In the more general case when ℓ is not equal to 1 we may establish that there exists a point (ξ, η, ζ) of $\mathfrak{a}$ such that

$$\min|\zeta_0(\xi_0^2 + \eta_0^2)| > \frac{2|D|\ell^2}{81(9+5\sqrt{3})M^*}, \tag{2.4}$$

where the minimum is over all points $(\xi_0, \eta_0, \zeta_0) \equiv (\xi, \eta, \zeta) \pmod 1$, for a particular value M^* which depends on the field in question. However, we cannot establish a relationship with Cassels' result similar to 2.3.

2.2 Suppose that $\mathcal{K}$ is any three dimensional lattice which contains an infinite sequence of points $P_n = (\beta_n, \gamma_n, \alpha_n)$ such that

$$|\alpha_n| > |\alpha_{n+1}|$$
$$|\beta_n^2 + \gamma_n^2| < |\beta_{n+1}^2 + \gamma_{n+1}^2|$$

LEMMA 2.1

Define $$M = \max_n |\alpha_n(\beta_{n+1}^2 + \gamma_{n+1}^2)|$$

then, given p, q such that $pq^2 \geqslant M$, there is a point of the lattice, $P = (\beta, \gamma, \alpha)$, not equal to $(0,0,0)$, such that

$$|\beta^2 + \gamma^2| \leq q^2$$
$$|\alpha| \leq p$$

This result is best possible for the value of the lower bound of pq^2 when the sequence $\{\beta_n, \gamma_n, \alpha_n\}$ is a sequence of relative minima of the lattice and is periodic.

PROOF OF LEMMA 2.1

Given p, we define n by

$$|\alpha_n| > p \geqslant |\alpha_{n+1}|$$

which is possible since the sequence $\{\alpha_n\}$ is decreasing. If

$$q^2 < |\beta_{n+1}^2 + \gamma_{n+1}^2|$$

then
$$pq^2 < |\alpha_n||\beta_{n+1}^2 + \gamma_{n+1}^2| \leqslant M$$

which is false. Hence

$$q^2 \geqslant |\beta_{n+1}^2 + \gamma_{n+1}^2|$$

and $(\beta_{n+1}, \gamma_{n+1}, \alpha_{n+1})$ is the required point.

If the sequence $\{\beta_n, \gamma_n, \alpha_n\}$ is a sequence of relative minima of the lattice, for any rational integer n there is no point (β, γ, α) for which

$$|\alpha| < |\alpha_n|$$

and
$$|\beta^2 + \gamma^2| < |\beta_{n+1}^2 + \gamma_{n+1}^2| .$$

If the sequence is periodic, there exists a rational integer m for which

$$M = \alpha_m(\beta_{m+1}^2 + \gamma_{m+1}^2).$$

Let $M' = M - \delta$ for some positive real number δ and let p, q be such that

$$M' \leqslant pq^2 < M$$

$$p < |\alpha_m|$$

$$q < |\beta_{m+1}^2 + \gamma_{m+1}^2|^{\frac{1}{2}}$$

then any point (β, γ, α) satisfying

$$|\beta^2 + \gamma^2| \leqslant q^2 \quad \text{and} \quad |\alpha| \leqslant p$$

must also satisfy

$$|\beta^2 + \gamma^2| < |\beta_{m+1}^2 + \gamma_{m+1}^2| \quad \text{and} \quad |\alpha| < |\alpha_m|$$

which contradicts the definition of $\{\beta_n, \gamma_n, \alpha_n\}$ as a sequence of relative minima. Hence M is best possible in this case.

2.3 Let the linear forms L_1, L_2, L_3 be defined by

$$\begin{aligned} L_1 &= x + y\theta + z\lambda \\ L_2 &= x + y\phi + z\psi \\ L_3 &= x + y\bar{\phi} + z\bar{\psi} \end{aligned} \qquad 2.5$$

where x, y, z are rational, so that L_2 and $L_3 = \bar{L}_2$ are the algebraic conjugates of L_1.

The matrix

$$\begin{pmatrix} 1 & \theta & \lambda \\ 1 & \phi & \psi \\ 1 & \bar{\phi} & \bar{\psi} \end{pmatrix}$$

has adjoint

$$\begin{pmatrix} \phi\bar{\psi} - \bar{\phi}\psi & \bar{\phi}\lambda - \theta\bar{\psi} & \theta\psi - \phi\lambda \\ \psi - \bar{\psi} & \bar{\psi} - \lambda & \lambda - \psi \\ \bar{\phi} - \phi & \theta - \bar{\phi} & \phi - \theta \end{pmatrix}.$$

Define the linear forms M_1, M_2, M_3 in the rational variables u, v, w by

$$\begin{aligned} M_1 &= \frac{1}{i}\{(\phi\bar{\psi} - \bar{\phi}\psi)u + (\psi - \bar{\psi})v + (\bar{\phi} - \phi)w\} \\ M_2 &= \frac{1}{i}\{(\bar{\phi}\lambda - \theta\bar{\psi})u + (\bar{\psi} - \lambda)v + (\theta - \bar{\phi})w\} \\ M_3 &= \frac{1}{i}\{(\theta\psi - \phi\lambda)u + (\lambda - \psi)v + (\phi - \theta)w\} \end{aligned} \qquad 2.6$$

then M_1 is real, M_2, M_3 are conjugate complex and are the algebraic conjugates of M_1; M_1, M_2, M_3 have determinant Δ^2. We also have

$$M_1L_1 + M_2L_2 + M_3L_3 = (xu + yv + zw)\Delta \qquad 2.7$$

These definitions of M_1, M_2, M_3, L_1, L_2, L_3 are then the same as those given for the ternary cubic case in Cassels (5).

2.4 There are rational integers a_λ, b_λ, c_λ, l_1, l_2, l_3, t_1, t_2, t_3, p_1, p_2, p_3 such that $\lambda, \psi, \bar{\psi}$ are the zeros of

$$x^3 - a_\lambda x^2 + b_\lambda x - c_\lambda \qquad 2.8$$

and

$$\lambda^2 = l_1\lambda + l_2\theta + l_3$$

$$\theta^2 = t_1\lambda + t_2\theta + t_3 \qquad 2.9$$

$$\theta\lambda = p_1\lambda + p_2\theta + p_3 \;;$$

also, equalities corresponding to 2.8 hold for ϕ, ψ and for $\bar{\phi}, \bar{\psi}$.

We have $\phi\bar{\psi} - \bar{\phi}\psi = (\phi - \bar{\phi})(a_\lambda - \lambda) + p_1(\bar{\psi} - \psi) + p_2(\bar{\phi} - \phi)$

and $(\phi + \bar{\phi})(\phi - \bar{\phi}) = t_1(\psi - \bar{\psi}) + t_2(\phi - \bar{\phi})$,

thus $\psi - \bar{\psi} = (\bar{\phi} - \phi)\left\{ \dfrac{\theta - a + t_2}{t_1} \right\}$

and so

$$M_1 = \frac{(\bar{\phi} - \phi)}{i}\left\{ u(\lambda - a_\lambda) + (v - up_1)\frac{(\theta - a)}{t_1} + w + up_2 + \frac{(v - up_1)}{t_1}t_2 \right\}$$

with similar expressions for M_2 and M_3.

Thus the linear forms M_1, M_2, M_3 may be given by

$$M_1 = \frac{(\bar{\phi} - \phi)}{it_1}\left\{ u\lambda t_1 + v\theta + w \right\}$$

$$M_2 = \frac{(\theta - \bar{\phi})}{it_1}\left\{ u\psi t_1 + v\phi + w \right\} \qquad 2.10$$

$$M_3 = \frac{(\phi - \theta)}{it_1}\left\{ u\bar{\psi} t_1 + v\bar{\phi} + w \right\}$$

and the set of points $\left(\dfrac{M_2 + M_3}{2}, \dfrac{M_2 - M_3}{2i}, M_1 \right)$, for integer values of u, v, w, forms a three dimensional lattice $\mathcal{K}_T$. We also note that $t_1 = l$, the index of P over K.

2.5 The general case when l may take any value is discussed in section 2.10.

We now restrict the consideration to the case when $l = 1$. We have $\lambda = \theta^2$, $\psi = \phi^2$ and $\bar{\psi} = \bar{\phi}^2$ thus

$$M_1 = \frac{(\bar\phi - \phi)}{i}\left\{u\theta^2 + v\theta + w\right\}$$
$$M_2 = \frac{(\theta - \bar\phi)}{i}\left\{u\phi^2 + v\phi + w\right\}$$
$$M_3 = \frac{(\phi - \theta)}{i}\left\{u\bar\phi^2 + v\bar\phi + w\right\},$$

then (β, γ, α), where α, $\beta \pm i\gamma$ are values of M_1, M_2, M_3 respectively, is a point of $\mathcal{K}_T$ if and only if there is a point (ξ, η, ζ) of $\mathcal{K}_\theta$ such that

$$\alpha = \frac{(\bar\phi - \phi)}{i}\zeta; \quad \beta + i\gamma = \frac{(\theta - \bar\phi)}{i}(\xi + i\eta); \quad \beta - i\gamma = \frac{(\phi - \theta)}{i}(\xi - i\eta).$$

In the field K we may find an infinite sequence of relative minima $\{\zeta_n\}$ which corresponds to an infinite sequence of points of $\mathcal{K}_\theta$, $\{\xi_n, \eta_n, \zeta_n\}$ for which

$$|\zeta_{n-1}| > |\zeta_n|$$
$$|\xi_{n-1}^2 + \eta_{n-1}^2| < |\xi_n^2 + \eta_n^2|.$$

Thus there is a sequence of points $\{\beta_n, \gamma_n, \alpha_n\}$ in $\mathcal{K}_T$, for which

$$\alpha_n = \frac{(\bar\phi - \phi)}{i}\zeta_n$$

so that $\quad |\alpha_n| = \left|\frac{\bar\phi - \phi}{i}\right||\zeta_n| > \left|\frac{\bar\phi - \phi}{i}\right||\zeta_{n+1}| = |\alpha_{n+1}|;$

that is $\quad |\alpha_n| > |\alpha_{n+1}|.$

Also

$$\beta_n + i\gamma_n = \frac{(\theta - \bar\phi)}{i}(\xi_n + i\eta_n)$$
$$\beta_n - i\gamma_n = \frac{(\phi - \theta)}{i}(\xi_n - i\eta_n)$$

so that

$$|\beta_n^2 + \gamma_n^2| = |(\theta - \bar\phi)(\phi - \theta)||\xi_n^2 + \eta_n^2| < |(\theta - \bar\phi)(\phi - \theta)||\xi_{n+1}^2 + \eta_{n+1}^2|$$
$$= |\beta_{n+1}^2 + \gamma_{n+1}^2|;$$

that is $\quad |\beta_n^2 + \gamma_n^2| < |\beta_{n+1}^2 + \gamma_{n+1}^2|.$

We also have the sequence $\{\beta_n, \gamma_n, \alpha_n\}$ a sequence of relative minima of the lattice $\mathcal{K}_T$; if not, for some integer n there is a point (β, γ, α) of $\mathcal{K}_T$ such that

$$|\beta^2 + \gamma^2| \leq |\beta_{n+1}^2 + \gamma_{n+1}^2|$$
$$|\alpha| < |\alpha_n|,$$

which implies that there is a point (ξ, η, ζ) of $\mathcal{K}_\theta$ for which

$$|\xi^2 + \eta^2| \leq |\xi_{n+1}^2 + \eta_{n+1}^2|$$
$$|\zeta| < |\zeta_n|$$

which contradicts the definition of $\{\xi_n, \eta_n, \zeta_n\}$ as a sequence of relative minima of $\mathcal{K}_\theta$.

Now let

$$M = \max_n |\zeta_n(\xi_{n+1}^2 + \eta_{n+1}^2)|$$

and

$$\begin{aligned} M_T &= \max_n |\alpha_n(\beta_{n+1}^2 + \gamma_{n+1}^2)| \\ &= \max_n |(\bar\phi - \phi)(\theta - \bar\phi)(\phi - \theta)||\zeta_n(\xi_{n+1}^2 + \eta_{n+1}^2)| \\ &= |\Delta| \max_n |\zeta_n(\xi_{n+1}^2 + \eta_{n+1}^2)| \\ &= |\Delta| M. \end{aligned}$$

2.6 Define E by

$$E(\xi, \eta, \zeta) = (\xi', \eta', \zeta')$$

when

$$\epsilon\zeta = \zeta'$$
$$\epsilon'(\xi + i\eta) = (\xi' + i\eta')$$
$$\epsilon''(\xi - i\eta) = (\xi' - i\eta'),$$

then for some rational integer $f > 0$ and every rational integer n

$$E(\xi_n, \eta_n, \zeta_n) = (\xi_{n+f}, \eta_{n+f}, \zeta_{n+f}) \quad \text{(see chapter 1)}$$

so that $\epsilon\zeta_n = \zeta_{n+f}$,

and if $\rho_\epsilon^2 = \epsilon'\epsilon''$,

$$\rho_\epsilon^2(\xi_n^2 + \eta_n^2) = (\xi_{n+f}^2 + \eta_{n+f}^2)$$

for every rational integer n.

Thus we have

$$\begin{aligned} |\zeta_{n+f}(\xi_{n+1+f}^2 + \eta_{n+1+f}^2)| &= |\epsilon\zeta_n\rho_\epsilon^2(\xi_{n+1}^2 + \eta_{n+1}^2)| \\ &= |\zeta_n(\xi_{n+1}^2 + \eta_{n+1}^2)| \end{aligned}$$

hence $$M = \max_{n_0 \leq n \leq n_0+f-1} |\zeta_n(\xi_{n+1}^2 + \eta_{n+1}^2)| . \qquad 2.11$$

Therefore, in calculating M only one loop of relative minima of K need be considered; we note that, since the sequence $\{\xi_n, \eta_n, \zeta_n\}$ is periodic, the sequence $\{\beta_n, \gamma_n, \alpha_n\}$ is also periodic.

We now see that the sequence $\{\beta_n, \gamma_n, \alpha_n\}$ satisfies the conditions of lemma 2.1, hence, given p, q such that $pq^2 \geq M_T$, there is a point of the lattice, (β, γ, α), not equal to $(0,0,0)$, such that

$$|\beta^2 + \gamma^2| \leq q^2$$

$$|\alpha| \leq p;$$

thus, by definition of (β, γ, α), there exist integer values of u, v, w, not all zero, such that

$$|M_1| \leq p, \quad |M_2| = |M_3| \leq q.$$

2.7 We now have the following lemma corresponding to lemma 12 of (5).

LEMMA 2.2

Let $k > 1$ be given. There is an infinite set of values α_n, μ_n, $\nu_n = \bar{\mu}_n$ of M_1, M_2, M_3 corresponding to integer values u_n, v_n, w_n of u, v, w, as used in the expressions 2.6, such that

$$\begin{aligned} &\text{(i)} \quad |\alpha_n \mu_n^2| \leq |\Delta| M \\ &\text{(ii)} \quad k|\alpha_n| \leq |\alpha_{n-1}| \\ &\text{(iii)} \quad |\mu_n^2||\alpha_{n-1}| \leq k|\Delta| M \\ &\text{(iv)} \quad |\mu_n| \geq |\mu_{n-1}| \end{aligned} \qquad 2.12$$

PROOF OF LEMMA 2.2

By construction of M_T there is a set of values α_0, μ_0, ν_0 satisfying (i). Now define α_n, μ_n, ν_n by induction, given $\alpha_{n-1}, \mu_{n-1}, \nu_{n-1}$

$$|\alpha_n| \leq k^{-1}|\alpha_{n-1}| \qquad \text{hence (ii) is satisfied}$$

$$|\mu_n^{*}| \leq \frac{k|\Delta|M}{|\alpha_{n-1}|} \qquad \text{hence (iii) is satisfied.}$$

α_n, μ_n, ν_n exist since $k^{-1}|\alpha_{n-1}| \dfrac{k|\Delta|M}{|\alpha_{n-1}|} = |\Delta|M$.

At each stage the smallest μ_n satisfying (iv) is chosen, otherwise μ_n instead of μ_{n-1} would have been chosen at the previous stage.

We now have the following two lemmas, reproduced from lemmas 13 and 14 of (5).

LEMMA 2.3

If $k > 2$, we may find values x_0, y_0, z_0 of x, y, z, as used in the definitions 2.5, such that

$$\| x_0 u_n + y_0 v_n + z_0 w_n \| \geq \frac{k - 2}{2(k - 1)}$$

for all n; where u_n, v_n, w_n are the values of u, v, w, in the definitions 2.6, corresponding to the values α_n, μ_n, ν_n of M_1, M_2, M_3, and

$$\|x\| = \min|m - x|$$

where the minimum is over rational integer values of m.

LEMMA 2.4

Suppose that $k > 2$

$$r = \left(\frac{k + k^{\frac{1}{2}}}{2}\right)^{\frac{1}{3}}, \qquad q = kr^{-2}$$

so that $qr^2 = k$, $q + 2q^{-\frac{1}{2}} = 2r + r^{-2} = 2^{\frac{2}{3}}\dfrac{(1 + k^{\frac{1}{2}} + k)}{(k + k^{\frac{1}{2}})^{\frac{2}{3}}} = \lambda$ (say).

If l, m, p are positive numbers such that

$$l m^2 \le p^3, \quad l \le qp, \quad m \le rp$$

then
$$l + 2m \le \lambda p.$$

2.8 Now let $\zeta, \xi + i\eta, \xi - i\eta$ be values taken by L_1, L_2, L_3 for some

$$(x, y, z) \equiv (x_0, y_0, z_0) \pmod{1},$$

and let r and q be defined in terms of k as for lemma 2.4.

Choose n such that

$$|\mu_n^2| \le r^2 |\zeta|^{\frac{2}{3}} |\xi^2 + \eta^2|^{-\frac{1}{3}} (|\Delta| M)^{\frac{2}{3}} \le |\mu_{n+1}^2|,$$

then by (iii) of lemma 2.2

$$|\alpha_n| \le \frac{k|\Delta| M}{|\mu_{n+1}^2|} \le kr^{-2} |\zeta|^{-\frac{2}{3}} |\xi^2 + \eta^2|^{\frac{1}{3}} (|\Delta| M)^{\frac{1}{3}}$$

$$|\alpha_n| \le q |\zeta|^{-\frac{2}{3}} |\xi^2 + \eta^2|^{\frac{1}{3}} (|\Delta| M)^{\frac{1}{3}}.$$

By applying lemma 2.4 with

$l = |\zeta\alpha_n|$, $m = |(\xi + i\eta)\mu_n|$ and $p = |\zeta|^{\frac{1}{3}} |\xi^2 + \eta^2|^{\frac{1}{3}} (|\Delta| M)^{\frac{1}{3}}$

we have

$$|\zeta\alpha_n| + 2|(\xi + i\eta)\mu_n| \le \lambda |\zeta|^{\frac{1}{3}} |\xi^2 + \eta^2|^{\frac{1}{3}} (|\Delta| M)^{\frac{1}{3}},$$

but

$$|\Delta| | xu_n + yv_n + zw_n| = |\zeta\alpha_n + (\xi + i\eta)\mu_n + (\xi - i\eta)\nu_n|$$
$$\le |\zeta\alpha_n| + 2|(\xi + i\eta)\mu_n|;$$

thus, since

$$\| x_0 u_n + y_0 v_n + z_0 w_n \| \ge \frac{k - 2}{2(k - 1)} \qquad \text{for all } n,$$

$$|\zeta(\xi^2 + \eta^2)| \ge \frac{|\Delta|^3}{|\Delta| M}\left(\frac{(k - 2)}{2(k - 1)\lambda} \right)^3 = \frac{|D|}{M} \frac{(k - 2)^3 (k + k^{\frac{1}{2}})^2}{2^5 (k - 1)^3 (1 + k^{\frac{1}{2}} + k)^3}$$
$$= \frac{|D| f(k)}{M\ 2^5}.$$

$f(k)$ attains a maximum, F, when $k = (\sqrt{3} + 1)^2$, so we have

$$|\zeta(\xi^2 + \eta^2)| \ge \frac{|D|}{M} \frac{(2 + 2\sqrt{3})^3 (5 + 3\sqrt{3})^2}{2^5 (3 + 2\sqrt{3})^3 (6 + 3\sqrt{3})^3} = \frac{2|D|}{81(9 + 5\sqrt{3})M} \ge \frac{|D|}{M.715.24\ldots}$$

that is the result 2.2.

2.9 For the second part of the result we note that in lemma 11 of (5) it is stated that:

if $p > 0$, $q > 0$ are given and $pq^2 \geqslant |\Delta|^2 3^{-\frac{1}{2}}$, then there exist integer values u, v, w (as in 2.10), not all zero, such that

$$|M_1| \leqslant p, \quad |M_2| = |M_3| \leqslant q;$$

but from lemma 2.1, if $p > 0$, $q > 0$ are given and $pq^2 \geqslant M_T = |\Delta| M$, there exist integer values u, v, w, not all zero, such that

$$|M_1| \leqslant p, \quad |M_2| = |M_3| \leqslant q.$$

But lemma 2.1 also states that $M_T = |\Delta| M$ is best possible as a lower bound of pq^2, thus we have

$$|\Delta| M \leqslant |\Delta|^2 3^{-\frac{1}{2}}$$

hence

$$\frac{2|D|}{81(9 + 5\sqrt{3})M} = \frac{|D| F}{M . 2^5} = \frac{|\Delta|^3 F}{M . |\Delta| . 2^5} \geqslant \frac{|\Delta|^3 F}{|\Delta|^2 3^{-\frac{1}{2}} 2^5} = \frac{|\Delta| 3^{\frac{1}{2}} F}{2^5} = \frac{2|\Delta|}{81(5 + 3\sqrt{3})}$$

that is

$$\frac{2|D|}{81(9 + 5\sqrt{3})M} \geqslant \frac{2|\Delta|}{81(5 + 3\sqrt{3})}$$

which is the result 2.3.

2.10 I return now to the case when l may have any value. We note, from 2.10, that (β, γ, α) is a point of $\mathcal{K}_T$ if and only if there is a point (ξ, η, ζ) in K, such that

(i) $$\zeta = x + y\theta + z\theta^2 = x' + y'\theta + zt_1\lambda$$

for some rational integers x, y, x', y', z

(ii) $\alpha = \dfrac{(\bar{\Phi} - \phi)}{il}\zeta$; $\beta + i\gamma = \dfrac{(\theta - \bar{\Phi})}{il}(\xi + i\eta)$; $\beta - i\gamma = \dfrac{(\phi - \theta)}{il}(\xi - i\eta)$.

We now define K^* to be that subset of K which has basis $(1, \theta, \theta^2)$, that is the subset with basis $(1, \theta, l\lambda)$. K^* is also a field, and the sublattice $\mathcal{K}_\theta^*$ of $\mathcal{K}_\theta$ which consists of those points (ξ, η, ζ), where $\zeta \in K^*$, is a multiplicative lattice. $\zeta = x + y\theta + z\ell\lambda$ is said to be an integer of K^* when x, y, z are all rational integers; and (ξ, η, ζ) is said to be an integer point of $\mathcal{K}_\theta^*$ when ζ is an integer of K^*.

Since $\mathcal{K}_\theta^*$ is a multiplicative lattice, we may find an infinite sequence of relative minima $\{\zeta_n^*\}$ in K^* which corresponds to an infinite sequence of integer points of $\mathcal{K}_\theta^*$, $\{\xi_n^*, \eta_n^*, \zeta_n^*\}$, for which

$$|\zeta_{n-1}^*| > |\zeta_n^*|$$

$$|\xi_{n-1}^{*2} + \eta_{n-1}^{*2}| < |\xi_n^{*2} + \eta_n^{*2}|,$$

and a corresponding sequence, $\{\beta_n, \gamma_n, \alpha_n\}$, in $\mathcal{K}_T$ such that

$$|\alpha_{n-1}| > |\alpha_n|$$

$$|\beta_{n-1}^2 + \gamma_{n-1}^2| < |\beta_n^2 + \gamma_n^2|.$$

However, this sequence in $\mathcal{K}_T$ is not necessarily a sequence of relative minima; nor can it be shown to be periodic, since the field K^* cannot be shown to have a fundamental automorphism.

Following the arguments of 2.5, 2.7 and 2.8 with M replaced by M^*, where

$$M^* = \max_n |\zeta_n^*(\xi_{n+1}^{*2} + \eta_{n+1}^{*2})|$$

so that

$$M_T = \max_n |\alpha_n(\beta_{n+1}^2 + \gamma_{n+1}^2)| = \frac{|\Delta|\ell M^*}{\ell^3} = \frac{|\Delta| M^*}{\ell^2},$$

and eventually we obtain

$$|\zeta(\xi^2 + \eta^2)| \geq \frac{2|D|\ell^2}{M^* 81(9 + 5\sqrt{3})},$$ the result 2.4.

2.11 For computing this method, the sequence of numbers $\theta_g^{(1)}, \ldots, \theta_g^{(k)}$, corresponding to the ideal of integers of the field, are calculated as described in chapter 1. We now observe that, in obtaining the products of these numbers to give the relative minima of the field, if $r_1\theta^2 + r_2\theta + r_3$, where r_1, r_2, r_3 are rational integers, is such a relative minimum, the coefficients r_1, r_2, r_3 become large in absolute value as the relative minima become closer to ϵ. This fact causes loss of accuracy in the calculation of $\alpha_n, \beta_n, \gamma_n$ and so in the calculation of M, even with double precision arithmetic.

Suppose

$$\epsilon = i_\epsilon\theta^2 + j_\epsilon\theta + k_\epsilon$$

then

$$\begin{aligned}\epsilon^{-1} = \epsilon'\epsilon'' &= (i_\epsilon\phi^2 + j_\epsilon\phi + k_\epsilon)(i_\epsilon\bar{\phi}^2 + j_\epsilon\bar{\phi} + k_\epsilon)\\ &= i_\epsilon^2(\theta^2 - a\theta + b)^2 + j_\epsilon^2(\theta^2 - a\theta + b) + k_\epsilon^2\\ &\quad + i_\epsilon j_\epsilon(\theta^2 - a\theta + b)(a - \theta)\\ &\quad + i_\epsilon k_\epsilon(\theta^2 - a^2 + 2b) + j_\epsilon k_\epsilon(a - \theta).\end{aligned}$$

From this expression we see that if the coefficients of $1, \theta, \theta^2$ in the expression for ϵ are $0(n)$ then those in the expression for ϵ^{-1} are $0(n^2)$.

2.12 We have a complete loop of relative minima of the field given by

$$1,\ \theta_g^{(1)},\ \theta_g^{(2)}\theta_g^{(1)},\ \ldots\ldots,\ \prod_{i=1}^{k}\theta_g^{(i)};$$

since $\prod_{i=1}^{k}\theta_g^{(i)}$ is the fundamental unit of the field

$$\Big(\prod_{i=j+1}^{k}\theta_g^{(i)}\Big)^{-1},\ \Big(\prod_{i=j+2}^{k}\theta_g^{(i)}\Big)^{-1},\ \ldots,\ \big(\theta_g^{(k)}\big)^{-1},\ 1,\ \theta_g^{(1)},\ \ldots,\ \prod_{i=1}^{j}\theta_g^{(i)}$$

is also a complete loop of relative minima of the field when j is an integer satisfying $0 \leqslant j \leqslant k$.

We choose j so that the order of magnitude of the coefficients of $1, \theta, \theta^2$ in the expression for $\prod_{i=1}^{j} \theta_g^{(i)}$ and in that for $(\prod_{i=j+1}^{k} \theta_g^{(i)})^{-1}$ will be approximately the same. In view of the result stated above for the coefficients in the expressions for ϵ and ϵ^{-1}, we choose $j = \left[\frac{2k}{3}\right]$ where $[i]$ represents the greatest integer less than i.

When this particular loop of relative minima has been calculated, we may calculate the α_n and β_n and so M; the loss of accuracy when using double precision arithmetic is not now significant. The multiplication and division routines used in calculating the relative minima check for the possibility of overflow, which in this case is interpreted as the result yielding an integer with more digits than double precision arithmetic allows significant figures.

In this way we find a lower bound on the inhomogeneous minimum of the field; for simplicity, in the program the constant 715.24... is replaced by 720.

CHAPTER 3

A METHOD WHICH USES CONGRUENCES TO FIND A POINT α IN K FOR WHICH $M(K,\alpha) \geq 1$.

3.1 I.1 is equivalent to the statement that there is no integer of K with norm of absolute value less than $|N(\beta)|$ congruent to ξ modulo β.

The method of congruences which is used to prove that there is no Euclidean Algorithm in a particular field is based on this fact, and may be summarized in the following steps:

(I) An integer β is chosen and representatives of each of its non-zero residue classes are calculated; suppose these representatives are denoted by $\xi_1, \xi_2, \ldots, \xi_{r_\beta}$ where $r_\beta = |N(\beta)| - 1$. Let $Z = \{\xi_j : 1 \leq j \leq r_\beta\}$ be the set of representatives.

(II) For each ideal $\mathfrak{J}$ of norm of absolute value less than $|N(\beta)|$, an integer α which produces it is calculated; we then have $\mathfrak{J} = (\alpha)$. Let the set of these integers be $\{\alpha_j : 1 \leq j \leq m\}$, then any integer of norm of absolute value less than $|N(\beta)|$ is of the form $\alpha_j \epsilon^w$ for some j satisfying $1 \leq j \leq m$ and some rational integer w.

(III) If h is the smallest positive rational integer for which $\epsilon^h \equiv 1 \ (\beta)$, we find the set Λ defined by

$$\Lambda = \{\xi_g : \xi_g \equiv \alpha_j \epsilon^w \ (\beta),\ 1 \leq j \leq m,\ 0 \leq w \leq h-1,\ \xi_g \in Z\}.$$

If $Z = \Lambda$ then no conclusion is reached about the existence of a Euclidean Algorithm in K. If there is a representative $\zeta = \zeta_L$ where $1 \leqslant L \leqslant r_\beta$ and ζ is in $(Z - \Lambda)$, there is no Euclidean Algorithm in K.

The remainder of this chapter describes the method of computing this algorithm.

3.2 An underlying problem of this method is to find, for any given positive rational integer n, the distinct ideals of norm n and the integers which produce them.

If $n = p$, a rational prime, the ideals and corresponding integers are found as described in chapter 1.

We now consider the case when $n = p^r$, where p is a rational prime and r is a positive rational integer not equal to 1.

It has been noted in chapter 1 that (p) has at most three distinct ideal factors; we also note that (p) has a square factor if and only if p divides D, the discriminant of the field. The possible factorizations of (p) and consequently the ideals of norm n are as follows

(i) (p) is a prime ideal in K hence there are no ideals of norm p; this may occur only if p does not divide D. There will only be an ideal of norm n if r is a multiple of 3, when the only such ideal is $(p^{r/3})$; if r is not a multiple of 3, (n) is a prime ideal in K.

(ii) $(p) = \mathfrak{J}.\mathfrak{Q}$ where $\mathfrak{J}$ is an ideal of norm p and $\mathfrak{Q}$ is a prime ideal of norm p^2; this may occur only if p does not divide D. There is one ideal (α) of norm p and one ideal (β) of norm p^2; the ideals of norm p^r

are $(\alpha^u \beta^{\frac{r-u}{2}})$ where 2 divides $r - u$ and $r \geq u \geq 0$.

(iii) $(p) = \mathfrak{J}^3$ where $\mathfrak{J}$ is an ideal of norm p; we only have this situation if p divides D. There is just one ideal (α) of norm p and, consequently, just one ideal (α^r) of norm p^r.

(iv) $(p) = \mathfrak{J}_1 \mathfrak{J}_2^2$ where $\mathfrak{J}_1$ and $\mathfrak{J}_2$ are ideals of norm p; this happens only if p divides D. There are two ideals (α_1) and (α_2) of norm p and the ideals of norm p^r are $(\alpha_1^u \alpha_2^{r-u})$ where $r \geq u \geq 0$.

(v) $(p) = \mathfrak{J}_1 \mathfrak{J}_2 \mathfrak{J}_3$ where $\mathfrak{J}_1$, $\mathfrak{J}_2$, $\mathfrak{J}_3$ are ideals of norm p; this occurs only if p does not divide D. There are three ideals (α_1), (α_2) and (α_3) of norm p, the ideals of norm p^r are $(\alpha_1^u \alpha_2^v \alpha_3^{r-u-v})$ where $r \geq u \geq 0$, $r \geq v \geq 0$, $r \geq u + v \geq 0$.

3.3 Finally we consider the case $n = p_1^{r_1} p_2^{r_2} \ldots p_u^{r_u}$ where $p_1, \ldots, p_u$ are rational primes and $r_1, \ldots, r_u$ are positive rational integers. The ideals of norm n are of the form $(\alpha_1 \alpha_2 \ldots \alpha_u)$ where (α_i) is an ideal of norm $p_i^{r_i}$ for $i = 1, \ldots, u$; all ideals of norm n are found by considering all products $\alpha_1 \ldots \alpha_u$ for all possible values of $\alpha_1, \ldots, \alpha_u$.

For both of the cases where n is composite, having found the ideals of norm a prime p, and the integers which produce them, for all p less than n; by using the expressions enumerated in section 3.2, it is possible to calculate all ideals of norm n and the integers which produce them.

3.4 Having chosen a value for β the next problem is to find a complete set of residues modulo β.

LEMMA 3.1

Suppose that r is the smallest positive rational integer for which $r + 1 \equiv 0 \ (\beta)$,

q is the smallest positive rational integer for which $(q + 1)\theta + w_1 \equiv 0 \ (\beta)$, for some w_1 satisfying $0 \leq w_1 \leq r$

and p is the smallest positive rational integer for which $(p + 1)\lambda + v_2\theta + w_2 \equiv 0 \ (\beta)$, for some w_2 satisfying $0 \leq w_2 \leq r$ and some v_2 satisfying $0 \leq v_2 \leq q$,

then $Z = \{\rho : \rho = u\lambda + v\theta + w; \ 0 \leq u \leq p, \ 0 \leq v \leq q, \ 0 \leq w \leq r\}$ is a complete set of residues modulo β.

PROOF OF LEMMA 3.1

Suppose that $d_1\lambda + d_2\theta + d_3$ is some integer of the field, then

$$d_1\lambda + d_2\theta + d_3 \equiv d_1^*\lambda + d_2'\theta + d_3' \quad (\beta)$$

for some rational integers d_2', d_3' and some rational integer d_1^* satisfying $0 \leq d_1^* \leq p$ since $(p + 1)\lambda \equiv -v_2\theta - w_2 \ (\beta)$,

$$d_1^*\lambda + d_2'\theta + d_3' \equiv d_1^*\lambda + d_2^*\theta + d_3'' \quad (\beta)$$

for some rational integer d_3'' and some rational integer d_2^* satisfying $0 \leq d_2^* \leq q$ since $(q + 1)\theta \equiv -w_1 \ (\beta)$,

$$d_1^*\lambda + d_2^*\theta + d_3'' \equiv d_1^*\lambda + d_2^*\theta + d_3^* \quad (\beta)$$

for some rational integer d_3^* which satisfies $0 \leq d_3^* \leq r$ since $r + 1 \equiv 0 \ (\beta)$.

Thus $d_1\lambda + d_2\theta + d_3 \equiv d_1^*\lambda + d_2^*\theta + d_3^*$ where $0 \leq d_1^* \leq p$,

$0 \leq d_2^* \leq q$, $0 \leq d_3^* \leq r$; that is every integer of the field is congruent to an integer of Z, thus Z contains a complete set of residues modulo β.

It remains to show that no two elements of Z are congruent to each other. Suppose

$$d_1\lambda + d_2\theta + d_3 \equiv e_1\lambda + e_2\theta + e_3 \quad (\beta)$$

where

$$0 \leq e_1 \leq d_1 \leq p$$

$$0 \leq d_2 \leq q, \quad 0 \leq e_2 \leq q$$

$$0 \leq d_3 \leq r, \quad 0 \leq e_3 \leq r,$$

then

$$(d_1 - e_1)\lambda + (d_2 - e_2)\theta + d_3 - e_3 \equiv 0 \quad (\beta) \qquad 3.1$$

and

$$0 \leq d_1 - e_1 \leq p.$$

If $d_2 \geq e_2$ and $d_3 \geq e_3$ we have

$$0 \leq d_2 - e_2 \leq q$$

$$0 \leq d_3 - e_3 \leq r,$$

thus 3.1 implies

$$d_1 = e_1, \quad d_2 = e_2, \quad d_3 = e_3$$

as a result of the definitions of p, q, and r.

If $d_2 \geq e_2$ and $d_3 < e_3$ we have

$$0 < r + 1 + (d_3 - e_3) \leq r$$

$$0 \leq d_2 - e_2 \leq q,$$

but

$$(d_1 - e_1)\lambda + (d_2 - e_2)\theta + r + 1 + (d_3 - e_3) \equiv 0 \quad (\beta)$$

as a result of the definition of r, this is a contradiction.

If $d_2 < e_2$ then

$$0 < q + 1 + (d_2 - e_2) \leq q$$

and w' may be chosen such that

$$0 \leq w' \leq r$$

and $\qquad w' \equiv w_1 + d_3 - e_3 \quad (\beta) \qquad$ from the definition of r,

but $\qquad (d_1 - e_1)\lambda + (q + 1 + d_2 - e_2)\theta + w' \equiv 0 \quad (\beta)$

as a result of the definitions of q and w_1. This again is a contradiction. Hence $d_1 = e_1$, $d_2 = e_2$, $d_3 = e_3$, thus Z is a complete set of residue classes modulo β.

3.5 The choice of the integer β is made so that the method may be most efficient. For every number α of K there is a positive rational integer h such that

$$\epsilon^h \alpha \equiv \alpha \quad (1),$$

and h is the smallest positive rational integer for which such a congruence is true. Hence

$$(\epsilon^h - 1)\alpha \equiv 0 \quad (1);$$

thus, if $\alpha = \frac{\xi}{\beta}$, β divides $\epsilon^h - 1$, that is

$$\epsilon^h \equiv 1 \quad (\beta).$$

Now suppose that $(\alpha_1), \ldots, (\alpha_{m_n})$ are the distinct ideals of norm n, then every integer of norm n is congruent to $\epsilon^w \alpha_j$ for some rational integers w and j satisfying $0 \leq w \leq h - 1$, $1 \leq j \leq m_n$. Thus, for given n, the smaller h the fewer incongruent integers there will be of norm n; hence, the smaller h the fewer incongruent integers there will be with norm of absolute value less than $|N(\beta)|$. Thus the smaller h the lower the probability will be of all the residue classes modulo β being covered.

3.6 For the real quadratic fields for which results are known ((2) and (21)), the numbers α for which $M(K) = M(K, \alpha)$ satisfy

$$\epsilon\alpha \equiv \alpha \ (1)$$

or $\epsilon\alpha \equiv -\alpha \ (1)$

or, in one case, $\epsilon^2\alpha \equiv -\alpha \ (1)$.

Thus the possible values of β are the factors of $\epsilon - 1, \epsilon + 1$ or of $\epsilon^2 + 1$. We note that if the ideals of norm n are $(\alpha_1), \ldots, (\alpha_u)$, any integer of norm n will be of the form $\pm\epsilon^k\alpha_i$ for some rational integers k and i such that $1 \leq i \leq u$. In considering the residue classes which contain integers of norm n we must, therefore, consider every integer of the form $\pm\epsilon^k\alpha_i$ for $0 \leq k \leq h - 1$ and $1 \leq i \leq u$. However, if we restrict the values of β to factors of $\epsilon - 1$ or $\epsilon + 1$, we only need consider the integers $\pm\alpha_i$ for $1 \leq i \leq u$. In order to restrict the number of integers β considered for any one field, only those values of β the norm of which is a rational prime or the cube of a rational prime are used; the latter are included so that any rational prime factors of $\epsilon - 1$ or of $\epsilon + 1$ are considered.

To prevent the time spent in searching for uncovered residue classes becoming too large, β was further restricted so that $|N(\beta)|$ was less than 500; this was found, by experiment, to be a reasonable limit, in particular since most fields for which there was a possibility of considering integers β with $|N(\beta)|$ greater than 500 gave overflow warnings. All routines involving multiplication or division where the numbers involved were likely to cause overflow, in the sense that the integer answer could have coefficients which consist of more digits than the number of significant figures allowed, included tests for the possibility of overflow, and monitored such possibilities.

CHAPTER 4

AN ADAPTATION OF A METHOD OF BARNES AND SWINNERTON-DYER FOR CUBIC FIELDS WITH COMPLEX CONJUGATES.

4.1 This chapter describes a method of isolating those points α in K for which $M(K,\alpha)$ is greater than a chosen bound. By this means we may either show that $M(K,\alpha) < 1$ for all α in K, so that K has a Euclidean Algorithm; or we may find a point α such that $M(K) = M(K,\alpha)$, in this way we determine the inhomogeneous minimum of the field and consequently whether or not it possesses a Euclidean Algorithm. The method described is an adaptation of that used by Barnes and Swinnerton-Dyer in (2).

4.2 If a number α in K is given by $\alpha = d(\theta) = d_1\theta^2 + d_2\theta + d_3$, where d_1, d_2, d_3 are rational numbers, let α be represented in the space $\mathcal{A}$ by

$$\tilde{\alpha} = (\operatorname{Re} d(\phi), \operatorname{Im} d(\phi), d(\theta)) \quad \text{(cartesian co-ordinates)}$$

$$= (|d(\phi)|, \arg d(\phi), d(\theta)) \quad \text{(cylindrical polar co-ordinates)}$$

then the isomorphism $\alpha \leftrightarrow \tilde{\alpha}$ establishes an isomorphism $K \leftrightarrow \mathcal{A}$. Now define

$$N(\tilde{\alpha}) = N(\alpha) = d(\theta)d(\phi)d(\bar{\phi})$$

$$= d(\theta)\left((\operatorname{Re} d(\phi))^2 + (\operatorname{Im} d(\phi))^2 \right),$$

thus, generally, if $\tilde{\alpha}$ is the point (ξ, η, ζ) then

$$N(\tilde{\alpha}) = \zeta(\xi^2 + \eta^2).$$

If α is an integer in K, $\tilde{\alpha}$ is said to be an integer point of $\mathcal{A}$. Let the transformation E on points of $\mathcal{A}$ be defined by

$$E(\tilde{\alpha}) = \tilde{\beta} \quad \text{when } \epsilon\alpha = \beta \text{ where } \alpha, \beta \text{ are in } K;$$

expressed in cylindrical polar co-ordinates, E is then the transformation

$$(\rho, \omega, \zeta) \to (\rho\rho_\epsilon, \omega + \omega_\epsilon, \zeta\zeta_\epsilon)$$

where $0 < \zeta_\epsilon = \epsilon < 1$, $\rho_\epsilon = \sqrt{\epsilon'\bar{\epsilon}'}$, so that $\rho_\epsilon^2 \zeta_\epsilon = 1$ and $\omega_\epsilon = \arg \epsilon'$.

4.3 If R is a set of points of $\mathfrak{a}$, the statement $\tilde{\alpha} \in R \pmod 1$ means that, for some integer $\tilde{\gamma}$ in $\mathfrak{a}$, $\tilde{\alpha} - \tilde{\gamma}$ is in R.

THEOREM 4.1

Let R be a bounded point set in the space $\mathfrak{a}$ such that, for some given set R^* in $\mathfrak{a}$ and some given integer point $\tilde{\gamma}$ in $\mathfrak{a}$, any point $\tilde{\alpha}$ in R has the property that either $E(\tilde{\alpha}) \in R^* \pmod 1$ or $E(\tilde{\alpha}) - \tilde{\gamma} \in R$; and further that $E^{-1}(\tilde{\alpha})$ is congruent to a point of R^* or of R. If $\tilde{\alpha} \in R$ and $E^n(\tilde{\alpha})$ is not congruent to a point of R^* for any $n \lessgtr 0$, $\tilde{\alpha}$ is the fixed point $\tilde{\beta}$ of E defined by

$$E(\tilde{\beta}) = \tilde{\beta} + \tilde{\gamma} \qquad \tilde{\beta} = (\xi_\beta, \eta_\beta, \zeta_\beta) = (\rho_\beta, \omega_\beta, \zeta_\beta).$$

The generalized form of this theorem, for algebraic fields of any given degree, is due to Cassels (quoted in (2)); since a proof was not readily available I provide one for this particular case, analogous to that given for the quadratic case in (2).

LEMMA 4.2

Let S be the transformation

$$(\rho, \omega, \zeta) \to (\sigma\rho, \omega + \omega_\sigma, \zeta/\sigma^2)$$

where $\sigma > 1$ and $-\pi < \omega_\sigma \leq \pi$; and let R be a bounded point set. Suppose $S^n(\tilde{\alpha}_1) \in R$ for all $n \geqslant 0$, then $\tilde{\alpha}_1$ lies on the line $\rho = 0$, the origin 0 belongs to the closure $\bar{R}$ of R, and $S^n(\tilde{\alpha}_1) \to 0$ as $n \to \infty$. If $S^n(\tilde{\alpha}_2) \in R$ for all $n \leq 0$ then $\tilde{\alpha}_2$ lies on the plane $\zeta = 0$ and $S^n(\tilde{\alpha}_2) \to 0$ as $n \to -\infty$.

