UNITS IN SOME ALGEBRAIC NUMBER FIELDS

A thesis presented in partial fulfilment of

the requirements for degree of

Master of Science

in Mathematics at

Massey University

Neville Stuart Jeans

1978

ABSTRACT

Dirichlet's theorem describes the structure of the group of units of the ring of algebraic integers of any algebraic number field. This theorem shows that any unit can be written in terms of a fundamental system of units. However Dirichlet's theorem does not suggest any method by which such a fundamental system of units (or indeed any units) can be obtained.

This thesis looks at three types of algebraic number fields for which a fundamental system of units contains one unit, the so called fundamental unit. In each case properties of units and the problem of obtaining a fundamental unit are discussed.

Chapter one is an introductory chapter which summarises the basic theory relevant to algebraic number fields of arbitrary degree. Basic properties of units and Dirichlet's theorem are also given.

Chapter two looks at units of Quadratic fields, $Q(\sqrt{d})$. Units of imaginary quadratic fields are mentioned briefly but the chapter is mainly concerned with the more complicated problem of obtaining real quadratic units. The relevant theory of simple continued fractions is presented and the way in which units can be obtained from the simple continued fraction expansion of $\sqrt{d}$ is outlined. The chapter then also looks at some recent papers dealing with the length of the period of $\sqrt{d}$ and concludes by showing how units can be obtained from the simple continued fraction expansion of $(1 + \sqrt{d})/2$ when $d \equiv 1 \pmod 4$.

Chapter three looks at units of pure cubic fields. The basic properties of pure cubic units are developed and reference is made to various algorithms which can be used to obtain pure cubic units. The main purpose of this chpater is to present the results of the paper 'Determining the Fundamental Unit of a Pure Cubic Field Given any Unit' (Jeans and Hendy [1978]). However in this thesis a different approach to that of the paper is used and for two of the results sharper bounds have been obtained. Several examples are given using the algorithm which is developed from these results.

Chapter four, which is original work, investigates the quartic fields, $Q(d^{\frac{1}{4}})$, where d is a square-free negative integer. Similarities between these quartic fields and the pure cubic and real quadratic fields are developed of which the main one is a quartic analogue of the results given in the paper mentioned above.

The examples given in chapter three required multiprecision computer programs and these programs have been listed in appendix one.

ACKNOWLEDGEMENT

I would like to thank my supervisor, Dr M D Hendy for the advice and encouragement he has offered during my work on this thesis.

CONTENTS

1 INTRODUCTION

This chapter gives a short summary of the basic theory which is relevant to this thesis. While the contents of this chapter have not been derived from any particular source, texts such as Richman [1971], Adams and Goldstein [1976], Clark [1971], Maxfield and Maxfield [1971], Cohn [1962], Niven and Zuckerman [1972], and Samuel [1970] give varying degrees of coverage of the material to be summarised in this chapter.

Notation

The symbols defined below will have the same meaning through out the thesis.

Z^+	-	the set $\{1, 2, 3, 4, \ldots\}$
Z	-	the set of rational integers
Q	-	the set of rational numbers
R	-	the set of real numbers
$Z[\alpha,\beta]$	-	the module $\{a_1\alpha + a_2\beta \mid a_1, a_2 \in Z\}$
(a,b)	-	the greatest common divisor of the integers a, b.
$[\ ]$	-	the greatest integer function
i	-	the square root of minus one.

In general, Greek letters will denote algebraic numbers and letters of the Roman alphabet will denote rational integers.

Algebraic Fields

Let F be a number field, that is F is a subfield of the field of complex numbers. The polynomial

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

$$a_n \neq 0,\ a_i \in F,$$

is called a polynomial over F and the set of all such polynomials forms an integral domain denoted by $F[x]$. p is said to be of degree n, written deg (p) = n. A monic polynomial is one in which the leading coefficient, a_n, is unity.

A number, α, is algebraic over F if it is the zero of some polynomial $f \in F[x]$.

Theorem 1.1

If α is algebraic over F, there exists a unique polynomial $f \in F(\alpha)$ such that

i) $f(\alpha) = 0$

ii) f is monic

iii) if $g \in F[x]$ and $g(\alpha) = 0$ then $f|g$

f is called the minimal polynomial for α and the degree of α is defined to be equal to deg(f). //

Theorem 1.2

The set $F(\alpha) = \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} | b_i \in F,$ n = deg $(\alpha)\}$ forms a number field which is a simple extension of F. It is the smallest field that contains both α and F. //

If $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \in F(\alpha)$ then

$b_0, b_1, \ldots, b_{n-1}$ are called the coefficients of β.

Theorem 1.3

$F(\alpha)$ is a vector space over F with basis $1, \alpha, \ldots, \alpha^{n-1}$. Consequently any $\beta \in F(\alpha)$ is algebraic over F and deg $(\beta) \leq$ deg (α). $F(\alpha)$ is an algebraic extension of F. //

The minimal polynomial for α can be factored as n distinct linear factors in C,

$$f(x) = (x - \alpha)(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{n-1})$$

The $n - 1$ numbers $\alpha_1, \alpha_2 \ldots, \alpha_{n-1}$ are called the conjugates of α.

Theorem 1.4

Let $\beta \in F(\alpha)$. Then $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ where $n = \deg(\alpha)$ and $b_j \in F$. Let g be the minimal polynomial for β. Define

$$\beta_j = b_0 + b_1\alpha_j + b_2\alpha_j + \ldots + b_{n-1}\alpha_j^{n-1}, \quad j = 1, 2, \ldots, n - 1 \quad (1)$$

where the α_j are the conjugates of α.

Let $h(x) = (x - \beta)(x - \beta_1) \ldots (x - \beta_{n-1})$

Then
i) each β_j is either equal to β or is a conjugate of β.
ii) h is a monic polynomial and $h \in F[x]$*.
iii) $h = g^p$ where deg (g) x p = deg (α), $p \in Z^+$
iv) $N(\beta) = \beta\beta_1\beta_2 \ldots \beta_{n-1}$, called the norm function (with respect to $F(\alpha)$) is a multiplicative homomorphism from $F(\alpha)$ into F
v) $N(\beta) = (-1)^n a_o$, where a_o is the constant term of the polynomial h. //

---

* i) and ii) follow from consideration of the automorphisms of $F(\alpha, \alpha_1, \ldots, \alpha_{n-1})$, the splitting field for f over F.

Algebraic Numbers, Number Fields and Integers

If we take F = Q in the previous section then any α algebraic over Q is called an algebraic number, $Q(\alpha)$ is called an algebraic number field, and for any $\beta \in Q(\alpha)$ $N(\beta)$ is necessarily a rational number.

Example 1.1

As an illustration of theorem 1.4, consider $\beta = 3 + 5\sqrt{2}$, whose minimal polynomial over Q is

$$f(x) = x^2 - 6x - 41$$

If we consider β to be an element of $Q(\sqrt{2})$ then

$$\beta_1 = 3 - 5\sqrt{2} ,$$

$$h_1(x) = x^2 - 6x - 41 = f(x) ,$$

and $$N_1(\beta) = -