PROOF OF LEMMA 4.2

Let $\tilde{\alpha}_1$ be the point $(\rho_1, \omega_1, \zeta_1)$ then

$$S^n(\tilde{\alpha}_1) = (\sigma^n \rho_1, \ \omega_1 + n\omega_\sigma, \ \zeta_1/\sigma^{2n}).$$

Thus, since R is bounded, $\sigma^n \rho_1$ is bounded as $n \to \infty$; hence, since $\sigma > 1$, it follows that $\rho_1 = 0$. Also

$$S^n(\tilde{\alpha}_1) = (\ 0, \ \omega_1 + n\omega_\sigma, \ \sigma^{-2n}\zeta_1) \to 0 \qquad \text{as } n \to \infty,$$

hence $0 \in \bar{R}$.

Similarly, if $\tilde{\alpha}_2 = (\rho_2, \omega_2, \zeta_2)$ then

$$S^n(\tilde{\alpha}_2) = (\sigma^n \rho_2, \ \omega_2 + n\omega_\sigma, \ \zeta_2/\sigma^{2n})$$

and ζ_2/σ^{2n} is bounded as $n \to -\infty$, hence $\zeta_2 = 0$ and

$$S^n(\tilde{\alpha}_2) = (\sigma^n \rho_2, \omega_2 + n\omega_\sigma, \ 0) \to 0 \qquad \text{as } n \to -\infty.$$

PROOF OF THEOREM 4.1

Suppose that $\tilde{\alpha}_0 \in R$ and that $E^n(\tilde{\alpha}_0)$ is not congruent to a point of R^* for any $n \geq 0$.

Let $\tilde{\gamma}$ be the point $(\xi_\gamma, \eta_\gamma, \zeta_\gamma) = (\rho_\gamma, \omega_\gamma, \zeta_\gamma)$ and define the transformation F by

$$F(\tilde{\alpha}) = E(\tilde{\alpha}) - \tilde{\gamma}.$$

Then, since $F(\tilde{\alpha}) \equiv E(\tilde{\alpha}) \pmod 1$ for all $\tilde{\alpha}$, $F^n(\tilde{\alpha}_0)$ is not congruent to a point of R^* for any $n \geq 0$.

If the origin is now changed to $\tilde{\beta}$, that is $\tilde{\alpha}' = \tilde{\alpha} - \tilde{\beta}$, the transformation F becomes

$$(\rho', \omega', \zeta') \to (\rho'\rho_\epsilon, \ \omega' + \omega_\epsilon, \ \zeta'\zeta_\epsilon)$$

$-\pi < \omega_\epsilon \leq \pi$, $\rho_\epsilon^2 \zeta_\epsilon = 1$ and $0 < \zeta_\epsilon < 1$ so that $\rho_\epsilon > 1$ and $\zeta_\epsilon = 1/\rho_\epsilon^2$

By hypothesis

$$\tilde{\alpha}_0 \in R$$

$$F(\tilde{\alpha}_0) = E(\tilde{\alpha}_0) - \tilde{\gamma} = \tilde{\delta}_1 \in R$$

$$F^2(\tilde{\alpha}_0) = F(\tilde{\delta}_1) = E(\tilde{\delta}_1) - \tilde{\gamma} = \tilde{\delta}_2 \in R$$

and ultimately

$$\tilde{\delta}_n = F^n(\tilde{\alpha}_0) \in R \quad \text{for all} \quad n \geq 0.$$

It now follows from lemma 4.2 that $\tilde{\beta} \in \bar{R}$, $\tilde{\delta}_n \to \tilde{\beta}$ as $n \to \infty$ and $\tilde{\alpha}_0$ lies on the line $\rho' = 0$, that is the line $\xi - \xi_\beta = \eta - \eta_\beta = 0$.

If $\tilde{\alpha}$ is a point in R such that $E^{-1}(\tilde{\alpha}) \in R$ (mod 1) then there is an integer point $\tilde{\mu}$ such that

$$E^{-1}(\tilde{\alpha}) = \tilde{\mu} + \tilde{\delta} \qquad \text{where } \tilde{\delta} \in R,$$

thus

$$\tilde{\alpha} = E(\tilde{\mu}) + E(\tilde{\delta}).$$

Since $\tilde{\alpha}$ is a point of R and, by hypothesis, $E(\tilde{\delta}) - \tilde{\gamma} \in R$, we have $E(\tilde{\mu}) = -\tilde{\gamma}$ so that $\tilde{\mu} = -E^{-1}(\tilde{\gamma})$ which is independent of $\tilde{\alpha}$. Hence there is an integer point $\tilde{\mu}$ such that, for any given $\tilde{\alpha}$ in R, either $E^{-1}(\tilde{\alpha}) \in R^*$ (mod 1) or $E^{-1}(\tilde{\alpha}) - \tilde{\mu} \in R$. Thus, by similar reasoning to that used for $n \geq 0$, in which for $n \leq 0$ we replace E by E^{-1} and $\tilde{\gamma}$ by $\tilde{\mu}$, we find that $\tilde{\alpha}_0$ lies on the plane $\zeta - \zeta_\beta = 0$. Hence $\tilde{\alpha}_0$ lies at the intersection of the line $\xi - \xi_\beta = \eta - \eta_\beta = 0$ with the plane $\zeta - \zeta_\beta = 0$, thus $\tilde{\alpha}_0 = \tilde{\beta}$.

4.4 Theorem 4.1 may be generalized to the case of a finite number of bounded point sets as follows.

THEOREM 4.3

Let $R_0, R_1, \ldots, R_{m-1}$ be a finite number of bounded point sets. Suppose that for some R^* and some integer points $\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_m$ every point $\tilde{\alpha}_i$ in R_i $(i = 0, 1, \ldots, m-1)$ has the property that either

$$E(\tilde{\alpha}_i) \in R^* \pmod 1$$

or $$E(\tilde{\alpha}_i) - \tilde{\gamma}_{i+1} \in R_{i+1} \qquad (\text{where } R_m \text{ is } R_0).$$

Let

$$\tilde{\gamma} = \tilde{\gamma}_m + E(\tilde{\gamma}_{m-1}) + E^2(\tilde{\gamma}_{m-2}) + \cdots + E^{m-1}(\tilde{\gamma}_1)$$

and let $\tilde{\beta}$ be the fixed point of E^m defined by

$$E^m(\tilde{\beta}) = \tilde{\beta} + \tilde{\gamma}.$$

Further suppose that any $\tilde{\alpha}_i$ in R_i has the property that either $E^{-1}(\tilde{\alpha}_i) \in R^* \pmod 1$ or $E^{-1}(\tilde{\alpha}_i) \in R_j \pmod 1$ for some j satisfying $0 \le j \le m-1$. If $\tilde{\alpha} \in R_0$ and $E^n(\tilde{\alpha})$ is not congruent to a point of R^* for any $n \geq 0$ then $\tilde{\alpha}$ is the fixed point $\tilde{\beta}$ of E^m.

PROOF OF THEOREM 4.3

First suppose that $\tilde{\alpha}$ is in R_0 and $E^n(\tilde{\alpha})$ is not congruent to a point of R^* for any $n \geq 0$. By hypothesis

$$\begin{array}{lll} E(\tilde{\alpha}) = \tilde{\alpha}_1 + \tilde{\gamma}_1 & & \tilde{\alpha}_1 \text{ in } R_1 \\ E(\tilde{\alpha}_1) = \tilde{\alpha}_2 + \tilde{\gamma}_2 & & \tilde{\alpha}_2 \text{ in } R_2 \\ \cdots\cdots\cdots & & \\ E(\tilde{\alpha}_{m-1}) = \tilde{\alpha}_m + \tilde{\gamma}_m & & \tilde{\alpha}_m \text{ in } R_m = R_0, \end{array}$$

thus

$$E^m(\tilde{\alpha}) = \tilde{\alpha}_m + \tilde{\gamma}_m + E(\tilde{\gamma}_{m-1}) + \cdots + E^{m-1}(\tilde{\gamma}_1)$$

$$E^m(\tilde{\alpha}) - \tilde{\gamma} = \tilde{\alpha}_m \text{ in } R_0.$$

Now suppose that $\tilde{\alpha}$ is in R_0 and $E^n(\tilde{\alpha})$ is not congruent to a point of R^* for any $n \leq 0$. By hypothesis for some i, $0 \leq i \leq m - 1$, there is an integer point $\tilde{\mu}_i$ such that

$$E^{-1}(\tilde{\alpha}) = \tilde{\delta}_i + \tilde{\mu}_i \qquad \tilde{\delta}_i \text{ in } R_i,$$

thus $\qquad \tilde{\alpha} = E(\tilde{\delta}_i) + E(\tilde{\mu}_i)$.

Also, by hypothesis,

$$E(\tilde{\delta}_i) - \tilde{\gamma}_{i+1} \in R_{i+1}$$

thus we have $R_{i+1} = R_0$, hence $i = m - 1$,

$$E(\tilde{\mu}_{m-1}) = -\tilde{\gamma}_m,$$

and so

$$\tilde{\mu}_{m-1} = -E^{-1}(\tilde{\gamma}_m)$$

which is independent of $\tilde{\alpha}$. Thus there is an integer $\tilde{\mu}_{m-1}$ such that

$$E^{-1}(\tilde{\alpha}) = \tilde{\delta}_{m-1} + \tilde{\mu}_{m-1} \qquad \tilde{\delta}_{m-1} \text{ in } R_{m-1}.$$

Similarly there are integers $\tilde{\mu}_{m-2}, \dots, \tilde{\mu}_0$ such that

$$E^{-1}(\tilde{\delta}_{m-1}) = \tilde{\delta}_{m-2} + \tilde{\mu}_{m-2} \qquad \tilde{\delta}_{m-2} \text{ in } R_{m-2}$$

$$\dots\dots\dots\dots\dots\dots$$

$$E^{-1}(\tilde{\delta}_1) = \tilde{\delta}_0 + \tilde{\mu}_0 \qquad \tilde{\delta}_0 \text{ in } R_0$$

and we have

$$E^{-m}(\tilde{\alpha}) = E^{-(m-1)}(\tilde{\mu}_{m-1}) + E^{-(m-2)}(\tilde{\mu}_{m-2}) + \dots + \tilde{\mu}_0 + \tilde{\delta}_0.$$

Hence

$$E^{-m}(\tilde{\alpha}) \in R_0 \pmod 1.$$

Thus, by applying theorem 4.1 with E replaced by E^m, theorem 4.3 follows.

4.5 A fundamental region $\mathfrak{F}$ of $\mathfrak{a}$ is one such that for every point $\tilde{\alpha}_1$ of $\mathfrak{a}$ there is a point $\tilde{\alpha}_2$ in $\mathfrak{F}$ such that

$$\tilde{\alpha}_1 \equiv \tilde{\alpha}_2 \pmod 1,$$

and for any two points $\tilde{\alpha}_1, \tilde{\alpha}_2$ both in $\mathfrak{F}$ the congruence holds if and only if $\tilde{\alpha}_1 = \tilde{\alpha}_2$.

The method of covering may now be summarized as follows

I. A fundamental region $\mathfrak{F}$ of $\mathfrak{a}$ is chosen.

II. Either a). For every number α in K, such that $\tilde{\alpha}$ is in $\mathfrak{F}$, it is shown that there exists an integer point $\tilde{\gamma}$ in $\mathfrak{a}$ such that, for a given real number $C < 1$,

$$|N(\tilde{\alpha} - \tilde{\gamma})| \leq C \qquad 4.1$$

If this is possible, K has a Euclidean Algorithm. For this case it is sufficient to show that 4.1 holds for every point of $\mathfrak{F}$.

or b). Regions $R_0, R_1, \ldots, R_{m-1}$ and integer points $\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_m$ in $\mathfrak{a}$ are found such that

(i) the conditions of theorem 4.3 are satisfied with

$$R^* = \mathfrak{F} - \bigcup_{i=0}^{m-1} R_i.$$

(ii) if $\tilde{\beta}$ is the fixed point of E^m satisfying

$$E^m(\tilde{\beta}) = \tilde{\beta} + \tilde{\gamma}$$

and $\min|N(\tilde{\beta} - \tilde{\delta})| = C$

where the minimum is over integers $\tilde{\delta}$ in $\mathfrak{a}$, for every point $\tilde{\alpha}$ in R^* for which α is in K

$$\min|N(\tilde{\alpha} - \tilde{\delta})| < C$$

where the minimum is over integers $\tilde{\delta}$ in $\mathfrak{a}$.

If II(b) is followed then $C = \max \min|N(\tilde{\alpha} - \tilde{\delta})|$ where the minimum is over all integers $\tilde{\delta}$ in $\mathfrak{a}$ and the maximum is over points $\tilde{\alpha}$ in $\mathfrak{a}$ for which α is in K; thus C is the inhomogeneous minimum of K, and so the field has a Euclidean Algorithm if and only if $C < 1$.

The alternatives II(a) and II(b) are provided since if it is possible to follow II(a) the method is shorter, as no consideration of transformation by the fundamental unit is required.

4.6 In order to satisfy the conditions of II(a) or of II(b), the fundamental region is divided into sub-regions $\mathfrak{F}_1, \ldots, \mathfrak{F}_n$. A finite set $\mathcal{I}$ of integer points of $\mathfrak{a}$ is chosen. Then, for given C we establish for every $\mathfrak{F}_i$, $i = 1, \ldots, n$, whether there is an integer point $\tilde{\gamma}$ in $\mathcal{I}$ such that

for every point $\tilde{\alpha}$ in $\mathfrak{F}_i$ $\quad |N(\tilde{\alpha} - \tilde{\gamma})| < C$. 4.2

Now each region $\mathfrak{F}_i$, for which there is no such $\tilde{\gamma}$, is itself subdivided and its sub-regions tested as were the regions $\mathfrak{F}_i$. After repetition of this testing a practical number of times, either II(a) will be satisfied or there will be regions $R_1, \ldots, R_m$ for which no integer point of $\mathcal{I}$ can be found which satisfies 4.2. Having calculated the transformations of points of $R_1, \ldots, R_m$ by E, we will have one or both of the following situations:

(i) There are regions $R_{\mu_1}, \ldots, R_{\mu_n}$ where $1 \leq \mu_i \leq m$ for $i = 1, \ldots, n$ such that, if $\tilde{\alpha}$ is in R_{μ_i}, for some rational integer j_i $E^{j_i}(\tilde{\alpha}) \equiv \mathcal{F} - \bigcup_{i=1}^{m} R_i \pmod 1$. In which case, for $i = 1, \ldots, n$ there is an integer point $\tilde{\gamma}_{\mu_i}$, not in $\mathcal{J}$, which satisfies 4.2 for $\tilde{\alpha}$ in R_{μ_i}.

(ii) For $\nu = 1, 2, \ldots, p$ there are regions $R_{\nu,0}, \ldots, R_{\nu,(m_\nu - 1)}$ and integer points $\tilde{\delta}_{\nu,1}, \ldots, \delta_{\nu,m_\nu}$ where $R_{\nu,i}$ belongs to the set $\{R_1, \ldots, R_m\}$ such that if $\tilde{\alpha}$ is in $R_{\nu,i}$,

$$E(\tilde{\alpha}) - \tilde{\delta}_{\nu,(i+1)} \text{ is in } R_{\nu,(i+1)} \quad \text{where } R_{\nu,m_\nu} = R_{\nu,0},$$

and if there are regions R_{μ_j} satisfying (i), $R_{\mu_j} \neq R_{\nu,i}$ for $\nu = 1, \ldots, p$, $i = 0, \ldots, m_\nu$, $j = 1, \ldots, n$.

In the second case each of the sets of regions $R_{\nu,0}, \ldots, R_{\nu,(m_\nu - 1)}$ satisfies theorem 4.3. Let $\tilde{\beta}_\nu$ be the corresponding fixed point of E^{m_ν}, $\tilde{\beta}_\nu$ in $R_{\nu,0}$, β_ν in K; then, if we have

$$C = \max_{\nu} \min_{\tilde{\delta}} |N(\tilde{\beta}_\nu - \tilde{\delta})|$$

where $1 \leq \nu \leq p$ and $\tilde{\delta}$ is an integer in $\mathfrak{a}$, where the maximum is attained for $\nu = \nu_0$, II(b) is satisfied with the regions $R_{\nu_0,0}, \ldots, R_{\nu_0,(m_{\nu_0}-1)}$. It should be noted that the sets $\{R_{\nu,0}, \ldots, R_{\nu,(m_\nu - 1)}\}$ for $\nu = 1, \ldots, p$ are not necessarily disjoint, and the value of ν_0 is not necessarily unique.

4.7 The fundamental region $\mathcal{F}$ is chosen in order to allow a simple and efficient algorithm for selecting the integer points in $\mathcal{J}$ so that, for a given integer $\tilde{\gamma}$ in $\mathcal{J}$ there is a high probability of the existence of a subregion $\mathcal{F}_\gamma$ of $\mathcal{F}$ which satisfies 4.2. With this in mind, $\mathcal{F}$ is chosen so that, if $\tilde{\alpha}$ in $\mathcal{F}$ is given by $\tilde{\alpha} = (\xi_\alpha, \eta_\alpha, \zeta_\alpha)$ and we define

$$\mathcal{D}_{\mathcal{J}} = \max_{\tilde{\alpha} \text{ in } \mathcal{J}} |(\xi_\alpha^2 + \eta_\alpha^2 + \zeta_\alpha^2)|,$$

then $\mathcal{D}_{\mathcal{J}}$ is as small as possible. The method used to do this is now described.

4.8 If $(1, \mathcal{M}(\theta), Q(\theta))$ is a basis for K where $\mathcal{M}$ is linear and monic in θ and Q is a quadratic with coefficient $\frac{1}{\ell}$ for θ^2,

$$[(0,0,0),\ (1,0,1),\ (\operatorname{Re}\mathcal{M}(\phi),\ \operatorname{Im}\mathcal{M}(\phi), \mathcal{M}(\theta)),\ (\operatorname{Re}Q(\phi),\ \operatorname{Im}Q(\phi), Q(\theta))]$$

is a basis for the lattice of integers of $\mathfrak{a}$. The actual choice of $\mathcal{M}$ and Q is made so that the scalar product

$$(1,0,1).(\operatorname{Re}\mathcal{M}(\phi),\ \operatorname{Im}\mathcal{M}(\phi), \mathcal{M}(\theta)) = \operatorname{Re}\mathcal{M}(\phi) + \mathcal{M}(\theta)$$

is a minimum over all possible choices of $\mathcal{M}$, say for $\mathcal{M}'$; and the scalar products

$$(1,0,1).(\operatorname{Re}Q(\phi),\ \operatorname{Im}Q(\phi),\ Q(\theta)) = \operatorname{Re}Q(\phi) + Q(\theta)$$

and

$$(\operatorname{Re}\mathcal{M}'(\phi),\ \operatorname{Im}\mathcal{M}'(\phi), \mathcal{M}'(\theta)).(\operatorname{Re}Q(\phi),\ \operatorname{Im}Q(\phi), Q(\theta))$$
$$= \operatorname{Re}\mathcal{M}'(\phi).\operatorname{Re}Q(\phi) + \operatorname{Im}\mathcal{M}'(\phi).\operatorname{Im}Q(\phi) + \mathcal{M}'(\theta).Q(\theta)$$

are each a minimum over all possible choices of Q, say for Q'.

$\mathcal{J}$ is then chosen to be the set of points (ξ, η, ζ) where

$$\begin{aligned} \xi &= x + y.\operatorname{Re}\mathcal{M}'(\phi) + z.\operatorname{Re}Q'(\phi) \\ \eta &= \quad\ \ y.\operatorname{Im}\mathcal{M}'(\phi) + z.\operatorname{Im}Q'(\phi) \\ \zeta &= x + y.\mathcal{M}'(\theta) + z.Q'(\theta) \end{aligned} \qquad 4.3$$

and $-\frac{1}{2} < x \leq \frac{1}{2}$, $-\frac{1}{2} < y \leq \frac{1}{2}$, $-\frac{1}{2} < z \leq \frac{1}{2}$.

We determine $\mathcal{M}'$ and Q' as follows. Suppose

$$\mathcal{M}(\theta) = \theta - k$$

and

$$Q(\theta) = \lambda - p\theta - q,$$

then we require

$\text{Re}\phi + \theta - 2k$ a minimum over all possible rational integer values of k.

Let

$$k_1 = [\text{Re}\phi + \theta]$$

and

$$k_2 = \begin{cases} k_1 & \text{if } k_1 \text{ is even} \\ k_1 + 1 & \text{if } k_1 \text{ is odd and } \text{Re}\phi + \theta > 0 \\ k_1 - 1 & \text{if } k_1 \text{ is odd and } \text{Re}\phi + \theta < 0, \end{cases}$$

then k_2 is even and is that even integer closest to $\text{Re}\phi + \theta$. If $k' = \frac{1}{2}k_2$, $\mathcal{M}'(\theta) = \theta - k'$ satisfies the conditions stated above for $\mathcal{M}'(\theta)$. To find the rational integer values of p and q such that $Q(\theta)$ satisfies the conditions for $Q'(\theta)$, we require

$$\text{Re}\psi + \lambda - p(\text{Re}\phi + \theta) - 2q$$

and

$$\begin{aligned} \text{Re}\,\psi(\text{Re}\phi - k') + \text{Im}\psi\,\text{Im}\phi + \lambda(\theta - k') \\ - p(\text{Re}\,\phi\,(\text{Re}\phi - k') + \text{Im}\phi\,\text{Im}\phi + \theta(\theta - k')) \\ - q(\text{Re}\,\phi + \theta - 2k') \end{aligned}$$

to be a minimum over all rational integers p and q. Suppose p_r and q_r are the real numbers which when substituted for p and q respectively cause the above two expressions to become zero. Let

$$p_\epsilon = \begin{cases} \frac{1}{2} & \text{if } p_r > 0 \\ -\frac{1}{2} & \text{if } p_r < 0 \end{cases}$$

$$q_\epsilon = \begin{cases} \frac{1}{2} & \text{if } q_r > 0 \\ -\frac{1}{2} & \text{if } q_r < 0, \end{cases}$$

and $\qquad p' = [p_r + p_\epsilon]$

$\qquad q' = [q_r + q_\epsilon]$;

$Q(\theta) = \lambda - p'\theta - q'$ then satisfies the conditions stated above for $Q'(\theta)$.

4.9 The method of subdivision of $\mathcal{F}$ is chosen to simplify the testing for an integer for which a sub-region satisfies 4.2. The smallest cuboid $\mathcal{C}$ which contains all points of $\mathcal{F}$, and which has faces parallel to the co-ordinate planes, is chosen. $\mathcal{C}$ is then divided into 10x10x10 similar cuboids $\mathcal{C}_{ijk}$, $i = 1, \ldots, 10$; $j = 1, \ldots, 10$; $k = 1, \ldots, 10$. Each $\mathcal{C}_{ijk}$ has a flag $\mathcal{L}_{ijk}$ which is set to 2 for those regions which do not contain any point of $\mathcal{F}$ and to 1 otherwise. $\mathcal{L}_{ijk}$ is subsequently set to 0 when an integer point $\tilde{\gamma}$ is found for which $\mathcal{C}_{ijk}$ satisfies 4.2.

If the region $\mathcal{C}^*$ to be tested is the set of points (ξ, η, ζ) for which

$$\xi_1 \leq \xi \leq \xi_2$$

$$\eta_1 \leq \eta \leq \eta_2$$

$$\zeta_1 \leq \zeta \leq \zeta_2$$

then $\mathcal{C}^*$ intersects with $\mathcal{F}$ only if at least one of (ξ_i, η_j, ζ_k) $(i = 1, 2;\ j = 1, 2;\ k = 1, 2)$ lies in $\mathcal{F}$; which is so if there is a set i, j, k with $i = 1$ or 2, $j = 1$ or 2, $k = 1$ or 2 such that

$$\xi_i = x + y.\mathrm{Re}\,M'(\phi) + z.\mathrm{Re}\,Q'(\phi)$$

$$\eta_j = \qquad y.\mathrm{Im}\,M'(\phi) + z.\mathrm{Im}\,Q'(\phi)$$

$$\zeta_k = x + y.M'(\theta) + z.Q'(\theta)$$

where $|x| \leq \frac{1}{2}$, $|y| \leq \frac{1}{2}$, $|z| \leq \frac{1}{2}$.

If $\tilde{\gamma}$ is the point $(\xi_\gamma, \eta_\gamma, \zeta_\gamma)$, it is an integer point for which $\mathscr{C}^*$ satisfies 4.2 only if, when we define

$$\xi_d = \max(|\xi_2 - \xi_\gamma|, \ |\xi_1 - \xi_\gamma|)$$

$$\eta_d = \max(|\eta_2 - \eta_\gamma|, \ |\eta_1 - \eta_\gamma|)$$

$$\zeta_d = \max(|\zeta_2 - \zeta_\gamma|, \ |\zeta_1 - \zeta_\gamma|),$$

we have $\zeta_d(\xi_d^2 + \eta_d^2) < C$.

After testing using all points of $\mathscr{J}$, those $\mathscr{C}_{ijk}$ for which $\mathcal{L}_{ijk}$ is equal to 1 are subdivided and tested as was $\mathscr{C}$. The process is continued, using further subdivisions, until those regions for which an integer point cannot be found to satisfy 4.2 can be combined to give regions $R_0, \ldots, R_{m-1}$ to satisfy II(b), or until II(a) is shown to be satisfied.

4.10 The choice of $\mathscr{F}$ as a fundamental region such that if $\tilde{\alpha}$ is in $\mathscr{F}$, $-\tilde{\alpha}$ is in $\mathscr{F}$ has the following advantages

(i) When considering the set of sub-regions of the original region $\mathscr{C}$, we need only consider those points (ξ, η, ζ), given by 4.3, for which $|x| \leq \frac{1}{2}$, $|y| \leq \frac{1}{2}$, $0 \leq z \leq \frac{1}{2}$. When subsequently testing these sub-regions all points must be considered.

(ii) The quantities involved in the above expressions are all of the same order of magnitude, usually of absolute value less than 10; so with an accuracy of fifteen significant figures, as on the computer used, rounding error will not cause inaccuracies in the results when C is quoted to just four decimal places, as in the program used.

4.11 I now turn to the choice of the set $\mathcal{J}$ of integer points. Suppose that $\mathcal{C}$ is the set of (ξ, η, ζ) for which

$$\xi_\ell \leq \xi \leq \xi_u$$
$$\eta_\ell \leq \eta \leq \eta_u$$
$$\zeta_\ell \leq \zeta \leq \zeta_u$$

and that the cuboids $\mathcal{C}^{(i)}$, i = 1, . . . ,n, for which we are trying to find integer points to satisfy 4.2, are the sets of (ξ, η, ζ) for which

$$\xi_\ell^{(i)} \leq \xi \leq \xi_u^{(i)}$$
$$\eta_\ell^{(i)} \leq \eta \leq \eta_u^{(i)}$$
$$\zeta_\ell^{(i)} \leq \zeta \leq \zeta_u^{(i)}$$

where

$$\xi_u^{(i)} - \xi_\ell^{(i)} = 10^{-h}(\xi_u - \xi_\ell) = \xi_h \quad \text{say}$$
$$\eta_u^{(i)} - \eta_\ell^{(i)} = 10^{-h}(\eta_u - \eta_\ell) = \eta_h \quad \text{say}$$
$$\zeta_u^{(i)} - \zeta_\ell^{(i)} = 10^{-h}(\zeta_u - \zeta_\ell) = \zeta_h \quad \text{say}$$

$$\xi_\ell^{(i)} = m_{1i}\xi_h + \xi_\ell; \quad \eta_\ell^{(i)} = m_{2i}\eta_h + \eta_\ell; \quad \zeta_\ell^{(i)} = m_{3i}\zeta_h + \zeta_\ell$$

for some positive rational integer h and non-negative rational integers m_{1i}, m_{2i}, m_{3i}.

It is required that the set $\mathcal{J}$ should contain those integer points $\tilde{\gamma} = (\xi_\gamma, \eta_\gamma, \zeta_\gamma)$ such that

for some $\mathcal{C}^{(i)}$, all $\tilde{\alpha} = (\xi_\alpha, \eta_\alpha, \zeta_\alpha)$ in $\mathcal{C}^{(i)}$ satisfy $|N(\tilde{\alpha} - \tilde{\gamma})| < C$ 4.4

and as few other points as possible. Now

$$|N(\tilde{\alpha} - \tilde{\gamma})| = |(\zeta_\alpha - \zeta_\gamma)((\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2)|$$

thus bounds may be found for ξ_γ, η_γ, ζ_γ, for those $\tilde{\gamma}$ for which there is a high probability that 4.4 holds, in terms of the bounds on $\xi_\alpha, \eta_\alpha, \zeta_\alpha$ for $\tilde{\alpha}$ in $\mathscr{C}$.

In order that

$$|(\zeta_\alpha - \zeta_\gamma)((\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2)| < C \qquad \text{for all } \tilde{\alpha} \text{ in } \mathscr{C}^{(i)}$$

$$|(\zeta_\alpha - \zeta_\gamma)| < \frac{C}{((\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2)} \qquad \text{for all } \tilde{\alpha} \text{ in } \mathscr{C}^{(i)} \qquad 4.5$$

$$|(\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2| < \frac{C}{|(\zeta_\alpha - \zeta_\gamma)|} \qquad \text{for all } \tilde{\alpha} \text{ in } \mathscr{C}^{(i)} \qquad 4.6$$

Thus we may either restrict the values of ξ_γ and η_γ and so find bounds for ζ_γ, or restrict the value of ζ_γ and so find bounds for ξ_γ and η_γ.

First of all we restrict the values of ξ_γ, and η_γ, so that they are close to the values of ξ_α and η_α for $\tilde{\alpha}$ in $\mathscr{C}$, by the inequalities

$$\xi_\ell - 0.1 \leq \xi \leq \xi_u + 0.1$$

$$\text{and} \qquad \eta_\ell - 0.1 \leq \eta \leq \eta_u + 0.1 \qquad 4.7$$

The constant 0.1 is chosen bearing in mind that the critical value for C, so far as the Euclidean Algorithm is concerned, is 1.

With ξ_γ, η_γ satisfying 4.7, a sufficient condition for ζ_γ satisfying 4.4 is

$$|(\zeta_\alpha - \zeta_\gamma)| < \frac{C}{\rho_n^2}$$

where $\rho_n^2 = \max|(\xi - \xi_\gamma)^2 + (\eta - \eta_\gamma)^2|$,

and the maximum is over all points $\tilde{\beta} = (\xi, \eta, \zeta)$ where $\tilde{\beta}$ is in $\mathscr{C}^{(i)}$ and $|N(\tilde{\beta} - \tilde{\gamma})| < C$. A necessary bound for ρ_n is then $\frac{1}{2}(\xi_n^2 + \eta_n^2)^{\frac{1}{2}}$. $\frac{1}{2}\max\{\xi_n, \eta_n\}$ was in fact used as this lower bound since it was thought to be a more efficient expression to use when programming, although

$$\frac{1}{\sqrt{2}}\left(\frac{1}{2}(\xi_n^2 + \eta_n^2)^{\frac{1}{2}}\right) \leq \frac{1}{2}\max\{\xi_n, \eta_n\} \leq \frac{1}{2}(\xi_n^2 + \eta_n^2)^{\frac{1}{2}}$$

so that some extra points would be included in $\mathscr{S}$. However, it was found necessary to impose bounds on the coefficients $x_\gamma, y_\gamma, z_\gamma$, where $\zeta_\gamma = x_\gamma + y_\gamma M'(\theta) + z_\gamma Q'(\theta)$; with the result that ζ_γ does not come near the bound calculated, using either of the above bounds for ρ_h, when C is close to 1. Thus a necessary condition for the integer point $\tilde{\gamma}$ to be included in the set $\mathcal{J}$ is that when $\tilde{\gamma}$ satisfies 4.7 it further satisfies

$$|\zeta_\alpha - \zeta_\gamma| < \frac{4C}{(\max\{\xi_h, \eta_h\})^2} \quad \text{for all } \tilde{\alpha} \text{ in } \mathcal{C}^{(i)}$$

for which a necessary condition is

$$\zeta_l - \frac{4C}{(\max\{\xi_h, \eta_h\})^2} \leq \zeta_\gamma \leq \zeta_u + \frac{4C}{(\max\{\xi_h, \eta_h\})^2}. \qquad 4.8$$

We now find necessary conditions for $\tilde{\gamma}$ in $\mathcal{J}$ by first restricting the value of ζ_γ so that it is close to the values taken by ζ_α for $\tilde{\alpha}$ in $\mathcal{C}$, we use the inequality

$$\zeta_l - 0.1 \leq \zeta_\gamma \leq \zeta_u + 0.1 \qquad 4.9$$

With ζ_γ satisfying 4.9 a sufficient condition for ξ_γ, η_γ satisfying 4.6 is

$$|(\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2| < \frac{C}{Z_h} \qquad \text{where } Z_h = \max|\zeta - \zeta_\gamma|$$

and the maximum is taken over all points $\tilde{\beta} = (\xi, \eta, \zeta)$ where $\xi_l^{(i)} \leq \xi \leq \xi_u^{(i)}$, $\eta_l^{(i)} \leq \eta \leq \eta_u^{(i)}$ and $|N(\tilde{\beta} - \tilde{\gamma})| < C$. A necessary lower bound for Z_h is then $\frac{1}{2}\zeta_h$. Thus a necessary condition for the integer point $\tilde{\gamma}$ to be included in $\mathcal{J}$ is that when it satisfies 4.9 it further satisfies

$$|(\xi_\alpha - \xi_\gamma)^2 + (\eta_\alpha - \eta_\gamma)^2| < \frac{2C}{\zeta_h}$$

for which necessary conditions are

$$\xi_l - \left(\frac{2C}{\zeta_h}\right)^{\frac{1}{2}} \leq \xi_\gamma \leq \xi_u + \left(\frac{2C}{\zeta_h}\right)^{\frac{1}{2}}$$

and

$$\eta_l - \left(\frac{2C}{\zeta_h}\right)^{\frac{1}{2}} \leq \eta_\gamma \leq \eta_u + \left(\frac{2C}{\zeta_h}\right)^{\frac{1}{2}} \qquad 4.10$$

4.12 Having found the regions $R_1, \ldots, R_m$ for which there is no integer point $\tilde{\gamma}$ satisfying 4.2, it is necessary to determine with which of these regions the translates of the regions, $E(R_1), \ldots, E(R_m)$, intersect.

We suppose that, for some n where $1 \leq n \leq m$, R_n is the set of points (ξ, η, ζ) which satisfy

$$\xi_1^{(n)} \leq \xi \leq \xi_2^{(n)}$$
$$\eta_1^{(n)} \leq \eta \leq \eta_2^{(n)}$$
$$\zeta_1^{(n)} \leq \zeta \leq \zeta_2^{(n)}$$

For each of these vertices, $(\xi_i^{(n)}, \eta_j^{(n)}, \zeta_k^{(n)})$ $i = 1,2$, $j = 1,2$, $k = 1,2$, we find the cylindrical polar co-ordinates $(\rho_{(i,j)}^{(n)}, \alpha_{(i,j)}^{(n)}, \zeta_k^{(n)})$. If the fundamental unit ϵ has cylindrical polar co-ordinates $(\rho_\epsilon, \alpha_\epsilon, \zeta_\epsilon)$, the transform of a point (ρ, α, ζ) by ϵ is $(\rho\rho_\epsilon, \alpha + \alpha_\epsilon, \zeta\zeta_\epsilon)$; thus transforms of the vertices of R_n will be $(\rho_{(i,j)}^{(n)} \rho_\epsilon, \alpha_{(i,j)}^{(n)} + \alpha_\epsilon, \zeta_k^{(n)} \zeta_\epsilon)$ for $i = 1,2$, $j = 1,2$, $k = 1,2$. $E(R_n)$ is then the cuboid with these points as vertices. We suppose now that $E(R_n)$ is the set of points (ξ, η, ζ) which satisfy

$$\xi_{1\epsilon}^{(n)} \leq \xi \leq \xi_{2\epsilon}^{(n)}$$
$$\eta_{1\epsilon}^{(n)} \leq \eta \leq \eta_{2\epsilon}^{(n)}$$
$$\zeta_{1\epsilon}^{(n)} \leq \zeta \leq \zeta_{2\epsilon}^{(n)}.$$

We wish to find the set $\mathcal{J}$ of those points $\tilde{\gamma}$ which cause $E(R_n) - \tilde{\gamma}$ to intersect with the original fundamental region $\mathcal{F}$, in order that we may find which of $R_1, \ldots, R_m$, if any, intersect with the translates of $E(R_n)$.

For each triplet (i, j, k) we find a triad $(x_{ijk}^{(n)}, y_{ijk}^{(n)}, z_{ijk}^{(n)})$

such that

$$\begin{aligned}
\xi^{(n)}_{i\epsilon} &= x^{(n)}_{ijk} + y^{(n)}_{ijk}\,\mathrm{Re}\,\mathcal{M}'(\phi) + z^{(n)}_{ijk}\,\mathrm{Re}\,Q'(\phi) \\
\eta^{(n)}_{j\epsilon} &= \phantom{x^{(n)}_{ijk} +{}} y^{(n)}_{ijk}\,\mathrm{Im}\,\mathcal{M}'(\phi) + z^{(n)}_{ijk}\,\mathrm{Im}\,Q'(\phi) \\
\zeta^{(n)}_{k\epsilon} &= x^{(n)}_{ijk} + y^{(n)}_{ijk}\,\mathcal{M}'(\theta) + z^{(n)}_{ijk}\,Q'(\theta).
\end{aligned}$$

The rational integers X_ℓ, X_u, Y_ℓ, Y_u, Z_ℓ, Z_u are then defined such that X_ℓ, Y_ℓ, Z_ℓ are the greatest and X_u, Y_u, Z_u are the least rational integers to satisfy

$$\begin{aligned}
X_\ell &\le x^{(n)}_{ijk} \le X_u \\
Y_\ell &\le y^{(n)}_{ijk} \le Y_u \\
Z_\ell &\le z^{(n)}_{ijk} \le Z_u
\end{aligned}$$

over all i, j, k where $i = 1,2$, $j = 1,2$, $k = 1,2$. The possible integers $\tilde{\gamma} = (\xi_\gamma, \eta_\gamma, \zeta_\gamma)$ are then among those which satisfy

$$\begin{aligned}
\xi_\gamma &= x + y.\mathrm{Re}\,\mathcal{M}'(\phi) + z.\mathrm{Re}\,Q'(\phi) \\
\eta_\gamma &= \phantom{x +{}} y.\mathrm{Im}\,\mathcal{M}'(\phi) + z.\mathrm{Im}\,Q'(\phi) \\
\zeta_\gamma &= x + y.\mathcal{M}'(\theta) + z.Q'(\theta)
\end{aligned}$$

where

$$\begin{aligned}
X_\ell &\le x \le X_u \\
Y_\ell &\le y \le Y_u \\
Z_\ell &\le z \le Z_u;
\end{aligned}$$

we define $\mathcal{J}$ to be the set of integer points which satisfy these conditions. For each integer $\tilde{\gamma}$ in $\mathcal{J}$ we then test whether, for $p = 1, \ldots, m$, $R_p + \tilde{\gamma}$ intersects with $E(R_n)$.

4.13 The program which performs this testing calculates the basis of the lattice and then reads the values of the coefficients of the vertices of $R_1, \ldots, R_m$ as data, in a format with ten decimal places. To ensure that no points are lost due to rounding error the values of $\xi_1^{(n)}$, $\eta_1^{(n)}$ and $\zeta_1^{(n)}$ for $n = 1, \ldots, m$ are decreased by 10^{-10} and the values of $\xi_2^{(n)}$, $\eta_2^{(n)}$ and $\zeta_2^{(n)}$ are increased by 10^{-10} before any transformations are performed. The values of $\rho_\epsilon, \alpha_\epsilon, \zeta_\epsilon$ will be accurate within the limits of the machine, that is fifteen significant figures, as the coefficients of ϵ relative to the basis $(1, M'(\theta), Q'(\theta))$ are read in as rational integers and $\rho_\epsilon, \alpha_\epsilon, \zeta_\epsilon$ are determined using the basis which is calculated.

Since $0 < \epsilon < 1$ we also have

$$\zeta_{1\epsilon}^{(n)} = \zeta_1^{(n)} \zeta_\epsilon$$

$$\zeta_{2\epsilon}^{(n)} = \zeta_2^{(n)} \zeta_\epsilon$$

$$\xi_{1\epsilon}^{(n)} = \min_{i,j} \left(\rho_{(i,j)}^{(n)} \rho_\epsilon \cos(\alpha_{(i,j)}^{(n)} + \alpha_\epsilon)\right) \quad i = 1,2,\ j = 1,2.$$

$$\eta_{1\epsilon}^{(n)} = \min_{i,j} \left(\rho_{(i,j)}^{(n)} \rho_\epsilon \sin(\alpha_{(i,j)}^{(n)} + \alpha_\epsilon)\right) \quad i = 1,2,\ j = 1,2.$$

$$\xi_{2\epsilon}^{(n)} = \max_{i,j} \left(\rho_{(i,j)}^{(n)} \rho_\epsilon \cos(\alpha_{(i,j)}^{(n)} + \alpha_\epsilon)\right) \quad i = 1,2,\ j = 1,2.$$

$$\eta_{2\epsilon}^{(n)} = \max_{i,j} \left(\rho_{(i,j)}^{(n)} \rho_\epsilon \sin(\alpha_{(i,j)}^{(n)} + \alpha_\epsilon)\right) \quad i = 1,2,\ j = 1,2.$$

CHAPTER 5

THE MINIMUM OF $\frac{\alpha}{1-\epsilon^n}$.

5.1 For a given number $\frac{\alpha}{1-\epsilon^n}$, where α is an algebraic integer, we wish to find the minimum C of $|N(\frac{\alpha}{1-\epsilon^n} - \gamma)|$ for integers γ in K; from I.3, if C is greater than or equal to 1 then the field is non-Euclidean. The special number $\frac{\alpha}{1-\epsilon^n}$ is chosen since for every number ζ in K there is a positive rational integer n such that

$$\epsilon^n \zeta \equiv \zeta \quad (1)$$

thus, if $\zeta = \frac{\alpha}{\beta}$,

$$(1 - \epsilon^n)\frac{\alpha}{\beta} \equiv 0 \quad (1)$$

hence β divides $1 - \epsilon^n$; therefore, without loss of generality, we may restrict β to values of the form $1 - \epsilon^n$.

We obtain bounds for the coefficients p, q, r in the canonical representation of γ as $p\lambda + q\theta + r$: using these bounds we can conduct a computer search for possible γ. The bounds are obtained by showing that values of $N(\frac{\alpha}{1-\epsilon^n} - \gamma)$ are equal to those taken by a restricted set of γ's, since the norm remains unchanged under certain transformations of the lattice of integers.

5.2 In the trivial case when $\frac{\alpha}{1-\epsilon^n}$ is an integer then C = 0. In the following it will be assumed that $\frac{\alpha}{1-\epsilon^n}$ is not an integer of K.

LEMMA 5.1

The number $\frac{\alpha}{1 - \epsilon^n}$ transforms into itself if the elements of K are transformed by

$$T: \gamma \to \frac{\gamma - \alpha}{\epsilon^n} \qquad 5.1$$

PROOF OF LEMMA 5.1 trivial.

For any given integer γ in K

$$N\left(\frac{\alpha}{1 - \epsilon^n} - T(\gamma)\right) = N\left(\frac{\alpha}{1 - \epsilon^n} - \frac{(\gamma - \alpha)}{\epsilon^n}\right)$$

$$= N\left(\frac{\alpha\epsilon^n + \alpha - \alpha\epsilon^n - \gamma(1 - \epsilon^n)}{\epsilon^n(1 - \epsilon^n)}\right)$$

$$= N\left(\frac{1}{\epsilon^n}\left(\frac{\alpha}{1 - \epsilon^n} - \gamma\right)\right)$$

$$= N\left(\frac{\alpha}{1 - \epsilon^n} - \gamma\right)$$

since $N(\epsilon^n) = 1$ and N is multiplicative.

We now have

LEMMA 5.2

$$N\left(\frac{\alpha}{1 - \epsilon^n} - T^i(\gamma)\right) = N\left(\frac{\alpha}{1 - \epsilon^n} - \gamma\right)$$

for every rational integer i.

5.3 If τ_l is an arbitrary real number such that $\tau_l > \frac{\alpha}{1 - \epsilon^n}$, under the transformation 5.1 the set of integers γ in K for which $\gamma \geq \tau_l$ is transformed into that set for which

$$\gamma \geq \frac{\tau_l - \alpha}{\epsilon^n} > \tau_l \qquad \text{since } 0 < \epsilon^n < 1 \text{ when } n \geq 1.$$

If τ_u is an arbitrary real number such that $\tau_u < \frac{\alpha}{1 - \epsilon^n}$, the set of integers γ for which $\gamma \leq \tau_u$ is transformed into that set for which

$$\gamma \leq \frac{\tau_u - \alpha}{\epsilon^n} < \tau_u \qquad \text{since } 0 < \epsilon^n < 1 \text{ when } n \geq 1.$$

Now define the sets A and B:

$$A = \left\{\gamma : \gamma \text{ integer in K and } \tau_l \leq \gamma < \frac{\tau_l - \alpha}{\epsilon^n}\right\}$$

$$B = \left\{\gamma : \gamma \text{ integer in K and } \frac{\tau_u - \alpha}{\epsilon^n} < \gamma \leq \tau_u\right\}.$$

Suppose γ is an integer in K which satisfies

$$\frac{\alpha}{1-\epsilon^n} < \gamma < \tau_\ell$$

and that $T^i(\gamma)$ does not belong to A for any rational integer i, in particular for any positive rational integer i. We have

$$\gamma > \frac{\alpha}{1-\epsilon^n}, \quad T(\gamma) = \frac{\gamma - \alpha}{\epsilon^n}$$

so that

$$T(\gamma) - \frac{\alpha}{1-\epsilon^n} = \frac{\gamma - \frac{\alpha}{1-\epsilon^n}}{\epsilon^n} > 0$$

since $0 < \epsilon^n < 1$. Thus

$$T^i(\gamma) > \frac{\alpha}{1-\epsilon^n}$$

for every positive rational integer i.

Since $\gamma < \tau_\ell$, $T(\gamma) < \frac{\tau_\ell - \alpha}{\epsilon^n}$, but $T(\gamma)$ does not belong to A hence

$$T(\gamma) < \tau_\ell.$$

Thus $T^i(\gamma) < \tau_\ell$ for every positive rational integer i.

We now have

$$\frac{\alpha}{1-\epsilon^n} < T^i(\gamma) < \tau_\ell$$

for every positive rational integer i, so that

$$\frac{\alpha}{1-\epsilon^n} < \frac{\gamma - \alpha\sum_{j=0}^{i-1}\epsilon^{nj}}{\epsilon^{ni}} < \tau_\ell$$

for every positive rational integer i,

$$\gamma < \epsilon^{ni}\tau_\ell + \alpha\sum_{j=0}^{i-1}\epsilon^{nj}$$

for every positive rational integer i, hence

$$\gamma < e + \frac{\alpha}{1-\epsilon^n}$$

where e is arbitrarily small since τ_ℓ is fixed and $0 < \epsilon^n < 1$; but this contradicts

$$\frac{\alpha}{1-\epsilon^n} < \gamma.$$

Thus, for some positive rational integer i, $T^i(\gamma)$ belongs to A.

Now suppose that γ is an integer in K which satisfies

$$\frac{\tau_\ell - \alpha}{\epsilon^n} < \gamma$$

and that $T^i(\gamma)$ does not belong to A for any rational integer i, in particular for any negative rational integer i.

$\gamma > \frac{\tau_\ell - \alpha}{\epsilon^n}$ hence $T^{-1}(\gamma) > \tau_\ell$.

$T^{-1}(\gamma)$ does not belong to A hence

$$T^{-1}(\gamma) > \frac{\tau_\ell - \alpha}{\epsilon^n},$$

consequently

$$T^{-i}(\gamma) > \frac{\tau_\ell - \alpha}{\epsilon^n}$$

for every positive rational integer i. Therefore, we have

$$\gamma\epsilon^{in} + \sum_{j=0}^{i-1}\alpha\epsilon^{jn} > \frac{\tau_\ell - \alpha}{\epsilon^n}$$

for every positive rational integer i, thus

$$\gamma > \epsilon^{-in}\left\{\frac{\tau_\ell - \alpha}{\epsilon^n} - \sum_{j=0}^{i-1}\alpha\epsilon^{jn}\right\}$$

for every positive rational integer i since $0 < \epsilon^n < 1$.

Hence $\gamma > M$ for arbitrarily large M since τ_ℓ and α are fixed,

$$0 < \epsilon^n < 1 \quad \text{and} \quad \frac{\tau_\ell - \alpha}{\epsilon^n} - \frac{\alpha}{1 - \epsilon^n} = \frac{\tau_\ell(1 - \epsilon^n) - \alpha}{\epsilon^n(1 - \epsilon^n)} > 0.$$

This contradicts any particular choice of γ; hence, if γ is an integer such that

$$\gamma > \frac{\alpha}{1 - \epsilon^n} \tag{5.3}$$

then for some rational integer i, $T^i(\gamma)$ belongs to A.

Similarly, if γ is an integer such that

$$\gamma < \frac{\alpha}{1 - \epsilon^n} \tag{5.4}$$

then for some rational integer i, $T^i(\gamma)$ belongs to B.

From lemma 5.2, 5.3 and 5.4, for any integer γ_1 in K there is an integer γ_2 in $A \cup B$ such that

$$N\left(\frac{\alpha}{1 - \epsilon^n} - \gamma_1\right) = N\left(\frac{\alpha}{1 - \epsilon^n} - \gamma_2\right).$$

Thus, if C_1 is any positive real number and there is an integer γ_1 in K such that

$$|N(\frac{\alpha}{1-\epsilon^n} - \gamma_1)| < C_1, \qquad 5.5$$

there is an integer γ_2 in $A \cup B$ such that 5.5 holds with γ_1 replaced by γ_2. In particular if

$$C = \min|N(\frac{\alpha}{1-\epsilon^n} - \gamma)|$$

where the minimum is over integers γ in K, we have

$$C = \min|N(\frac{\alpha}{1-\epsilon^n} - \gamma)|$$

where the minimum is over integers γ in $A \cup B$.

5.4 Following the notation described in the introduction, the number $\gamma = p_\gamma\lambda + q_\gamma\theta + r_\gamma$ may be represented in the space $\mathcal{A}$ by the point $\tilde{\gamma} = (\xi_\gamma, \eta_\gamma, \zeta_\gamma)$ where

$$\zeta_\gamma = p_\gamma\lambda + q_\gamma\theta + r_\gamma$$

$$\xi_\gamma = p_\gamma \operatorname{Re}\psi + q_\gamma \operatorname{Re}\phi + r_\gamma$$

$$\eta_\gamma = p_\gamma \operatorname{Im}\psi + q_\gamma \operatorname{Im}\phi .$$

If

$$\Delta = \begin{vmatrix} \lambda & \theta & 1 \\ \operatorname{Re}\psi & \operatorname{Re}\phi & 1 \\ \operatorname{Im}\psi & \operatorname{Im}\phi & 0 \end{vmatrix}$$

we have

$$p_\gamma = \begin{vmatrix} \zeta_\gamma & \theta & 1 \\ \xi_\gamma & \operatorname{Re}\phi & 1 \\ \eta_\gamma & \operatorname{Im}\phi & 0 \end{vmatrix} / \Delta$$

$$q_\gamma = \begin{vmatrix} \lambda & \zeta_\gamma & 1 \\ \mathrm{Re}\psi & \xi_\gamma & 1 \\ \mathrm{Im}\psi & \eta_\gamma & 0 \end{vmatrix} \Big/ \Delta$$

$$r_\gamma = \begin{vmatrix} \lambda & \theta & \zeta_\gamma \\ \mathrm{Re}\psi & \mathrm{Re}\phi & \xi_\gamma \\ \mathrm{Im}\psi & \mathrm{Im}\phi & \eta_\gamma \end{vmatrix} \Big/ \Delta \, .$$

$\dfrac{\alpha}{1-\epsilon^n} = \zeta_{\alpha^*}$ may be represented by the point

$$\tilde{\zeta}_{\alpha^*} = (\xi_{\alpha^*}, \eta_{\alpha^*}, \zeta_{\alpha^*}).$$

In searching for the points $\tilde{\gamma}$ for which

$$\left| N\left(\frac{\alpha}{1-\epsilon^n} - \gamma\right)\right| \leq C_1 \qquad 5.6$$

for some chosen positive real number C_1, if τ_l, τ_u are arbitrarily chosen real numbers such that

$$\tau_u < \frac{\alpha}{1-\epsilon^n} < \tau_l,$$

from the above it is sufficient to consider those $\tilde{\gamma}$ for which

$$\tau_l \leq \zeta_\gamma < \frac{\tau_l - \alpha}{\epsilon^n} \qquad 5.7$$

and $$\tau_u \geq \zeta_\gamma > \frac{\tau_u - \alpha}{\epsilon^n} \, . \qquad 5.8$$

5.5 Consider, first of all, those $\tilde{\gamma}$ which satisfy 5.7. If

$$|(\zeta_\gamma - \zeta_{\alpha^*})\{(\xi_\gamma - \xi_{\alpha^*})^2 + (\eta_\gamma - \eta_{\alpha^*})^2\}| \leq C_1,$$

since $$\zeta_\gamma \geq \tau_l > \zeta_{\alpha^*}$$

we have

$$(\xi_\gamma - \xi_{\alpha^*})^2 + (\eta_\gamma - \eta_{\alpha^*})^2 \leq \frac{C_1}{\tau_l - \zeta_{\alpha^*}} = \sigma_1^2 \quad \text{say.}$$

Thus, in searching for those $\tilde{\gamma}$ satisfying 5.6 and 5.7, it is sufficient to consider those $\tilde{\gamma}$ which also satisfy

$$\xi_{\alpha^*} - \sigma_1 \leq \xi_\gamma \leq \xi_{\alpha^*} + \sigma_1$$

$$\eta_{\alpha^*} - \sigma_1 \leq \eta_\gamma \leq \eta_{\alpha^*} + \sigma_1 \, .$$

From the bounds on ζ_γ, ξ_γ, η_γ, we may calculate $p_\gamma^{(1)}$, $p_\gamma^{(2)}$, $q_\gamma^{(1)}$, $q_\gamma^{(2)}$, $r_\gamma^{(1)}$, $r_\gamma^{(2)}$ such that, to find those $\tilde{\gamma}$ satisfying 5.6 and 5.7, it is sufficient to consider those $\tilde{\gamma}$ for which

$$p_\gamma^{(1)} \leq p_\gamma \leq p_\gamma^{(2)} \tag{5.9}$$

$$q_\gamma^{(1)} \leq q_\gamma \leq q_\gamma^{(2)} \tag{5.10}$$

$$r_\gamma^{(1)} \leq r_\gamma \leq r_\gamma^{(2)}. \tag{5.11}$$

We now suppose $p_\gamma^{(2)} - p_\gamma^{(1)} \leq q_\gamma^{(2)} - q_\gamma^{(1)}$, then, since

$$\eta_\gamma = p_\gamma \mathrm{Im}\psi + q_\gamma \mathrm{Im}\phi,$$

for any $\tilde{\gamma}$ with p_γ satisfying 5.9, which also satisfies 5.6 and 5.7 we have

$$\frac{\eta_{\alpha^*} - \sigma_1 - p_\gamma \mathrm{Im}\psi}{\mathrm{Im}\phi} \leq q_\gamma \leq \frac{\eta_{\alpha^*} + \sigma_1 - p_\gamma \mathrm{Im}\psi}{\mathrm{Im}\phi} \tag{5.12}$$

since ϕ may be chosen such that $\mathrm{Im}\phi$ is positive.

$$\xi_\gamma = p_\gamma \mathrm{Re}\psi + q_\gamma \mathrm{Re}\phi + r_\gamma$$

thus, for any $\tilde{\gamma}$ with p_γ satisfying 5.9 and q_γ satisfying 5.12, for which 5.6 and 5.7 hold

$$\xi_{\alpha^*} - \sigma_1 - p_\gamma \mathrm{Re}\psi - q_\gamma \mathrm{Re}\phi \leq r_\gamma \leq \xi_{\alpha^*} + \sigma_1 - p_\gamma \mathrm{Re}\psi - q_\gamma \mathrm{Re}\phi.$$

In this way we obtain bounds on the values of p_γ, q_γ and r_γ; and so have a finite number of possibilities for $\tilde{\gamma}$ satisfying 5.6 and 5.7.

If $p_\gamma^{(2)} - p_\gamma^{(1)} > q_\gamma^{(2)} - q_\gamma^{(1)}$ then, for any $\tilde{\gamma}$ with q_γ satisfying 5.10 which also satisfies 5.6 and 5.7 we have

$$\frac{\eta_{\alpha^*} - \sigma_1 - q_\gamma \mathrm{Im}\phi}{\mathrm{Im}\psi} \leq p_\gamma \leq \frac{\eta_{\alpha^*} + \sigma_1 - q_\gamma \mathrm{Im}\phi}{\mathrm{Im}\psi} \tag{5.13}$$

since $\mathrm{Im}\psi > 0$ as $\mathrm{Im}\psi = \dfrac{2\mathrm{Re}\phi\mathrm{Im}\phi + t\mathrm{Im}\phi + s}{\ell}$, ϕ is chosen such that $\mathrm{Im}\phi$ is positive, $\theta + 2\mathrm{Re}\phi = a$ hence $\mathrm{Re}\phi = \dfrac{a - \theta}{2} > 0$ since $a \geq 1$ and $0 < \theta < 1$.

We now have, for any $\tilde{\gamma}$ with q_γ satisfying 5.10 and p_γ

satisfying 5.13,

$$\xi_{\alpha^*} - \sigma_1 - p_\gamma \mathrm{Re}\psi - q_\gamma \mathrm{Re}\phi \le r_\gamma \le \xi_{\alpha^*} + \sigma_1 - p_\gamma \mathrm{Re}\psi - q_\gamma \mathrm{Re}\phi \,.$$

Again we have bounds on the possible values of p_γ, q_γ and r_γ, and so a finite number of possibilities for $\tilde{\gamma}$ satisfying 5.6 and 5.7.

5.6 Now we consider those $\tilde{\gamma}$ satisfying 5.8

$$\tau_u \geq \xi_\gamma > \frac{\tau_u - \alpha}{\epsilon^n} \quad \text{hence} \quad \xi_{\alpha^*} > \tau_u \geq \xi_\gamma$$

and if

$$|(\xi_\gamma - \xi_{\alpha^*})\{(\xi_\gamma - \xi_{\alpha^*})^2 + (\eta_\gamma - \eta_{\alpha^*})^2\}| \le C_1$$

we have

$$(\xi_\gamma - \xi_{\alpha^*})^2 + (\eta_\gamma - \eta_{\alpha^*})^2 \le \frac{C_1}{\xi_{\alpha^*} - \tau_u} = \sigma_2^2 \quad \text{say.}$$

Thus in the same way as that used for $\tilde{\gamma}$ satisfying 5.6 and 5.7 with σ_1 replaced by σ_2, we may find a finite number of possibilities for $\tilde{\gamma}$ satisfying 5.6 and 5.8.

5.7 In some cases the range of values of γ in A and B may be very large, we, therefore, choose integers $\tau_l^{(1)}, \ldots, \tau_l^{(k)}$ such that

$$\frac{\alpha}{1 - \epsilon^n} < \tau_l = \tau_l^{(1)} < \ldots\ldots < \tau_l^{(k)} = \frac{\tau_l - \alpha}{\epsilon^n}$$

and integers $\tau_u^{(1)}, \ldots, \tau_u^{(m)}$ such that

$$\frac{\tau_u - \alpha}{\epsilon^n} = \tau_u^{(m)} < \ldots\ldots < \tau_u^{(1)} = \tau_u < \frac{\alpha}{1 - \epsilon^n} \,.$$

Then, using the method outlined above for $\tilde{\gamma}$ satisfying 5.7, we consider, in turn, those $\tilde{\gamma}$ satisfying

$$\tau_l^{(i)} \le \xi_\gamma < \tau_l^{(i+1)} \qquad \text{for } i = 1, \ldots, k - 1$$

replacing τ_l by $\tau_l^{(i)}$ throughout.

We then use the method outlined above for $\tilde{\gamma}$ satisfying 5.8

to consider, in turn, those $\tilde{\gamma}$ satisfying

$$\tau_u^{(i+1)} < \xi_\gamma \le \tau_u^{(i)} \qquad \text{for } i = 1, \ldots, m-1$$

replacing τ_u by $\tau_u^{(i)}$ throughout.

5.7 When determining $\left|N\left(\frac{\alpha}{1-\epsilon^n} - \gamma\right)\right|$ for γ in $A \cup B$, we first determine the integer $\alpha - \gamma(1-\epsilon^n)$ then calculate its norm and divide this by $N(1-\epsilon^n)$. The integers involved in these calculations often become very large; consequently double precision arithmetic is used, and a message is monitored when the quantities involved are likely to cause integer overflow, that is a loss of accuracy in the double precision entities.

CHAPTER 6

A NUMERICAL CONSIDERATION OF THE METHODS EMPLOYED.

6.1 This chapter gives an example of the application of each of the methods of this thesis, using the cubic field with discriminant -199 as example. Also included in this chapter are descriptions of some of the basic routines employed and observations on the limitations of the methods.

6.2 Each of the methods described involves the determination of the real zero θ of the defining polynomial of the field, a basis for the field, and a basis for the lattice of integers.

If a field has defining polynomial $x^3 - ax^2 + bx - c$, the zeroes are the roots of the equation $x^3 - ax^2 + bx - c = 0$; we make the substitution $y = 3x - a$, that is $x = \frac{y+a}{3}$, then

$$y^3 - qy - n = 0 \qquad 6.1$$

where $q = 3a^2 - 9b$, $n = 27c - 9ab + 2a^3$;
if we now let $q = 3uv$, $n = u^3 + v^3$ then $\Theta = u + v$ is the real zero of the polynomial 6.1. This theory is used to determine Θ and $\theta = \frac{\Theta + a}{3}$, the former is required for the application of Voronoi's algorithm which is initially referred to in chapter 1.

The cubic field K with discriminant -199 has defining polynomial $x^3 - 2x^2 + 5x - 3$ thus

$$n = 7, \quad q = -33$$

and we obtain

$$\theta = .73727772.....$$

$$\Theta = .21183316.....$$

The index of the polynomial relative to the field is 1, thus the basis is $(1, \theta, \lambda)$ where $\lambda = \theta^2$. We now have the basis for the lattice of integers

$(0,0,0)$, $(1,0,1)$, (.63136113..., 1.9158303...., .73727772...),

(-3.2717892...., 2.4191617...., .54357843...).

6.3 Most of the methods employed require the determination of the coefficients of $1, \theta, \lambda$ in the expressions for θ^2, λ^2 and $\theta\lambda$; these values are subsequently used in routines for the product and the quotient of two algebraic numbers. For the field K we find, since $\lambda = \theta^2$,

$$\theta^2 = 1\lambda + 0\theta + 0$$

$$\lambda^2 = -1\lambda - 7\theta + 6$$

$$\theta\lambda = 2\lambda - 5\theta + 3.$$

Some of the methods require the determination of the norm of an algebraic number, the product of two algebraic numbers or the quotient of two algebraic numbers. It is in the routines for these operations that there is the greatest danger of integer overflow; to prevent undetected overflow, the coefficients with respect to the basis of the field of the algebraic integer or integers involved are tested to ensure that the coefficients of the resultant integer will not require more significant figures than possible with the computer in order to give an exact result.

When the product of n coefficients is involved, for single precision arithmetic we ensure that no product may exceed 10^{14-t}, and for double precision arithmetic we ensure that no product may exceed 10^{29-t}, where, in each case, t is the smallest power of 10 which exceeds the greatest constant multiplier of the products of coefficients involved in the particular subroutine in question.

6.4 I now turn to the adaptation of Cassels' result described in chapter 2. We start with the ideal

$$(1, \theta, \theta^2) = (1, \frac{6 + 3\Theta}{9}, \frac{4 + 4\Theta + \Theta^2}{9})$$

which has reduced form

$$(1, \frac{3 - 3\Theta}{9}, \frac{7 + \Theta + \Theta^2}{9}),$$

and the next ideal in the loop is also this ideal. The reduced ideal, expressed in terms of θ, is given by

$$(1, 1 - \theta , 1 - \theta + \theta^2),$$

and we see that one complete sequence of relative minima is

$$1, 1 - \theta$$

and $\epsilon = 1 - \theta$. We then have

$$M = 3.8063007$$

thus $\dfrac{|D|}{720M} = .0726$;

in fact $\dfrac{|D|}{715.244M} = .0731$ $\dfrac{|\Delta|}{412.944} = .0342.$

Using the method for fields in the table of (1) no results concerning the existence of the Euclidean algorithm could be found. The field with discriminant -160087 was shown to have 44 distinct relative minima, thus the chain calculated consisted of $\left[\frac{44 + 1}{3}\right] = 15$ relative minima "before" 1 and 29 "after". The resultant value of M was 188.308... so that

$$\frac{|D|}{720M} = 1.1807 > 1,$$

hence the field does not possess a Euclidean Algorithm.

Similarly, for the field with discriminant -169571 $M = 167.136\ldots$ thus

$$\frac{|D|}{720M} = 1.4091 > 1$$

and this field does not possess a Euclidean Algorithm.

6.5 For the method described in chapter 3 we have $\epsilon = 1 - \theta$ hence $\epsilon - 1 = -\theta$ and $N(\epsilon - 1) = -3$. Thus the only divisor of $\epsilon - 1$ is $\epsilon - 1$ itself, and multiples of it by the fundamental unit. However, any integer of norm 2 or 3 will have the fundamental unit of the field, or its negative, as a member of its non-zero residue classes; consequently, no result can be obtained by considering residue classes modulo $\epsilon - 1$. $\epsilon + 1 = -\theta + 2$ has norm 7, thus any factor, not a power of the fundamental unit, must be a multiple of $\epsilon + 1$ by a power of the fundamental unit.

The method used for calculating integers of a given norm causes congruences to be considered modulo $\beta = \theta^2 - \theta + 5 = (\epsilon + 1)/\epsilon$. We then have $\epsilon \equiv -1\ (\beta)$ thus $-\epsilon \equiv 1\ (\beta)$. There are no integers of norm 2 and so none of norms 4 or 6. $3 = \theta(\theta^2 - 2\theta + 5)$ where $\theta^2 - 2\theta + 5$ is an algebraic prime of norm 9. Thus integers of norm 3 are either congruent to $\theta \equiv 2\ (\beta)$ or to $-\theta \equiv 5\ (\beta)$. There are no integers of norm 5. Thus we see that there are no integers of norm less than $|N(\beta)|$ congruent to 3 or 4 modulo β, and so the field does not possess a Euclidean Algorithm.

When using this method it was found that, as the size of the coefficients of the fundamental unit with respect to the field increased, the magnitude of the norms of $\epsilon - 1$ and of $\epsilon + 1$ also increased and had prime factors of norm greater than 500, with the result that no conclusion was reached; also, for such fields, overflow warning messages were given, both in calculating the integers of a given norm and in establishing to which congruence class any particular integer belonged, thus invalidating any results which may have been obtained. With these points in mind only those fields with discriminant of absolute value less than 5,000 were investigated by means of the program, but some additional ones were investigated "by hand".

Generally, when α is an integer of norm less than $|N(\beta)|$, we determine to which congruence class it belongs by establishing for which ξ_j, where $1 \leq j \leq r_\beta$, β divides $\xi_j - \alpha$. However, this method becomes time consuming when $|N(\beta)|$ is large; we note that when $|N(\beta)|$ is a rational prime the residue classes modulo β are represented by the rational integers $0, 1, \ldots, |N(\beta)|-1$ and we have $\theta \equiv i_\theta \ (\beta)$ and $\lambda \equiv i_\lambda$ for some rational integers i_θ and i_λ satisfying $0 \leq i_\theta \leq |N(\beta)| - 1$ and $0 \leq i_\lambda \leq |N(\beta)| - 1$; hence, for any $\alpha = p\lambda + q\theta + r$ we have $\alpha \equiv pi_\lambda + qi_\theta + r \ (\beta)$. By reducing the expression modulo $|N(\beta)|$ we establish to which residue class α belongs. In some cases this modification reduced the time taken to establish a result from over 120 seconds of central processor time to less than 5 seconds.

6.6 We now consider the adaptation of the method of Barnes and Swinnerton-Dyer as described in chapter 4. Starting from the basis for K and the corresponding basis for $\mathfrak{a}$ described above, and following the arguments of 4.8, we obtain the basis

$(1, \theta - 1, \theta^2 - \theta + 2)$ for K then the corresponding basis for $\mathfrak{a}$ is

$(0,0,0)$, $(1,0,1)$, $(-.3686388604,\ 1.9158303963,\ -.2627222793)$,

$(-1.9031503584,\ .5033313285,\ 1.8063007167)$.

This results in $\mathcal{C}$ being the set of points (ξ, η, ζ) given by

$$|\xi| \le 1.6358946094$$

$$|\eta| \le 1.2095808624$$

$$|\zeta| \le 1.5345114980.$$

In the following a region which satisfies 4.2 will be said to be covered.

On subdivision of $\mathcal{C}$ into sub-regions, with C = .9999, there are 14 uncovered regions with $\zeta \ge 0$; but only one of these regions contains uncovered sub-regions itself, namely R_1, that given by

$$-1.3087156875 \le \xi \le -.9815367656$$

$$.9676646899 \le \eta \le 1.2095808624$$

$$.3069022996 \le \zeta \le .6138045992.$$

R_1 contains five uncovered sub-regions but only two of these contain uncovered sub-regions themselves, namely

R_{11} :

$$-1.2759977953 \le \xi \le -1.2432799031$$

$$1.0160479244 \le \eta \le 1.0402395416$$

$$.3682827595 \le \zeta \le .3989729895$$

R_{12} :

$$-1.2759977953 \leq \xi \leq -1.2432799031$$

$$1.0402395416 \leq \eta \leq 1.0644311589$$

$$.3682827595 \leq \zeta \leq .3989729895$$

On further subdivision, R_{11} contains three uncovered sub-regions, two of which themselves contain uncovered sub-regions, namely

R_{111} :

$$-1.2629106384 \leq \xi \leq -1.2596388492$$

$$1.0354012182 \leq \eta \leq 1.0378203799$$

$$.3744208055 \leq \zeta \leq .3774898285$$

R_{112} :

$$-1.2596388492 \leq \xi \leq -1.2563670600$$

$$1.0354012182 \leq \eta \leq 1.0378203799$$

$$.3744208055 \leq \zeta \leq .3774898285$$

R_{12} contains four uncovered sub-regions, but none of these contain uncovered sub-regions themselves.

R_{111} contains two and R_{112} five uncovered sub-regions which are all contained in the region R given by

$$-1.2599660281 \leq \xi \leq -1.2589844914$$

$$1.0366107991 \leq \eta \leq 1.0378203800$$

$$.3756484147 \leq \zeta \leq .3759553170,$$

thus any point $\tilde{\alpha}$ in $\mathfrak{F}$ with $|N(\tilde{\alpha} - \tilde{\gamma})| > .9999$, where $\tilde{\gamma}$ is an integer in $\mathfrak{I}$, must be in R or in R_-, where R_- is the set of those points $\tilde{\alpha}$ for which $-\tilde{\alpha}$ is in R.

We find that any point $\tilde{\alpha}$ in R satisfies either

$$E(\tilde{\alpha}) - \tilde{\gamma} \text{ is in } R_- \text{ where } \gamma = (1 + 2(\theta - 1))$$

or $\qquad E(\tilde{\alpha}) \in (\mathcal{F} - (R \cup R_-)) \pmod 1$.

Thus any point $\tilde{\alpha}$ in R satisfies either

$$E^2(\tilde{\alpha}) - E(\tilde{\gamma}) + \tilde{\gamma} \text{ is in } R$$

or $\qquad E(\tilde{\alpha}) - \tilde{\gamma} \in (\mathcal{F} - (R \cup R_-)) \pmod 1$.

In the latter case $\tilde{\alpha}$ must have minimum less than .9999.

The required fixed point $\tilde{\beta}$ of E^2 is given by

$$\epsilon^2\beta - \epsilon(2\theta - 1) + 2\theta - 1 = \beta,$$

where $\qquad \epsilon = -\theta + 1, \quad \epsilon^2 = \theta^2 - 2\theta + 1$

and we have

$$(\theta^2 - 2\theta + 1)\beta - (-2\theta^2 + 3\theta - 1) + 2\theta - 1 = \beta$$

$$\beta = \frac{-2\theta^2 + \theta}{\theta^2 - 2\theta} = \frac{-2\theta^2 + \theta}{\epsilon^2 - 1}.$$

It now remains to calculate

$$\min_{\tilde{\delta}} |N(\tilde{\beta} - \tilde{\delta})|,$$

where the minimum is over integers δ in K; this will be done using the method described in chapter 5. From above, we know that for every $\tilde{\alpha}$ in $\mathcal{F}$ such that $\tilde{\alpha}$ is not equal to $\tilde{\beta}$

$$\min_{\tilde{\delta}} |N(\tilde{\alpha} - \tilde{\delta})| < .9999.$$

6.7 When using the method of chapter 4, it was found that as the absolute value of the discriminant of the field increased, the number of uncovered sub-regions of a particular region became large with $C = .9999$, the "crucial" value in the investigation of the Euclidean Algorithm. To avoid very large amounts of output, when the number of uncovered sub-regions of a particular region exceeded a bound given as data at run-time, only the number of sub-regions, and not their nature, was printed; when the nature of the sub-regions was required, a modified version of the program was used, this determined and printed the bounds on the co-ordinates of points in the smallest cuboid, with sides parallel to the co-ordinate axes, which contained all of the uncovered sub-regions of a given region.

However, even with the modified program, it was found that the number of regions to be considered, when attempting to satisfy II(a) or II(b) of chapter 4, became so large as to make the method require a large amount of computing for those fields of discriminants -680 and -687, and completely impractical for that with discriminant -1004. Consequently, with the exception of the field with discriminant -1004, no investigation was made of fields after that with discriminant -687 in the table of (1).

6.8 I now turn to the determination of the minimum of $\dfrac{-2\theta^2+\theta}{\epsilon^2-1} = \dfrac{2\theta^2-\theta}{1-\epsilon^2}$ using the method of chapter 5.

Note that

$$\frac{2\theta^2-\theta}{1-\epsilon^2} \equiv \frac{3\theta}{1-\epsilon^2} \pmod 1$$

and

$$\frac{3\theta}{1-\epsilon^2} = \frac{3}{-\theta+2} = \frac{3\theta^2+15}{7} = \frac{3.5435784374+15}{7} = 2.375819331 = \zeta_{\alpha^*}$$

$\alpha^* = \dfrac{3\theta}{1-\epsilon^2} = \dfrac{3\theta^2+15}{7}$ is fixed under ϵ^2, and $\alpha^* > 0$; α^* is used here instead of $\dfrac{2\theta^2-\theta}{1-\epsilon^2}$ to simplify calculations.

$\tilde{\alpha}^*$ is the point $\left\{\mathrm{Re}\left\{\dfrac{3\phi^2+15}{7}\right\}, \mathrm{Im}\left\{\dfrac{3\phi^2+15}{7}\right\}, \dfrac{3\theta^2+15}{7}\right\}$

$$\mathrm{Re}\left\{\frac{3\phi^2+15}{7}\right\} = \frac{3\mathrm{Re}\phi^2+15}{7} = .740661764 = \xi_{\alpha^*}$$

$$\mathrm{Im}\left\{\frac{3\phi^2+15}{7}\right\} = \frac{3\mathrm{Im}\phi^2}{7} = 1.036783597 = \eta_{\alpha^*}$$

that is, $\tilde{\alpha}^*$ is the point $\{.740661764, 1.036783597, 2.375819331\}$

$$= \{\xi_{\alpha^*}, \eta_{\alpha^*}, \zeta_{\alpha^*}\}.$$

If $\tau_l = 5$ and $\tau_u = -5$ we have $\tau_u < \zeta_{\alpha*} < \tau_l$. We wish to consider those points $\tilde{\gamma} = (\xi_\gamma, \eta_\gamma, \zeta_\gamma)$ for which

$$|N(\tilde{\alpha}^* - \tilde{\gamma})| \leq 2$$

where 2 is chosen as a value greater than 1. We note that if

$$\begin{aligned} \xi_\gamma &= p_\gamma \mathrm{Re}\phi^2 + q_\gamma \mathrm{Re}\phi + r_\gamma \\ \eta_\gamma &= p_\gamma \mathrm{Im}\phi^2 + q_\gamma \mathrm{Im}\phi \\ \zeta_\gamma &= p_\gamma \theta^2 \quad + q_\gamma \theta \quad + r_\gamma \end{aligned} \qquad 6.2$$

we have

$$\begin{aligned} p_\gamma &= -.271619232\ldots\xi_\gamma - .015016455\ldots\eta_\gamma + .271619232\ldots\zeta_\gamma \\ q_\gamma &= .342979656\ldots\xi_\gamma + .540928484\ldots\eta_\gamma - .342979656\ldots\zeta_\gamma \\ r_\gamma &= -.105224901\ldots\xi_\gamma - .390651899\ldots\eta_\gamma + 1.105224901\ldots\zeta_\gamma \end{aligned}$$

check: the determinant of the coefficients is $-.14177624 = -\sqrt{\frac{4}{199}}$ and $-\sqrt{\frac{199}{4}}$ = the determinant of the coefficients of the equations 6.2.

Following the reasoning of chapter 5, we first consider those points $\tilde{\gamma}$ for which

$$\tau_l \leq \zeta_\gamma \leq \frac{\tau_l - 3\theta}{\epsilon^2};$$

using the notation of chapter 5

$$\sigma_1 = \left(\frac{2}{5 - \zeta_{\alpha*}}\right)^{\frac{1}{2}} = .873007817$$

and we have

$$\begin{aligned} \xi_{\alpha*} - \sigma_1 &= -.132346053 \leq \xi_\gamma \leq \xi_{\alpha*} + \sigma_1 = 1.613669581 \\ \eta_{\alpha*} - \sigma_1 &= .163775780 \leq \eta_\gamma \leq \eta_{\alpha*} + \sigma_1 = 1.909791414 \\ \tau_l &= \quad 5 \quad \leq \zeta_\gamma \leq \frac{\tau_l - 3\theta}{\epsilon^2} = 20.394753039. \end{aligned}$$

We now obtain the bounds

$$\begin{aligned} .891114170 &\leq p_\gamma \leq 11.005480200 \\ -13.811379521 &\leq q_\gamma \leq -.128381867 \\ 4.610262640 &\leq r_\gamma \leq 44.595233710 \end{aligned}$$

hence

$$1 \le p_\gamma \le 11$$

$$-13 \le q_\gamma \le -1$$

$$5 \le r_\gamma \le 44.$$

For each value of p_γ we may obtain smaller ranges for q_γ, then for r_γ, as follows

$$q_\gamma = \frac{\eta_\gamma - p_\gamma \operatorname{Im}\phi^2}{\operatorname{Im}\phi}$$

hence

$$.085485532 - 1.262722280p_\gamma \le q_\gamma \le .996847852 - 1.262722280p_\gamma$$

$$r_\gamma = \xi_\gamma - p_\gamma \operatorname{Re}\phi^2 - q_\gamma \operatorname{Re}\phi$$

thus

$$-.132346053 + 3.271789219p_\gamma - .6313611396q_\gamma$$
$$\le r_\gamma \le 1.613669581 + 3.271789219p_\gamma - .6313611396q_\gamma.$$

$p_\gamma = 1$ requires $q_\gamma = -1$ $\begin{cases} r_\gamma = 4 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = 1 \\ \text{or } r_\gamma = 5 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = 1 \end{cases}$

$p_\gamma = 2$ requires $q_\gamma = -2$ $\begin{cases} r_\gamma = 8 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{33}{21} \\ \text{or } r_\gamma = 9 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{27}{21} \end{cases}$

$p_\gamma = 3$ requires $q_\gamma = -3$ $\begin{cases} r_\gamma = 12 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{81}{21} \\ \text{or } r_\gamma = 13 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{111}{21} \end{cases}$

$p_\gamma = 4$ gives no integer values of q_γ.

$p_\gamma = 5$ requires $q_\gamma = -6$ $\quad r_\gamma = 21 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{72}{21}$

$p_\gamma = 6$ requires $q_\gamma = -7$ $\begin{cases} r_\gamma = 24 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{261}{21} \\ \text{or } r_\gamma = 25 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = 1 \end{cases}$

$p_\gamma = 7$ requires $q_\gamma = -8$ $\begin{cases} r_\gamma = 28 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{339}{21} \\ \text{or } r_\gamma = 29 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{216}{21} \end{cases}$

$p_\gamma = 8$ requires $q_\gamma = -10 \begin{cases} \phantom{\text{or }} r_\gamma = 33 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{441}{21} \\ \text{or } r_\gamma = 34 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{783}{21} \end{cases}$

$p_\gamma = 9$ requires $q_\gamma = -11 \begin{cases} \phantom{\text{or }} r_\gamma = 37 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{87}{21} \\ \text{or } r_\gamma = 38 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{591}{21} \end{cases}$

$p_\gamma = 10$ requires $q_\gamma = -12$ $\quad r_\gamma = 41 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = 1$

$p_\gamma = 11$ requires $q_\gamma = -13$ $\quad r_\gamma = 45 \Rightarrow |N(\tilde{\alpha}^* - \tilde{\gamma})| = \frac{369}{21}$.

We must now consider those points $\tilde{\gamma}$ for which

$$\tau_u \geq \zeta_\gamma \geq \frac{\tau_u - \alpha}{\epsilon^n}$$

and we have

$$\sigma_2 = \left(\frac{2}{\zeta_{\alpha^*} + 5}\right)^{\frac{1}{2}} = .52072672...$$

hence

$$\xi_{\alpha^*} - \sigma_2 \leq \xi_\gamma \leq \xi_{\alpha^*} + \sigma_2$$
$$\eta_{\alpha^*} - \sigma_2 \leq \eta_\gamma \leq \eta_{\alpha^*} + \sigma_2$$
$$\frac{\tau_u - 3\theta}{\epsilon^2} \leq \zeta_\gamma \leq \tau_u$$

and we proceed as above to reach eventually the conclusion

$$\min_\gamma \left|N\left(\frac{3\theta}{1 - \epsilon^2} - \gamma\right)\right| = 1.$$

We now have the result that the cubic field with discriminant -199 does not possess a Euclidean Algorithm; it has inhomogeneous minimum 1 and this minimum is attained at the numbers congruent to $\pm \frac{(1 + 3\theta^2)}{7}$ (mod 1).

6.9 For the method of chapter 5, as the value of n increases ϵ^n becomes so small that the range of values of p_γ, q_γ, r_γ to be considered becomes too large to be practical. For the field of discriminant -680 it was found that no result could be obtained with $n = 3$ within 60 seconds central processor time.

PART II

THE PROGRAMS USED AND THE RESULTS OBTAINED.

CHAPTER 7

THE PROGRAM RELMIN

This program is that used for the method of chapter 2. In this and other program descriptions the subroutines will be described before the main program; widely used values are passed between the subroutines by means of COMMON variables.

FUNCTION IOF(I)

The answer returned is the greatest power of 10 which exceeds the value of I. This value is required when we are determining bounds which are used for the prevention of integer overflow.

SUBROUTINE BASEH

The field has defining polynomial $x^3 - IA.x^2 + IB.x - IC$, discriminant IDET, and the index of the polynomial over the field is INDEX. The routine determines the values PH = Θ, IQ = Q = q, INN = RN = n, HHH = Θ^2 and ZZ = HHH − q, where Θ, q and n are as defined in 6.2. These values are all required in the application of Voronoi's algorithm in the subroutine MINIMA. The values IL1, IL2, IL3, IT1, IT2, IT3, IP1, IP2, IP3 where

$$\lambda^2 = IL1.\lambda + IL2.\theta + IL3$$

$$\theta^2 = IT1.\lambda + IT2.\theta + IT3$$

$$\theta\lambda = IP1.\lambda + IP2.\theta + IP3$$

are also determined. From these values we now have a basis for the lattice of integers

(0,0,0), (R(1),U(1),H(1)), (R(2),U(2),H(2)), (R(3),U(3),H(3))

Finally the subroutine is used to determine the upper bounds on the product of the coefficients of the algebraic integers for the subroutines MULTCD and DIVCD, which are used for double precision multiplication and division respectively.

The subroutines SUB(I,J,K,L), INVER(I,J,K,KDET), ICF(IJ,IK,IL,IH), ICF2(IJ,IK,IL,IH) and MULT(J1,J2,J3,K1,K2,K3,L1,L2,L3) are those used by Angell in (1) chapter 6.

SUBROUTINE PHITH(I1,I2,I3,ID,J1,J2,J3,JD)

Given I1, I2, I3, ID, this routine finds J1, J2, J3, JD such that

$$\frac{I1 + I2.\Theta + I3.\Theta^2}{ID} = \frac{J1.\lambda + J2.\theta + J3}{JD}$$

SUBROUTINE DIVCD(L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR)

L, M, N and LR are determined such that

$$\frac{L.\lambda + M.\theta + N}{LR} = \left(\frac{L1.\lambda + M1.\theta + N1}{LN}\right)/\left(\frac{L2.\lambda + M2.\theta + N2}{LD}\right);$$

the coefficients in the numerator and denominator are first tested for the possibility of overflow.

SUBROUTINE MULTCD(L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR)

L, M, N and LR are determined such that

$$\frac{L.\lambda + M.\theta + N}{LR} = \left(\frac{L1.\lambda + M1.\theta + N1}{LN}\right).\left(\frac{L2.\lambda + M2.\theta + N2}{LD}\right);$$

again the coefficients in the numerator and denominator are first tested for the possibility of overflow.

DOUBLE FUNCTION DCI(X,Y,Z,RD)

The answer returned is the co-ordinate of $X + Y.\theta + Z.\lambda$

in the ξ, η or ζ direction when RD is the array R, U or H respectively.

SUBROUTINE MINIMA

SECTION 1 of this routine closely follows the subroutine UNIT of (1) chapter 6. On exit from SECTION 1 we have a loop of N lattices

$$\left(1, \frac{\text{IAN}(1,\text{J}) + \text{IAN}(2,\text{J}).\Theta + \text{IAN}(3,\text{J}).\Theta^2}{\text{NP}(\text{J})}, \frac{\text{JAN}(1,\text{J}) + \text{JAN}(2,\text{J}).\Theta + \text{JAN}(3,\text{J}).\Theta^2}{\text{NP}(\text{J})}\right)$$

for J = 1, . . . , N, and the first and Nth lattices are the same. From these lattices we obtain a sequence of relative minima

$$\text{L}(1,\text{ILAT}).\lambda + \text{L}(2,\text{ILAT}).\theta + \text{L}(3,\text{ILAT})$$

for ILAT = 1, . . . , N; and if NQP = [N/3] + 1 we have

$$\text{L}(1,\text{NQP}).\lambda + \text{L}(2,\text{NQP}).\theta + \text{L}(3,\text{NQP}) = 1.$$

From these relative minima we obtain the value REMN which is the value M of chapter 2; thus we obtain the value of DET/720.REMN where DET is a real variable with the same value as IDET.

THE MAIN PROGRAM.

The main program simply co-ordinates the execution of the subroutines, and reads and prints relevant information about the fields.

Following the reasoning of chapter 2, this program only gives a meaningful result when INDEX = 1.

CHAPTER 8

THE PROGRAM CONG

The method of chapter 3 is put into practice by using this program. The subroutines ICF2(IJ,IK,IL,IH), SUB(I,J,K,L), ICF(IJ,IK,IL,IH), INVER(I,J,K,KDET), MULT(J1,J2,J3,K1,K2,K3,L1,L2,L3), DIVCD(L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,R) and IOF(I) are as for the program RELMIN. The subroutine MULT2(A,B,C,D,E,F,G,H,I) is the double precision version of MULT as described in chapter 6 of (1).

SUBROUTINE BASE

This routine is basically similar to BASEH in the program RELMIN. BASE does not calculate a basis for the lattice of integers. Additionally, BASE finds upper bounds for the product of the coefficients of the algebraic integers for the subroutines MULTC and DIVC.

SUBROUTINE FACTOR(NN,NF,NP,NL,I)

This routine is used to determine the rational prime factors of NN which are less than 500. NL is chosen by the calling routine to be an integer greater than the number of distinct rational prime factors of NN. Finally I is the number of distinct rational prime factors of NN and these factors are in the array NF such that NP(I) is the power to which NF(I) is a factor of NN. In the routine we note that an integer n has at least one factor less than $n^{\frac{1}{2}}$, unless it is prime.

SUBROUTINE IDEAL(N,ISC)

IDEAL is a simplified version of the subroutine FACTOR of (1) chapter 6; IDEAL finds the ideals of norm N, where N is restricted to be a rational prime.

$$\mathrm{NORL(KB)} = N((\theta^2 + \mathrm{KT}.\theta + \mathrm{KB})/L)$$

where L is the index of the polynomial $x^3 - \mathrm{IA}x^2 + \mathrm{IB}x - \mathrm{IC}$, and KT, KS are such that $\lambda = \dfrac{\theta^2 + \mathrm{KT}\theta + \mathrm{KS}}{L}$; and

$$\mathrm{NORN(J)} = N(\theta + J).$$

The ideals of norm N are

$$(A(I),\ B(I).\theta + C(I),\ D(I).\lambda + E(I).\theta + G(I))$$

for $I = 1, \ldots, \mathrm{ISC}$.

SUBROUTINE CHANGE(I,J,K,L,I1,J1,K1)

The integers I, J, K, L are supplied to the routine; I1, J1, K1 are found such that $\mathrm{I1}.\lambda + \mathrm{J1}.\theta + \mathrm{K1} = (\mathrm{I}.\theta^2 + \mathrm{J}.\theta + \mathrm{K})/L$.

SUBROUTINE PRIN(INK)

This subroutine, as the subroutine MINIMA of chapter 7, is based on the subroutine UNIT of (1).

When INK is equal to 1, starting from the basis $(1, \theta, \lambda)$ the routine finds the reduced basis for the unit ideal of the field, which is given by

$$\left(1,\ \frac{\mathrm{MU1} + \mathrm{MU2}\Theta + \mathrm{MU3}\Theta^2}{\mathrm{IGU1}},\ \frac{\mathrm{NU1} + \mathrm{NU2}\Theta + \mathrm{NU3}\Theta^2}{\mathrm{IGU1}}\right).$$

When INK is greater than 1, given the ideal $(\mathrm{JA},\ \mathrm{JB}.\theta + \mathrm{JC},\ \mathrm{JD}.\lambda + \mathrm{JE}.\theta + \mathrm{JF})$ of norm INK the routine finds an integer $\mathrm{JP}.\lambda + \mathrm{JR}.\theta + \mathrm{JS}$ which produces the ideal. These calculations are based on the theory of chapter 1.

PRIN also includes tests on the arguments of the routines MULT2 and CHANGE to check for the possibility of integer overflow.

DOUBLE FUNCTION FDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)

The answer returned is the value of the determinant

$$\begin{vmatrix} I1 & I2 & I3 \\ J1 & J2 & J3 \\ K1 & K2 & K3 \end{vmatrix} .$$

In the program RELMIN this was written as a function statement in the subroutine DIVCD; but the compiler used for this program appeared to loop when attempting to optimise the expression for the determinant, this was overcome by compiling this subroutine alone without full optimisation. The different compiler was used since the one for this program considerably increased the compile-time but greatly reduced the run-time; the latter was important for this program due to the extent to which it was used.

FUNCTION IALMOD(IP,IR,IS,JP,JR,JS)

If $JP.\lambda + JR.\theta + JS$ divides $IP.\lambda + IR.\theta + IS$, the answer returned is 0; the answer 1 is returned otherwise. The result is obtained by testing whether the denominator of the quotient of these two algebraic integers is 1.

SUBROUTINE INCON(JP,JR,JS,M,ICP,ICR,ICS,LIC)

$$NORN(JJ,J) = N(JJ.\theta + J)$$

The routine sets $ICP(I).\lambda + ICR(I).\theta + ICS(I)$ for $I = 1, . . , M$

to representatives of the non-zero residue classes modulo $JP.\lambda + JR.\theta + JS$ where $M = |N(JP.\lambda + JR.\theta + JS)| - 1$. Also $LIC(I)$ is set to 1 for $I = 1, \ldots, M$.

SUBROUTINE MODAL(KP,KR,KS,ICP,ICR,ICS,LIC,M,JP,JR,JS)

M is again $|N(JP.\lambda + JR.\theta + JS)| - 1$. The routine finds the values of I, where $1 \leq I \leq M$ such that $KP.\lambda + KR.\theta + KS$ or $-(KP.\lambda + KR.\theta + KS)$ is congruent to $ICP(I).\lambda + ICR(I).\theta + ICS(I)$ modulo $JP.\lambda + JR.\theta + JS$. For these values of I, LIC(I) is set to 0.

When IPRIME equals 0, $JP.\lambda + JR.\theta + JS$ does not have norm a rational prime and the representatives of the residue classes must be tested in turn until the relevant ones are found.

When IPRIME equals 1, $JP.\lambda + JR.\theta + JS$ is an algebraic prime and we have $\theta \equiv ITHETA$ and $\lambda \equiv ILAM$ hence

$$KP.\lambda + KR.\theta + KS \equiv KP.ILAM + KR.ITHETA + KS \equiv KPRS$$

and $$-(KP.\lambda + KR.\theta + KS) \equiv -KPRS.$$

When IPRIME equals 2, $KP.\lambda + KR.\theta + KS$ is equal to θ or to λ and we only wish to find the residue class to which $+\theta$ or $+\lambda$ belong.

SUBROUTINE TEST

Each integer of norm MF is considered, where MF is a factor of $N(\epsilon + 1)$ or of $N(\epsilon - 1)$. We have $IM.\lambda + JM.\theta + KM$ equal to $\epsilon + 1$ or to $\epsilon - 1$, as appropriate, and $JP.\lambda + JR.\theta + JS$ is the integer of norm MF currently being considered. $ICL = MF - 1$.

First, we test whether $JP.\lambda + JR.\theta + JS$ divides $IM.\lambda + JM.\theta + KM$; if so, we find the representatives of the set of non-zero residue classes modulo $JP.\lambda + JR.\theta + JS$, otherwise we turn to the next integer of norm MF. The set of representatives is $ICP(I).\lambda + ICR(I).\theta + ICS(I)$ for $I = 1, \ldots, ICL$. We note that if and only if $JP.\lambda + JR.\theta + JS$ has norm a rational prime, the set of representatives of its non-zero residue classes will be $1, \ldots, ICL$ hence $ICS(ICL) = ICL$. When $JP.\lambda + JR.\theta + JS$ has norm a rational prime, IPRIME is set to 2 and we find the values ILAM and ITHETA such that $ILAM \equiv \lambda\ (JP.\lambda + JR.\theta + JS)$ and $ITHETA \equiv \theta\ (JP.\lambda + JR.\theta + JS)$, IPRIME is then set to 1; the initial setting $ILAM = ITHETA = 0$ allows for the case when $JP.\lambda + JR.\theta + JS$ divides θ or λ. Those values LIC(I) which have been set to 0 in finding ILAM and ITHETA are reset to 1. In the case when the norm of $JP.\lambda + JR.\theta + JS$ does not have norm a rational prime IPRIME is set to 0.

We now test for the residue classes to which $+\epsilon$ and $-\epsilon$ belong, and then find which other residue classes contain integers of norm less than MF; finally JCOUNT is the number of residue classes which do not contain such an integer. If JCOUNT equals 0 we go on to the next integer of norm MF. When JCOUNT does not equal 0 the representatives of the residue classes which do not contain an integer of norm less than MF are printed together with the nature of $JP.\lambda + JR.\theta + JS$, and we set EUCLID to 1 to indicate that the field does not possess a Euclidean Algorithm.

Originally MP is the power to which MF is a factor of

$N(IM.\lambda + JM.\theta + KM)$, it is reduced by 1 each time that an integer of norm MF has been considered in the manner described above, which indicates that the integer is a factor of $IM.\lambda + JM.\theta + KM$; MP = 0 causes exit from the routine.

SUBROUTINE DIVC(L1,M1,N1,L2,M2,N2,L,M,N)

KDET(I1,I2,I3,J1,J2,J3,K1,K2,K3) is the single precision version of the double precision function FDET.

The routine yields the quotient

$$L.\lambda + M.\theta + N = (L1.\lambda + M1.\theta + N1)/(L2.\lambda + M2.\theta + N2)$$

and is used only when we know that the quotient is an algebraic integer. The routine also includes tests for the possibility of integer overflow.

SUBROUTINE MULTC(L1,M1,N1,L2,M2,N2,L,M,N)

The routine gives the product

$$L.\lambda + M.\theta + N = (L1.\lambda + M1.\theta + N1).(L2.\lambda + M2.\theta + N2)$$

and also checks for the possibility of integer overflow.

DOUBLE FUNCTION DNORM(IP,IR,IS)

The answer returned is

$$N(IP.\lambda + IR.\theta + IS)$$

and checks are made for the possibility of integer overflow.

THE MAIN PROGRAM

The program reads the details of the field to give defining polynomial $x^3 - IA.x^2 + IB.x - IC$, discriminant $-IDET$ and the index of the polynomial relative to the field is INDEX; the fundamental unit of the field is $\dfrac{I.\theta^2 + J.\theta + K}{L}$. The subroutine

BASE is called; then we use the routine CHANGE to give the rational integers I1, J1, K1 such that $\epsilon = I1.\lambda + J1.\theta + K1$. We now set the rational integers AA, BB, CC, DD, EE, FF such that the ideal (AA, BB.θ + CC, DD.λ + EE.θ + FF) is the unit ideal, then call PRIN(1) to find the reduced basis of this ideal.

EUCLID is set to 0 to indicate that the Euclidean property of the field is unknown, and ICHECK is set to -1 as we begin to consider congruences modulo integers which are factors of $\epsilon - 1$.

Eventually IP(I).λ + IR(I).θ + IS(I) for I = 1, . . . , MAPC − 1 will be the integers so far calculated which produce distinct ideals; thus MAPC points to the first "empty" element of the arrays IP, IR, IS and so is set to 1 here. We now set IM.λ + JM.θ + KM = $\epsilon - 1$ and MAX to be the greatest member of the set

$$\{ f : f = p \text{ or } f = p^3, \ p \text{ a rational prime}, \ f \text{ divides } |N(\epsilon - 1)| \text{ and } f < 500 \}.$$

On this cycle MLX will be set to 2 and we now turn to the determination of all distinct algebraic integers of norm of absolute value between 2 and MAX inclusive. These integers are determined according to the theory of chapter 3, and we have the integers of norm INORM as IP(I).λ + IR(I).θ + IS(I) for I between MAP(INORM,1) and MAP(INORM,2).

The method allows for a maximum of 2000 integers of norm of absolute value at most MAX. Reaching this limit, or an attempt to exceed it, would result in the printing of a diagnostic and the value of MAX being reduced so that the above condition is satisfied.

We now go on to consider the rational integers MF, where MF is either a rational prime or the cube of a rational prime, MF divides $N(\text{IM}.\lambda + \text{JM}.\theta + \text{KM})$, and MF is at most MAX. If, after a call on the subroutine TEST, EUCLID is equal to 1, we know that the field does not possess a Euclidean Algorithm and so proceed no further. When all rational integers MF have been considered we set $\text{IM}.\lambda + \text{JM}.\theta + \text{KM}$ to $\epsilon + 1$, and ICHECK to 1 to indicate that factors of $\epsilon + 1$ are being considered. We now repeat the above process noting that:

if MLX is first set to MAX, MAX is set to the greatest member of the set
$\{ f: f = p \text{ or } f = p^3, \ p \text{ a rational prime}, \ f \text{ divides } |N(\epsilon + 1)| \text{ and } f < 500 \}$,
we only need to calculate the integers of norm of absolute value between MLX and MAX on this second cycle.

We consider congruences modulo integers with norm the cube of a rational prime to ensure that all the rational prime factors of $\epsilon + 1$ and $\epsilon - 1$ are taken into account.

CHAPTER 9

THE PROGRAMS CUBOID, FCUB AND CUBX

These three programs, which are basically similar, are those used to put the method of chapter 4 into practice. CUBOID is that used for the first subdivision of the smallest cuboid which contains the fundamental region, then FCUB is used for subsequent subdivisions. CUBX is used to find the smallest cuboid which contains the uncovered sub-regions of a particular region, when the number of such sub-regions is large.

The function subroutine CI is the single precision version of the function subroutine DCI of chapter 7.

SUBROUTINE BASIS

This subroutine is basically the same as the subroutine BASEH of chapter 7, with the following exceptions. Only the values T and S where $\lambda = (\theta^2 + T.\theta + S)/INDEX$ are found and not the other coefficients in the expressions for θ^2, λ^2 and $\theta\lambda$. No bounds to be used for the prevention of integer overflow are found since they are not necessary for this program. Additionally, this routine adjusts the basis, given in the arrays R, U and H, to be that one which corresponds to the basis $(1, M'(\theta), Q'(\theta))$ for the field as described in 4.8. Details of the basis of the field and that of the lattice are printed only for the program CUBOID.

SUBROUTINE BOUND(R,AL,AU)

We note that a basis for a fundamental region of the lattice is

$$(0,0,0),\ (1,0,1) = (R(1),U(1),H(1)),\ (R(2),U(2),H(2)),$$
$$(R(3),U(3),H(3)) \qquad 9.1$$

where R, U, H are the COMMON arrays of the main program. Thus the vertices of this region are given by (ξ, η, ζ) where

$$\begin{aligned} \xi &= x.R(1) + y.R(2) + z.R(3) \\ \eta &= x.U(1) + y.U(2) + z.U(3) \\ \zeta &= x.H(1) + y.H(2) + z.H(3) \end{aligned} \qquad 9.2$$

and x, y, z each take the values 0, 1.

BOUND is used to find the maximum and minimum values of ξ, η or ζ when R is the main program array R, U or H respectively.

SUBROUTINE USE

This routine is used to determine the set $\mathcal{S}$ of integer points to be used in testing. $\mathcal{S}$ consists of the points corresponding to the integers of K given by PM(I) + PN(I).θ + PO(I).λ for I = 1, . . . , KZ. If KZ reaches the value 1000 no more integers are added to the set.

SUBROUTINE COVER(X,Y,Z,L,ICOUNT)

For each element of $\mathcal{S}$, this routine determines for which sub-regions of the region under consideration 4.2 is satisfied, that is we have these sub-regions covered. If at any stage we find that all sub-regions are covered, a return to the calling program is made immediately. ICOUNT is the number of sub-regions left uncovered after consideration of any element of $\mathcal{S}$. When an element of ξ is found such that we show that the sub-region with vertices

$$(X(I + t_i), Y(J + t_j), Z(K + t_k)) \quad \text{for } t_i = 0,1; \ t_j = 0,1; \ t_k = 0,1, \qquad 9.3$$

is covered, we set $L(I,J,K)$ to 0.

We note that for the program CUBOID we are considering the whole of the cuboid containing the fundamental region, and this cuboid is symmetrical about the origin; so we need only consider those regions containing points (ξ, η, ζ) which are in regions 9.3 where K takes values between 6 and 10.

THE MAIN PROGRAM CUBOID

The details of the field are first read; the field has discriminant -IDET, defining polynomial $x^3 - IA.x^2 + IB.x - IC$ and this polynomial has index relative to the field INDEX.

The subroutine BASIS is called to determine the basis of the field. We now use the subroutine BOUND to find the values XL, XU, YL, YU, ZL, ZU such that the smallest cuboid containing the fundamental region with vertices 9.2 is the set of points (ξ, η, ζ) such that

$$XL \leq \xi \leq XU$$
$$YL \leq \eta \leq YU$$
$$ZL \leq \zeta \leq ZU.$$

We then adjust these values so that the similar fundamental region which is symmetric about the origin is contained in the cuboid which is the set of points (ξ, η, ζ) such that

$$|\xi| \leq XU = -XL$$
$$|\eta| \leq YU = -YL$$
$$|\zeta| \leq ZU = -ZL.$$

BK is assigned the value C of chapter 4. CIN = .1 is the ratio of the side of a sub-region which we are attempting to cover to that of the original cuboid containing the fundamental region, that is the value 10^{-h} of chapter 4. AM was a value used when the program was employed to find the inhomogeneous minimum of a field; it was a measure of the amount by which the value of C was to be altered if the number of uncovered sub-regions was greater than the value LIMIT. Since we are only concerned here with the Euclidean property of the field, LIMIT was made so large that the value of C was not adjusted.

IBC is the greatest absolute value of the coefficients of the integer points, this bound was used to prevent the number of elements of $\mathcal{J}$ becoming too large. For the fields with the smaller values of IDET this value was fixed at 10 in the program, but it was found necessary to be able to make it smaller as the value of IDET increased. The subroutine USE is then called.

The sub-regions are to be those with vertices 9.3 for I = 1, . . . , 10; J = 1, . . . , 10; K = 1, . . . , 10; and by symmetry we need only consider the values K = 6, . . . , 10. For these values of I, J, K we set L(I,J,K) to 1 to indicate that the corresponding sub-region has not yet been "covered", in the sense of 6.6. Then we determine the values of the elements of the arrays X, Y and Z.

We now wish to set L(I,J,K) to 2 for those sub-regions which do not intersect with the fundamental region. We note that if (ξ, η, ζ) is a point of the cuboid,

$$\begin{aligned} \xi &= x.R(1) + y.R(2) + z.R(3) \\ \eta &= x.U(1) + y.U(2) + z.U(3) \qquad\qquad 9.4 \\ \zeta &= x.H(1) + y.H(2) + z.H(3) \end{aligned}$$

for some real numbers x, y, z. This point is also a point of the fundamental region only if

$$|x| \leq \frac{1}{2}, \quad |y| \leq \frac{1}{2}, \quad |z| \leq \frac{1}{2}.$$

Thus a sub-region intersects with the fundamental region only if at least one of its vertices satisfies these conditions.

It should be pointed out that the determinant of the coefficients in 9.4 is

$$\begin{vmatrix} 1 & Re\phi - k & Re\psi - p.Re\phi - q \\ 0 & Im\phi & Im\psi - p.Im\phi \\ 1 & \theta - k & \lambda - p.\theta - q \end{vmatrix}$$

$$= \begin{vmatrix} 1 & Re\phi & Re\psi \\ 0 & Im\phi & Im\psi \\ 1 & \theta & \lambda \end{vmatrix}$$

$$= \frac{1}{2i}\begin{vmatrix} 1 & \phi & \psi \\ 1 & \bar{\phi} & \bar{\psi} \\ 1 & \theta & \lambda \end{vmatrix}$$

which has absolute value $\frac{i\Delta}{2i} = \frac{\Delta}{2}$, where $\Delta = IDET^{\frac{1}{2}}$.

But, from the choice of $Im\phi$ as positive, we have

$$\begin{vmatrix} 1 & Re\phi & Re\psi \\ 0 & Im\phi & Im\psi \\ 1 & \theta & \lambda \end{vmatrix} = \frac{1}{INDEX}\begin{vmatrix} 1 & Re\phi & Re\phi^2 \\ 0 & Im\phi & Im\phi^2 \\ 1 & \theta & \theta^2 \end{vmatrix}$$

$$= \frac{(\mathrm{Im}\phi.\theta^2 + \mathrm{Re}\phi.\mathrm{Im}\phi^2 - \mathrm{Re}\phi^2.\mathrm{Im}\phi - \mathrm{Im}\phi^2.\theta)}{\mathrm{INDEX}}$$

$$= (\mathrm{Im}\phi.\theta^2 + \mathrm{Re}\phi.2.\mathrm{Re}\phi.\ \mathrm{Im}\phi - ((\mathrm{Re}\phi)^2 - (\mathrm{Im}\phi)^2).\mathrm{Im}\phi$$

$$- 2.\mathrm{Re}\phi.\mathrm{Im}\phi.\theta)/\mathrm{INDEX}$$

$$= \frac{\mathrm{Im}\phi}{\mathrm{INDEX}}(\theta^2 - 2.\mathrm{Re}\phi.\mathrm{Im}\phi + (\mathrm{Re}\phi)^2 + (\mathrm{Im}\phi)^2)$$

$$> 0$$

thus the value of the determinant is $\frac{1}{2}\,\mathrm{IDET}^{\frac{1}{2}}$. Consequently, the efficiency of this program could have been improved by using this expression.

We now call the subroutine COVER to find the number ICOUNT of sub-regions which are left uncovered, and print the value of ICOUNT. If ICOUNT is not equal to 0, and is less than LIMIT, the values of X(I), Y(J), Z(K) for those regions for which L(I,J,K) is equal to 1 are printed; these values are also punched onto cards for later use by FCUB.

THE MAIN PROGRAM FCUB

This program finds the smallest cuboid containing the fundamental region, then reads the values BK and IBC as in CUBOID. The value $\mathrm{CIN} = 10^{-h}$ must be read by this program, then the subroutine USE is called.

LIMIT is again the maximum number of uncovered regions for which the vertices are to be printed. M is the number of regions which are to be subdivided. Each of these regions is now treated as the cuboid containing the fundamental region was treated by CUBOID; with the exception that we must now consider the values $I = 1, \ldots, 10$; $J = 1, \ldots, 10$; $K = 1, \ldots, 10$.

THE MAIN PROGRAM CUBX

This program is basically the same as FCUB with the following exceptions. We do not read a value LIMIT. On return from the subroutine COVER we find the values XLW, XUP, YLW, YUP, ZLW, ZUP such that the uncovered sub-regions of the particular region in question are contained in the cuboid which consists of the set of points (ξ, η, ζ) where

$$XLW \leq \xi \leq XUP$$

$$YLW \leq \eta \leq YUP$$

$$ZLW \leq \zeta \leq ZUP.$$

CHAPTER 10

THE PROGRAM TRANS

From the programs of chapter 9 we find regions $R_1, \ldots, R_n$, we wish to determine the intersections of the transformations of these regions by the fundamental unit with the regions themselves; this program is used to achieve this. The subroutine BASIS and the function subroutine CI are the same as for the programs of chapter 9.

FUNCTION ADJ(R,U,I,J)

This determines the value of

$$R(I).U(J) - R(J).U(I) = \begin{vmatrix} R(I) & U(I) \\ R(J) & U(J) \end{vmatrix}$$

SUBROUTINE UPLW(RL,RU,TR)

On return from this subroutine

$$RL = \min(RL,TR)$$

$$RU = \max(RU,TR)$$

SUBROUTINE ROUNDI(RC,IR)

IR takes the value of RC rounded to the nearest integer.

FUNCTION DCORR(X,J)

When this function subroutine is called, X is a bound on the co-ordinates of one of the uncovered regions. J = 1 indicates that X is a lower bound and the answer returned is X - 0.1. J = 2 indicates that X is an upper bound and the answer returned is X + 0.1. In this way we avoid the possibility of rounding error concealing the intersection of an uncovered region with the transform of some uncovered region.

THE MAIN PROGRAM TRANS

We note that if the point (ξ, η, ζ) has cylindrical polar co-ordinates (ρ, α, ζ), and the point of the lattice corresponding to the fundamental unit has cylindrical polar co-ordinates $(\rho_\epsilon, \alpha_\epsilon, \zeta_\epsilon = \epsilon)$, the transform of the point by the fundamental unit has cylindrical polar co-ordinates

$$(\rho\rho_\epsilon, \alpha + \alpha_\epsilon, \zeta\zeta_\epsilon).$$

We will define R_{-J} to be the set of points $\tilde{\xi}$ where $-\tilde{\xi}$ is in R_J. $R_J + \tilde{\gamma}$ will be defined as the set of points $\tilde{\xi} + \tilde{\gamma}$ where $\tilde{\xi}$ is in R_J.

TRANS reads the values EXC, EYC, EZC where

$$\epsilon = \text{EXC.H}(1) + \text{EYC.H}(2) + \text{EZC.H}(3).$$

It should be noted that EXC, EYC, EZC are the coefficients of ϵ relative to the basis $(1, M'(\theta), Q'(\theta))$ and not $(1, \theta, \lambda)$. (EX,EY,EZ) are the cartesian co-ordinates of the point $\tilde{\epsilon}$ of the lattice of integers, and (ER,EALP,EZ) are its cylindrical polar co-ordinates.

N is the number of regions to be considered; these regions are R_I for I = 1, . . . , N where R_I is the set of points (ξ, η, ζ) such that

$$X(1,I) \leq \xi \leq X(2,I)$$

$$Y(1,I) \leq \eta \leq Y(2,I)$$

$$Z(1,I) \leq \zeta \leq Z(2,I)$$

for I = 1, . . . , N. When N is large, which usually means greater than 15, the amount of time taken to consider the intersection of the transform of each region with the appropriate translates of the original region becomes large; consequently, M1 and M2 are read such that the transforms of the regions R_I for I = M1, . . . , M2 are considered in this run.

We now consider each region in turn. For the vertex (X(II,I), Y(JJ,I), Z(KK,I)) we determine its cylindrical polar co-ordinates (RA,ALP,Z(KK,I)), and from these the cylindrical polar co-ordinates of its transform by the fundamental unit (TRA,TALP,TZ); we note that RA and ALP, and consequently TRA and TALP, are independent of Z(KK,I) and so may be determined in an outer loop. This vertex is then the point $\tilde{\zeta}$ where ζ = TXC.H(1) + TYC.H(2) + TZC.H(3). After inspecting the eight vertices, the transformed region is the set of points (ξ, η, ζ) where

$$\text{XL} \leq \xi \leq \text{XU}$$
$$\text{YL} \leq \eta \leq \text{YU}$$
$$\text{ZL} \leq \zeta \leq \text{ZU};$$

and if ζ = x.H(1) + y.H(2) + z.H(3)

$$\text{XLC} \leq x \leq \text{XUC}$$
$$\text{YLC} \leq y \leq \text{YUC}$$
$$\text{ZLC} \leq z \leq \text{ZUC}.$$

Since the fundamental region consists of the points $\tilde{\zeta}$ where ζ = x.H(1) + y.H(2) + z.H(3) and $|x| \leq \frac{1}{2}$, $|y| \leq \frac{1}{2}$, $|z| \leq \frac{1}{2}$, if XLC, XUC, YLC, YUC, ZLC, ZUC, when rounded to the nearest integer, become IXL, IXU, IYL, IYU, IZL, IZU respectively, we must consider for each integer point $\tilde{\gamma}$, where $\gamma = x.H(1) + y.H(2) + z.H(3)$, x is between IXL and IXU, y is between IYL and IYU, z is between IZL and IZU, whether $R_J + \tilde{\gamma}$ or $R_{-J} + \tilde{\gamma}$ intersects with $E(R_I)$ for J between 1 and N. IFLAG is set to 1 when at least one such region R_J is found.

CHAPTER 11

THE PROGRAM EXCEP

The method of chapter 5 is implemented by this program. The subroutine BASES is basically the same as the subroutine BASEH of RELMIN, but the bounds which it finds for the prevention of integer overflow are for the arguments of DNORM and MULTD. The subroutine MULTD is the double precision version of the subroutine MULTC of the program CONG. The function subroutine DCI is the same routine as that for the program RELMIN. The function subroutine DAJ is the double precision version of the function ADJ of the program TRANS. The subroutine CHANGE and the function subroutine DNORM are the same as those for the program CONG.

LOWUP(XT,XV,XW,XL,XU)

The routine finds XL and XU such that

$$XL \leq XT.Y(1) + XV.Y(2) + XW.Y(3)$$

where $$YL(I) \leq Y(I) \leq YU(I) \quad \text{for } I = 1,2,3$$

and the arrays YL and YU are passed across to the subroutine as COMMON arrays.

LIMITL(XXL,IXL)

IXL is the least integer greater than XXL. A diagnostic is given if the resultant integer would require more than 14 digits; that is if the integer would come close to the limits of accuracy of the machine.

LIMITU(XXU,IXU)

IXU is the greatest integer less than XXU. A diagnostic is again given if the resultant integer would require more than 14 digits.

THE MAIN PROGRAM EXCEP

The field being considered has discriminant -IDET, defining polynomial x^3 - IA.x^2 + IB.x - IC and the index of the polynomial relative to the field is INDEX. BASES is called to find the details of the basis of the field and of the lattice of integers. If we are finding the minimum of $\frac{\alpha}{1-\epsilon^n}$, then $\alpha = \frac{\text{IZ.}\theta^2 + \text{IY.}\theta + \text{IX}}{\text{ID}}$ and $1 - \epsilon^n = \frac{\text{JZ.}\theta^2 + \text{JY.}\theta + \text{JX}}{\text{JD}}$ and H(2) = θ. We then have

$$\text{AX} + \text{AY.}\theta + \text{AZ.}\lambda = \text{I1X} + \text{I1Y.}\theta + \text{I1Z.}\lambda = \frac{\text{IZ.}\theta^2 + \text{IY.}\theta + \text{IX}}{\text{ID}}$$

$$\text{BX} + \text{BY.}\theta + \text{BZ.}\lambda = \text{J1X} + \text{J1Y.}\theta + \text{J1Z.}\lambda = \frac{\text{JZ.}\theta^2 + \text{JY.}\theta + \text{JX}}{\text{JD}}$$

and we obtain AN = α, BE = $1 - \epsilon^n$.

The transformation on the lattice is $Q \rightarrow \frac{Q - \alpha}{\epsilon^n} = \frac{Q - \text{AN}}{1 - \text{BE}}$, so we determine the values BP = 1 - BE and ABP = -AN/(1 - BE). CK = SK is the value of C_1 of chapter 5; CK is a double precision quantity, SK is single precision.

The conjugates of α are ANV $\pm$ i.ANW and those of $1-\epsilon^n$ are BEV $\pm$ i.BEW, then the conjugates of $\frac{\alpha}{1-\epsilon^n}$ are ABV $\pm$ i.ABW. BNORM is the norm of $1 - \epsilon^n$.

TL1 = SL1 is the value τ_1 of chapter 5; then TU1 = $\frac{\text{TL1} - \alpha}{\epsilon^n}$. We are to investigate the range of values of ζ_γ of chapter 5 in sections given by

$$\text{TL} \leq \zeta_\gamma < \text{TU} \qquad \text{such that TU} - \text{TL} \leq 100.$$

With this in mind we set TL = TL1 and TU = min(TU1, TL + 100).

RMINIM is to eventually take the value of the minimum of $\frac{\alpha}{1-\epsilon^n}$; it is initially set to the value SK, which should be chosen by the user so that it will be greater than the minimum. NEXT is set to 1 when we are considering values of ζ_γ greater than $\frac{\alpha}{1-\epsilon^n}$, and to 2 when we are considering values of ζ_γ less than $\frac{\alpha}{1-\epsilon^n}$.

SB is the value σ_1 of chapter 5. We must consider the integers $\tilde{\gamma} = (\xi_\gamma, \eta_\gamma, \zeta_\gamma)$ such that

$$\mathrm{VL} \leq \xi_\gamma \leq \mathrm{VU}$$

$$\mathrm{WL} \leq \eta_\gamma \leq \mathrm{WU}$$

$$\mathrm{TL} \leq \zeta_\gamma \leq \mathrm{TU}.$$

If
$$\zeta_\gamma = p.\lambda + q.\theta + r$$
for some rational integers p, q and r, we investigate the values of p and q where

$$\mathrm{IPL} \leq p \leq \mathrm{IPU}$$

$$\mathrm{IQL} \leq q \leq \mathrm{IQU},$$

the range of values for r will be found for any particular pair of values of p and q. If the range of integer values for p or that for q is null, a diagnostic is printed and the program terminates. We determine which of p and q has the smaller range of values. If p has the smaller range, for each value of p we determine the integer values IQLT, IQUT such that we must consider the reduced range of values of q given by

$$\mathrm{IQLT} \leq q \leq \mathrm{IQUT}.$$

Then for each value of q in this range, we determine the integer values ISLT, ISUT such that we must consider the values of r in the range

$$\mathrm{ISLT} \leq r \leq \mathrm{ISUT}.$$

For each value of r we then determine the value of $N\left(\frac{\alpha}{1 - \epsilon^n} - \gamma\right)$ in the form $N(\alpha - \gamma(1 - \epsilon^n))/N(1 - \epsilon^n)$. When q has the smaller range, for each value of q we determine the range for p, then for each value of p we determine the range for r.

Having considered the range of values of ξ_γ given by $\mathrm{TL} \leq \xi_\gamma \leq \mathrm{TU}$, if TU is less than TU1, TL is set to the value TU and TU to min(TU1, TU + 100) then the above process is repeated; when TU = TU1 we go on to consider values of ξ_γ less than $\frac{\alpha}{1 - \epsilon^n}$. First NEXT is set to NEXT + 1 = 2, TU1 = SU1 is the value of τ_u of chapter 5, then $\mathrm{TL1} = \frac{\mathrm{TU1} - \alpha}{\epsilon^n}$. Again we are to consider values of ξ_γ in "sections", therefore, we set TU = TU1 and TL = max(TU - 100, TL1). SB is now the value ϵ_2 of chapter 5. The relevant integers are investigated in the manner described above; then, if TL > TL1, we set TU = TL and then TL = max(TU - 100, TL1), otherwise we print the value of RMINIM and stop.

CHAPTER 12

THE RESULTS OBTAINED

The following table includes all the results obtained by the methods of this thesis. For each field we give the discriminant, D, the coefficients a, b, c of the defining polynomial $x^3 - ax^2 + bx - c$, and the index, L, of the polynomial relative to the field, as given in the table in (1).

The "property" of the field is indicated by E if the field possesses a Euclidean Algorithm and by N if it does not. The last column has an entry when further information about the field is included at the end of this chapter, the entry is a reference to that information.

The results for the first fifteen fields, those with discriminants between -23 and -152 inclusive, were obtained by Godwin (18); these fields were not investigated by the methods of this thesis, but the results are included here for the sake of completeness.

D	L	a, b, c			Property	
-23	1	4	5	1	E	(1)
-31	1	3	4	1	E	(1)
-44	1	4	6	2	E	(1)
-59	1	3	5	2	E	(1)
-76	1	2	4	2	E	(1)
-83	1	5	9	4	E	(1)
-87	1	4	7	3	E	(1)
-104	1	6	11	4	E	(1)
-107	1	2	4	1	E	(1)
-108	1	6	12	6	E	(1)
-116	1	5	8	2	E	(1)
-135	1	3	6	3	E	(1)
-139	1	4	6	1	E	(1)
-140	1	3	5	1	E	(1)
-152	1	8	19	10	E	(1)
-172	1	7	15	7	E	(2)
-175	1	5	10	5	E	(3)
-199	1	2	5	3	N	(4)
-200	1	4	7	2	E	
-204	1	5	9	3	E	
-211	1	6	10	1	E	
-212	1	2	5	2	E	
-216	1	3	6	2	E	
-231	1	7	16	9	E	

D	L	a, b, c			Property	
−239	1	6	11	3	E	
−243	1	6	12	5	E	
−244	1	10	29	18	E	
−247	1	6	13	7	E	
−255	1	5	8	1	E	
−268	1	7	13	1	E	
−300	1	8	18	6	E	
−307	1	4	8	3	N	
−324	1	9	24	14	E	
−327	1	8	19	9	N	(5)
−335	1	4	9	5	N	
−339	1	7	15	6	N	
−351	1	3	6	1	N	
−356	2	5	12	4	E	
−364	1	3	7	3	N	
−367	1	4	7	1	N	
−379	1	5	9	2	E	
−411	1	2	6	3	E	
−419	1	9	23	10	E	
−424	2	7	16	4	E	
−431	2	9	26	16	E	
−436	1	6	13	6	N	(6)
−439	1	7	14	3	N	
−440	2	6	14	4	E	

D	L	a, b, c			Property	
−451	1	10	28	13	E	
−459	1	9	21	2	N	
−460	1	2	6	2	E	
−472	1	9	22	6	E	
−484	1	4	9	4	E	
−492	1	4	8	2	E	
−499	1	3	7	2	E	
−503	2	7	18	8	E	
−515	1	8	20	11	E	
−516	2	8	22	12	E	
−519	1	10	29	17	E	(7)
−524	1	5	11	5	N	
−527	1	3	8	5	N	
−543	1	5	10	3	E	(8)
−547	1	8	18	5	N	
−567	1	9	24	13	N	
−620	1	11	35	23	N	
−628	2	7	20	12	E	
−652	2	4	12	4	E	
−655	1	7	16	7	N	
−671	1	6	11	1	N	
−675	1	6	12	3	N	
−679	1	6	13	5	N	
−687	1	4	9	3	E	(9)

D	L	a, b, c			Property
-695	1	8	21	13	N
-755	1	4	10	5	N
-759	1	2	7	3	N
-808	1	5	10	2	N
-812	1	11	33	13	N
-823	1	9	22	5	N
-839	1	8	19	7	N
-863	1	7	18	11	N
-883	2	8	23	12	N
-908	2	9	23	3	N
-940	1	9	25	15	N
-959	1	4	11	7	N
-972	1	6	12	2	N
-983	1	2	7	1	N
-1004	1	6	14	6	N
-1007	1	7	14	1	N
-1011	1	11	35	22	N
-1036	2	6	16	4	N
-1048	2	5	16	8	N
-1059	1	7	17	8	N
-1075	2	7	18	4	N
-1087	1	5	12	5	N
-1135	1	10	27	7	N
-1147	1	10	30	19	N

D	L	a, b, c			Property
−1164	1	7	15	3	N
−1172	2	7	21	11	N
−1175	1	3	8	1	N
−1187	1	2	8	5	N
−1191	1	14	55	39	N
−1196	1	5	13	7	N
−1207	1	11	34	17	N
−1208	2	4	13	2	N
−1219	1	12	40	21	N
−1231	1	10	29	15	N
−1235	1	10	28	11	N
−1259	1	13	47	28	N
−1267	1	2	8	3	N
−1291	1	9	25	14	N
−1292	1	12	38	10	N
−1295	1	7	16	5	N
−1315	1	13	45	16	N
−1316	2	4	14	4	N
−1319	1	9	26	17	N
−1327	1	6	13	3	N
−1351	1	8	21	11	N
−1355	1	6	14	5	N
−1363	1	11	31	2	N
−1383	1	4	11	5	N

D	L	a, b, c			Property
-1388	1	2	8	2	N
-1407	1	11	32	7	N
-1431	1	6	15	7	N
-1448	2	6	17	4	N
-1452	1	10	26	2	N
-1547	1	7	15	2	N
-1567	1	8	19	5	N
-1579	1	6	16	9	N
-1580	1	4	10	2	N
-1583	1	11	36	25	N
-1599	3	7	24	9	N
-1603	2	12	43	28	N
-1615	1	3	10	5	N
-1619	1	8	22	13	N
-1647	1	12	39	15	N
-1675	1	4	12	7	N
-1687	1	9	22	3	N
-1700	2	2	13	4	N
-1708	1	10	28	10	N
-1736	2	9	29	17	N
-1743	1	13	48	33	N
-1751	3	11	36	9	N
-1755	2	9	30	20	N
-1763	1	14	52	19	N

D	L	a, b, c			Property
-1772	1	7	19	11	N
-1807	1	2	9	5	N
-1815	1	5	12	3	N
-1868	2	7	23	13	N
-1871	1	2	9	7	N
-1895	1	12	41	25	N
-1955	1	11	35	20	N
-1959	1	2	9	3	N
-1967	3	8	27	9	N
-2023	1	4	11	3	N
-2036	2	2	14	8	N
-2039	1	7	20	13	N
-2047	1	3	10	3	N
-2063	3	10	31	3	N
-2159	1	10	29	13	N
-2167	1	13	44	9	N
-2199	3	9	30	9	N
-2207	1	10	27	5	N
-2228	1	6	17	10	N
-2235	1	10	28	9	N
-2283	3	9	33	18	N
-2315	1	5	13	4	N
-2316	1	7	17	5	N
-2372	1	4	13	8	N

D	L	a, b, c			Property
−2403	1	12	42	29	N
−2420	2	8	25	10	N
−2423	3	11	42	27	N
−2444	1	9	23	5	N
−2479	1	12	37	3	N
−2491	2	10	31	10	N
−2503	1	7	18	7	N
−2515	1	12	40	19	N
−2540	2	11	39	25	N
−2579	1	11	33	10	N
−2591	3	10	39	27	N
−2599	1	11	36	23	N
−2604	1	2	10	6	N
−2627	1	2	10	7	N
−2636	2	12	44	28	N
−2647	1	4	13	7	N
−2668	1	9	25	11	N
−2699	2	9	26	4	N
−2708	2	9	29	13	N
−2723	1	3	11	4	N
−2732	1	6	14	2	N
−2759	1	5	12	1	N
−2791	1	10	31	19	N
−2795	2	5	18	4	N

D	L	a, b, c			Property
−2796	1	5	13	3	N
−2803	1	5	15	8	N
−2855	1	14	55	37	N
−2860	2	10	32	12	N
−2879	1	4	11	1	N
−2895	3	9	30	5	N
−2915	1	8	20	5	N
−2951	1	5	14	5	N
−2956	1	6	16	6	N
−3011	1	9	23	4	N
−3039	1	7	20	11	N
−3043	2	6	19	2	N
−3055	1	15	58	11	N
−3059	2	6	23	14	N
−3107	1	13	43	2	N
−3127	1	16	69	37	N
−3148	2	16	72	52	N
−3159	1	3	12	7	N
−3159	1	12	39	13	N
−3176	2	3	17	7	N
−3179	1	13	45	14	N
−3191	1	12	41	23	N
−3212	2	6	20	4	N
−3235	1	9	25	10	N

D	L		a, b, c		Property
−3244	1	12	40	18	N
−3259	1	4	14	9	N
−3263	1	9	26	13	N
−3308	2	8	24	4	N
−3311	1	8	21	7	N
−3331	1	5	13	2	N
−3359	1	4	13	5	N
−3371	1	3	11	2	N
−3404	2	2	16	4	N
−3439	1	14	51	11	N
−3451	1	10	28	7	N
−3483	2	3	18	12	N
−3495	1	10	27	3	N
−3543	3	10	37	15	N
−3547	3	8	28	3	N
−3560	2	13	45	5	N
−3575	3	7	28	9	N
−3591	1	3	12	5	N
−3599	1	11	34	13	N
−3615	1	2	11	7	N
−3619	1	10	32	21	N
−3647	1	7	18	5	N
−3671	1	8	19	1	N
−3687	3	6	27	11	N

D	L	a, b, c			Property
−3695	1	2	11	5	N
−3711	1	5	16	9	N
−3756	2	5	19	3	N
−3767	1	6	17	7	N
−3783	3	5	26	13	N
−3820	2	4	20	12	N
−3831	1	11	36	21	N
−3915	2	9	30	12	N
−3916	1	7	19	7	N
−3935	3	4	25	15	N
−3943	1	13	46	19	N
−3980	2	11	35	5	N
−3991	1	2	11	3	N
−3999	3	9	36	19	N
−4007	1	10	31	17	N
−4012	1	8	24	14	N
−4023	3	6	27	9	N
−4039	1	5	14	3	N
−4075	1	14	52	17	N
−4076	2	7	27	17	N
−4111	1	16	71	51	N
−4147	1	8	20	3	N
−4175	1	8	23	11	N
−4191	3	3	24	17	N

D	L	a, b, c			Property
−4239	1	3	12	3	N
−4255	1	7	20	9	N
−4291	2	14	51	2	N
−4295	3	11	44	25	N
−4307	1	9	23	2	N
−4359	1	17	80	61	N
−4364	1	5	17	11	N
−4411	2	4	19	4	N
−4455	1	9	24	5	N
−4487	1	14	53	23	N
−4511	1	10	33	23	N
−4555	2	7	26	12	N
−4556	2	10	36	20	N
−4559	1	9	26	11	N
−4567	1	9	28	17	N
−4575	3	2	23	19	N
−4639	1	6	19	11	N
−4691	1	8	24	13	N
−4699	1	14	54	29	N
−4715	2	15	62	28	N
−4727	1	5	16	7	N
−4735	1	14	55	35	N
−4771	2	8	27	8	N
−4823	1	13	48	29	N

D	L	a, b, c			Property	
-4831	1	17	76	29	N	
-4844	1	8	20	2	N	
-4859	1	2	12	7	N	
-4903	3	10	41	23	N	
-4908	1	2	12	6	N	
-4935	3	7	30	9	N	
-4963	1	18	88	59	N	
-10011	3	10	42	9	N	
-10019	2	16	75	56	N	
-10028	2	17	75	7	N	
-19899	3	18	96	61	N	
-19927	2	6	31	2	N	
-19939	1	9	31	12	N	
-19976	2	22	129	68	N	
-160087	1	0	1	77	N	(10)
-169571	1	1	35	22	N	(10)

We now have the additional information concerning the indicated fields.

(1) These results are those obtained by Godwin (18).

(2) The inhomogeneous minimum is $\frac{3}{4}$ and is attained at numbers congruent to $\pm\left(\frac{6\theta^2 - 25\theta + 14}{1 - \epsilon} \right)$.

(3) The inhomogeneous minimum is $\frac{3}{5}$ and is attained at numbers congruent to $\pm\left(\frac{3\theta^2 - 6\theta + 3}{1 - \epsilon} \right)$.

(4) The inhomogeneous minimum is 1 and is attained at numbers congruent to $\pm\left(\frac{3\theta}{1 - \epsilon^2} \right)$.

(5) The inhomogeneous minimum is $\frac{101}{99}$ and is attained at numbers congruent to $\pm\left(\frac{4\theta^2 - 4\theta + 1}{1 - \epsilon^2} \right)$ and transforms of them by the fundamental unit.

(6) The inhomogeneous minimum is $\frac{79}{78}$ and is attained at numbers congruent to $\pm\left(\frac{29\theta^2 - 33\theta + 10}{1 - \epsilon^2} \right)$.

(7) Numbers congruent to $\pm\left(\frac{19\theta^2 - 213\theta - 155}{1 - \epsilon^4} \right)$, and transforms of them by the fundamental unit, have minimum $\frac{44712}{45747}$, thus the inhomogeneous minimum of the field is at least this value but is less than 1.

(8) Numbers congruent to $\pm\left(\frac{-5\theta^2 + 68\theta - 23}{1 - \epsilon^3} \right)$, and transforms of them by the fundamental unit, have minimum $\frac{7593}{8343}$, thus the inhomogeneous minimum of the field is at least this value but is less than 1.

(9) Numbers congruent to $\pm\left(\frac{9\theta^2 - 27\theta + 8}{1 - \epsilon^2} \right)$, and transforms of them by the fundamental unit, have minimum $\frac{937}{945}$, thus the

inhomogeneous minimum of the field is at least this value but is less than 1.

(10) These results were obtained by the method of chapter 2.

REFERENCES

1. ANGELL, I.O., 'The tabulation of complex cubic fields with units and class numbers', Ph.D. Thesis, London 1971.

2. BARNES, E.S. and SWINNERTON-DYER, H.P.F., 'The Inhomogeneous Minima of Binary Quadratic Forms' (1), Acta Mathematica 87 (1952), 259-323.

3. BERG, E., 'Über die Existenz eines Euklidischen Algorithmus in quadratischen Zahlkörpen', Kungl. Fysiogr Sällskapeti Lund Förhandlingar 5 (1935), 1-6.

4. BEHRBOHM, H. and REDEI, L., 'Der Euklidische Algorithmus in quadratischen Körpen', J. fur Math. 174 (1936), 192-205.

5. CASSELS, J.W.S., 'The Inhomogeneous Minimum of Binary Quadratic, Ternary Cubic and Quarternary Quartic Forms' and Addendum, Proc. Cambridge Phil. Soc. 48 (1952), 72-86 and 519-520.

6. CHATLAND, H. and DAVENPORT, H., 'Euclid's Algorithm in Real Quadratic Fields', Canadian J. Math. 2 (1950), 289-296.

7. CHATLAND, H., 'On the Euclidean Algorithm in Quadratic Number Fields', Bull. Amer. Math. Soc. 55 (1949), 948-953.

8. DAVENPORT, H., 'Indefinite Binary Quadratic Forms, and Euclid's Algorithm in Real Quadratic Fields', Proc. London Math. Soc. (2) 53 (1951), 65-82.

9. DAVENPORT, H., 'Indefinite Binary Quadratic Forms', Quart. J. Math. (Oxford) (2) 1 (1950), 54-62.

10. DAVENPORT, H., 'On the Product of Three Non-Homogeneous Linear Forms', Proc. Cambridge Phil. Soc. 43 (1947), 137-152.

11. DAVENPORT, H., 'Euclid's Algorithm in Cubic Fields of Negative Discriminant', Acta Mathematica 84 (1950), 159-179.

12. DAVENPORT, H., 'Euclid's Algorithm in certain Quartic Fields', Transactions Amer. Math. Soc. 68 (1950), 508-532.

13. DELONE, B.N. and FADEEV, D.K., 'Theory of Irrationalities of the Third Degree', Translations Amer. Math. Soc. Vol. 10.

14. ENNOLA, V., 'On the Inhomogeneous Minimum of Indefinite Binary Quadratic Forms and Euclid's Algorithm in Real Quadratic Fields', Ann. Univ. Turku Ser. AI 28 (1958), 9-26.

15. ERDÖS, P. and KO, C., 'Note on the Euclidean Algorithm', J. London Math. Soc. 13 (1938), 3-8.

16. GODWIN, H.J., 'On the Inhomogeneous Minima of Totally Real Cubic Norm-Forms', J. London Math. Soc. 40 (1965), 623-627.

17. GODWIN, H.J., 'On Euclid's Algorithm in some Quartic and Quintic Fields', J. London Math. Soc. 40 (1965), 699-704.

18. GODWIN, H.J., 'On Euclid's Algorithm in some Cubic Fields with Signature One', Quart. J. Math. (Oxford) (2) 18 (1967), 333-338.

19. GODWIN, H.J., 'On the Product of Five Homogeneous Linear Forms', J. London Math. Soc. 25 (1950), 331-339.

20. GODWIN, H.J., 'On the Inhomogeneous Minima of certain Norm-Forms', J. London Math. Soc. 30 (1955), 114-119.

21. GODWIN, H.J., unpublished.

22. HARDY, G.H. and WRIGHT, E.M., 'Introduction to the Theory of Numbers', Clarendon Press, Oxford, 4th ed. (1960).

23. HEILBRONN, H., 'On Euclid's Algorithm in Cubic Self-Conjugate Fields', Proc. Cambridge Phil. Soc. 46 (1950), 377-382.

24. HEILBRONN, H., 'On Euclid's Algorithm in Real Quadratic Fields', Proc. Cambridge Phil. Soc. 34 (1938), 521-526.

25. INKERI, K., 'Uber den Euklidischen Algorithmus in quadratischen Zahlkorpen', Annales Academiae Scientarum Fennicae 41 (1947), 5-34.

26. SAMET, P.A., 'The Product of Non-Homogeneous Linear Forms I', Proc. Cambridge Phil. Soc. 50 (1954), 372-379.

27. SAMET, P.A., 'The Product of Non-Homogeneous Linear Forms II', Proc. Cambridge Phil. Soc. 50 (1954), 380-390.

28. SMITH, J.R., 'On Euclid's Algorithm in some Cyclic Cubic Fields', J. London Math. Soc. 44 (1969), 577-582.

29. SWINNERTON-DYER, H.P.F., 'The Inhomogeneous Minima of Complex Cubic Norm Forms', Proc. Cambridge Phil. Soc. 50 (1954), 209-219.

EUCLID'S ALGORITHM IN CUBIC FIELDS

WITH COMPLEX CONJUGATES

APPENDIX

ELIZABETH MARY TAYLOR

ROYAL HOLLOWAY COLLEGE, LONDON

Supervisor : PROFESSOR H J GODWIN

CONTENTS

The listings of the programs

and their subroutines. Each program listing is preceded by a title page which gives

1. the program name
2. the names of those subroutines which it uses and which are listed in the same section
3. the names of those subroutines which it uses and which have been listed in a previous section.

Listings of those routines copied from Angell(1), or which are modifications of subroutines of Angell are included for completeness.

THE PROGRAM RELMIN

SUBROUTINES - ALL LISTED IN THIS SECTION

```
      PROGRAM RELMIN(INPUT,OUTPUT)
C
C...THIS PROGRAM FINDS A LOWER BOUND FOR THE INHOMOGENEOUS MINIMUM OF
C...THE FIELD.
C
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
C...READ IN DETAILS OF THE FIELD. A BLANK CARD WHICH SETS IDET TO ZERO,
C...INDICATES THE END OF THE DATA DECK.
    2 READ 101,IDET,INDEX,IA,IB,IC
  101 FORMAT(I6,I2,3I5)
      IF(IDET.EQ.0) STOP
C...THE FIELD NOW BEING CONSIDERED HAS DISCRIMINANT -IDET, IT IS K(X)
C...WHERE X**3-IA*X**2+IB*X-IC=0.
      IDETM=-IDET
      PRINT 102, IDETM,INDEX,IA,IB,IC
  102 FORMAT(1H1,1X,26HTHE FIELD HAS DISCRIMINANT,I8,6H INDEX,I3,28H AND
     1 POLYNOMIAL COEFFICIENTS,3I6)
C...NOW FIND X WHERE THE FIELD IS K(X) AND ALSO A BASIS FOR THE FIELD.
      CALL BASEH
      PRINT 103
  103 FORMAT(/,1X,45HTHE FIELD IS K(X) AND HAS BASIS (Y,X,1) WHERE)
      ASSIG1=4HX**2 £ ASSIG2=4HY**2 £ ASSIG3=4HX*Y
      PRINT 104,ASSIG1,IT1,IT2,IT3
      PRINT 104,ASSIG2,IL1,IL2,IL3
      PRINT 104,ASSIG3,IP1,IP2,IP3
  104 FORMAT(12X,A4,2H =,I10,3HY +,I10,3HX +,I10)
C...NOW FIND THE LOOP OF IDEALS STARTING WITH 1 AND A CHAIN OF RELATIVE
C...MINIMA FOR THIS FIELD.
      CALL MINIMA
C...REPEAT THE CYCLE
      GO TO 2
      END
```

```
      SUBROUTINE BASEH
      DOUBLE R,U,H,A,B,C,V1,V2,V3,V4,V5,V6,V7,D,T,S,XIN
      DOUBLE IOBD,IOBDD
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D3/R(3),U(3),H(3)
      COMMON/D10/PH,ZZ,HHH/D9/IQ,INN,Q,RN
      COMMON/D16/IOBD,IOBDD
C
C...WHEN CONSIDERING THE FIELD K(X) SUPPOSE PH=3*X-IA THEN PH
C...SATISFIES AN EQUATION PH**3-IQ*PH-INN=0. FIND PH AND PH*PH-IQ
C...FOR USE IN THE SUBROUTINE MINIMA.
C
      A=FLOAT(IA) £ B=FLOAT(IB) £ C=FLOAT(IC)
      IQ=3*IA*IA-9*IB
      INN=27*IC-9*IA*IB+2*IA*IA*IA
      Q=FLOAT(IQ)
      RN=FLOAT(INN)
      V1=FLOAT(IQ/3)
      V2=FLOAT(INN)
      V3=DSQRT(V2**2-4.0D0*V1**3)
      V4=(V2+V3)/2.0D0
      V5=(V2-V3)/2.0D0
      IF(V4.NE.0.0D0) GO TO 51
      V6=0.0D0 £ GO TO 52
   51 D=1.0D0
      IF(V4.GE.0.0D0) GO TO 53
      V4=-V4 £ D=-1.0D0
   53 V6=DEXP((DLOG(V4))/3.0D0)*D
   52 IF(V5.NE.0.0D0) GO TO 54
      V7=0.0D0 £ GO TO 55
   54 D=1.0D0
      IF(V5.GE.0.0D0) GO TO 56
      V5=-V5 £ D=-1.0D0
   56 V7=DEXP((DLOG(V5))/3.0D0)*D
   55 PH=SNGL(V6+V7) £ HHH=PH*PH
      ZZ=HHH-Q
      H(2)=(V6+V7+A)/3.0D0
      R(2)=(A-H(2))/2.0D0
      U(2)=DSQRT(C/H(2)-R(2)*R(2))
      H(1)=1.0D0 £ R(1)=1.0D0 £ U(1)=0.0D0
C...R(N)+I.U(N) AND R(N)-I.U(N) ARE THE CONJUGATES OF H(N) FOR N=1,2,3.
C
C...(H(1),H(2),H(3))=(1,X,Y) IS A BASIS FOR THE FIELD.
C...Y=(X**2+IT*X+IS)/INDEX. IT AND IS ARE NOW CALCULATED.
C
      IN=INDEX
      IN2=IN**2 £ IN3=IN2*IN
      IF(INDEX.NE.1) GO TO 1
      IT=0 £ IS=0 £ GO TO 2
```

```
    1 K1=IA**2-2*IB £ K4=IB**2-2*IA*IC £ K5=IA*IB-3*IC
      DO 3 ITC=1,IN
      IT=ITC-1
      DO 4 ISC=1,IN
      IS=ISC-1
      JA=K1+IT*IA+3*IS
      IF(MOD(JA,IN).NE.0) GO TO 4
      JB=K4+IT**2*IB+3*IS**2+IT*K5+2*IS*K1+2*IS*IT*IA
      IF(MOD(JB,IN2).NE.0) GO TO 4
      JC=IS**3+IT**3*IC+IC**2+IS**2*IT*IA+IS*K4+IS*IT**2*IB+IT*IB*IC
     1+IT**2*IA*IC+IS**2*K1+IS*IT*K5
      IF(MOD(JC,IN3).NE.0) GO TO 4
      GO TO 2
    4 CONTINUE
    3 CONTINUE
    2 IT1=INDEX
      IT2=-IT
      IT3=-IS
      ML=2*IA*IT+IA*IA+2*IS+IT*IT-IB
      IL1=ML/IN
      IL2=(-IT*ML+2*IS*IT+IC-2*IB*IT-IA*IB)/IN2
      IL3=(-IS*ML+2*IC*IT+IA*IC+IS*IS)/IN2
      MP=IA+IT
      IP1=MP
      IP2=(IS-IB-IT*MP)/IN
      IP3=(IC-IS*MP)/IN
      T=FLOAT(IT) £ S=FLOAT(IS) £ XIN=FLOAT(INDEX)
      H(3)=(H(2)*H(2)+T*H(2)+S)/XIN
      R(3)=(R(2)*R(2)-U(2)*U(2)+T*R(2)+S)/XIN
      U(3)=(2.0D0*R(2)*U(2)+T*U(2))/XIN
C
C...NOW FIND A BOUND ON THE RELEVANT PRODUCTS OF ARGUMENTS OF MULTCD AND
C...DIVCD FOR TESTING FOR THE POSSIBILITY OF OVERFLOW.
C
      IL1A=IABS(IL1) £ IL2A=IABS(IL2) £ IL3A=IABS(IL3)
      IT1A=IABS(IT1) £ IT2A=IABS(IT2) £ IT3A=IABS(IT3)
      IP1A=IABS(IP1) £ IP2A=IABS(IP2) £ IP3A=IABS(IP3)
      IOBL=MAX0(IL1A,IL2A,IL3A)
      IOBT=MAX0(IT1A,IT2A,IT3A)
      IOBP=MAX0(IP1A,IP2A,IP3A)
      ILTP=MAX0(IOBL,IOBT,IOBP)
      ILTP1=IOF(ILTP)
      IOBS=29-ILTP1
      IOBD=10.0D0**IOBS
      IF(IOBL.GT.IOBP) GO TO 20
      IF(IOBP.GT.IOBT) GO TO 21
      IOBAS=IOBP*IOBT
      GO TO 22
   21 IOBAS=IOBP*IOBP
      GO TO 22
```

```
   20 IF(IOBP.GT.IOBT) GO TO 23
      IOBAS=IOBL*IOBT
      GO TO 22
   23 IOBAS=IOBL*IOBP
   22 IOBSS=IOF(IOBAS)
      IOBS=29-IOBSS
      IOBDD=10.0D0**IOBS
      RETURN
      END
```

```
      SUBROUTINE MINIMA
      DOUBLE L(3,99),DA,DB,DC,ZPL,DD,DE,DF,ZPJ,Z0,X1,Y1,XY1
      DOUBLE REMN,RNMN,R,U,H,DCI
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/KX,KY,KZ,IX,IY,IZ,JX,JY,JZ
      COMMON/D3/R(3),U(3),H(3)
      COMMON/D7/M1,M2,M3,N1,N2,N3,A,B,C/D8/MB(3)
      COMMON/D10/PH,ZZ,HHH/D9/IQ,IN,Q,RN
      DIMENSION LI(8),JAN(3,99),K(4,3),NPJ(99),NP(99),IAN(3,99)
C...RHO IS THE SQUARE OF THE DISTANCE OF THE POINT P+V*PH+W*PH**2
C...FROM THE REAL AXIS.
      RHO(P,V,W)=((P+W*Q)**2-V*(V*Q+W*RN))+(W*W*RN-V*P)*PH
     1+(V*V-W*(P+W*Q))*HHH
      N=1

C**** SECTION 1 **********************************************************

C...BEGIN WITH THE IDEAL (1,X,Y).
      LI(1)=1 £ LI(4)=0 £ LI(3)=INDEX £ LI(2)=0
      LI(7)=1 £ LI(6)=-IY £ LI(5)=-IZ £ LI(8)=INDEX
C...BASIS FOR LATTICE IS
C...       [1,(M1+M2*PH+M3*PH**2)/IG,(N1+N2*PH+N3*PH**2)/IG].
      IG=9*LI(1)*LI(8) £ M1=9*LI(2)+3*IA*LI(3)+LI(4)*IA*IA
                         N1=9*LI(5)+3*IA*LI(6)+LI(7)*IA*IA
      M2=3*LI(3)+2*LI(4)*IA
      N2=3*LI(6)+2*LI(7)*IA
      M3=LI(4) £ N3=LI(7)
C..... A,B,C ARE COEFFICIENTS OF THE ASSOCIATED BINARY QUADRATIC FORM
      A=B=C=0.
C...PARTS (I),.....,(VIII) ARE THE STEPS OF VORONOI'S ALGORITHM AS
C...DESCRIBED IN DELONE AND FADDEEV.
C....  ( I )  ..............................................................
C..... TEST THAT  M2*N3-M3*N2 IS GREATER THAN 0   .........
10    IF(M2*N3-M3*N2 .GT.0.) GO TO 20
      I1=M1 £ I2=M2 £ I3= M3
      M1=N1 £ M2=N2 £ M3= N3
      N1=I1 £ N2=I2 £ N3=I3
C....  ( II )  .............................................................
C..... PRODUCTION OF INITIAL VALUES OF A,B,C    ........
20    R1=M1 £ R2=M2 £ R3=M3
      S1=N1 £ S2=N2 £ S3=N3
      G=IG
      A=R2*R2+R2*R3*PH+R3*R3*ZZ
      B=R2*S2+(R2*S3+R3*S2)*PH*0.5+R3*S3*ZZ
      C=S2*S2+S2*S3*PH+S3*S3*ZZ
C....  ( III )  ............................................................
C... (III) AND (IV) FIND THE TWO BASIS ELEMENTS OF THE REDUCED HEXAGON
C...OF ZELLING.
      IF(B.GT.0.)GO TO 22
      CALL SUB(0,1,-1,0)
```

```
C....  ( IV ) ..............................................................
22     IF(A-B.LT.0.) GO TO 32
       IF(C-B.GT.0.) GO TO 50
32     IF(A-C.GT.0.) GO TO 40
       ID=INT(B/A)
       CALL SUB(1,-ID,0,1)
       GO TO 22
40      ID=INT(B/C)
       CALL SUB(1,0,-ID,1)
       GO TO 22
C....  ( V )  ..............................................................
C...TO FIND THE TWO ZELLING HEXAGON BASIS ELEMENTS WHICH COVER THE
C...NEGATIVE 'XSI' AXIS.
50     R2=M2 £ R3=M3 £ S2=N2 £ S3=N3
       RB=R2-R3*PH £ RD=S2-S3*PH
       RUP=RD-RB
       IF(RB.LT.0.) GO TO 60
       IF(RD.LT.0.) GO TO 90
       IF(RUP.GT.0.) GO TO 55
       CALL SUB(0,-1,1,1)
       GO TO 90
55     CALL SUB(-1,-1,1,0)
       GO TO 90
60     IF(RD.LT.0.) GO TO 70
       CALL SUB(-1,0,0,-1)
       GO TO 90
70     IF(RD-RB.GT.0.) GO TO 80
       CALL SUB(1,1,-1,0)
       GO TO 90
80     CALL SUB(0,1,-1,-1)
C....  ( VI )  ..............................................................
C...FINDING THE PINHEADS CORRESPONDING TO (M1+M2*PH+M3*PH**2)/IG AND
C...(N1+N2*PH+N3*PH**2)/IG.
90     R1=M1 £ R2=M2 £ R3=M3
       S1=N1 £ S2=N2 £ S3=N3
       T=(R1+R2*PH+R3*HHH)/G
       I=IFIX(T)
       IF(T.GT.0.) GO TO 4001
       I=I-1
4001   M1=M1-I*IG
       S=(S1+S2*PH+S3*HHH)/G
       I=IFIX(S)
       IF(S.GT.0.) GO TO 4002
       I=I-1
4002   N1=N1-I*IG
C....  ( VII )  .............................................................
C...CHOOSING THE TWO ELEMENTS OF THE REDUCED BASIS OF THE LATTICE FROM
C...THE SEVEN POSSIBILITIES BY FINDING THE TWO WITH MINIMUM RHO VALUE.
200    R1=M1 £ S1=N1  £  G2=2.*G
       XA=(2.*(R1+R3*Q)-R2*PH-R3*HHH)/G2
```

```
      XC=(2.*(S1+S3*Q)-S2*PH-S3*HHH)/G2
      IF(XA-0.5.GT.0.) GO TO 201
      K(1,1)=M1 £ K(1,2)=M2 £ K(1,3)=M3
      GO TO 202
201   K(1,1)=IG-M1 £ K(1,2)= -M2 £ K(1,3)= -M3
202   IF(XC-0.5.GT.0.) GO TO 203
      K(2,1)=N1 £ K(2,2)=N2 £ K(2,3)=N3
      GO TO 204
203   K(2,1)=IG-N1 £ K(2,2)= -N2 £ K(2,3)= -N3
204   T=(R1+R2*PH+R3*HHH)/G
      S=(S1+S2*PH+S3*HHH)/G
      IF(T-S.LT.0.) GO TO 220
      IF(XA-XC.GT.0.5) GO TO 210
      K(3,1)=M1-N1 £ K(3,2)=M2-N2 £ K(3,3)=M3-N3
      GO TO 240
210   K(3,1)=IG-M1+N1 £ K(3,2)= -M2+N2 £ K(3,3)= -M3+N3
      GO TO 240
220   IF(XC-XA.GT.0.5) GO TO 230
      K(3,1)=N1-M1 £ K(3,2)=N2-M2 £ K(3,3)=N3-M3
      GO TO 240
230   K(3,1)=IG-N1+M1 £ K(3,2)= -N2+M2 £ K(3,3)= -N3+M3
240   RZ0=RHO(FLOAT(K(1,1)),FLOAT(K(1,2)),FLOAT(K(1,3)))
      RZ1=RHO(FLOAT(K(2,1)),FLOAT(K(2,2)),FLOAT(K(2,3)))
      RZ2=RHO(FLOAT(K(3,1)),FLOAT(K(3,2)),FLOAT(K(3,3)))
      IF(RZ2.LT.RZ0) GO TO 280
      IF(RZ2.LT.RZ1) GO TO 260
      IF(T+S.GT.1.)GO TO 250
      IF(XA+XC.GT.0.5) GO TO 250
      K(4,1)=M1+N1 £ K(4,2)=M2+N2 £ K(4,3)=M3+N3
      RZ3=RHO(FLOAT(K(4,1)),FLOAT(K(4,2)),FLOAT(K(4,3)))
      IF(RZ3.GT.RZ0) GO TO 245
      IF(RZ3.GT.RZ1) GO TO 244
      M1=K(4,1) £ M2=K(4,2) £ M3=K(4,3)
      IF(RZ0.GT.RZ1) GO TO 243
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
243   N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
      GO TO 300
244   M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
      N1=K(4,1) £ N2=K(4,2) £ N3=K(4,3)
      GO TO 300
245   IF(RZ3.GT.RZ1) GO TO 250
      M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
      N1=K(4,1) £ N2=K(4,2) £ N3=K(4,3)
      GO TO 300
250   IF(RZ0.GT.RZ1) GO TO 255
      M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
      N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
      GO TO 300
255   M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
```

```
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
260   M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
      N1=K(3,1) £ N2=K(3,2) £ N3=K(3,3)
      GO TO 300
280   IF(RZ1.GT.RZ2) GO TO 290
      M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
      N1=K(3,1) £ N2=K(3,2) £ N3=K(3,3)
      GO TO 300
290   IF(RZ0.GT.RZ1) GO TO 295
      M1=K(3,1) £ M2=K(3,2) £ M3=K(3,3)
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
295   M1=K(3,1) £ M2=K(3,2) £ M3=K(3,3)
      N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
C....  ( VIII ) ..........................................................
300   JAN(1,N)=N1 £ JAN(2,N)=N2 £ JAN(3,N)=N3 £ NP(N)=IG
      IAN(1,N)=M1 £ IAN(2,N)=M2 £ IAN(3,N)=M3
      NQQ=N-1
C...... FIND THE INVERSE OF THE SECOND BASIS ELEMENT,THE FIRST RELATIVE
C..... OF THE LATTICE          ............
8988  CALL INVER(M1,M2,M3,JDET)
      I1=MB(1)*IG £ I2=MB(2)*IG £ I3=MB(3)*IG
      CALL ICF(I1,I2,I3,IF1)
C..... DIVIDE LATTICE BY SECOND BASIS ELEMENT AND PRODUCE A NEW LATTICE
      CALL MULT(MB(1),MB(2),MB(3),N1,N2,N3,J1,J2,J3)
      CALL ICF(J1,J2,J3,IF2)
      CALL ICF(IF1,IF2,JDET,IF)
      M1=J1/IF £ M2=J2/IF £ M3=J3/IF
      N1=I1/IF £ N2=I2/IF £ N3=I3/IF £ IG=JDET/IF
      IF(N.EQ.1) GO TO 501
C...CHECK IF OLD LATTICE COMPLETED THE LOOP.
      IF(IAN(1,N).NE.IAN11) GO TO 502
      IF(IAN(2,N).NE.IAN21) GO TO 502
      IF(IAN(3,N).NE.IAN31) GO TO 502
      IF(JAN(1,N).NE.JAN11) GO TO 502
      IF(JAN(2,N).NE.JAN21) GO TO 502
      IF(JAN(3,N).NE.JAN31) GO TO 502
      IF(NP(N).EQ.NP1) GO TO 600
      GO TO 502
  501 IAN11=IAN(1,1) £ IAN21=IAN(2,1) £ IAN31=IAN(3,1)
      JAN11=JAN(1,1) £ JAN21=JAN(2,1) £ JAN31=JAN(3,1) £ NP1=NP(1)
  502 N=N+1
C.....IF N.GT.99 PRINT DIAGNOSTIC..........
      IF(N.LT.99) GO TO 10
      PRINT 1111
1111  FORMAT(39H LATTICE LOOP HAS MORE THAN 99 MEMBERS )
      GO TO 7
C**** SECTION 2 ***********************************************************
```

```
C...NOW PRINT OUT THE LATTICES IN THIS CHAIN.
  600 PRINT 112
  112 FORMAT(/,1X,81HTHE ELEMENTS OF THE LOOP ARE, WHEN EXPRESSED IN TER
     1MS OF THE BASIS (1,PHI,PHI**2))
      DO 700 JIM=1,N
      PRINT 113,IAN(1,JIM),IAN(2,JIM),IAN(3,JIM),NP(JIM),JAN(1,JIM),
     1JAN(2,JIM),JAN(3,JIM),NP(JIM)
  113 FORMAT(/,1X,3I15,* /*,I5,/,3X,3I15,* /*,I5)
700   CONTINUE
      PRINT 114
  114 FORMAT(//,1X,57HWHEN EXPRESSED IN TERMS OF THE BASIS (Y,X,1) THESE
     1 BECOME)
C...WHEN THE THIRD ELEMENT OF EACH LATTICE BASIS HAS BEEN PRINTED THEN
C...IT IS NO LONGER NEEDED AND SO THE ARRAY JAN MAY BE USED TO STORE THE
C...VALUES OF THE COEFFICIENTS OF THE SECOND ELEMENT IN TERMS OF THE
C...BASIS (Y,X,1), SO THAT SECOND ELEMENT IS
C...     JAN(1,JIM)*Y+JAN(2,JIM)*X+JAN(3,JIM).
      DO 800 JIM=1,N
      CALL PHITH(IAN(1,JIM),IAN(2,JIM),IAN(3,JIM),NP(JIM),NIAN1,NIAN2,
     1NIAN3,NNPI)
      CALL PHITH(JAN(1,JIM),JAN(2,JIM),JAN(3,JIM),NP(JIM),NJAN1,NJAN2,
     1NJAN3,NNPJ)
      PRINT 113,NIAN1,NIAN2,NIAN3,NNPI,NJAN1,NJAN2,NJAN3,NNPJ
      JAN(1,JIM)=NIAN1
      JAN(2,JIM)=NIAN2
      JAN(3,JIM)=NIAN3
      NPJ(JIM)=NNPI
  800 CONTINUE
C
C...THE RELATIVE MINIMA ARE TO BE L(1,ILAT)*Y+L(2,ILAT)*X+L(3,ILAT) FOR
C...ILAT=1,N. THE RELATIVE MINIMUM 1 IS TO BE PUT AT 'ABOUT ONE THIRD'
C...OF THE WAY ALONG THE CHAIN.
      NQH=N/3
      NQP=NQH+1
      NQM=N
      L(1,NQP)=0.0D0
      L(2,NQP)=0.0D0
      L(3,NQP)=1.0D0
C...NOW CALCULATE THOSE RELATIVE MINIMA WHICH COME 'BEFORE' 1.
      DO 900 ILAT=1,NQH
      NQPP=NQP
      NQP=NQP-1
      NQM=NQM-1
      DD=JAN(1,NQM) £ DE=JAN(2,NQM) £ DF=JAN(3,NQM)
      ZPJ=NPJ(NQM)
      CALL DIVCD(L(1,NQPP),L(2,NQPP),L(3,NQPP),1.0D0,DD,DE,DF,ZPJ,DA,DB,
     1DC,ZPL)
      L(1,NQP)=DA
      L(2,NQP)=DB
```

```
      L(3,NQP)=DC
  900 CONTINUE
C...NOW CALCULATE THOSE RELATIVE MINIMA WHICH COME 'AFTER' 1.
      NQU=NQQ-NQH £ NQPP=NQH+1
      DO 901 ILAT=1,NQU
      NQP=NQPP
      NQPP=NQPP+1
      DD=JAN(1,ILAT) £ DE=JAN(2,ILAT) £ DF=JAN(3,ILAT)
      ZPJ=NPJ(ILAT)
      CALL MULTCD(L(1,NQP),L(2,NQP),L(3,NQP),1.D0,DD,DE,DF,ZPJ,DA,DB,
     1DC,ZPL)
      L(1,NQPP)=DA
      L(2,NQPP)=DB
      L(3,NQPP)=DC
  901 CONTINUE
C
C...NOW PRINT OUT THIS CHAIN OF RELATIVE MINIMA.
C...FOR N=1 TO NQQ CALCULATE Z(N)*(X(N+1)*X(N+1)+Y(N+1)*Y(N+1)) WHERE
C...Z(N) IS THE NTH RELATIVE MINIMUM OF THE CHAIN AND X(N)+I.Y(N),
C...X(N)-I.Y(N) ARE ITS CONJUGATES.
C
      PRINT 115
  115 FORMAT(/,1X,34HTHE RELATIVE MINIMA ARE AS FOLLOWS)
      Z0=DCI(L(3,1),L(2,1),L(1,1),H)
      REMN=1.0D0
      PRINT 116,L(1,1),L(2,1),L(3,1)
  116 FORMAT(/,1X,3D24.16)
      DO 902 ILAT=2,N
      DD=L(1,ILAT) £ DE=L(2,ILAT) £ DF=L(3,ILAT)
      PRINT 116,DD,DE,DF
      X1=DCI(DF,DE,DD,R)
      Y1=DCI(DF,DE,DD,U)
      XY1=X1*X1+Y1*Y1
      RNMN=DABS(Z0*XY1)
      PRINT 990,Z0,X1,Y1,XY1,RNMN
  990 FORMAT(/,1X,3HZ0=,D24.16,4H X1=,D24.16,4H Y1=,D24.16,/,1X,11HGIVIN
     1G XY1=,D24.16,10H AND RNMN=,D24.16)
      Z0=DCI(DF,DE,DD,H)
      IF(RNMN.GT.REMN) REMN=RNMN
  902 CONTINUE
C
C...NOW FIND AND PRINT THE CALCULATED LOWER BOUND ON THE MINIMUM OF THE
C...FIELD.
C
      PRINT 970,REMN
  970 FORMAT(6H REMN=,D24.16)
      REMNR=REMN
      DET=FLOAT(IDET)
      VALUE=DET/(720.0*REMNR)
      PRINT 980,VALUE
```

```
  980 FORMAT(/,9H DET/720M,F20.4)
      RETURN
      END
```

```
      SUBROUTINE SUB(I ,J,K,L)
C
C...ALTERS THE BASIS OF THE LATTICE AND CALCULATES THE NEW VALUES OFA,B AND C.
C
      COMMON/D7/M1,M2,M3,N1,N2,N3,A,B,C
      RI=I £ RJ=J £ RK=K £ RL=L
      A1=A*RI*RI+2.*B*RI*RK+C*RK*RK
      B1=RI*RJ*A+B*(RI*RL+RJ*RK)+C*RK*RL
      C1=A*RJ*RJ+2.*B*RJ*RL+C*RL*RL
      A=A1 £ B=B1 £ C=C1
      I1=M1 £ I2=M2 £ I3=M3 £ J1=N1 £ J2=N2 £ J3=N3
      M1=I*I1+K*J1 £ M2=I*I2+K*J2 £ M3=I*I3+K*J3
      N1=J*I1+L*J1 £ N2=J*I2+L*J2 £ N3=J*I3+L*J3
      RETURN
      END
```

```
      SUBROUTINE INVER(I,J,K,KDET)
C
C...FINDS THE INVERSE OF THE ALGEBRAIC INTEGER I+J*PH+K*PH**2
C...THE INVERSE IS (N(1,1)+N(1,2)*PH+N(1,3)*PH**2)/KDET.
C
      COMMON/D9/IQ,IN,Q,RN/D8/N(3)
      LA=I £ LB=J£ LC=K
      LD=IN*K £ LE=I+IQ*K £ LF=J
      LG=IN*J £ LH=IQ*J+IN*K £ LI=I+IQ*K
      N(1)=LE*LI-LH*LF
      N(2)=LC*LH-LB*LI £ N(3)=LB*LF-LE*LC
      MA=N(1) £ MB=LG*LF-LD*LI £ MC=LD*LH-LG*LE
      JDET=LA*MA+LB*MB+LC*MC
      KDET=IABS(JDET)
      IF(JDET.GT.0) GO TO 10
      DO 5 JZ=1,3
      N(JZ)=-N(JZ)
5     CONTINUE
10    CONTINUE
      CALL ICF(N(1),N(2),N(3),IZ)
      CALL ICF(IZ,IZ,KDET,IY)
      N(1)=N(1)/IY £ N(2)=N(2)/IY £ N(3)=N(3)/IY
      KDET=KDET/IY
      RETURN
      END
```

```
      SUBROUTINE ICF(IJ,IK,IL,IH)
C
C..... FINDS IH ,THE H.C.F. OF THE ABSOLUTE VALUES OF 3 INTEGERS IJ,IK,IL.
C
      N=1 £ J=IABS(IJ) £ K=IABS(IK) £ L=IABS(IL)
1     IF(K.EQ.0) GO TO 7
      IF(J.NE.0) GO TO 9
      J=K £ GO TO 1
7     IF(J.NE.0) GO TO 8
      IH=IL £ GO TO 50
8     K=J £ GO TO 1
9     IF(J.LT.K) GO TO 10
      I=J £ J=K £ K=I
10    M=MOD(K,J)
      IF(M.EQ.0) GO TO 30
      IF(M.EQ.1) GO TO 31
      K=J £ J=M £ GO TO 10
30    IH=J
      IF(N.EQ.2) GO TO 50
      N=N+1 £ J=IH £ K=L £ GO TO 1
31    IH=1
50    RETURN
      END
```

```
      SUBROUTINE ICF2(IJ,IK,IL,IH)
C
C     DOUBLE PRECISION VERSION OF ICF
C
      DOUBLE IJ,IK,IL,IH,J,K,L,H,I
      N=1
      J=IJ £ K=IK £ L=IL
      IF(IJ.GT.0.) GO TO 100
      J=-J
100   IF(IK.GT.0.) GO TO 101
      K=-K
101   IF(IL.GT.0.) GO TO 102
      L=-L
102    CONTINUE
1     IF(K.EQ.0) GO TO 7
      IF(J.NE.0) GO TO 9
      J=K £ GO TO 1
7     IF(J.NE.0) GO TO 8
      IH=L £ GO TO 50
8     K=J £ GO TO 1
9     IF(J.LT.K) GO TO 10
      I=J £ J=K £ K=I
10    H=DMOD(K,J)
      IF(H.EQ.0.) GO TO 30
      IF(H.EQ.1) GO TO 31
      K=J £ J=H £ GO TO 10
30    IH=J
      IF(N.EQ.2) GO TO 50
      N=N+1 £ J=IH £ K=L £ GO TO 1
31    IH=1
50    RETURN
      END
```

```
      SUBROUTINE MULT(J1,J2,J3,K1,K2,K3,L1,L2,L3)
C
C...MULTIPLIES J1+J2*PH+J3*PH**2 BY K1+K2*PH+K3*PH**2 TO GIVE
C...L1+L2*PH+L3*PH**2.
C
      COMMON/D9/I1,I2,Q,RN
      L1=J1*K1+I2*(J3*K2+J2*K3)
      L2=J1*K2+K1*J2+I1*(J3*K2+J2*K3)+I2*J3*K3
      L3=J1*K3+J2*K2+J3*K1+I1*J3*K3
      RETURN
      END
```

```
      SUBROUTINE PHITH(I1,I2,I3,ID,J1,J2,J3,JD)
C
C...(I1+I2*PH+I3*PH**2)/ID=(J1*Y+J2*X+J3)/JD
C
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      J3=I1-IA*I2+I3*IA*IA £ J2=3*I2-6*IA*I3
      J1=9*I3 £ JD=ID
      J3=J3+J1*IT3 £ J2=J2+J1*IT2 £ J1=J1*IT1
      CALL ICF(JD,J1,J2,JF)
      JF2=JF
      CALL ICF(J3,JF,JF2,JFF)
      J1=J1/JFF £ J2=J2/JFF £ J3=J3/JFF £ JD=JD/JFF
      RETURN
      END
```

```
      SUBROUTINE DIVCD(L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR)
C
C...DIVCD IS A DOUBLE PRECISION ROUTINE WHICH FINDS THE QUOTIENT OF
C...(L1*Y+M1*X+N1)/LN AND (L2*Y+M2*X+N2)/LD, IT IS (L*Y+M*X+N)/LR.
C
      DOUBLE L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR,I1,I2,I3,J1,J2,J3,K1,K2,K3
      DOUBLE JDET,KDET,IHF,LG,LRA
      DOUBLE IOBD,IOBDD,LA,MA,NA,DDIV1,DDIV2,DDIV
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D16/IOBD,IOBDD
      KDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)=I1*J2*K3+I2*J3*K1+I3*J1*K2
     1-I1*J3*K2-I2*J1*K3-I3*J2*K1
C...FIRST TEST FOR THE POSSIBILITY OF OVERFLOW.
      LA=DABS(L1) £ MA=DABS(M1) £ NA=DABS(N1)
      DDIV1=DMAX1(LA,MA,NA)
      LA=DABS(L2) £ MA=DABS(M2) £ NA=DABS(N2)
      DDIV2=DMAX1(LA,MA,NA)
      IF(DDIV1.GT.DDIV2) GO TO 1
      DDIV=DDIV2*DDIV2*DDIV2
      GO TO 2
    1 DDIV=DDIV1*DDIV2*DDIV2
    2 IF(DDIV.LT.IOBDD) GO TO 3
      PRINT 50
   50 FORMAT(1X,10(1H*),27HDANGER OF OVERFLOW IN DIVCD,10(1H*))
    3 I1=L2*IL1+IP1*M2+N2
      I2=L2*IL2+IP2*M2
      I3=L2*IL3+IP3*M2
      J1=IP1*L2+M2*IT1
      J2=IP2*L2+M2*IT2+N2
      J3=IP3*L2+M2*IT3
      K1=L2 £ K2=M2 £ K3=N2
      JDET=KDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)
      L=KDET(L1,M1,N1,J1,J2,J3,K1,K2,K3)*LD
      M=KDET(I1,I2,I3,L1,M1,N1,K1,K2,K3)*LD
      N=KDET(I1,I2,I3,J1,J2,J3,L1,M1,N1)*LD
      LR=JDET*LN
      CALL ICF2(L,M,N,IHF)
      LRA=LR
      CALL ICF2(IHF,LRA,LR,LG)
      L=L/LG £ M=M/LG £ N=N/LG £ LR=LR/LG
      RETURN
      END
```

```
      SUBROUTINE MULTCD(L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR)
C
C...MULTCD IS A DOUBLE PRECISION ROUTINE WHICH FINDS THE PRODUCT OF
C...(L1*Y+M1*X+N1)/LN AND (L2*Y+M2*X+N2)/LD, IT IS (L*Y+M*X+N)/LR.
C
      DOUBLE L1,M1,N1,LN,L2,M2,N2,LD,L,M,N,LR,IP,Y1,Y2,Z
      DOUBLE IOBD,IOBDD,LA,MA,NA,MULT1,MULT2,MULT
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D16/IOBD,IOBDD
C...FIRST TEST FOR THE POSSIBILITY OF OVERFLOW.
      LA=DABS(L1) £ MA=DABS(M1) £ NA=DABS(N1)
      MULT1=DMAX1(LA,MA,NA)
      LA=DABS(L2) £ MA=DABS(M2) £ NA=DABS(N2)
      MULT2=DMAX1(LA,MA,NA)
      MULT=MULT1*MULT2
      IF(MULT.LT.IOBD) GO TO 1
      PRINT 50
   50 FORMAT(1X,10(1H*),28HDANGER OF OVERFLOW IN MULTCD,10(1H*))
    1 IP=L1*M2+L2*M1
      L=L1*L2*IL1+IP*IP1+M1*M2*IT1+L1*N2+L2*N1
      M=L1*L2*IL2+IP*IP2+M1*M2*IT2+M1*N2+M2*N1
      N=L1*L2*IL3+IP*IP3+M1*M2*IT3+N1*N2
      LR=LN*LD
      CALL ICF2(L,M,N,Y1)
      Y2=Y1
      CALL ICF2(Y2,Y1,LR,Z)
      L=L/Z £ M=M/Z £ N=N/Z £ LR=LR/Z
      RETURN
      END
```

```
      DOUBLE FUNCTION DCI(X,Y,Z,RD)
      DOUBLE X,Y,Z,RD(3)
      DCI=X*RD(1)+Y*RD(2)+Z*RD(3)
      RETURN
      END
```

```
      FUNCTION IOF(I)
C...I IS LESS THAN 10**IOF(I).
      IFL=I
      IFL1=0
    1 IFL1=IFL1+1
      IFL=IFL/10
      IF(IFL.GT.0) GO TO 1
      IOF=IFL1
      RETURN
      END
```

THE PROGRAM CONG

SUBROUTINES

IN THIS SECTION		IN PREVIOUS SECTION	
BASE	34	SUP	15
FACTOR	37	INVER	16
IDEAL	38	ICF	17
PRIN	40	ICF2	18
MULT2	45	MULT	19
CHANGE	46	DIVCD	21
TEST	47	IOF	24
INCON	50		
MODAL	52		
IALMOD	53		
DIVC	54		
MULTC	55		
DNORM	56		
FDET	57		

```
      PROGRAM CONG(INPUT,OUTPUT)
C...THIS PROGRAM TESTS WHETHER ANY OF THE RESIDUE CLASSES MODULO THE
C...FACTORS OF E+1 AND E-1 CONTAIN ANY INTEGERS NOT CONGRUENT TO AN
C...INTEGER WITH NORM LESS IN ABSOLUTE VALUE THAN THE ABSOLUTE VALUE OF
C...THE NORM OF THE MODULUS UNDER CONSIDERATION. IF THIS IS SO THEN THE
C...FIELD BEING CONSIDERED IS NON-EUCLIDEAN. OTHERWISE NO CONCLUSION IS
C...REACHED.
      COMMON/D20/MU1,MU2,MU3,NU1,NU2,NU3,IGU1
C
C...INITIALIZING
C
      INTEGER A,B,C,D,E,F
      INTEGER EUCLID,AA,BB,CC,DD,EE,FF
      DOUBLE DNORM,DIM,DJM,DKM,DN
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D3/MF,MP,MAP(500,2)
      COMMON/D4/IP(2000),IR(2000),IS(2000)
      COMMON/D5/IM,JM,KM
      COMMON/D6/EUCLID
      COMMON/D11/A(3),B(3),C(3),D(3),E(3),F(3)
      COMMON/D12/AA,BB,CC,DD,EE,FF,IPP,IRR,ISS
      COMMON/D21/I,J,K
      DIMENSION NF(100), NP(100)
      DIMENSION IPW(100),IRW(100),ISW(100)
C
C...THE PROGRAM BEGINS
C
   40 READ 101,IDET,INDEX,IA,IB,IC,I,J,K,L
      IF(IDET.EQ.0) STOP
  101 FORMAT(I6,I2,3I5,3I16,I3)
C...THE FIELD BEING CONSIDERED HAS DISCRIMINANT -IDET, AND IS K(X) WHERE
C..X**3-IA*X**2+IB*X-IC=0. THE FUNDAMENTAL UNIT OF THE FIELD IS
C...E=(I*X**2+J*X+K)/L.
      IDETM=-IDET
      PRINT 102,IDETM,INDEX,IA,IB,IC
  102 FORMAT(1H1,1X,26HTHE FIELD HAS DISCRIMINANT,I8,7H, INDEX,I3,
     129H, AND POLYNOMIAL COEFFICIENTS,3I6)
      CALL BASE
C...AN INTEGRAL BASIS FOR THE FIELD IS (1,X,Y) WHERE
C...      X**2=IT1*Y + IT2*X + IT3
C...      Y**2=IL1*Y + IL2*X + IL3
C...      X*Y =IP1*Y + IP2*X + IP3
C...AND SO Y=(X**2-IT2*X-IT3)/IT1, IT1=INDEX.
      PRINT 103
  103 FORMAT(/,1X,45HTHE FIELD IS K(X) AND HAS BASIS (Y,X,1) WHERE)
      ASSIG1=4HX**2 £ ASSIG2=4HY**2 £ ASSIG3=4HX*Y
      PRINT 104,ASSIG1,IT1,IT2,IT3
      PRINT 104,ASSIG2,IL1,IL2,IL3
      PRINT 104,ASSIG3,IP1,IP2,IP3
```

```
  104 FORMAT(12X,A4,2H =,I10,3HY +,I10,3HX +,I10)
      CALL CHANGE(I,J,K,L,I1,J1,K1)
C...E=(I*X**2+J*X+K)/L=I1*Y+J1*X+K1
      I=I1 £ J=J1 £ K=K1
C...E=I*Y+J*X+K
  108 FORMAT(1X,26HTHE UNIT OF THE FIELD IS (,I16,1H,,I16,1H,,I16,1H))
      PRINT 108,I,J,K
C...THE 'REDUCED' FORM OF THE UNIT IDEAL IS NOW CALCULATED.
      AA=BB=DD=1 £ CC=EE=FF=0
      CALL PRIN(1)
      EUCLID=0 £ ICHECK=-1
      MAPC=1
C...EUCLID=0 WHEN THE EUCLIDEAN PROPERTY OF THE FIELD IS UNKNOWN AND IS
C...EQUAL TO 1 WHEN THE FIELD IS FOUND TO BE NON-EUCLIDEAN.
C...MAPC IS A POINTER TO THE NEXT 'EMPTY' ELEMENT OF (IP,IR,IS).
C...ICHECK=-1 WHEN CONSIDERING E-1 AND ICHECK=1 WHEN CONSIDERING E+1
C...WE NOW BEGIN A CONSIDERATION OF E-1.
      MAX=0
      IM=I £ JM=J £ KM=K-1
C...IM*Y+JM*X+KM=E+ICHECK.
   31 DIM=IM £ DJM=JM £ DKM=KM
      DN=DNORM(DIM,DJM,DKM)
      N=DN
      DN=DABS(DN)
      IF(DN.LT.1.0D14) GO TO 956
      PRINT 957,ICHECK
  957 FORMAT(1X,10(1H*),10HNORM OF E+,I2,24HIS TOO LARGE FOR INTEGER,
     110(1H*))
      GO TO 20
  956 PRINT 107,ICHECK,N
  107 FORMAT(/,1X,36HNOW CONSIDER THE FACTORIZATION OF E+,I2,15H WHICH H
     1AS NORM,I16)
      N=IABS(N)
      EN=FLOAT(N) £ REN=SQRT(EN) £ MAXR=IFIX(REN)+1 £ MAXF=MAXR/2+1
      MAXF=MIN0(100,MAXF)
C...MAXF IS AN UPPER BOUND FOR THE NUMBER OF DISTINCT PRIME FACTORS
C...OF N.
      CALL FACTOR(N,NF,NP,MAXF,NFC)
C...NFC IS THE EXACT NUMBER OF DISTINCT PRIME FACTORS OF N. NP(I) IS THE
C...POWER TO WHICH NF(I) IS A FACTOR OF N.
C...NOW FIND MAX WHICH IS THE LARGEST NUMBER OF
C...(F:F=R OR R**3 WHERE R IS A FACTOR OF N).
      IZERO=0
      IF(ICHECK.EQ.-1) GO TO 15
      IF(MAX.NE.MBX) GO TO 17
   15 MBX=1
      DO 2 II=1,NFC
      IF(NP(II).LT.3) GO TO 21
      MBXX1=NF(II)**3
      IF(MBXX1.LT.500) GO TO 22
```

```
   21 MBXX1=NF(II)
      IF(MBXX1.GT.500) GO TO 2
   22 MBX=MAX0(MBX,MBXX1)
    2 CONTINUE
      IF(MBX.GT.1) GO TO 1
      PRINT 105,ICHECK
  105 FORMAT(1X,2HE+,I2,29H HAS NO FACTORS LESS THAN 500)
      MAX=MBX
      GO TO 20
    1 IF(MBX.LE.MAX) GO TO 17
      MLX=MAX0(2,MAX+1)
      MAX=MBX
      PRINT 109,MLX,MAX
  109 FORMAT(1X,49H ALL INTEGERS WITH NORM OF ABSOLUTE VALUE BETWEEN,I5,
     14H AND,I5,25H INCLUSIVE ARE CALCULATED)
C...ALL INTEGERS WITH NORM BETWEEN MLX AND MAX ARE NOW CALCULATED.
      DO 3 INORM=MLX,MAX
      IF(INORM.EQ.2) GO TO 8
      FNORM=FLOAT(INORM) £ RNORM=SQRT(FNORM) £ NNORM=IFIX(RNORM)
      DO 7 INM=2,NNORM
      IF(MOD(INORM,INM).EQ.0) GO TO 9
    7 CONTINUE
      GO TO 8
    9 MAP(INORM,1)=MAPC £ NNORM=INORM/2
C.....HAVING REACHED THIS POINT INORM IS COMPOSITE SO FIND THE ALGEBRAIC
C.....INTEGERS OF NORM INORM BY CONSIDERING THE PRIME FACTORS OF INORM.
C.....MAP(INORM,1) IS THE FIRST POSITION IN THE ARRAYS (IP,IR,IS) IN
C.....WHICH AN INTEGER OF NORM INORM APPEARS. NNORM IS THE GREATEST
C.....POSSIBLE PROPER RATIONAL INTEGRAL FACTOR OF INORM.
      IP(MAPC)=0 £ IR(MAPC)=0 £ IS(MAPC)=1
C.....SET THIS FIRST POSITION INITIALLY TO 1 SO THAT AS PRIME FACTORS OF
C.....INORM ARE FOUND, THE ALGEBRAIC INTEGERS OF NORM THESE PRIMES
C.....RAISED TO THE POWER TO WHICH THEY DIVIDE INORM CAN BE MULTIPLIED
C.....TOGETHER SO THAT ALL THE INTEGERS OF NORM INORM ARE FOUND.
      MAPC=MAPC+1 £ IINORM=INORM
C...IINORM IS SET TO INORM HERE SO THAT AS PRIME FACTORS OF INORM ARE
C...FOUND IINORM MAY BE DIVIDED BY A SUITABLE POWER OF THAT PRIME WHILE
C...SAVING INORM.
      DO 50 INM=2,NNORM
C.....LOOK FOR A FACTOR OF IINORM I.E. A PRIME FACTOR OF INORM.
      IF(MOD(IINORM,INM).NE.0) GO TO 50
C.....HAVING FOUND A PRIME FACTOR, FIND TO WHAT POWER, INPW, IT DIVIDES
C.....IINORM.
      INPW=0
   81 IF(MOD(IINORM,INM).NE.0) GO TO 80
      IINORM=IINORM/INM £ INPW=INPW+1
      GO TO 81
   80 IF(MAP(INM,1).EQ.-1) GO TO 51
      ISM=MAP(INM,2)-MAP(INM,1)+1
      IF(ISM.EQ.1) GO TO 52
```

```
      IF(ISM.EQ.2) GO TO 53
C.....HAVING REACHED THIS POINT INM HAS THREE DISTINCT ALGEBRAIC FACTORS
C.....SO ALL ALGEBRAIC INTEGERS OF NORM INM**INPW ARE PUT IN THE ARRAYS
C.....(IPW,IRW,ISW).
      IS1=MAP(INM,1) £ IS2=IS1+1 £ IS3=IS2+1
      IPS1=IP(IS1) £ IRS1=IR(IS1) £ ISS1=IS(IS1)
      IPS2=IP(IS2) £ IRS2=IR(IS2) £ ISS2=IS(IS2)
      IPS3=IP(IS3) £ IRS3=IR(IS3) £ ISS3=IS(IS3)
      INPWP=INPW+1 £ IWC=0
      DO 82 JMAP1P=1,INPWP
      JMAP1=JMAP1P-1
      LIMIT=INPWP-JMAP1
      DO 82 JMAP2P=1,LIMIT
      JMAP2=JMAP2P-1
      JMAP3=INPW-(JMAP1+JMAP2) £ IWC=IWC+1
      IF(IWC.GT.100) GO TO 97
      IPWP=0 £ IRWP=0 £ ISWP=1
      IF(JMAP1.EQ.0) GO TO 84
      DO 83 JPW=1,JMAP1
      CALL MULTC(IPWP,IRWP,ISWP,IPS1,IRS1,ISS1,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   83 CONTINUE
   84 IF(JMAP2.EQ.0) GO TO 86
      DO 85 JPW=1,JMAP2
      CALL MULTC(IPWP,IRWP,ISWP,IPS2,IRS2,ISS2,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   85 CONTINUE
   86 IF(JMAP3.EQ.0) GO TO 89
      DO 87 JPW=1,JMAP3
      CALL MULTC(IPWP,IRWP,ISWP,IPS3,IRS3,ISS3,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   87 CONTINUE
   89 IPW(IWC)=IPWP £ IRW(IWC)=IRWP £ ISW(IWC)=ISWP
   82 CONTINUE
C...THERE ARE IWC INTEGERS OF NORM INM**INPW CONTAINED IN (IPW,IRW,ISW).
      GO TO 99
   53 IS1=MAP(INM,1) £ IS2=IS1+1
      IPS1=IP(IS1) £ IRS1=IR(IS1) £ ISS1=IS(IS1)
      IPS2=IP(IS2) £ IRS2=IR(IS2) £ ISS2=IS(IS2)
C.....HAVING REACHED THIS POINT INM HAS TWO DISTINCT ALGEBRAIC FACTORS.
      INPWP=INPW+1 £ IWC=0
      DO 92 JMAP1P=1,INPWP
      JMAP1=JMAP1P-1
      JMAP2=INPW-JMAP1 £ IWC=IWC+1
      IF(IWC.GT.100) GO TO 97
      IPWP=0 £ IRWP=0 £ ISWP=1
      IF(JMAP1.EQ.0) GO TO 94
      DO 93 JPW=1,JMAP1
      CALL MULTC(IPWP,IRWP,ISWP,IPS1,IRS1,ISS1,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
```

```
   93 CONTINUE
   94 IF(JMAP2.EQ.0) GO TO 91
      DO 95 JPW=1,JMAP2
      CALL MULTC(IPWP,IRWP,ISWP,IPS2,IRS2,ISS2,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   95 CONTINUE
   91 IPW(IWC)=IPWP £ IRW(IWC)=IRWP £ ISW(IWC)=ISWP
   92 CONTINUE
C.....THERE ARE NOW IWC INTEGERS WITH NORM INM**INPW.
      GO TO 99
   52 IMAP=MAP(INM,1)
      IPS1=IP(IMAP) £ IRS1=IR(IMAP) £ ISS1=IS(IMAP)
C.....HAVING REACHED THIS POINT INM HAS JUST ONE LINEAR FACTOR.
      IF(INPW.EQ.1) GO TO 55
      IF(MOD(IDET,INM).EQ.0) GO TO 55
C.....INM DIVIDES THE DISCRIMINANT OF THE FIELD IF AND ONLY IF INM HAS A
C.....SQUARE FACTOR, I.E. IN THIS INSTANCE IF INM IS THE CUBE OF AN
C.....ALGEBRAIC INTEGER. HENCE IF INM DOES NOT DIVIDE IDET THEN INM HAS
C.....ONE LINEAR AND ONE QUADRATIC FACTOR.
      CALL MULTC(IPS1,IRS1,ISS1,IPS1,IRS1,ISS1,IPL2,IRL2,ISL2)
      CALL DIVC(0,0,INM,IPS1,IRS1,ISS1,IPQ,IRQ,ISQ)
C.....(IPL2,IRL2,ISL2) AND (IPQ,IRQ,ISQ) ARE THE TWO DISTINCT ALGEBRAIC
C.....INTEGERS OF NORM INM**2.
      IF(MOD(INPW,2).EQ.0) GO TO 56
      INPW2=(INPW-1)/2 £ INPW=1 £ GO TO 57
   56 INPW2=INPW/2 £ INPW=0
   57 INPW2P=INPW2+1 £ IWC=0
      DO 64 JMAP1P=1,INPW2P
      JMAP1=JMAP1P-1
      JMAP2=INPW2-JMAP1
      IWC=IWC+1
      IF(IWC.GT.100) GO TO 97
      IPWP=0 £ IRWP=0 £ ISWP=1
      IF(JMAP1.EQ.0) GO TO 65
      DO 66 JPW=1,JMAP1
      CALL MULTC(IPWP,IRWP,ISWP,IPL2,IRL2,ISL2,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   66 CONTINUE
   65 IF(JMAP2.EQ.0) GO TO 63
      DO 68 JPW=1,JMAP2
      CALL MULTC(IPWP,IRWP,ISWP,IPQ,IRQ,ISQ,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   68 CONTINUE
   63 IPW(IWC)=IPWP £ IRW(IWC)=IRWP £ ISW(IWC)=ISWP
   64 CONTINUE
C.....IWC IS THE NUMBER OF INTEGERS WITH NORM INM**PW WHERE PW=INPW IF
C.....INPW WAS EVEN AND INPW-1 IF INPW WAS ODD.
      IF(INPW.EQ.0) GO TO 99
      GO TO 67
   55 IWC=1 £ IPW(IWC)=0 £ IRW(IWC)=0 £ ISW(IWC)=1
```

```
C.....55 IS REACHED EITHER IF INPW WAS ORIGINALLY 1 OR IF INM HAS NO
C.....QUADRATIC FACTOR . IN EITHER OF THESE CASES IF PA IS THE ALGEBRAIC
C.....INTEGER OF NORM INM THEN PA**INPW IS THE ONLY INTEGER OF NORM
C.....INM**INPW.
   67 DO 62 JWC=1,IWC
      IPWP=IPW(JWC) £ IRWP=IRW(JWC) £ ISWP=ISW(JWC)
      DO 69 JPW=1,INPW
      CALL MULTC(IPWP,IRWP,ISWP,IPS1,IRS1,ISS1,IPWW,IRWW,ISWW)
      IPWP=IPWW £ IRWP=IRWW £ ISWP=ISWW
   69 CONTINUE
      IPW(JWC)=IPWP £ IRW(JWC)=IRWP £ ISW(JWC)=ISWP
   62 CONTINUE
C.....IWC IS THE NUMBER OF ALGEBRAIC INTEGERS OF NORM INM**INPW.
   99 MPC=MAPC-1 £ LMAP=MAP(INORM,1) £ KMAP=MAPC-LMAP
      DO 88 JMAP=LMAP,MPC
      IPP=IP(JMAP) £ IRR=IR(JMAP) £ ISS=IS(JMAP)
      DO 88 JPW=1,IWC
      KMAP1=JMAP+(JPW-1)*KMAP
      IF(KMAP1.GT.2000) GO TO 90
      CALL MULTC(IPP,IRR,ISS,IPW(JPW),IRW(JPW),ISW(JPW),IP(KMAP1),
     1IR(KMAP1),IS(KMAP1))
   88 CONTINUE
      MAPC=MAPC+(IWC-1)*KMAP
      IF(MAPC.LE.2000) GO TO 96
   90 PRINT 900,MAX
  900 FORMAT(1X,68HMORE THAN 2000 INTEGERS WITH NORM AT MOST MAX IF MAX
     1IS GREATER THAN,I5)
      GO TO 16
   96 IF(IINORM.EQ.1) GO TO 61
      GO TO 50
   51 IF(MOD(INPW,3).NE.0) GO TO 60
C.....THIS POINT IS REACHED IF INM HAS NO ALGEBRAIC FACTORS, THUS THE
C.....ONLY POSSIBLE INTEGERS WITH NORM DIVISIBLE BY INM ARE POWERS OF
C.....INM. THUS THERE ARE ONLY INTEGERS OF NORM INM**INPW AND SO OF
C.....INORM IF INPW IS A MULTIPLE OF 3.
      INWP=INPW/3 £ MPC=MAPC-1 £ LMAP=MAP(INORM,1)
      DO 58 JMAP=LMAP,MPC
      IPU=IP(JMAP) £ IRU=IR(JMAP) £ ISU=IS(JMAP)
      DO 59 JPW=1,INWP
      IPP=IPU £ IRR=IRU £ ISS=ISU
      CALL MULTC(IPP,IRR,ISS,0,0,INM,IPU,IRU,ISU)
   59 CONTINUE
      IP(JMAP)=IPU £ IR(JMAP)=IRU £ IS(JMAP)=ISU
   58 CONTINUE
      IF(MAPC.GT.2000) GO TO 90
      IF(IINORM.EQ.1) GO TO 61
   50 CONTINUE
   60 MAPC=MAP(INORM,1) £ MAP(INORM,1)=-1 £ GO TO 3
C...MAP(INORM,1)=-1 INDICATES THAT THERE ARE NO INTEGERS OF NORM INORM.
   61 MAP(INORM,2)=MAPC-1 £ GO TO 3
```

```
C...MAP(INORM,2) IS THE LAST POSITION IN THE ARRAYS (IP,IR,IS) IN WHICH
C...AN INTEGER OF NORM INORM APPEARS.
   97 PRINT 901,INORM
  901 FORMAT(1X,71HTHERE ARE MORE THAN 100 INTEGERS OF NORM P**A WHERE P
     1**A IS A FACTOR OF,I5)
      GO TO 16
    8 CALL IDEAL(INORM,ISC)
C...THIS POINT IS REACHED WHEN INORM IS A RATIONAL PRIME, ITS ALGEBRAIC
C...FACTORS ARE NOW CALCULATED. THERE ARE ISC SUCH FACTORS WHERE ISC IS
C...AT MOST 3.
      IF(ISC.NE.0) GO TO 70
C...IF INORM IS ALSO AN ALGEBRAIC PRIME THEN THERE ARE NO INTEGERS OF
C...NORM INORM.
      MAP(INORM,1)=-1 £ GO TO 3
   70 MAP(INORM,1)=MAPC
      DO 10 IFILL=1,ISC
      AA=A(IFILL) £ BB=B(IFILL) £ CC=C(IFILL)
      DD=D(IFILL) £ EE=E(IFILL) £ FF=F(IFILL)
      CALL PRIN(INORM)
      IP(MAPC)=IPP £ IR(MAPC)=IRR £ IS(MAPC)=ISS
      MAPC=MAPC+1
      IF(MAPC.LE.2000) GO TO 10
      IF(IFILL.EQ.ISC) IZERO=1
      PRINT 900,MAX
      GO TO 16
   10 CONTINUE
      MAP(INORM,2) =MAPC-1
    3 CONTINUE
      GO TO 17
   16 MAX=INORM-1+IZERO
   17 DO 6 II=1,NFC
C...RUN THROUGH THE POSSIBLE NORM VALUES FOR FACTORS OF E+ICHECK-1
      MP=NP(II) £ MF=NF(II)
      IF(MF.LE.3) GO TO 23
      IF(MF.GT.MAX) GO TO 6
      IF(MAP(MF,1).EQ.-1) GO TO 23
      CALL TEST
      IF(EUCLID.EQ.1) GO TO 40
C...IF THE EUCLIDEAN PROPERTY OF THE FIELD IS STILL UNKNOWN FIND IF
C...MF**3 IS A FACTOR OF NORM(IM*Y+JM*X+KM) OTHERWISE STOP.
   23 IF(MP.LT.3) GO TO 6
C...MF**3 DOES NOT DIVIDE NORM(IM*Y+JM*X+KM) GO ON TO NEXT POSSIBLE
C...PRIME NORM VALUE.
      MF=MF**3 £ MP=1
      IF(MF.GT.MAX) GO TO 6
      CALL TEST
      IF(EUCLID.EQ.1) GO TO 40
    6 CONTINUE
C...NOW AS POSSIBLE NORM VALUES OF THE MODULI TO BE CONSIDERED WE HAVE
C...GONE THROUGH ALL THE PRIME FACTORS OF IM*Y+JM*X+KM AND THEIR CUBES.
```

```
C...HAVING REACHED NO CONCLUSION WE GO ON TO A CONSIDERATION OF THE
C...FACTORS OF E+1 IF IM*Y+JM*X+KM=E-1 AND END OTHERWISE.
   20 IF(ICHECK.EQ.1) GO TO 30
      ICHECK=1 £ IM=I £ JM=J £ KM=K+1
      GO TO 31
   30 PRINT 106
  106 FORMAT(1X,30HNO CONCLUSION HAS BEEN REACHED)
      GO TO 40
      END
```

```
      SUBROUTINE BASE
      DOUBLE IUBM,IOBD
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D10/H,ZZ,HHH/D9/IQ,INN,Q,V2
      COMMON/D15/IUBN,IOB,IOBDS/D16/IUBM,IOBD
C...WHEN CONSIDERING THE FIELD K(X) SUPPOSE H=3*X-IA THEN H SATISFIES AN
C...EQUATION H**3-IQ*H-INN=0. FIND H AND H**2-IQ FOR USE IN THE
C...SUBROUTINE PRIN.
      IQ=3*IA*IA-9*IB
      INN=27*IC-9*IA*IB+2*IA*IA*IA
      Q=FLOAT(IQ)
      V1=Q/3.0
      V2=FLOAT(INN)
      V3=SQRT(V2**2-4.0*V1**3)
      V4=(V2+V3)/2.0
      V5=(V2-V3)/2.0
      IF(V4.NE.0.0) GO TO 51
      V6=0.0 £ GO TO 52
   51 D=1.0
      IF(V4.GE.0.0) GO TO 53
      V4=-V4 £ D=-1.0
   53 V6=EXP((ALOG(V4))/3.0)*D
   52 IF(V5.NE.0.0) GO TO 54
      V7=0.0 £ GO TO 55
   54 D=1.0
      IF(V5.GE.0.0) GO TO 56
      V5=-V5 £ D=-1.0
   56 V7=EXP((ALOG(V5))/3.0)*D
   55 H=V6+V7 £ HHH=H*H
      ZZ=HHH-Q
C...NOW FIND IT AND IS SUCH THAT (1,X,Y), WHERE Y=(X*X+IT*X+IS)/INDEX,
C...IS A BASIS FOR THE FIELD.
      IN=INDEX
      IN2=IN**2 £ IN3=IN2*IN
      K1=IA*IA-2*IB £ K2=IA*IC £ K3=IB*IC
      K4=IB*IB-2*IA*IC £ K5=IA*IB-3*IC £ IC2=IC*IC
      IF(INDEX.NE.1) GO TO 1
      IT=0 £ IS=0 £ GO TO 2
    1 DO 3 ITC=1,IN
      IT=ITC-1
      DO 4 ISC=1,IN
      IS=ISC-1
      JA=K1+IT*IA+3*IS
      IF(MOD(JA,IN).NE.0) GO TO 4
      JB=K4+IT**2*IB+3*IS**2+IT*K5+2*IS*K1+2*IS*IT*IA
      IF(MOD(JB,IN2).NE.0) GO TO 4
      JC=IS**3+IT**3*IC+IC**2+IS**2*IT*IA+IS*K4+IS*IT**2*IB+IT*IB*IC
     1+IT**2*IA*IC+IS**2*K1+IS*IT*K5
      IF(MOD(JC,IN3).NE.0) GO TO 4
```

```
      GO TO 2
    4 CONTINUE
    3 CONTINUE
C...NOW FIND THE COEFFICIENTS OF Y,X AND 1 IN THE EXPRESSIONS FOR Y*Y,
C...X*X AND X*Y...
C...      Y*Y=IL1*Y+IL2*X+IL3         ...
C...      X*X=IT1*Y+IT2*X+IT3         ...
C...      X*Y=IP1*Y+IP2*X+IP3         ...
    2 IT1=INDEX
      IT2=-IT
      IT3=-IS
      ML=2*IA*IT+IA*IA+2*IS+IT*IT-IB
      IL1=ML/IN
      IL2=(-IT*ML+2*IS*IT+IC-2*IB*IT-IA*IB)/IN2
      IL3=(-IS*ML+2*IC*IT+IA*IC+IS*IS)/IN2
      MP=IA+IT
      IP1=MP
      IP2=(IS-IB-IT*MP)/IN
      IP3=(IC-IS*MP)/IN
C...FIND AN UPPER BOUND, A POWER OF 10, FOR THE ARGUMENTS OF DNORM
C...WHICH WILL NOT GIVE RISE TO OVERFLOW.
      K1P=IABS(K1) £ K4P=IABS(K4) £ K5P=IABS(K5)
      NF=MAX0(K1P,K2,K3,K4P,K5P,IC2)
      IONF=IOF(NF)
      IONS=(29-IONF)/3
      IUBN=10**IONS
C...NOW FIND AN UPPER BOUND FOR THE ARGUMENTS OF MULT2.
      IQA=IABS(IQ) £ INNA=IABS(INN)
      NON=MAX0(IQA,INNA)
      ION=IOF(NON)
      IOMS=29-ION
      IUBM=10.0D0**IOMS
C...FIND SIMILAR BOUNDS FOR THE ARGUMENTS OF MULTC,DIVC AND DIVCD.
      IL1A=IABS(IL1) £ IL2A=IABS(IL2) £ IL3A=IABS(IL3)
      IT1A=IABS(IT1) £ IT2A=IABS(IT2) £ IT3A=IABS(IT3)
      IP1A=IABS(IP1) £ IP2A=IABS(IP2) £ IP3A=IABS(IP3)
      IOBL=MAX0(IL1A,IL2A,IL3A)
      IOBT=MAX0(IT1A,IT2A,IT3A)
      IOBP=MAX0(IP1A,IP2A,IP3A)
      IOBAS=MAX0(IOBL,IOBT,IOBP)
      IOBSS=IOF(IOBAS)
      IOBS=14-IOBSS
      IOB=10**IOBS
      IF(IOBL.GT.IOBP) GO TO 20
      IF(IOBP.GT.IOBT) GO TO 21
      IOBAS=IOBP*IOBT
      GO TO 22
   21 IOBAS=IOBP*IOBP
      GO TO 22
   20 IF(IOBP.GT.IOBT) GO TO 23
```

```
      IOBAS=IOBL*IOBT
      GO TO 22
   23 IOBAS=IOBL*IOBP
   22 IOBSS=IOF(IOBAS)
      IOBS=14-IOBSS £ IOBSD=29-IOBSS
      IOBDS=10**IOBS £ IOBD=10.0D0**IOBSD
      RETURN
      END
```

```
      SUBROUTINE FACTOR(NN,NF,NP,NL,I)
C...THE SUBROUTINE FACTOR FINDS THE FACTORS OF NN WHICH ARE LESS THAN
C...500 AND PUTS THEM IN THE ARRAY NF. NP(I) IS THE POWER TO WHICH NF(I)
C...IS A FACTOR OF NN. NL IS AN UPPER BOUND ON THE NUMBER OF POSSIBLE
C...DISTINCT PRIME FACTORS OF NN. FROM THE MAIN PROGRAM NL IS AT MOST
C...100.
      DIMENSION NF(NL),NP(NL)
      N=NN
      EN=FLOAT(N) £ RN=SQRT(EN) £ NR=IFIX(RN)
C...NR IS THE GREATEST INTEGER LESS THAN SQRT(N) AND SO N CAN HAVE AT
C...MOST ONE FACTOR GREATER THAN NR.
      I=0 £ JF=1
    3 JF=JF+1 £ JP=0
      IF(JF.GT.NR) GO TO 6
      IF(JF.GT.500) GO TO 7
    1 IF(MOD(N,JF).NE.0) GO TO 4
      JP=JP+1 £ N=N/JF
      EN=FLOAT(N) £ RN=SQRT(EN) £ NR=IFIX(RN)
      IF(N.NE.1) GO TO 1
      GO TO 5
    4 IF(JP.EQ.0) GO TO 3
      I=I+1 £ NF(I)=JF £ NP(I)=JP
      IF(I.GE.NL) GO TO 7
      GO TO 3
    6 JF=N £ JP=1
    5 I=I+1 £ NF(I)=JF £ NP(I)=JP
    7 RETURN
      END
```

```
      SUBROUTINE IDEAL(N,ISC)
      INTEGER A,B,C,D,E,G
C...IDEAL FINDS THE IDEALS (A(I),B(I)*X+C(I),D(I)*Y+E(I)*X+G(I))
C...FOR I=1,ISC OF NORM N WHERE N IS A RATIONAL PRIME, HENCE
C...ISC=0,1,2, OR 3.
      COMMON/D1/IA,IB,IC,L,IDET
      COMMON/D2/KX,KY,KZ,IX,IY,IZ,JX,JY,JZ
      COMMON/D11/A(3),B(3),C(3),D(3),E(3),G(3)
      DIMENSION MY(6,3)
C...NORL(KB)=NORM(X**2+KT*X+KB)/L
      NORL(KB)=(IC*IC+IC*KT*KT*KT+KB*KB*KB+IB*IC*KT+(IB*IB-2*IA*IC)*KB
     1+(IA*IC+IB*KB)*KT*KT+((IA*IA-2*IB)+IA*KT)*KB*KB+(IA*IB-3*IC)*KT
     2*KB)/(L*L*L)
C...NORN(J)=NORM(X+J)
      NORN(J)=IC+J*(IB+J*(IA+J))
      INDEX=L
      KT=-IY £ KS=-IZ

C**** SECTION 1 ************************************************************

      ISC=0
C......LOOP FOR VALUES OF J I.E. C(ISC).......
      DO 4 JJ=1,N
      J=JJ-1
C...N MUST DIVIDE NORM(X+J)
      IF(MOD(NORN(J),N).NE.0) GO TO 4
C......LOOP FOR VALUES OF K I.E. G(ISC)......
      DO 6 KK=1,N
      K=KK-1
      KB=K*L+KS
C......N MUST DIVIDE NORM(Y+K)......
      IF(MOD(NORL(KB),N).NE.0) GO TO 6

C**** SECTION 2 ************************************************************

C..... MULTIPLES OF IDEAL MEMBERS BY INTEGERS MUST BE IDEAL MEMBERS   ..
C......MY(IT,1)*Y+MY(IT,2)*X+MY(IT,3) IS THE PRODUCT OF ONE OF (X,Y)
C......WITH ONE OF THE BASIS ELEMINTS OF THE IDEAL. IT VARIES FROM 1 TO
C......6 SO THAT EVERY CASE IS CONSIDERED.
      MY(1,1)=0 £ MY(1,2)=N £ MY(1,3)=0 £ MY(2,1)=N £ MY(2,2)=0
      MY(2,3)=0 £ MY(3,1)=IX £ MY(3,2)=J+IY £ MY(3,3)=IZ £ MY(4,1)=J+JX
      MY(4,2)=JY £ MY(4,3)=JZ £ MY(5,1)=JX £ MY(5,2)=JY+K £ MY(5,3)=JZ
      MY(6,1)=KX+K £ MY(6,2)=KY £ MY(6,3)=KZ
      DO 8 IT=1,6
C...CHECKS THAT MY(IT,1)*Y+MY(IT,2)*X+MY(IT,3) BELONGS TO THE IDEAL.
      NA=MY(IT,1) £ NB=MY(IT,2) £ NC=MY(IT,3)
      NC=NC-NA*K-NB*J
      IF(MOD(NC,N).NE.0) GO TO 6
8     CONTINUE
      ISC=ISC+1
```

```
      A(ISC)=N £ B(ISC)=1 £ C(ISC)=J £ D(ISC)=1 £ E(ISC)=0 £ G(ISC)=K
    6 CONTINUE
    4 CONTINUE
      RETURN
      END
```

```
      SUBROUTINE PRIN(INK)
      DOUBLE X,Y,Z,DA,DB,DC,DD,DE,DF,DG,DH,DI,Y2
      DOUBLE IUBM,IOBD
      DOUBLE DAXMUL,DXMUL1,DXMUL2
      DOUBLE DDA,DDB,DDC
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/KX,KY,KZ,IX,IY,IZ,JX,JY,JZ
      COMMON/D7/M1,M2,M3,N1,N2,N3,A,B,C/D8/MB(3)
      COMMON/D10/H,ZZ,HHH/D9/IQ,IN,Q,RN
      COMMON/D12/JA,JB,JC,JD,JE,JF,JP,JR,JS
      COMMON/D16/IUBM,IOBD
      COMMON/D20/MU1,MU2,MU3,NU1,NU2,NU3,IGU1
      DIMENSION LI(8),IAN(3,99),JAN(3,99),NP(99),K(4,3)
C...RHO IS THE SQUARE OF THE DISTANCE OF THE POINT U+V*H+W*H**2 FROM
C...THE REAL AXIS.
      RHO(U,V,W)=((U+W*Q)**2-V*(V*Q+W*RN))+(W*W*RN-V*U)*H
     1+(V*V-W*(U+W*Q))*HHH
      N=1

C**** SECTION 1 ******************************************************

      LI(1)=JA £ LI(4)=0 £ LI(3)=JB*INDEX £ LI(2)=JC*INDEX
      LI(7)=JD £ LI(6)=JE*INDEX-IY*LI(7)
      LI(5)=JF*INDEX-IZ*LI(7) £ LI(8)=INDEX
C...BASIS FOR LATTICE IS [1,(M1+M2*H+M3*H**2)/IG,(N1+N2*H+N3*H**2)/IG]
      IG=9*LI(1)*LI(8) £ M1=9*LI(2)+3*IA*LI(3)+LI(4)*IA*IA
                         N1=9*LI(5)+3*IA*LI(6)+LI(7)*IA*IA
      M2=3*LI(3)+2*LI(4)*IA
      N2=3*LI(6)+2*LI(7)*IA
      M3=LI(4) £ N3=LI(7)
C..... A,B,C ARE COEFFICIENTS OF THE ASSOCIATED BINARY QUADRATIC FORM
      A=B=C=0.
C...PARTS (I)....(VIII) ARE THE STEPS OF VORONOI'S ALGORITHM AS
C...DESCRIBED IN DELONE AND FADDEEV.
C....  ( I )  .........................................................
C..... TEST THAT  M2*N3-M3*N2 IS GREATER THAN 0   .........
   10 IF(M2*N3-M3*N2.GT.0) GO TO 20
      I1=M1 £ I2=M2 £ I3= M3
      M1=N1 £ M2=N2 £ M3= N3
      N1=I1 £ N2=I2 £ N3=I3
C....  ( II )  ........................................................
C..... PRODUCTION OF INITIAL VALUES OF A,B,C    ........
   20 R1=M1 £ R2=M2 £ R3=M3
      S1=N1 £ S2=N2 £ S3=N3
      G=IG
      A=R2*R2+R2*R3*H+R3*R3*ZZ
      B=R2*S2+(R2*S3+R3*S2)*H*0.5+R3*S3*ZZ
      C=S2*S2+S2*S3*H+S3*S3*ZZ
C....  ( III )  .......................................................
C..... (III) AND (IV) FIND TWO BASIS ELEMENTS OF THE REDUCED HEXAGON OF
```

```
C...ZELLING.
      IF(B.GT.0.)GO TO 22
      CALL SUB(0,1,-1,0)
C....  ( IV ) ............................................................
22    IF(A-B.LT.0.) GO TO 32
      IF(C-B.GT.0.) GO TO 50
32    IF(A-C.GT.0.) GO TO 40
      ID=INT(B/A)
      CALL SUB(1,-ID,0,1)
      GO TO 22
40     ID=INT(B/C)
      CALL SUB(1,0,-ID,1)
      GO TO 22
C....  ( V ) .............................................................
C...TO FIND THE TWO ZELLING HEXAGON BASIS ELEMENTS WHICH COVER THE
C...NEGATIVE 'XSI' AXIS.
50    R2=M2 £ R3=M3 £ S2=N2 £ S3=N3
      RB=R2-R3*H £ RD=S2-S3*H
      RUP=RD-RB
      IF(RB.LT.0.) GO TO 60
      IF(RD.LT.0.) GO TO 90
      IF(RUP.GT.0.) GO TO 55
      CALL SUB(0,-1,1,1)
      GO TO 90
55    CALL SUB(-1,-1,1,0)
      GO TO 90
60    IF(RD.LT.0.) GO TO 70
      CALL SUB(-1,0,0,-1)
      GO TO 90
70    IF(RD-RB.GT.0.) GO TO 80
      CALL SUB(1,1,-1,0)
      GO TO 90
80    CALL SUB(0,1,-1,-1)
C....  (VI) ..............................................................
C...FINDING THE PINHEADS CORRESPONDING TO (M1+M2*H+M3*H**2)/IG AND
C...(N1+N2*H+N3*H**2)/IG.
90    R1=M1 £ R2=M2 £ R3=M3
      S1=N1 £ S2=N2 £ S3=N3
      T=(R1+R2*H+R3*HHH)/G
      I=IFIX(T)
      IF(T.GT.0.) GO TO 4001
      I=I-1
4001  M1=M1-I*IG
      S=(S1+S2*H+S3*HHH)/G
      I=IFIX(S)
      IF(S.GT.0.) GO TO 4002
      I=I-1
4002  N1=N1-I*IG
C....  ( VII ) ...........................................................
C...CHOOSING THE TWO ELEMENTS OF THE REDUCED BASIS OF THE LATTICE FROM
```

```
C...THE SEVEN POSSIBILITIES BY FINDING THE TWO WITH MINIMUM RHO VALUE.
200   R1=M1 £ S1=N1  £  G2=2.*G
      XA=(2.*(R1+R3*Q)-R2*H-R3*HHH)/G2
      XC=(2.*(S1+S3*Q)-S2*H-S3*HHH)/G2
      IF(XA-0.5.GT.0.) GO TO 201
      K(1,1)=M1 £ K(1,2)=M2 £ K(1,3)=M3
      GO TO 202
201   K(1,1)=IG-M1 £ K(1,2)= -M2 £ K(1,3)= -M3
202   IF(XC-0.5.GT.0.) GO TO 203
      K(2,1)=N1 £ K(2,2)=N2 £ K(2,3)=N3
      GO TO 204
203   K(2,1)=IG-N1 £ K(2,2)= -N2 £ K(2,3)= -N3
204   T=(R1+R2*H+R3*HHH)/G
      S=(S1+S2*H+S3*HHH)/G
      IF(T-S.LT.0.) GO TO 220
      IF(XA-XC.GT.0.5) GO TO 210
      K(3,1)=M1-N1 £ K(3,2)=M2-N2 £ K(3,3)=M3-N3
      GO TO 240
210   K(3,1)=IG-M1+N1 £ K(3,2)= -M2+N2 £ K(3,3)= -M3+N3
      GO TO 240
220   IF(XC-XA.GT.0.5) GO TO 230
      K(3,1)=N1-M1 £ K(3,2)=N2-M2 £ K(3,3)=N3-M3
      GO TO 240
230   K(3,1)=IG-N1+M1 £ K(3,2)= -N2+M2 £ K(3,3)= -N3+M3
240   RZ0=RHO(FLOAT(K(1,1)),FLOAT(K(1,2)),FLOAT(K(1,3)))
      RZ1=RHO(FLOAT(K(2,1)),FLOAT(K(2,2)),FLOAT(K(2,3)))
      RZ2=RHO(FLOAT(K(3,1)),FLOAT(K(3,2)),FLOAT(K(3,3)))
      IF(RZ2.LT.RZ0) GO TO 280
      IF(RZ2.LT.RZ1) GO TO 260
      IF(T+S.GT.1.)GO TO 250
      IF(XA+XC.GT.0.5) GO TO 250
      K(4,1)=M1+N1 £ K(4,2)=M2+N2 £ K(4,3)=M3+N3
      RZ3=RHO(FLOAT(K(4,1)),FLOAT(K(4,2)),FLOAT(K(4,3)))
      IF(RZ3.GT.RZ0) GO TO 245
      IF(RZ3.GT.RZ1) GO TO 244
      M1=K(4,1) £ M2=K(4,2) £ M3=K(4,3)
      IF(RZ0.GT.RZ1) GO TO 243
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
243   N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
      GO TO 300
244   M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
      N1=K(4,1) £ N2=K(4,2) £ N3=K(4,3)
      GO TO 300
245   IF(RZ3.GT.RZ1) GO TO 250
      M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
      N1=K(4,1) £ N2=K(4,2) £ N3=K(4,3)
      GO TO 300
250   IF(RZ0.GT.RZ1) GO TO 255
      M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
```

```
      N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
      GO TO 300
255   M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
260   M1=K(1,1) £ M2=K(1,2) £ M3=K(1,3)
      N1=K(3,1) £ N2=K(3,2) £ N3=K(3,3)
      GO TO 300
280   IF(RZ1.GT.RZ2) GO TO 290
      M1=K(2,1) £ M2=K(2,2) £ M3=K(2,3)
      N1=K(3,1) £ N2=K(3,2) £ N3=K(3,3)
      GO TO 300
290   IF(RZ0.GT.RZ1) GO TO 295
      M1=K(3,1) £ M2=K(3,2) £ M3=K(3,3)
      N1=K(1,1) £ N2=K(1,2) £ N3=K(1,3)
      GO TO 300
295   M1=K(3,1) £ M2=K(3,2) £ M3=K(3,3)
      N1=K(2,1) £ N2=K(2,2) £ N3=K(2,3)
C....  ( VIII )  .......................................................
  300 JAN(1,N)=N1 £ JAN(2,N)=N2 £ JAN(3,N)=N3 £ NP(N)=IG
      IAN(1,N)=M1 £ IAN(2,N)=M2 £ IAN(3,N)=M3
      IF(INK.EQ.1) GO TO 9
      NOO=N-1
C...... FIND THE INVERSE OF THE SECOND BASIS ELEMENT,THE FIRST RELATIVE
C...MINIMUM OF THE LATTICE.
8988  CALL INVER(M1,M2,M3,JDET)
      I1=MB(1)*IG £ I2=MB(2)*IG £ I3=MB(3)*IG
      CALL ICF(I1,I2,I3,IF1)
C..... DIVIDE LATTICE BY SECOND BASIS ELEMENT AND PRODUCE A NEW LATTICE
      CALL MULT(MB(1),MB(2),MB(3),N1,N2,N3,J1,J2,J3)
      CALL ICF(J1,J2,J3,IF2)
      CALL ICF(IF1,IF2,JDET,IF)
      M1=J1/IF £ M2=J2/IF £ M3=J3/IF
      N1=I1/IF £ N2=I2/IF £ N3=I3/IF £ IG=JDET/IF
      IF(N.EQ.1) GO TO 501
C.....CHECK IF THE OLD LATTICE IS THE UNIT LATTICE.....
      IF(IAN(1,N).NE.MU1) GO TO 501
      IF(IAN(2,N).NE.MU2) GO TO 501
      IF(IAN(3,N).NE.MU3) GO TO 501
      IF(JAN(1,N).NE.NU1) GO TO 501
      IF(JAN(2,N).NE.NU2) GO TO 501
      IF(JAN(3,N).NE.NU3) GO TO 501
      IF(NP(N).EQ.IGU1) GO TO 600
501   N=N+1
C.....IF N.GT.99 PRINT DIAGNOSTIC..........
      IF(N.LT.99) GO TO 10
      PRINT 1111
 1111 FORMAT(38H LATTICE LOOP HAS MORE THAN 99 MEMBERS)
      GO TO 7
```

```
C**** SECTION 2 ************************************************************

C...SECTION 2 IS ENTERED WHEN THE LATTICE LOOP IS COMPLETE. IT
C...MULTIPLIES ALL THE RELATIVE MINIMA TOGETHER TO GIVE AN INTEGER OF
C...NORM INK.
  600 DB=DC=0 £ DA=LI(1) £ NPD=1
      DO 700 JIM=1,NQQ
      DD=IAN(1,JIM) £ DE=IAN(2,JIM) £ DF=IAN(3,JIM)
      DDA=DABS(DA) £ DDB=DABS(DB) £ DDC=DABS(DC)
      DXMUL1=DMAX1(DDA,DDB,DDC)
      DDA=DABS(DD) £ DDB=DABS(DE) £ DDC=DABS(DF)
      DXMUL2=DMAX1(DDA,DDB,DDC)
      DAXMUL=DXMUL1*DXMUL2
      IF(DAXMUL.LT.IUBM) GO TO 601
      PRINT 650,INK
  650 FORMAT(1X,10(1H*),40HDANGER OF OVERFLOW WITH INTEGERS OF NORM,I5,
     110(1H*))
  601 CALL MULT2(DA,DB,DC,DD,DE,DF,DG,DH,DI)
      NPD=NPD*NP(JIM)
      X=NPD
      CALL ICF2(X,DG,DH,Y)
      Y2=Y
      CALL ICF2(Y,Y2,DI,Z)
      DA=DG/Z £ DB=DH/Z £ DC=DI/Z
      NPD=X/Z
700   CONTINUE
      DD=DC*9.D0 £ DE=3.D0*DB-DC*6.D0*IA
      DF=IA*IA*DC-IA*DB+DA £ DG=NPD
      CALL ICF2(DG,DD,DE,DH)
      CALL ICF2(DH,DF,DH,DI)
      DD=DD/DI £ DE=DE/DI £ DF=DF/DI £ DG=DG/DI
      DDA=DABS(DD) £ DDB=DABS(DE) £ DDC=DABS(DF)
      IF(DDA.GE.1.0D14) GO TO 701
      IF(DDB.GE.1.0D14) GO TO 701
      IF(DDC.LT.1.0D14) GO TO 702
  701 PRINT 650,INK
  702 JP1=DD £ JR1=DE £ JS1=DF £ JD=DG
      CALL CHANGE(JP1,JR1,JS1,JD,JP,JR,JS)
      GO TO 7
9     MU1=M1 £ MU2=M2 £ MU3=M3 £ NU1=N1 £ NU2=N2 £ NU3=N3 £ IGU1=IG
7     RETURN
      END
```

```
      SUBROUTINE MULT2(A,B,C,D,E,F,G,H,I)
C
C     DOUBLE PRECISION VERSION OF MULT
C
      DOUBLE A,B,C,D,E,F,G,H,I,DQ,DN
      COMMON/D9/IQ,IN,Q,RN
      DQ=Q £ DN=RN
      G=A*D+DN*(B*F+C*E)
      H=A*E+B*D+DQ*(B*F+C*E)+DN*C*F
      I=A*F+B*E+C*D+DQ*C*F
      RETURN
      END
```

```
      SUBROUTINE CHANGE(I,J,K,L,I1,J1,K1)
C...CHANGE FINDS I1,J1,K1 SUCH THAT I1*Y+J1*X+K1=(I*X**2+J*X+K)/L.
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      I1=(I*IT1)/L £ J1=(I*IT2+J)/L £ K1=(I*IT3+K)/L
      RETURN
      END
```

```
      SUBROUTINE TEST
C...THIS SUBROUTINE TRIES CONGRUENCES TO MODULI OF NORM MF WHERE MF IS A
C...FACTOR OF NORM(E+ICHECK) AND SETS EUCLID TO 1 IF NOT ALL THE RESIDUE
C...CLASSES TO ONE OF THE MODULI OF NORM MF CONTAIN AN INTEGER OF NORM
C...LESS THAN MF.
      INTEGER EUCLID
      DOUBLE IM,JM,KM,JP,JR,JS
      COMMON/D3/MF,MP,MAP(500,2)
      COMMON/D4/IP(2000),IR(2000),IS(2000)
      COMMON/D5/IIM,JJM,KKM/D6/EUCLID
      COMMON/D21/I,J,K
      COMMON/D30/ITHETA,ILAM,IPRIME
      DIMENSION ICP(500),ICR(500),ICS(500),ICD(500),LIC(500)
      IM=IIM £ JM=JJM £ KM=KKM
      JCOUNT=-1
      LMAP1=MAP(MF,1) £ LMAP2=MAP(MF,2)
      DO 7 JJ=LMAP1,LMAP2
C...NOW USE IN TURN EACH OF THE ALGEBRAIC INTEGERS OF NORM MF.
      JP=IP(JJ) £ JR=IR(JJ) £ JS=IS(JJ)
      JJP=JP £ JJR=JR £ JJS=JS
C...CHECK TO SEE IF JP*Y+JR*X+JS IS A FACTOR OF IM*Y+JM*X+KM IF IT IS
C...NOT GO ON TO THE NEXT NUMBER OF NORM MF.
      IF(IALMOD(IM,JM,KM,JP,JR,JS).EQ.1) GO TO 7
      ICL=MF-1
C...ICL IS THE NUMBER OF NON-ZERO RESIDUE CLASSES MODULO (JP,JR,JS).
      CALL INCON(JP,JR,JS,ICL,ICP,ICR,ICS,LIC)
C...LIC(I) IS SET TO 1 INITIALLY AND TO 0 WHEN AN INTEGER OF NORM LESS
C...THAN MF IS FOUND TO BELONG TO ICP(I)*Y+ICR(I)*X+ICS(I). NOW RUN
C...THROUGH THE INTEGERS WITH NORM LESS THAN MF AND ELIMINATE THE
C...RESIDUE CLASSES TO WHICH THEY BELONG.
      IPRIME=0
      ITHETA=0 £ ILAM=0
C...IPRIME=1 WHEN X AND Y ARE CONGRUENT TO RATIONAL INTEGERS AND
C...IPRIME=0 OTHERWISE.
      IF(ICS(ICL).NE.ICL) GO TO 20
      IPRIME=2
C...IPRIME=2 WHEN FINDING THE VALUES OF ILAM AND OF ITHETA.
      CALL MODAL(1,0,0,ICP,ICR,ICS,LIC,ICL,JP,JR,JS)
      DO 21 JJC=1,ICL
      IF(LIC(JJC).NE.0) GO TO 21
      ILAM=JJC
      LIC(JJC)=1
      GO TO 22
   21 CONTINUE
   22 CALL MODAL(0,1,0,ICP,ICR,ICS,LIC,ICL,JP,JR,JS)
      DO 23 JJC=1,ICL
      IF(LIC(JJC).NE.0) GO TO 23
      ITHETA=JJC
      LIC(JJC)=1
      GO TO 24
```

```
   23 CONTINUE
   24 IPRIME=1
      PRINT 999,ITHETA,ILAM
  999 FORMAT(26H MODULUS IS PRIME, ITHETA=,I5,6H ILAM=,I5)
C...X IS CONGRUENT TO ITHETA AND Y TO ILAM.
   20 CALL MODAL(I,J,K,ICP,ICR,ICS,LIC,ICL,JP,JR,JS)
      DO 8 JJC=2,ICL
      IF(MAP(JJC,1).EQ.-1) GO TO 8
      MMAP1=MAP(JJC,1) £ MMAP2=MAP(JJC,2)
      DO 9 JJD=MMAP1,MMAP2
      KP=IP(JJD) £ KR=IR(JJD) £ KS=IS(JJD)
      CALL MODAL(KP,KR,KS,ICP,ICR,ICS,LIC,ICL,JP,JR,JS)
    9 CONTINUE
      JCOUNT=0
      DO 10 ICOUNT=1,ICL
      IF(LIC(ICOUNT).EQ.0) GO TO 10
      JCOUNT=JCOUNT+1
      ICD(JCOUNT)=ICOUNT
   10 CONTINUE
C.....JCOUNT IS THE NUMBER OF RESIDUE CLASSES STILL UNCOVERED. IF THE
C.....RESIDUE CLASSES ARE ALL COVERED GO ON TO CONGRUENCES TO ANOTHER
C.....MODULUS, OTHERWISE GO ON TO INTEGERS OF A GREATER NORM.
      IF(JCOUNT.EQ.0) GO TO 11
    8 CONTINUE
C...NOW THE ONLY REMAINING RESIDUE CLASSES WITH LIC=1 ARE THOSE WHICH
C...DO NOT CONTAIN AN INTEGER OF NORM LESS THAN MF.
C...IF JCOUNT=-1 THEN THERE ARE NO INTEGERS WITH NORM LESS THAN MF
C...OTHER THAN E AND SO WE GO ON TO FIND WHICH RESIDUE CLASSES ARE
C...UNCOVERED SINCE THIS HAS NOT BEEN DONE.
      IF(JCOUNT.NE.-1) GO TO 13
      JCOUNT=0
      DO 12 ICT=1,ICL
      IF(LIC(ICT).EQ.0) GO TO 12
      JCOUNT=JCOUNT+1
      ICD(JCOUNT)=ICT
   12 CONTINUE
      IF(JCOUNT.EQ.0) GO TO 11
C...IF THERE ARE STILL SOME UNCOVERED RESIDUE CLASSES THEN THE FIELD IS
C...NON-EUCLIDEAN SO THIS FACT IS PRINTED TOGETHER WITH THE MODULUS AND
C...UNCOVERED RESIDUE CLASSES.
   13 PRINT 102,JJP,JJR,JJS
  102 FORMAT(1X,67HTHE FIELD IS SHOWN TO BE NON-EUCLIDEAN WHEN CONSIDERI
     1NG CONGRUENCES,/,1X,14HTO THE MODULUS,3I16,/,1X,39HWHEN THE UNCOVE
     2RED RESIDUE CLASSES ARE-)
      DO 14 ICT=1,JCOUNT
      ID=ICD(ICT)
      PRINT 103,ICP(ID),ICR(ID),ICS(ID)
  103 FORMAT(15X,3I16)
   14 CONTINUE
      EUCLID=1
```

```
C...SETTING EUCLID TO 1 INDICATES THE FIELD IS NON-EUCLIDEAN.
      GO TO 15
   11 MP=MP-1
      IF(MP.EQ.0) GO TO 15
    7 CONTINUE
   15 RETURN
      END
```

```
      SUBROUTINE INCON(JP,JR,JS,M,ICP,ICR,ICS,LIC)
C...INCON FINDS THE RESIDUE CLASSES MODULO JP*Y+JR*X+JS EXCLUDING THE
C...ZERO RESIDUE CLASS. THESE ARE ICP(I)*Y+ICR(I)*X+ICS(I) FOR I=1,M,
C...THE CORRESPONDING LIC(I) IS SET TO 1. M=NORM(JP*Y+JR*X+JS)-1.
      DOUBLE DJ,DJJ,JP,JR,JS,DARG1,DARG2
      COMMON/D1/IA,IB,IC,INDEX,IDET
      DIMENSION ICP(M),ICR(M),ICS(M),LIC(M)
C...NORN(JJ,J)=NORM(JJ*X+J).
      NORN(JJ,J)=JJ*JJ*JJ*IC+J*(JJ*JJ*IB+J*(JJ*IA+J))
      MM=M+1
      JJP=JP £ JJR=JR £ JJS=JS
      PRINT 160,JJP,JJR,JJS,MM
  160 FORMAT(/,1X,35HCONGRUENCES ARE CONSIDERED MODULO (,I15,1H,,I15,1H,
     1,I15,1H),/,1X,14HWHICH HAS NORM,I15)
      DO 1 I=1,M
      ICP(I)=ICR(I)=ICS(I)=0 £ LIC(I)=1
    1 CONTINUE
      IP=IR=IS=0
      IPP=IRR=ISS=1
C...FIRST CALCULATE IS SUCH THAT 0,1,...,IS ARE INCONGRUENT MODULO
C...JP*Y+JR*X+JS.
      DO 2 J=1,MM
      IF(MOD(J*J*J,MM).NE.0) GO TO 2
      JJP=JP £ JJR=JR £ JJS=JS
      DJ=J
      DARG1=0.D0 £ DARG2=0.D0
      IF(IALMOD(DARG1,DARG2,DJ,JP,JR,JS).EQ.1) GO TO 2
      IS=J-1 £ GO TO 3
    2 CONTINUE
    3 ISS=IS+1
      IF(ISS.EQ.MM) GO TO 7
      IS2=MIN0(ISS,MM/ISS)
C...NOW FIND IR SUCH THAT R*X+S FOR R=0,IR AND S=0,IS ARE INCONGRUENT
C...MODULO JP*Y+JR*X+JS.
      DO 4 JJ=1,IS2
      DO 10 JL=1,ISS
      J=JL-1
      IF(MOD(NORN(JJ,J),MM).NE.0) GO TO 10
      DJJ=JJ £ DJ=J
      DARG1=0.D0
      IF(IALMOD(DARG1,DJJ,DJ,JP,JR,JS).EQ.1) GO TO 10
      IR=JJ-1 £ GO TO 5
   10 CONTINUE
    4 CONTINUE
    5 IRR=IR+1
      IF((ISS*IRR).EQ.MM) GO TO 7
      IPP=MM/(ISS*IRR)
      IP=IPP-1
C...THE RESIDUE CLASSES ARE NOW (P*Y+R*X+S) P=0,IP, R=0,IR, S=0,IS.
    7 IJK=0
```

```
      DO 8 II=1,IPP
      I=II-1
      DO 8 JJ=1,IRR
      J=JJ-1
      DO 8 KK=1,ISS
      K=KK-1
      IF((I.EQ.0).AND.(J.EQ.0).AND.(K.EQ.0)) GO TO 8
      IJK=IJK+1
      ICP(IJK)=I £ ICR(IJK)=J £ ICS(IJK)=K
    8 CONTINUE
      PRINT 161,IP,IR,IS
  161 FORMAT(4X,46HTHE RESIDUE CLASSES ARE (P*Y+R*X+S) WHERE P=0,,I4,
     15H R=0,,I4,5H S=0,,I4,/,1X,18HP,R,S NOT ALL ZERO)
      RETURN
      END
```

```
      SUBROUTINE MODAL(KP,KR,KS,ICP,ICR,ICS,LIC,M,JP,JR,JS)
C...MODAL FINDS WHICH ICP(I)*Y+ICR(I)*X+ICS(I) IS CONGRUENT TO
C...+OR-(KP*Y+KR*X+KS) MODULO JP*Y+JR*X+JS AND SETS THE CORRESPONDING
C...LIC(I) TO 0.
      DOUBLE IP,IR,IS,JP,JR,JS
      COMMON/D30/ITHETA,ILAM,IPRIME
      DIMENSION ICP(M),ICR(M),ICS(M),LIC(M)
      IF(IPRIME.NE.1) GO TO 5
      MM=M+1
      KKP=MOD(KP,MM)
      KKR=MOD(KR,MM)
      KKS=MOD(KS,MM)
      KPRS=KKP*ILAM+KKR*ITHETA+KKS
      KPRS=MOD(KPRS,MM)
      IF(KPRS.LT.0) KPRS=MM+KPRS
      LIC(KPRS)=0
      KPRS=MM-KPRS
      LIC(KPRS)=0
      RETURN
    5 DO 1 I=1,M
      IP=KP-ICP(I) £ IR=KR-ICR(I) £ IS=KS-ICS(I)
      MODIAL =IALMOD(IP,IR,IS,JP,JR,JS)
      IF(LIC(I).NE.0) LIC(I)=MODIAL
      IF(MODIAL.EQ.0) GO TO 3
    1 CONTINUE
    3 IF(IPRIME.EQ.2) RETURN
      DO 2 I=1,M
      IP=KP+ICP(I) £ IR=KR+ICR(I) £ IS=KS+ICS(I)
      MODIAL=IALMOD(IP,IR,IS,JP,JR,JS)
      IF(LIC(I).NE.0) LIC(I)=MODIAL
      IF(MODIAL.EQ.0) GO TO 4
    2 CONTINUE
    4 RETURN
      END
```

```
      FUNCTION IALMOD(IP,IR,IS,JP,JR,JS)
C...THE FUNCTION IALMOD TAKES THE VALUE 0 IF JP*Y+JR*X+JS DIVIDES
C...IP*Y+IR*X+IS. OTHERWISE IT TAKES THE VALUE 1.
      DOUBLE IP,IR,IS,JP,JR,JS,ID,JD,LP,LR,LS,LD
      IALMOD=0
      ID=1.D0 £ JD=1.D0
      CALL DIVCD(IP,IR,IS,ID,JP,JR,JS,JD,LP,LR,LS,LD)
      IF(LD.NE.1.D0) IALMOD=1
      RETURN
      END
```

```
      SUBROUTINE DIVC(L1,M1,N1,L2,M2,N2,L,M,N)
C...THE SUBROUTINE DIVC FINDS THE QUOTIENT OF THE TWO ALGEBRAIC NUMBERS
C...L1*Y+M1*X+N1 AND L2*Y+M2*X+N2 IN THE CUBIC FIELD WITH INTEGRAL
C...BASIS (1,X,Y), WHERE X**3-IA*X**2+IB*X-IC=0, AND SETS THIS QUOTIENT
C...TO L*Y+M*X+N.
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D15/IURN,IOB,IOBDS
      KDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)=I1*J2*K3+I2*J3*K1+I3*J1*K2
     1-I1*J3*K2-I2*J1*K3-I3*J2*K1
C...FIRST TEST FOR THE POSSIBILITY OF OVERFLOW.
      LA=IABS(L1) £ MA=IABS(M1) £ NA=IABS(N1)
      IDIV1=MAX0(LA,MA,NA)
      LA=IABS(L2) £ MA=IABS(M2) £ NA=IABS(N2)
      IDIV2=MAX0(LA,MA,NA)
      IF(IDIV1.GT.IDIV2) GO TO 1
      IDIV=IDIV2*IDIV2*IDIV2
      GO TO 2
    1 IDIV=IDIV1*IDIV2*IDIV2
    2 IF(IDIV.LT.IOBDS) GO TO 3
      PRINT 50
   50 FORMAT(1X,10(1H*),26HDANGER OF OVERFLOW IN DIVC,10(1H*))
    3 I1=L2*IL1+IP1*M2+N2
      I2=L2*IL2+IP2*M2
      I3=L2*IL3+IP3*M2
      J1=IP1*L2+M2*IT1
      J2=IP2*L2+M2*IT2+N2
      J3=IP3*L2+M2*IT3
      K1=L2 £ K2=M2 £ K3=N2
      JDET=KDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)
      L=KDET(L1,M1,N1,J1,J2,J3,K1,K2,K3)/JDET
      M=KDET(I1,I2,I3,L1,M1,N1,K1,K2,K3)/JDET
      N=KDET(I1,I2,I3,J1,J2,J3,L1,M1,N1)/JDET
      RETURN
      END
```

```
      SUBROUTINE MULTC(L1,M1,N1,L2,M2,N2,L,M,N)
C...THE SUBROUTINE MULTC FINDS THE PRODUCT OF THE TWO ALGEBRAIC NUMBERS
C...L1*Y+M1*X+N1 AND L2*Y+M2*X+N2 IN THE CUBIC FIELD WITH INTEGRAL
C...BASIS (1,X,Y), WHERE X**3-IA*X**2+IB*X-IC=0, AND SETS THIS PRODUCT
C...TO L*Y+M*X+N.
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D15/IUBN,IOB,IOBDS
C...FIRST TEST FOR THE POSSIBILITY OF OVERFLOW.
      LA=IABS(L1) £ MA=IABS(M1) £ NA=IABS(N1)
      MULT1=MAX0(LA,MA,NA)
      LA=IABS(L2) £ MA=IABS(M2) £ NA=IABS(N2)
      MULT2=MAX0(LA,MA,NA)
      MULT=MULT1*MULT2
      IF(MULT.LT.IOB) GO TO 1
      PRINT 50
   50 FORMAT(1X,10(1H*),27HDANGER OF OVERFLOW IN MULTC,10(1H*))
    1 IP=L1*M2+L2*M1
      L=L1*L2*IL1+IP*IP1+M1*M2*IT1+L1*N2+N1*L2
      M=L1*L2*IL2+IP*IP2+M1*M2*IT2+M1*N2+N1*M2
      N=L1*L2*IL3+IP*IP3+M1*M2*IT3+N1*N2
      RETURN
      END
```

```
      DOUBLE FUNCTION DNORM(IP,IR,IS)
C...DNORM(IP,IR,IS)=NORM(IP*Y+IR*X+IS).
      DOUBLE IP,IR,IS,P,R,S,AD,BD,CD,DEX,DEX3,DIUBN,DT2,DT3
      DOUBLE PA,RA,SA
      COMMON/D1/IA,IB,IC,INDEX,IDET
      COMMON/D2/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D15/IUBN,IOB,IOBDS
      AD=IA £ BD=IB £ CD=IC £ DEX=INDEX
      DEX3=DEX*DEX*DEX
      DIUBN=IUBN £ DT2=IT2 £ DT3=IT3
C...NOW FIND P,R,S SUCH THAT (P*X**2+R*X+S)/INDEX=IP*Y+IR*X+IS.
      P=IP
      R=IR*DEX-DT2*IP
      S=IS*DEX-DT3*IP
C...IF ANY OF P,R,S ARE SO LARGE THAT THEY MAY CAUSE 'OVERFLOW' IN THE
C...CALCULATION OF DNORM THEN PRINT A DIAGNOSTIC.
      PA=DABS(P) £ RA=DABS(R) £ SA=DABS(S)
      IF(PA.GE.DIUBN) GO TO 1
      IF(RA.GE.DIUBN) GO TO 1
      IF(SA.LT.DIUBN) GO TO 2
    1 PRINT 100
  100 FORMAT(/,1X,10(1H*),48HDANGER OF OVERFLOW WHEN USING THE FUNCTION
     1DNORM,10(1H*))
    2 DNORM=(P*P*P*CD*CD+R*R*R*CD+S*S*S+P*P*(R*BD*CD+S*(BD*BD-2.0D0*AD*
     1CD))+R*R*(P*AD*CD+S*BD)+S*S*(P*(AD*AD-2.0D0*BD)+R*AD)+P*R*S*(AD*BD
     2-3.0D0*CD))/DEX3
    3 RETURN
      END
```

```
      DOUBLE FUNCTION FDET(I1,I2,I3,J1,J2,J3,K1,K2,K3)
      DOUBLE I1,I2,I3,J1,J2,J3,K1,K2,K3
      FDET=I1*J2*K3+I2*J3*K1+I3*J1*K2-I1*J3*K2-I2*J1*K3-I3*J2*K1
      RETURN
      END
```

THE PROGRAMS CUBOID, FCUB AND CUBX

SUBROUTINES - ALL LISTED IN THIS SECTION

```
      PROGRAM CUBOID(INPUT,OUTPUT,PUNCH)

      COMMON/D1/IA,IB,IC,INDEX,IDET/D2/R(3),U(3),H(3)
      COMMON/D3/PM(1000),PN(1000),PO(1000),KZ/D4/BK,CIN
      COMMON/D7/XL,XU,YL,YU,ZL,ZU,XE,YE,ZE
      COMMON/D8/IBC
      DIMENSION X(11),Y(11),Z(11),L(10,10,10)
      CNOM(CX,CY,CZ,DX,DY,DZ)=CX*DX+CY*DY+CZ*DZ

C...READ IN THE DETAILS OF THE FIELD AND FIND A BASIS.   THEN FIND THE
C...SMALLEST CUBOID CONTAINING THE FUNDAMENTAL REGION OF POINTS
C...(XC,YC,ZC) RELATIVE TO THE BASIS FOR WHICH -0.5≤XC≤0.5; -0.5≤YC≤0.5;
C...-0.5≤ZC≤0.5.
  111 FORMAT(I6,I2,3I5)
      READ 111,IDET,INDEX,IA,IB,IC
      CALL BASIS
      CALL BOUND(R,XL,XU)
      XE=XU-XL
      CALL BOUND(U,YL,YU)
      YE=YU-YL
      CALL BOUND(H,ZL,ZU)
      ZE=ZU-ZL
      XU=XE/2.0 £ XL=-XU
      YU=YE/2.0 £ YL=-YU
      ZU=ZE/2.0 £ ZL=-ZU
  116 FORMAT(/,2X,*THE SMALLEST CUBOID WITH EDGES PARALLEL TO THE CO-ORD
     1INATE AXES*,/,1X,*WHICH CONTAINS A FUNDAMENTAL REGION CONTAINS THO
     2SE POINTS (X,Y,Z) WHERE*,/,5X,*X IS BETWEEN*,F8.4,1X,*AND*,F8.4,/,
     35X,*Y IS BETWEEN*,F8.4,1X,*AND*,F8.4,/,5X,*Z IS BETWEEN*,F8.4,1X,
     4*AND*,F8.4)
      PRINT 116,XL,XU,YL,YU,ZL,ZU
C...THE SMALLEST CUBOID CONTAINING THE FUNDAMENTAL REGION IS GIVEN BY
C...XL≤X≤XU, YL≤Y≤YU, ZL≤Z≤ZU.

C...READ IN THE DETAILS OF THE SUB-DIVISION.
C...FIND THE SUITABLE INTEGER POINTS WITH COEFFICIENTS LESS THAN IBC.
C...INITIALIZE THE MARKER ARRAY L, SETTING L(I,J,K) TO 2 FOR THOSE
C...SUB-REGIONS OF THE CUBOID WHICH DO NOT INTERSECT THE FUNDAMENTAL
C...REGION AND TO 1 OTHERWISE.
  112 FORMAT(F7.4)
      READ 112,BK
      READ 112,AM
      CIN=.1000
  119 FORMAT(I5)
      READ 119,IBC
      CALL USE
      READ 119,LIMIT
      DO 12 I=1,10
      DO 12 J=1,10
      DO 12 K=6,10
```

```
   12 L(I,J,K)=1
      DO 13 I=1,11
      FI=FLOAT(I-1) £ RX=FI*CIN
      X(I)=XL+RX*XE £ Y(I)=YL+RX*YE £ Z(I)=ZL+RX*ZE
   13 CONTINUE
      BDET=R(1)*U(2)*H(3)+R(2)*U(3)*H(1)+R(3)*U(1)*H(2)-R(1)*U(3)*H(2)
     1-R(2)*U(1)*H(3)-R(3)*U(2)*H(1)
      X12=(U(1)*H(2)-U(2)*H(1))/BDET
      X23=(U(2)*H(3)-U(3)*H(2))/BDET
      X31=(U(3)*H(1)-U(1)*H(3))/BDET
      Y12=(H(1)*R(2)-H(2)*R(1))/BDET
      Y23=(H(2)*R(3)-H(3)*R(2))/BDET
      Y31=(H(3)*R(1)-H(1)*R(3))/BDET
      Z12=(R(1)*U(2)-R(2)*U(1))/BDET
      Z23=(R(2)*U(3)-R(3)*U(2))/BDET
      Z31=(R(3)*U(1)-R(1)*U(3))/BDET
      DO 35 I=1,10
      DO 25 J=1,10
      DO 15 K=6,10
      DO 36 I1=1,2
      DO 26 J1=1,2
      DO 16 K1=1,2
      I2=I+I1-1 £ J2=J+J1-1 £ K2=K+K1-1
      XC=CNOM(X(I2),Y(J2),Z(K2),X23,Y23,Z23)
      YC=CNOM(X(I2),Y(J2),Z(K2),X31,Y31,Z31)
      ZC=CNOM(X(I2),Y(J2),Z(K2),X12,Y12,Z12)
      IF((ABS(XC).LE.0.5).AND.(ABS(YC).LE.0.5).AND.(ABS(ZC).LE.0.5))
     1GO TO 15
   16 CONTINUE
   26 CONTINUE
   36 CONTINUE
      L(I,J,K)=2
   15 CONTINUE
   25 CONTINUE
   35 CONTINUE

C...NOW FIND WHICH REGIONS ARE LEFT UNCOVERED.  BY ALTERATION OF BK,
C...IF NECESSARY, REDUCE THE NUMBER OF UNCOVERED REGIONS TO LESS THAN
C...LIMIT.
  118 FORMAT(/,1X,*BK=*,F7.4)
    8 PRINT 118,BK
      CALL COVER(X,Y,Z,L,ICOUNT)
      PRINT 113,ICOUNT
  113 FORMAT(1X,*THERE ARE NOW*,I5,1X,*UNCOVERED REGIONS*)
      IF(ICOUNT.GT.LIMIT) GO TO 19
      IF(ICOUNT.EQ.0) GO TO 3
  201 FORMAT(I6)
      PUNCH 201,IDET
  101 FORMAT(1X,*THESE HAVE VERTICES:*)
      PRINT 101
```

```
      DO 17 I=1,10
      DO 17 J=1,10
      DO 17 K=6,10
      IF(L(I,J,K).NE.1) GO TO 17
  102 FORMAT(2X,3F15.10)
      PRINT 102,X(I),Y(J),Z(K)
  202 FORMAT(3F15.10)
      PUNCH 202,X(I),Y(J),Z(K)
   17 CONTINUE
      GO TO 3
   19 IF(ICOUNT.LE.100) GO TO 9
      AN=AM £ GO TO 11
    9 AN=0.1*AM
   11 BK=BK+CIN*AN £ GO TO 8
    3 STOP
      END
```

```
      PROGRAM FCUB(INPUT,OUTPUT,PUNCH)
      COMMON/D1/IA,IB,IC,INDEX,IDET/D2/R(3),U(3),H(3)
      COMMON/D3/PM(1000),PN(1000),PO(1000),KZ/D4/BK,CIN
      COMMON/D7/XL,XU,YL,YU,ZL,ZU,XE,YE,ZE
      COMMON/D8/IBC
      DIMENSION X(11),Y(11),Z(11),L(10,10,10)
      CNOM(CX,CY,CZ,DX,DY,DZ)=CX*DX+CY*DY+CZ*DZ
C...READ IN THE DETAILS OF THE FIELD AND FIND A BASIS.   THEN FIND THE
C...SMALLEST CUBOID CONTAINING THE FUNDAMENTAL REGION OF POINTS
C...(XC,YC,ZC) RELATIVE TO THE BASIS FOR WHICH -0.5≤XC≤0.5:
C...-0.5≤YC≤0.5: -0.5≤ZC≤0.5.
  111 FORMAT(I6,I2,3I5)
      READ 111,IDET,INDEX,IA,IB,IC
      CALL BASIS
      CALL BOUND(R,XL,XU)
      XE=XU-XL
      CALL BOUND(U,YL,YU)
      YE=YU-YL
      CALL BOUND(H,ZL,ZU)
      ZE=ZU-ZL
      XU=XE/2.0 £ XL=-XU
      YU=YE/2.0 £ YL=-YU
      ZU=ZE/2.0 £ ZL=-ZU
C...READ THE DETAILS OF THE SUBDIVISION AND FIND THE SUITABLE
C...INTEGER POINTS.  THEN READ IN THE NUMBER OF REGIONS WHICH ARE
C...TO BE CONSIDERED.
  112 FORMAT(F7.4)
      READ 112,BK
      READ 112,CIN
  119 FORMAT(I5)
      READ 119,IBC
      CALL USE
      READ 119,LIMIT
      READ 119,M
      DO 3 ICT=1,M
C...NOW WORK THROUGH EACH REGION IN TURN.   FIRST INITIALIZE THE MARKER
C. ..ARRAY L, SETTING L(I,J,K) TO 2 FOR THOSE SUBREGIONS OF THE
C...CUBOID WHICH DO NOT INTERSECT THE FUNDAMENTAL REGION AND TO 1 OTHERWISE.
  120 FORMAT(3F15.10)
      READ 120,XB,YB,ZB
  121 FORMAT(/,1X,*THE REGION BEING SUBDIVIDED HAS VERTEX*,/,1X,3F15.10)
      PRINT 121,XB,YB,ZB
      DO 13 I=1,11
      FI=FLOAT(I-1) £ RX=FI*CIN
      X(I)=XB+RX*XE £ Y(I)=YB+RX*YE £ Z(I)=ZB+RX*ZE
   13 CONTINUE
```

```
      DO 12 I=1,10
      DO 12 J=1,10
      DO 12 K=1,10
   12 L(I,J,K)=1
      BDET=R(1)*U(2)*H(3)+R(2)*U(3)*H(1)+R(3)*U(1)*H(2)-R(1)*U(3)*H(2)
     1-R(2)*U(1)*H(3)-R(3)*U(2)*H(1)
      X12=(U(1)*H(2)-U(2)*H(1))/BDET
      X23=(U(2)*H(3)-U(3)*H(2))/BDET
      X31=(U(3)*H(1)-U(1)*H(3))/BDET
      Y12=(H(1)*R(2)-H(2)*R(1))/BDET
      Y23=(H(2)*R(3)-H(3)*R(2))/BDET
      Y31=(H(3)*R(1)-H(1)*R(3))/BDET
      Z12=(R(1)*U(2)-R(2)*U(1))/BDET
      Z23=(R(2)*U(3)-R(3)*U(2))/BDET
      Z31=(R(3)*U(1)-R(1)*U(3))/BDET
      DO 41 I=1,10
      DO 31 J=1,10
      DO 21 K=1,10
      DO 42 I1=1,2
      DO 32 J1=1,2
      DO 22 K1=1,2
      I2=I+I1-1 £ J2=J+J1-1 £ K2=K+K1-1
      XC=CNOM(X(I2),Y(J2),Z(K2),X23,Y23,Z23)
      YC=CNOM(X(I2),Y(J2),Z(K2),X31,Y31,Z31)
      ZC=CNOM(X(I2),Y(J2),Z(K2),X12,Y12,Z12)
      IF((ABS(XC).LE.0.5).AND.(ABS(YC). LE.0.5).AND.(ABS(ZC).LE.0.5))
     1GO TO 21
   22 CONTINUE
   32 CONTINUE
   42 CONTINUE
      L(I,J,K)=2
   21 CONTINUE
   31 CONTINUE
   41 CONTINUE

C...NOW FIND WHICH SUB-REGIONS ARE LEFT UNCOVERED WITH THE GIVEN VALUE
C...OF BK.   IF THIS NUMBER IS LESS THAN OR EQUAL TO LIMIT THEN PRINT
C...OUT THE VERTICES OF THE UNCOVERED REGIONS.
      CALL COVER(X,Y,Z,L,ICOUNT)
  113 FORMAT(1X,*IT CONTAINS*,I5,1X,*UNCOVERED REGIONS*)
      PRINT 113,ICOUNT
      IF(ICOUNT.EQ.0) GO TO 3
      IF(ICOUNT.GT.LIMIT) GO TO 3
  101 FORMAT(1X,*THESE HAVE VERTICES*)
      PRINT 101
  201 FORMAT(I6)
      PUNCH 201,IDET
      DO 17 I=1,10
      DO 17 J=1,10
      DO 17 K=1,10
```

```
      IF(L(I,J,K).NE.1) GO TO 17
  102 FORMAT(2X,3F15.10)
      PRINT 102,X(I),Y(J),Z(K)
      PUNCH 120,X(I),Y(J),Z(K)
   17 CONTINUE
    3 CONTINUE
      STOP
      END
```

```
      PROGRAM CUBX(INPUT,OUTPUT,PUNCH)
      COMMON/D1/IA,IB,IC,INDEX,IDET/D2/R(3),U(3),H(3)
      COMMON/D3/PM(1000),PN(1000),PO(1000),KZ/D4/BK,CIN
      COMMON/D7/XL,XU,YL,YU,ZL,ZU,XE,YE,ZE
      COMMON/D8/IBC
      DIMENSION X(11),Y(11),Z(11),L(10,10,10)
      CNOM(CX,CY,CZ,DX,DY,DZ)=CX*DX+CY*DY+CZ*DZ

C...READ IN THE DETAILS OF THE FIELD AND FIND A BASIS.   THEN FIND THE
C...SMALLEST CUBOID CONTAINING THE FUNDAMENTAL REGION OF POINTS
C...(XC,YC,ZC) RELATIVE TO THE BASIS FOR WHICH -0.5≤XC≤0.5;
C...-0.5≤YC≤0.5; -0.5≤ZC≤0.5.
  111 FORMAT(I6,I2,3I5)
      READ 111,IDET,INDEX,IA,IB,IC
      CALL BASIS
      CALL BOUND(R,XL,XU)
      XE=XU-XL
      CALL BOUND(U,YL,YU)
      YE=YU-YL
      CALL BOUND(H,ZL,ZU)
      ZE=ZU-ZL
      XU=XE/2.0 £ XL=-XU
      YU=YE/2.0 £ YL=-YU
      ZU=ZE/2.0 £ ZL=-ZU

C...READ IN THE DETAILS OF THE SUBDIVISION AND FIND THE SUITABLE
C...INTEGER POINTS.  THEN READ IN THE NUMBER OF REGIONS WHICH ARE
C...TO BE CONSIDERED.
  112 FORMAT(F7.4)
      READ 112,BK
      READ 112,CIN
  119 FORMAT(I5)
      READ 119,IBC
      CALL USE
      READ 119,M

      DO 3 ICT=1,M
C...NOW WORK THROUGH EACH REGION IN TURN.   FIRST INITIALIZE THE MARKER
C...ARRAY L, SETTING L(I,J,K) TO 2 FOR THOSE SUBREGIONS OF THE
C...CUBOID WHICH DO NOT INTERSECT THE FUNDAMENTAL REGION AND TO 1 OTHERWISE.
  120 FORMAT(3F15.10)
      READ 120,XB,YB,ZB
  121 FORMAT(/,1X,*THE REGION BEING SUBDIVIDED HAS VERTEX*,/,1X,3F15.10)
      PRINT 121,XB,YB,ZB
      DO 13 I=1,11
      FI=FLOAT(I-1) £ RX=FI*CIN
      X(I)=XB+RX*XE £ Y(I)=YB+RX*YE £ Z(I)=ZB+RX*ZE
   13 CONTINUE
      DO 12 I=1,10
```

```
      DO 12 J=1,10
      DO 12 K=1,10
   12 L(I,J,K)=1
      BDET=R(1)*U(2)*H(3)+R(2)*U(3)*H(1)+R(3)*U(1)*H(2)-R(1)*U(3)*H(2)
     1-R(2)*U(1)*H(3)-R(3)*U(2)*H(1)
      X12=(U(1)*H(2)-U(2)*H(1))/BDET
      X23=(U(2)*H(3)-U(3)*H(2))/BDET
      X31=(U(3)*H(1)-U(1)*H(3))/BDET
      Y12=(H(1)*R(2)-H(2)*R(1))/BDET
      Y23=(H(2)*R(3)-H(3)*R(2))/BDET
      Y31=(H(3)*R(1)-H(1)*R(3))/BDET
      Z12=(R(1)*U(2)-R(2)*U(1))/BDET
      Z23=(R(2)*U(3)-R(3)*U(2))/BDET
      Z31=(R(3)*U(1)-R(1)*U(3))/BDET
      DO 41 I=1,10
      DO 31 J=1,10
      DO 21 K=1,10
      DO 42 I1=1,2
      DO 32 J1=1,2
      DO 22 K1=1,2
      I2=I+I1-1 £ J2=J+J1-1 £ K2=K+K1-1
      XC=CNOM(X(I2),Y(J2),Z(K2),X23,Y23,Z23)
      YC=CNOM(X(I2),Y(J2),Z(K2),X31,Y31,Z31)
      ZC=CNOM(X(I2),Y(J2),Z(K2),X12,Y12,Z12)
      IF(ABS(XC).GT.0.5) GO TO 22
      IF(ABS(YC).GT.0.5) GO TO 22
      IF(ABS(ZC).LE.0.5) GO TO 21
   22 CONTINUE
   32 CONTINUE
   42 CONTINUE
      L(I,J,K)=2
   21 CONTINUE
   31 CONTINUE
   41 CONTINUE

C...NOW FIND WHICH SUB-REGIONS ARE LEFT UNCOVERED WITH THE GIVEN VALUE
C...OF BK.   IF THIS NUMBER IS LESS THAN OR EQUAL TO LIMIT THEN PRINT
C...BOUNDS FOR THE REGION CONTAINING THE UNCOVERED REGIONS.
      CALL COVER(X,Y,Z,L,ICOUNT)
  113 FORMAT(1X,*IT CONTAINS*,I5,1X,*UNCOVERED REGIONS*)
      PRINT 113,ICOUNT
      IF(ICOUNT.EQ.0) GO TO 3
  101 FORMAT(1X,*THESE HAVE VERTICES BETWEEN*)
      PRINT 101
  201 FORMAT(I6)
      PUNCH 201,IDET
      XLW=10.0 £ XUP=-10.0
      YLW=10.0 £ YUP=-10.0
      ZLW=10.0 £ ZUP=-10.0
      DO 17 I=1,10
```

```
      DO 17 J=1,10
      DO 17 K=1,10
      IF(L(I,J,K).NE.1) GO TO 17
      IF(X(I).LT.XLW) XLW=X(I)
      IF(X(I).GT.XUP) XUP=X(I)
      IF(Y(J).LT.YLW) YLW=Y(J)
      IF(Y(J).GT.YUP) YUP=Y(J)
      IF(Z(K).LT.ZLW) ZLW=Z(K)
      IF(Z(K).GT.ZUP) ZUP=Z(K)
   17 CONTINUE
  901 FORMAT(/,5X,A2,2F15.10)
      AX=2HX: £ AY=2HY: £ AZ=2HZ:
      PRINT 901,AX,XLW,XUP
      PRINT 901,AY,YLW,YUP
      PRINT 901,AZ,ZLW,ZUP
      XUP=XUP+CIN*XE £ YUP=YUP+CIN*YE £ ZUP=ZUP+CIN*ZE
  904 FORMAT(/,* GIVING LOWER AND UPPER BOUNDS RESPECTIVELY ON X,Y,Z:*)
      PRINT 904
  902 FORMAT(5X,3F15.10)
      PRINT 902,XLW,YLW,ZLW
      PRINT 902,XUP,YUP,ZUP
  903 FORMAT(3F15.10)
      PUNCH 903,XLW,YLW,ZLW
      PUNCH 903,XUP,YUP,ZUP
    3 CONTINUE
      STOP
      END
```

```
      SUBROUTINE BASIS

      COMMON/D1/IA,IB,IC,INDEX,IDET/D2/R(3),U(3),H(3)
      A=FLOAT(IA) £ B=FLOAT(IB) £ C=FLOAT(IC) £ IN=INDEX
C...FIND H(2) WHERE THE FIELD IS K(H(2)) AND ALSO R(2) AND U(2) WHERE
C...R(2)+I.U(2) AND R(2)-I.U(2) ARE THE CONJUGATES OF H(2).
      V1=-(B-(A**2)/3.0)/3.0
      V2=-(A*B/3.0-2.0*A**3/27.0-C)
      V3=SQRT(V2**2-4.0*V1**3)
      V4=(V2+V3)/2.0
      V5=(V2-V3)/2.0
      IF(V4.NE.0.0) GO TO 51
      V6=0.0 £ GO TO 52
   51 D=1.0
      IF(V4.GE.0.0) GO TO 53
      V4=-V4 £ D=-1.0
   53 V6=EXP((ALOG(V4))/3.0)*D
   52 IF(V5.NE.0.0) GO TO 54
      V7=0.0 £ GO TO 55
   54 D=1.0
      IF(V5.GE.0.0) GO TO 56
      V5=-V5 £ D=-1.0
   56 V7=EXP((ALOG(V5))/3.0)*D
   55 H(2)=V6+V7+A/3.0
      R(2)=(A-H(2))/2.0
      U(2)=SQRT(C/H(2)-R(2)**2)
      H(1)=1.0 £ R(1)=1.0 £ U(1)=0.0
C...(R(1),U(1),H(1))=(1,0,1) IS THE LATTICE POINT CORRESPONDING TO UNITY

C...FIND T AND S WHERE Y=(H(2)↑2+T.H(2)+S)/INDEX IS SUCH THAT
C...(1,H(2),Y) IS A BASIS OF THE FIELD.
      IF(INDEX.NE.1) GO TO 57
      T=0.0 £ S=0.0 £ GO TO 58
   57 K1=IA**2-2*IB £ K4=IB**2-2*IA*IC £ K5=IA*IB-3*IC
      IN2=IN**2 £ IN3=IN2*IN
      DO 59 ITC=1,IN
      IT=ITC-1
      DO 60 ISC=1,IN
      IS=ISC-1
      JA=K1+IT*IA+3*IS
      IF(MOD(JA,IN).NE.0) GO TO 60
      JB=K4+IT**2*IB+3*IS**2+IT*K5+2*IS*K1+2*IS*IT*IA
      IF(MOD(JB,IN2).NE.0) GO TO 60
      JC=IS**3+IT**3*IC+IC**2+IS**2*IT*IA+IS*K4+IS*IT**2*IB+IT*IB*IC
     1+IT**2*IA*IC+IS**2*K1+IS*IT*K5
      IF(MOD(JC,IN3).NE.0) GO TO 60
      T=FLOAT(IT) £ S=FLOAT(IS) £ GO TO 58
   60 CONTINUE
   59 CONTINUE
   58 XIN=FLOAT(INDEX)
```

```
      H(3)=(H(2)**2+T*H(2)+S)/XIN
      R(3)=(R(2)**2-U(2)**2+T*R(2)+S)/XIN
      U(3)=(2.0*R(2)*U(2)+T*U(2))/XIN
C...R(3)+I.U(3) AND R(3)-I.U(3) ARE THE CONJUGATES OF H(3).
      IDETM=-IDET
      PRINT 501,IDETM,INDEX,IA,IB,IC,H(2),T,S,H(3)
  501 FORMAT(1H1,1X,*THE FIELD HAS DISCRIMINANT*,I7,* INDEX*,I4,/,1X,*AN
     1D POLYNOMIAL COEFFICIENTS A=*,I4,* B=*,I4,* C=*,I4,//,2X,*A BASIS
     2FOR THIS FIELD IS (1,H,L), L=(H.H+T.H+S)/INDEX,*,/,1X,*WHERE H=*,
     3F7.4,* T=*,F6.1,* S=*,F6.1,* AND L=*,F7.4)

C...FROM THE BASIS FOUND ABOVE FIND ANOTHER SUCH THAT THE FUNDAMENTAL
C...REGION IS 'ALMOST RECTANGULAR'.
      ID=1
      IF((R(2)+H(2)).LT.0.0) ID=-1
      IAK=IFIX(R(2)+H(2))
      IF(MOD(IAK,2).NE.0) IAK=IAK+ID
      AK=FLOAT(IAK)/2.0
      A1=R(3)+H(3) £ B1=R(2)+H(2) £ C1=2.0
      A2=R(3)*(R(2)-AK)+U(2)*U(3)+H(3)*(H(2)-AK)
      B2=R(2)*(R(2)-AK)+U(2)*U(2)+H(2)*(H(2)-AK)
      C2=R(2)+H(2)-2.0*AK
      DET=B1*C2-B2*C1
      P=(A1*C2-A2*C1)/DET
      Q=(B1*A2-B2*A1)/DET
      DP=DQ=1.0
      IF(P.LT.0.0) DP=-1.0
      IF(Q.LT.0.0) DQ=-1.0
      IP=IFIX(P) £ AP=FLOAT(IP)
      IF(ABS(P-AP).GT.0.5) AP=AP+DP
      IQ=IFIX(Q) £ AQ=FLOAT(IQ)
      IF(ABS(Q-AQ).GT.0.5) AQ=AQ+DQ
      R(3)=R(3)-AP*R(2)-AQ
      U(3)=U(3)-AP*U(2)
      H(3)=H(3)-AP*H(2)-AQ
      R(2)=R(2)-AK
      H(2)=H(2)-AK
  502 FORMAT(/,2X,*THE NEW BASIS IS 1,H-AK,L-AP.H-AQ WHERE AK=*,F6.1,
     1* AP=*,F6.1,* AQ=*,F6.1)
      PRINT 502,AK,AP,AQ
  503 FORMAT(1X,*THUS GIVING THE BASIS FOR THE LATTICE OF INTEGERS*)
      PRINT 503
  504 FORMAT(1X,3F15.10)
      DO 61 I=1,3
   61 PRINT 504,R(I),U(I),H(I)
      RETURN
      END
```

```
      SUBROUTINE USE
      COMMON/D2/R(3),U(3),H(3)/D3/PM(1000),PN(1000),PO(1000),KZ
      COMMON/D4/BK,CIN/D7/XL,XU,YL,YU,ZL,ZU,XE,YE,ZE
      COMMON/D8/IBC
C...FIND THE BOUNDS ON THE CARTESIAN CO-ORDINATES OF 'SUITABLE'
C...INTEGER POINTS.
      XYM=AMAX1(XE,YE)
      SQT1=SQRT(2.0*BK/(CIN*ZE))
      SQT2=4.0*BK/((CIN*XYM)**2)
      A1=XL-SQT1 £ A2=XU+SQT1
      B1=YL-SQT1 £ B2=YU+SQT1
      C1=ZL-SQT2 £ C2=ZU+SQT2
C...WORK THROUGH ALL THE INTEGER POINTS WITH COEFFICIENTS LESS THAB IBC
C...IN ABSOLUTE VALUE.  STARTING WITH THOSE 'NEAREST' TO THE
C...FUNDAMENTAL REGION.
      KZ=0
      IBCT=3*IBC+1 £ IBCP=IBC+1
      DO 35 ISIG=1,IBCT
      IMU=MIN0(ISIG,IBCP)
      DO 31 IM21=1,IMU
      IM2=IM21-1
      INU=MIN0((ISIG-IM2),IBCP)
      DO 30 IN21=1,INU
      IN2=IN21-1
      IO2=ISIG-(IM2+IN2+1)
      IF(IO2.GT.IBC) GO TO 30
      DO 41 IMT=1,2
      IMM=1
      IF(IMT.EQ.2) IMM=-1
      DO 42 INT=1,2
      INN=1
      IF(INT.EQ.2) INN=-1
      DO 37 IOT=1,2
      IOO=1
      IF(IOT.EQ.2) IOO=-1
      IM1=IMM*IM2 £ IN1=INN*IN2 £ IO1=IOO*IO2
      RM=FLOAT(IM1) £ RN=FLOAT(IN1) £ RO=FLOAT(IO1)
      IF(KZ.EQ.0) GO TO 36
C...TEST TO SEE THAT THIS INTEGER IS NOT ALREADY IN THE LIST,  WHICH
C...MAY HAPPEN WHEN ONE OF THE COEFFICIENTS IS ZERO.
      IZ2=MAX0(1,(KZ-8))
      DO 39 JZ=IZ2,KZ
      IF((RM.EQ.PM(JZ)).AND.(RN.EQ.PN(JZ)).AND.(RO.EQ.PO(JZ))) GO TO 37
   39 CONTINUE
C...TEST TO FIND WHETHER THE INTEGER IS 'SUITABLE'
   36 RJ=CI(RM,RN,RO,R) £ UJ=CI(RM,RN,RO,U) £ HJ=CI(RM,RN,RO,H)
      IF(RJ.LT.(XL-0.1)) GO TO 34 £ IF(RJ.GT.(XU+0.1)) GO TO 34
   32 IF(UJ.LT.(YL-0.1)) GO TO 34 £ IF(UJ.GT.(YU+0.1)) GO TO 34
```

```
      IF(HJ.LT.C1) GO TO 34 £ IF(HJ.LT.C2) GO TO 33
   34 IF(HJ.LT.(ZL-0.1)) GO TO 37 £ IF(HJ.GT.(ZU+0.1)) GO TO 37
      IF(RJ.LT.A1) GO TO 37 £ IF(RJ.GT.A2) GO TO 37
      IF(UJ.LT.B1) GO TO 37 £ IF(UJ.GT.B2) GO TO 37
   33 KZ=KZ+1 £ PM(KZ)=RM £ PN(KZ)=RN £ PO(KZ)=RO
C...TEST WHETHER THE ARRAYS HOLDING THE INTEGERS ARE 'FULL'.
      IF(KZ.GE.1000) GO TO 40
   37 CONTINUE
   42 CONTINUE
   41 CONTINUE
   30 CONTINUE
   31 CONTINUE
   35 CONTINUE
  302 FORMAT(/,2X,*FOR DISSECTING THE FUNDAMENTAL REGION INTO (1/CIN)↑3
     1SUB-REGIONS WHERE CIN=*,F7.4,/,1X,*AND TAKING THE VALUE OF BK TO B
     2E*,F7.4,*, THEN*,I5,* INTEGER POINTS ARE USED*)
   40 PRINT 302,CIN,BK,KZ
      RETURN
      END
```

```
      SUBROUTINE BOUND(R,AL,AU)

C...AL IS THE MINIMUM OF THE EIGHT 'R' CO-ORDINATES AND AU IS THE
C...MAXIMUM.
      DIMENSION R(3)
      ZERO=0.0
      ARG1=R(1)+R(2) £ ARG2=R(2)+R(3) £ ARG3=R(3)+R(1)
      ARG4=R(1)+R(2)+R(3)
      AL=AMIN1(ZERO,R(1),R(2),R(3),ARG1,ARG2,ARG3,ARG4)
      AU=AMAX1(ZERO,R(1),R(2),R(3),ARG1,ARG2,ARG3,ARG4)
      RETURN
      END
```

```
      SUBROUTINE COVER(X,Y,Z,L,ICOUNT)
      COMMON/D2/R(3),U(3),H(3)/D3/PM(1000),PN(1000),PO(1000),KZ
      COMMON/D4/BK,CIN
      DIMENSION X(11),Y(11),Z(11),L(10,10,10)
C...FOR EACH INTEGER SET THE L MARKERS OF THE REGIONS WHICH IT COVERS
C...TO ZERO AND COUNT THE NUMBER OF REMAINING UNCOVERED REGIONS.
      DO 13 IE=1,KZ
      PX=CI(PM(IE),PN(IE),PO(IE),R)
      PY=CI(PM(IE),PN(IE),PO(IE),U)
      PZ=CI(PM(IE),PN(IE),PO(IE),H)
      ICOUNT=0
      DO 20 I=1,10
      DO 19 J=1,10
      DO 18 K=6,10
      IF(L(I,J,K).NE.1) GO TO 18
      XD=AMAX1(ABS(X(I)-PX),ABS(X(I+1)-PX))
      YD=AMAX1(ABS(Y(J)-PY),ABS(Y(J+1)-PY))
      ZD=AMAX1(ABS(Z(K)-PZ),ABS(Z(K+1)-PZ))
      TD=ZD*(XD**2+YD**2)
      IF(TD.LT.BK) GO TO 12
      ICOUNT=ICOUNT+1 £ GO TO 18
   12 L(I,J,K)=0
   18 CONTINUE
   19 CONTINUE
   20 CONTINUE
C...IF ALL THE REGIONS ARE NOW COVERED RETURN TO THE MAIN PROGRAM.
      IF(ICOUNT.EQ.0) GO TO 15
   13 CONTINUE
   15 RETURN
      END
```

```
      FUNCTION CI(X,Y,Z,R)
C...THIS GIVES THE 'R' CO-ORDINATE OF THE POINT WITH COEFFICIENTS (X,Y,Z)
      DIMENSION R(3)
      CI=X*R(1)+Y*R(2)+Z*R(3)
      RETURN
      END
```

```
      SUBROUTINE COVER(X,Y,Z,L,ICOUNT)

      COMMON/D2/R(3),U(3),H(3)/D3/PM(1000),PN(1000),PO(1000),KZ
      COMMON/D4/BK,CIN
      DIMENSION X(11),Y(11),Z(11),L(10,10,10)
C...FOR EACH INTEGER SET THE L MARKERS OF THE REGIONS WHICH IT COVERS
C...TO ZERO AND COUNT THE NUMBER OF REMAINING UNCOVERED REGIONS.
      DO 13 IE=1,KZ
      PX=CI(PM(IE),PN(IE),PO(IE),R)
      PY=CI(PM(IE),PN(IE),PO(IE),U)
      PZ=CI(PM(IE),PN(IE),PO(IE),H)
      ICOUNT=0
      DO 20 I=1,10
      DO 19 J=1,10
      DO 18 K=1,10
      IF(L(I,J,K).NE.1) GO TO 18
      XD=AMAX1(ABS(X(I)-PX),ABS(X(I+1)-PX))
      YD=AMAX1(ABS(Y(J)-PY),ABS(Y(J+1)-PY))
      ZD=AMAX1(ABS(Z(K)-PZ),ABS(Z(K+1)-PZ))
      TD=ZD*(XD**2+YD**2)
      IF(TD.LT.BK) GO TO 12
      ICOUNT=ICOUNT+1 £ GO TO 18
   12 L(I,J,K)=0
   18 CONTINUE
   19 CONTINUE
   20 CONTINUE
C...IF ALL THE REGIONS ARE NOW COVERED RETURN TO THE MAIN PROGRAM.
      IF(ICOUNT.EQ.0) GO TO 15
   13 CONTINUE
   15 RETURN
      END
```

THE PROGRAM TRANS

SUBROUTINES

IN THIS SECTION		IN PREVIOUS SECTION	
ADJ	81	BASIS	68
UPLW	82	CI	74
ROUNDI	83		
DCORR	84		

```
      PROGRAM TRANS(INPUT,OUTPUT)
C...THIS PROGRAM TRANSFORMS THE N UNCOVERED REGIONS AND DETERMINES THE
C...INTERSECTION OF THE TRANSFORMS WITH THE ORIGINAL REGIONS.
      COMMON/D1/IA,IB,IC,INDEX,IDET/D2/R(3),U(3),H(3)
      DIMENSION X(2,100),Y(2,100),Z(2,100)
C...(R(I),U(I),H(I)) I=1,3 IS A BASIS FOR THE LATTICE OF INTEGERS.
C...A MAXIMUM OF 100 UNCOVERED REGIONS MAY BE CONSIDERED WHERE THE ITH
C...REGION HAS LOWER LIMITS ON ITS CARTESIAN CO-ORDINATES
C...(X(1,I),Y(1,I),Z(1,I)) AND UPPER LIMITS (X(2,I),Y(2,I),Z(2,I)).
      CNOM(CX,CY,CZ,DX,DY,DZ)=CX*DX+CY*DY+CZ*DZ
C...THIS FUNCTION IS USED TO CALCULATE THE CO-ORDINATES OF A POINT
C...RELATIVE TO THE BASE WHEN ITS CARTESIAN CO-ORDINATES ARE KNOWN.
C...READ THE DETAILS OF THE FIELD.
      READ 100,IDET,INDEX,IA,IB,IC
  100 FORMAT(I6,I2,3I5)
      CALL BASIS
C...THE COEFFICIENTS OF THE FUNDAMENTAL UNIT RELATIVE TO THE BASIS
C...(H(1),H(2),H(3)) FOR THE FIELD ARE READ.
      READ 101,EXC,EYC,EZC
  101 FORMAT(3F15.10)
C...THE CARTESIAN THEN THE CYLINDRICAL POLAR CO-ORDINATES OF THE
C...FUNDAMENTAL UNIT ARE NOW CALCULATED.
      EX=CI(EXC,EYC,EZC,R)
      EY=CI(EXC,EYC,EZC,U)
      EZ=CI(EXC,EYC,EZC,H)
      ER=SQRT(EX*EX+EY*EY)
      EALP=ATAN2(EY,EX)
  112 FORMAT(/,47H THE UNIT HAS CO-ORDINATES RELATIVE TO THE BASE,
     13F15.10,/,23H CARTESIAN CO-ORDINATES,3F15.10,/,35H AND CYLINDRICAL
     2 POLAR CO-ORDINATES,3F15.10)
      PRINT 112,EXC,EYC,EZC,EX,EY,EZ,ER,EALP,EZ
C...READ N, THE NUMBER OF REGIONS TO BE CONSIDERED, THEN THE BOUNDS ON
C...THEIR CARTESIAN CO-ORDINATES.
      READ 102,N
  102 FORMAT(I5)
      DO 50 I=1,N
      DO 51 J=1,2
      READ 101,X(J,I),Y(J,I),Z(J,I)
      X(J,I)=DCORR(X(J,I),J)
      Y(J,I)=DCORR(Y(J,I),J)
      Z(J,I)=DCORR(Z(J,I),J)
   51 CONTINUE
   50 CONTINUE
      DET=FLOAT(IDET)
      BDET=SQRT(DET)/2.0
C...BDET IS THE DETERMINANT OF THE REAL LATTICE.  THE FOLLOWING NINE
C...VALUES ARE FOR USE IN CALCULATING COEFFICIENTS RELATIVE TO THE BASE
C...FROM CARTESIAN CO-ORDINATES.
      X12=ADJ(U,H,1,2)/BDET
      X23=ADJ(U,H,2,3)/BDET
```

```
      X31=ADJ(U,H,3,1)/BDET
      Y12=ADJ(H,R,1,2)/BDET
      Y23=ADJ(H,R,2,3)/BDET
      Y31=ADJ(H,R,3,1)/BDET
      Z12=ADJ(R,U,1,2)/BDET
      Z23=ADJ(R,U,2,3)/BDET
      Z31=ADJ(R,U,3,1)/BDET
C...READ M1,M2 WHERE REGIONS M1 UP TO M2 ARE TO BE CONSIDERED IN THIS
C...RUN.
      READ 102,M1
      READ 102,M2
  104 FORMAT(3H1 R,I3)
      DO 2 I=M1,M2
C...WORK THROUGH THE REGIONS ONE BY ONE.
      PRINT 104,I
C...FIRST FIND THE CYLINDRICAL POLAR CO-ORDINATES OF THE VERTICES OF THE
C...ITH REGION AND THEN THE CO-ORDINATES OF THE VERTICES OF THE TRANSFORM
      DO 4 II=1,2
      DO 5 JJ=1,2
      RA=SQRT(X(II,I)*X(II,I)+Y(JJ,I)*Y(JJ,I))
      ALP=ATAN2(Y(JJ,I),X(II,I))
      TRA=RA*ER
      TALP=ALP+EALP
      TX=TRA*COS(TALP)
      TY=TRA*SIN(TALP)
      DO 6 KK=1,2
      TZ=Z(KK,I)*EZ
C...NOW FIND THE CO-ORDINATES RELATIVE TO THE BASE OF THIS VERTEX OF
C...THE TRANSFORM
      TXC=CNOM(TX,TY,TZ,X23,Y23,Z23)
      TYC=CNOM(TX,TY,TZ,X31,Y31,Z31)
      TZC=CNOM(TX,TY,TZ,X12,Y12,Z12)
      PRINT 113,X(II,I),Y(JJ,I),Z(KK,I),RA,ALP,Z(KK,I),TRA,TALP,TZ,TX,
     1TY,TZ,TXC,TYC,TZC
  113 FORMAT(/,38H THE POINT WITH CARTESIAN CO-ORDINATES,3F15.10,/,
     135H HAS CYLINDRICAL POLAR CO-ORDINATES,3F15.10,/,64H IT IS TRANSFO
     2RMED INTO THAT WITH CYLINDRICAL POLAR CO-ORDINATES,3F15.10,/,
     333H WHICH HAS CARTESIAN CO-ORDINATES,3F15.10,/,38H AND CO-ORDINATE
     4S RELATIVE TO THE BASE,3F15.10)
C...XL,YL,ZL ARE TO BE THE LOWER LIMITS ON THE CARTESIAN CO-ORDINATES OF
C...REGION I AND XU,YU,ZU THE UPPER LIMITS. XLC,YLC,ZLC AND XUC,YUC,ZUC
C...ARE TO BE THE BOUNDS ON THE CO-ORDINATES RELATIVE TO THE BASE.
      IF(II.NE.1) GO TO 7
      IF(JJ.NE.1) GO TO 7
      IF(KK.NE.1) GO TO 7
      XL=XU=TX £ YL=YU=TY £ ZL=TZ
      XLC=XUC=TXC £ YLC=YUC=TYC £ ZLC=ZUC=TZC
      GO TO 6
    7 IF(KK.EQ.2) GO TO 9
      CALL UPLW(XL,XU,TX)
```

```
      CALL UPLW(YL,YU,TY)
    9 IF(II.NE.1) GO TO 8
      IF(JJ.NE.1) GO TO 8
      ZU=TZ
    8 CALL UPLW(XLC,XUC,TXC)
      CALL UPLW(YLC,YUC,TYC)
      CALL UPLW(ZLC,ZUC,TZC)
    6 CONTINUE
    5 CONTINUE
    4 CONTINUE
C...NOW FIND THE LIMITS ON THE CO-ORDINATES RELATIVE TO THE BASE OF
C...THE INTEGERS TO BE USED IN TRANSLATING THIS REGION BACK ON TO THE
C...FUNDAMENTAL REGION.
      CALL ROUNDI(XLC,IXL)
      CALL ROUNDI(XUC,IXU)
      CALL ROUNDI(YLC,IYL)
      CALL ROUNDI(YUC,IYU)
      CALL ROUNDI(ZLC,IZL)
      CALL ROUNDI(ZUC,IZU)
      PRINT 114,XL,YL,ZL,XU,YU,ZU,IXL,IYL,IZL,IXU,IYU,IZU
  114 FORMAT(//,5X,1HL,3F20.10,/,5X,1HU,3F20.10,/,13H INTEGERS:  L,3I6,/
     1,12X,1HU,3I6)
      IFLAG=0
C...IFLAG=0 WHEN NO REGION HAS BEEN FOUND WHICH INTERSECTS WITH A
C...TRANSLATE OF THE TRANSFORM OF REGION I. IFLAG=1 WHEN AT LEAST ONE
C...SUCH REGION HAS BEEN FOUND.  FOR EACH POSSIBLE TRANSLATING INTEGER
C...NOW FIND WHICH REGIONS INTERSECT.
      LEXTT=IXU-IXL+1 £ MEXTT=IYU-IYL+1 £ NEXTT=IZU-IZL+1
      RLAST=FLOAT(IXL)-1.0 £ RMAST=FLOAT(IYL)-1.0 £ RNAST=FLOAT(IZL)-1.0
      RL=RLAST
      DO 10 JL=1,LEXTT
      RL=RL+1.0
      IL=IFIX(RL)
      RM=RMAST
      DO 11 JM=1,MEXTT
      RM=RM+1.0
      IM=IFIX(RM)
      RN=RNAST
      DO 12 JN=1,NEXTT
      RN=RN+1.0
      IN=IFIX(RN)
      ZC=CI(RL,RM,RN,H)
      XC=CI(RL,RM,RN,R)
      YC=CI(RL,RM,RN,U)
C...FOR THIS INTEGER RUN THROUGH THE ORIGINAL UNCOVERED REGIONS.
      DO 15 J=1,N
C...CALCULATE THE BOUNDS ON THE TRANSLATE OF ORIGINAL REGION J BY
C...THE INTEGER (L,M,N)
      ZUC=Z(2,J)+ZC £ ZLC=Z(1,J)+ZC
      XUC=X(2,J)+XC £ XLC=X(1,J)+XC
```

```
      YUC=Y(2,J)+YC £ YLC=Y(1,J)+YC
      MJ=J
C...MJ IS SET TO J WHEN CONSIDERING THE JTH REGION AND TO -J WHEN
C...CONSIDERING ITS 'NEGATIVE'.
   14 IF(ZL.GT.ZUC) GO TO 17
      IF(ZU.LT.ZLC) GO TO 17
      IF(XL.GT.XUC) GO TO 17
      IF(XU.LT.XLC) GO TO 17
      IF(YL.GT.YUC) GO TO 17
      IF(YU.LT.YLC) GO TO 17
      PRINT 105,MJ,IL,IM,IN
  105 FORMAT(/,42H THIS REGION'S TRANSFORM INTERSECTS WITH R,I3,4H + [,
     13I5,1H])
      GO TO 16
   17 IF(MJ.LT.0) GO TO 15
      ZLC=-Z(2,J)+ZC £ ZUC=-Z(1,J)+ZC
      XLC=-X(2,J)+XC £ XUC=-X(1,J)+XC
      YLC=-Y(2,J)+YC £ YUC=-Y(1,J)+YC
      MJ=-J
      GO TO 14
   16 IFLAG=1
   15 CONTINUE
   12 CONTINUE
   11 CONTINUE
   10 CONTINUE
      IF(IFLAG.EQ.1) GO TO 2
      PRINT 106
  106 FORMAT(/,68H THIS REGION'S TRANSFORM DOES NOT INTERSECT WITH ANY O
     1RIGINAL REGION)
    2 CONTINUE
      STOP
      END
```

```
      FUNCTION ADJ(R,U,I,J)
      DIMENSION R(3),U(3)
      ADJ=R(I)*U(J)-R(J)*U(I)
      RETURN
      END
```

```
      SUBROUTINE UPLW(RL,RU,TR)
      IF(RL.LE.TR) GO TO 10
      RL=TR £ GO TO 11
   10 IF(RU.LT.TR) RU=TR
   11 RETURN
      END
```

```
      SUBROUTINE ROUNDI(RC,IR)
      ID=1
      IF(RC.LT.0.0) ID=-1
      IR=IFIX(RC)
      RIR=FLOAT(IR)
      IF(ABS(RC-RIR).GT.0.5) IR=IR+ID
      RETURN
      END
```

```
      FUNCTION DCORR(X,J)
C...THIS FUNCTION ALLOWS FOR ROUNDING ERROR ON THE BOUNDS ON THE
C...CARTESIAN CO-ORDINATES.
      CORR=1.0E-10
      DCORR=0.0
      IF(X.EQ.0.0) RETURN
      IF(J.EQ.2) GO TO 1
      DCORR=X-CORR
      RETURN
    1 DCORR=X+CORR
      RETURN
      END
```

THE PROGRAM EXCEP

SUBROUTINES

```
      PROGRAM EXCEP(INPUT,OUTPUT)
C
C...THIS PROGRAM FINDS THE MINIMUM OF THE ALGEBRAIC NUMBER A.
C
      DOUBLE R,U,H,AX,AY,AZ,BX,BY,BZ,AN,BE,BP,ABP,CK,ANV,ANW,BEV,BEW,ABD
      DOUBLE ABV,ABW,SB,TL1,TU1,TL,TU,VL,VU,WL,WU,PT,PV,PW,QT,QV,QW
      DOUBLE PL,PU,QL,QU,BDET,P,Q,S,PUA,QLT,QUT,PR,SLT,SUT,QUA
      DOUBLE PLT,PUT,QR
      DOUBLE DCI,DAJ,PQ,X,Y,Z,BNORM,APNORM,DNORM
      COMMON/D1/IDET,INDEX,IA,IB,IC/D2/R(3),U(3),H(3)
      COMMON/D3/TL,VL,WL,TU,VU,WU/D4/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D5/BDET
C...    H(3)*H(3)=IL1*H(3)+IL2*H(2)+IL3  ...
C...    H(2)*H(2)=IT1*H(3)+IT2*H(2)+IT3
C...    H(3)*H(2)=IP1*H(3)+IP2*H(2)+IP3
C...READ IN THE DETAILS OF THE FIELD.
      READ 100,IDET,INDEX,IA,IB,IC
  100 FORMAT(I6,I2,3I5)
      MDET=-IDET
      PRINT 200,MDET,INDEX,IA,IB,IC
  200 FORMAT(1H1,28H THIS FIELD HAS DISCRIMINANT,I7,6H INDEX,I2,28H AND
     1POLYNOMIAL COEFFICIENTS,3I6)
C...CALCULATE THE ZEROS OF THE DEFINING POLYNOMIAL AND A BASIS FOR THE
C...REAL LATTICE FOR THIS FIELD USING BASES.
      CALL BASES
C...H(2),R(2)+I.U(2) AND R(2)-I.U(2) ARE THE ZEROS. (H(1),H(2),H(3))
C...IS A BASIS FOR THE FIELD.
C
C...(IZ*H(2)**2+IY*H(2)+IX)/ID IS THE NUMERATOR AND
C...(JZ*H(2)**2+JY*H(2)+JZ)/JD IS THE DENOMINATOR OF THE ALGEBRAIC
C...NUMBER A. NOW READ THEIR COEFFICIENTS AND CALCULATE THEIR VALUES.
      READ 101,IZ,IY,IX,ID,JZ,JY,JX,JD
  101 FORMAT(8I10)
      CALL CHANGE(IZ,IY,IX,ID,I1Z,I1Y,I1X)
      CALL CHANGE(JZ,JY,JX,JD,J1Z,J1Y,J1X)
      AX=FLOAT(I1X) $ AY=FLOAT(I1Y) $ AZ=FLOAT(I1Z)
      BX=FLOAT(J1X) $ BY=FLOAT(J1Y) $ BZ=FLOAT(J1Z)
      AN=DCI(AX,AY,AZ,H)
      BE=DCI(BX,BY,BZ,H)
C...THE TRANSFORMATION ON THE LATTICE WHICH TAKES P INTO ITSELF IS
C...Q→ (Q-AN)/(1-BE). SO SAVE THE VALUES OF 1-BE AND OF -AN/(1-BE).
      BP=1.0D0-BE
      ABP=-AN/BP
C...THE TRANSFORMATION IS NOW Q→Q/BP+ABP.
C...READ THE LIMITING VALUE OF ABS(NORM(P-Q)).
      READ 102,SK
  102 FORMAT(F10.1)
      CK=SK
      PRINT 201,I1Z,I1Y,I1X,J1Z,J1Y,J1X,SK
  201 FORMAT(/,27H FOR COVERING THE POINT A=(,3I10,3H)/(,3I10,12H) WITH
```

```
     1BOUND,F5.1)
      ANV=DCI(AX,AY,AZ,R)
      ANW=DCI(AX,AY,AZ,U)
      BEV=DCI(BX,BY,BZ,R)
      BEW=DCI(BX,BY,BZ,U)
      ABD=BEV*BEV+BEW*BEW
      ABV=(ANV*BEV+ANW*BEW)/ABD
      ABW=(-ANV*BEW+BEV*ANW)/ABD
      BNORM=DNORM(BZ,BY,BX)
C...READ THE LOWER BOUND ON THE INTEGERS T WHICH ARE TO BE CONSIDERED
C...AND CALCULATE THE CORRESPONDING UPPER BOUND.
      READ 102,SL1
      TL1=SL1
      PRINT 205,SL1
  205 FORMAT(/,4H TL=,F10.4)
      TU1=TL1/BP+ABP
      TL=TL1
      TU=TL+100.0D0
      TU=DMIN1(TU,TU1)
C...CALCULATE THE LIMITS ON V AND W WHERE V+I.W AND V-I.W ARE THE
C...CONJUGATES OF T.
      RMINIM=SK
C...IF T=P*H(3)+Q*H(2)+S*H(1) AND T HAS CONJUGATES V+I.W AND V-I.W, NOW
C...FIND THE COEFFICIENTS OF T,V,W IN THE FOLLOWING EXPRESSIONS FOR P,Q
C...AND S.
C...        P=PT*T+PV*V+PW*W
C...        Q=QT*T+QV*V+QW*W
C...        S=ST*T+SV*V+SW*W
      BDET=FLOAT(IDET)
      BDET=DSQRT(BDET)/2.0
      PT=DAJ(R,U,1,2)
      PV=DAJ(U,H,1,2)
      PW=DAJ(H,R,1,2)
      QT=DAJ(R,U,3,1)
      QV=DAJ(U,H,3,1)
      QW=DAJ(H,R,3,1)
      NEXT=1
C...NEXT=1 FOR THE FIRST BRANCH OF VALUES OF T AND 2 FOR THE SECOND.
    6 SB=DSQRT(CK/(TL-(AN/BE)))
    3 VL=ABV-SB
      VU=ABV+SB
      WL=ABW-SB
      WU=ABW+SB
C...NOW CALCULATE THE BOUNDS ON P AND Q.
      CALL LOWUP(PT,PV,PW,PL,PU)
      CALL LOWUP(QT,QV,QW,QL,QU)
C...NOW FIND WHAT THE INTEGER LIMITS ON P AND Q ARE AND FIND WHICH HAS
C...THE SMALLER RANGE.
      CALL LIMITL(PL,IPL)
      CALL LIMITL(QL,IQL)
```

```
      CALL LIMITU(PU,IPU)
      CALL LIMITU(QU,IQU)
      IF(IPL.LE.IPU) GO TO 70
   71 PRINT 202,IPL,IPU,IQL,IQU
  202 FORMAT(/,19H THE RANGE FOR P IS,I5,3H TO,I5,13H AND FOR Q IS,I5,
     13H TO,I5)
      STOP
   70 IF(IQL.GT.IQU) GO TO 71
      IF((IPU-IPL).GT.(IQU-IQL)) GO TO 1
C...NOW P HAS THE SMALLER RANGE SO USING THE FACT THAT U(1)=0 AND SO
C...        W=Q*U(2)+P*U(3)
C...        Q=(W-P*U(3))/U(2).
C...THUS PROVIDED U(2)>0,WHICH IS SO, THE BOUNDS ON W AND EACH POSSIBLE
C...VALUE OF P Q MAY BE FURTHER RESTRICTED.
C...ALSO USING R(1)=1 AND SO
C...        S=V-Q*R(2)-P*R(3),
C...THE BOUNDS ON V AND EACH POSSIBLE PAIR OF VALUES OF P AND Q THE
C...POSSIBLE VALUES OF S MAY BE FOUND.   RUN THROUGH THE VALUES P FROM
C...IPL TO IPU.
      IPCOUNT=IPU-IPL+1
      P=FLOAT(IPL)-1.0
      DO 12 IPC=1,IPCOUNT
      P=P+1.0D0
C...FIND BOUNDS ON Q FOR THIS VALUE OF P
      PUA=P*U(3)/U(2)
      QLT=WL/U(2)-PUA
      QUT=WU/U(2)-PUA
C...AS SUITABLE VALUES OF Q ARE FOUND FOR EACH VALUE OF P: FOR EACH
C...PAIR P,Q FIND POSSIBLE S USING
C......V=S+Q*R(2)+P*R(3) .....SINCE R(1)=1
C...   SO S=T-Q*R(2)-P*R(3)
      CALL LIMITL(QLT,IQLT)
      CALL LIMITU(QUT,IQUT)
      IF(IQUT.LT.IQLT) GO TO 12
   30 IQCOUNT=IQUT-IQLT+1
      Q=FLOAT(IQLT)-1.0
      PR=P*R(3)
      DO 13 IQC=1,IQCOUNT
      Q=Q+1.0D0
      PQ=-Q*R(2)-PR
      SLT=VL+PQ
      SUT=VU+PQ
      CALL LIMITL(SLT,ISLT)
      CALL LIMITU(SUT,ISUT)
      IF(ISUT.LT.ISLT) GO TO 13
   31 ISCOUNT=ISUT-ISLT+1
      S=FLOAT(ISLT)-1.0
      DO 14 ISC=1,ISCOUNT
      S=S+1.0D0
      IP=P £ IQ=Q £ IS=S
```

```
      CALL MULTD(P,Q,S,BZ,BY,BX,Z,Y,X)
      X=X-AX £ Y=Y-AY £ Z=Z-AZ
      APNORM=DNORM(Z,Y,X)
      PRINT 203,IP,IQ,IS,APNORM,BNORM
  203 FORMAT(/,8H WITH P=,I10,3H Q=,I10,7H AND S=,I10,/,27H THEN NORM(P-
     1A) IS EQUAL TO,D24.18,1H/,D24.18)
      RMNM=DABS(APNORM/BNORM)
      IF(RMNM.LT.RMINIM)RMINIM=RMNM
   14 CONTINUE
   13 CONTINUE
   12 CONTINUE
      GO TO 2
    1 IQCOUNT=IQU-IQL+1
C...REACHING HERE INDICATES THAT Q HAS THE SMALLER RANGE SO USING THE
C...EXPRESSION FOR W P MAY BE RESTRICTED ASSUMING U(3)>0, WHICH IS SO.
C...THEN USING THE EXPRESSION FOR V, S MAY BE SIMILARLY RESTRICTED.
      Q=FLOAT(IQL)-1.0
      DO 15 IQC=1,IQCOUNT
      Q=Q+1.0D0
C...FIND BOUNDS ON P FOR THIS Q.
      QUA=Q*U(2)/U(3)
      PLT=WL/U(3)-QUA
      PUT=WU/U(3)-QUA
C...NOW FIND SUITABLE S.
      CALL LIMITL(PLT,IPLT)
      CALL LIMITU(PUT,IPUT)
      IF(IPUT.LT.IPLT) GO TO 15
   32 IPCOUNT=IPUT-IPLT+1
      P=FLOAT(IPLT)-1.0
      QR=Q*R(2)
      DO 16 IPC=1,IPCOUNT
      P=P+1.0D0
      PQ=-QR-P*R(3)
      SLT=VL+PQ
      SUT=VU+PQ
      CALL LIMITL(SLT,ISLT)
      CALL LIMITU(SUT,ISUT)
      IF(ISUT.LT.ISLT) GO TO 16
   33 ISCOUNT=ISUT-ISLT+1
      S=FLOAT(ISLT)-1.0
      DO 17 ISC=1,ISCOUNT
      S=S+1.0D0
      IS=S £ IQ=Q £ IP=P
      CALL MULTD(P,Q,S,BZ,BY,BX,Z,Y,X)
      X=X-AX £ Y=Y-AY £ Z=Z-AZ
      APNORM=DNORM(Z,Y,X)
      PRINT 203,IP,IQ,IS,APNORM,BNORM
      RMNM=DABS(APNORM/BNORM)
      IF(RMNM.LT.RMINIM)RMINIM=RMNM
   17 CONTINUE
```

```
   16 CONTINUE
   15  CONTINUE
C...THE NEXT SECTION OF THIS BRANCH OF VALUES OF T IS NOW CONSIDERED.
    2 IF(NEXT.EQ.2) GO TO 4
      IF(TU.GE.TU1) GO TO 5
C...WHEN TU REACHES THE VALUE TU1 THEN THIS BRANCH OF VALUES IS
C...COMPLETED SO THE OTHER IS NOW CONSIDERED.
      TL=TU
      TU=TU+100.0D0
      TU=DMIN1(TU,TU1)
      GO TO 6
    5 NEXT=NEXT+1
      READ 102,SU1
      TU1=SU1
      PRINT 206,SU1
  206 FORMAT(/,4H TU=,F10.1)
C...NOW READ THE UPPER BOUND ON THE LOWER BRANCH OF INTEGERS AND
C...CALCULATE THE LOWER BOUND
      TL1=TU1/BP+ABP
      TU=TU1
      TL=TU-100.0D0
      TL=DMAX1(TL,TL1)
    8 SB=DSQRT(CK/((AN/BE)-TU))
C...NOW REPEAT THE ABOVE WITH THESE LIMITS ON T AND THIS VALUE OF SB
      GO TO 3
    4 IF(TL.LE.TL1) GO TO 7
C...WHEN TL REACHES THE VALUE TL1 THEN THIS BRANCH OF VALUES IS
C...COMPLETED SO THE MINIMUM OF THIS POINT, RMINIM, IS PRINTED.
      TU=TL
      TL=TL-100.0D0
      TL=DMAX1(TL,TL1)
      GO TO 8
    7 PRINT 204,RMINIM
  204 FORMAT(/,30H THE MINIMUM FOR THIS POINT IS,F20.10)
      STOP
      END
```

```
      SUBROUTINE BASES
C
      DOUBLE A,B,C,R,U,H,V1,V2,V3,V4,V5,V6,V7,T,S,D,XIN
      DOUBLE IOBD
      COMMON/D1/IDET,INDEX,IA,IB,IC/D2/R(3),U(3),H(3)
      COMMON/D4/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D15/IUBN/D16/IOBD
      A=FLOAT(IA) £ B=FLOAT(IB) £ C=FLOAT(IC) £ IN=INDEX
C...FIND H(2) WHERE THE FIELD IS K(H(2)) AND ALSO R(2) AND U(2) WHERE
C...R(2)+I.U(2) AND R(2)-I.U(2) ARE THE CONJUGATES OF H(2).
      V1=-(B-(A**2)/3.0D0)/3.0D0
      V2=-(A*B/3.0D0-2.0D0*A**3/27.0D0-C)
      V3=DSQRT(V2**2-4.0D0*V1**3)
      V4=(V2+V3)/2.0D0
      V5=(V2-V3)/2.0D0
      IF(V4.NE.0.0D0) GO TO 51
      V6=0.0D0 £ GO TO 52
   51 D=1.0D0
      IF(V4.GE.0.0D0) GO TO 53
      V4=-V4 £ D=-1.0D0
   53 V6=DEXP((DLOG(V4))/3.0D0)*D
   52 IF(V5.NE.0.0D0) GO TO 54
      V7=0.0D0 £ GO TO 55
   54 D=1.0D0
      IF(V5.GE.0.0D0) GO TO 56
      V5=-V5 £ D=-1.0D0
   56 V7=DEXP((DLOG(V5))/3.0D0)*D
   55 H(2)=V6+V7+A/3.0D0
      R(2)=(A-H(2))/2.0D0
      U(2)=DSQRT(C/H(2)-R(2)**2)
      H(1)=1.0D0 £ R(1)=1.0D0 £ U(1)=0.0D0
C...(R(1),U(1),H(1))=(1,0,1) IS THE LATTICE POINT CORRESPONDING TO UNITY
C
C...FIND T AND S WHERE Y=(H(2)**2+T*H(2)+S)/INDEX.
C...(1,H(2),Y) IS A BASIS OF THE FIELD.
      IN2=IN*IN £ IN3=IN2*IN
      K1=IA*IA-2*IB £ K2=IA*IC £ K3=IB*IC
      K4=IB*IB-2*IA*IC £ K5=IA*IB-3*IC £ IC2=IC*IC
      IF(INDEX.NE.1) GO TO 57
      IT=0 £ IS=0
      T=0.0 £ S=0.0 £ GO TO 58
   57 DO 59 ITC=1,IN
      IT=ITC-1
      DO 60 ISC=1,IN
      IS=ISC-1
      JA=K1+IT*IA+3*IS
      IF(MOD(JA,IN).NE.0) GO TO 60
      JB=K4+IT**2*IB+3*IS**2+IT*K5+2*IS*K1+2*IS*IT*IA
      IF(MOD(JB,IN2).NE.0) GO TO 60
      JC=IS**3+IT**3*IC+IC**2+IS**2*IT*IA+IS*K4+IS*IT**2*IB+IT*IB*IC
```

```
     1+IT**2*IA*IC+IS**2*K1+IS*IT*K5
      IF(MOD(JC,IN3).NE.0) GO TO 60
      T=FLOAT(IT) £ S=FLOAT(IS) £ GO TO 58
   60 CONTINUE
   59 CONTINUE
   58 XIN=FLOAT(INDEX)
      H(3)=(H(2)**2+T*H(2)+S)/XIN
      R(3)=(R(2)**2-U(2)**2+T*R(2)+S)/XIN
      U(3)=(2.0D0*R(2)*U(2)+T*U(2))/XIN
      IT1=INDEX
      IT2=-IT
      IT3=-IS
      IML=2*IA*IT+IA*IA+2*IS+IT*IT-IB
      IL1=IML/INDEX
      IL2=(-IT*IML+2*IS*IT+IC-2*IB*IT-IA*IB)/IN2
      IL3=(-IS*IML+2*IC*IT+IA*IC+IS*IS)/IN2
      IP1=IA+IT
      IP2=(IS-IB-IT*IP1)/INDEX
      IP3=(IC-IS*IP1)/INDEX
      PRINT 100,((R(I),U(I),H(I)),I=1,3)
  100 FORMAT(/,27H A BASIS FOR THE LATTICE IS,/,15X,1HR,19X,1HU,19X,1HH,
     13(/,5X,3D20.10))
      I=2 £ J=3
      PRINT 101,I,I,IT1,IT2,IT3
      PRINT 101,J,J,IL1,IL2,IL3
      PRINT 101,I,J,IP1,IP2,IP3
  101 FORMAT(/,10X,2HH(,I1,4H)*H(,I1,2H)=,I10,6HH(3) +,I10,6HH(2) +,I10,
     14HH(1))
C...FIND AN UPPER BOUND, A POWER OF 10, FOR THE ARGUMENTS OF DNORM WHICH
C...WILL NOT GIVE RISE TO OVERFLOW.
      K1P=IABS(K1) £ K4P=IABS(K4) £ K5P=IABS(K5)
      NF=MAX0(K1P,K2,K3,K4P,K5P,IC2)
      IONF=IOF(NF)
      IONS=(29-IONF)/3
      IUBN=10**IONS
C...FIND BOUNDS FOR THE RELEVANT PRODUCTS OF MULTD SUCH THAT OVERFLOW
C...WILL NOT OCCUR.
      IL1A=IABS(IL1) £ IL2A=IABS(IL2) £ IL3A=IABS(IL3)
      IT1A=IABS(IT1) £ IT2A=IABS(IT2) £ IT3A=IABS(IT3)
      IP1A=IABS(IP1) £ IP2A=IABS(IP2) £ IP3A=IABS(IP3)
      ILTP=MAX0(IL1A,IL2A,IL3A,IT1A,IT2A,IT3A,IP1A,IP2A,IP3A)
      ILTP1=IOF(ILTP)
      IOBS=29-ILTP1
      IOBD=10.0D0**IOBS
      RETURN
      END
```

```
      SUBROUTINE MULTD(I1,J1,K1,I2,J2,K2,I,J,K)
C
C...MULTD FINDS THE PRODUCT OF I1*H(3)+J1*H(2)+K1*H(1) AND
C...I2*H(3)+J2*H(2)+K2*H(1). IT IS I*H(3)+J*H(2)+K*H(1)
C
      DOUBLE I1,J1,K1,I2,J2,K2,I,J,K,IP
      DOUBLE IOBD,IA,JA,KA,MULT1,MULT2,MULTP
      COMMON/D4/IL1,IL2,IL3,IT1,IT2,IT3,IP1,IP2,IP3
      COMMON/D16/IOBD
      IA=DABS(I1) $ JA=DABS(J1) $ KA=DABS(K1)
      MULT1=DMAX1(IA,JA,KA)
      IA=DABS(I2) $ JA=DABS(J2) $ KA=DABS(K2)
      MULT2=DMAX1(IA,JA,KA)
      MULTP=MULT1*MULT2
      IF(MULTP.LT.IOBD) GO TO 1
      PRINT 50
   50 FORMAT(1X,10(1H*),27HDANGER OF OVERFLOW IN MULTD,10(1H*))
    1 IP=I1*J2+I2*J1
      I=I1*I2*IL1+IP*IP1+J1*J2*IT1+I1*K2+I2*K1
      J=I1*I2*IL2+IP*IP2+J1*J2*IT2+J1*K2+J2*K1
      K=I1*I2*IL3+IP*IP3+J1*J2*IT3+K1*K2
      RETURN
      END
```

```
      SUBROUTINE LOWUP(XT,XV,XW,XL,XU)
C
C...THIS SUBROUTINE FINDS XL,XU SUCH THAT
C...               X=XT*Y(1)+XV*Y(2)+XW*Y(3)
C...IS BETWEEN XL AND XU, WHERE Y(I) IS BETWEEN YL(I) AND YU(I),I=1,3.
C
      DOUBLE XT,XV,XW,XL,XU,X(3),YL,YU
      COMMON/D3/YL(3),YU(3)
      X(1)=XT £ X(2)=XV £ X(3)=XW
      XL=XU=0.0D0
      DO 1 I=1,3
      IF(X(I).LT.0.0D0) GO TO 2
      XL=XL+YL(I)*X(I)
      XU=XU+YU(I)*X(I)
      GO TO 1
    2 XL=XL+YU(I)*X(I)
      XU=XU+YL(I)*X(I)
    1 CONTINUE
      RETURN
      END
```

```
      SUBROUTINE LIMITL(XXL,IXL)
C
C...IXL IS THE SMALLEST INTEGER GREATER THAN XXL.
C
      DOUBLE XXL,XXLA
      XXLA=DABS(XXL)
      IF(XXLA.LT.1.0D14) GO TO 1
      PRINT 50
   50 FORMAT(1X,10(1H*),35HMORE THAN 14 DIGITS IN THIS INTEGER,10(1H*))
    1 XL=SNGL(XXL)
      IXL=IFIX(XL)
      IF(FLOAT(IXL)-XL)4,5,5
    4 IXL=IXL+1
    5 RETURN
      END
```

```
      SUBROUTINE LIMITU(XXU,IXU)
C
C...IXU IS THE GREATEST INTEGER LESS THAN XXU.
C
      DOUBLE XXU,XXUA
      XXUA=DABS(XXU)
      IF(XXUA.LT.1.0D14) GO TO 1
      PRINT 50
   50 FORMAT(1X,10(1H*),35HMORE THAN 14 DIGITS IN THIS INTEGER,10(1H*))
    1 XU=SNGL(XXU)
      IXU=IFIX(XU)
      IF(FLOAT(IXU)-XU)4,4,5
    5 IXU=IXU-1
    4 RETURN
      END
```

```
      DOUBLE FUNCTION DAJ(R,U,I,J)
      DOUBLE BDET,R(3),U(3)
      COMMON/D5/BDET
      DAJ=(R(I)*U(J)-R(J)*U(I))/BDET
      RETURN
      END
```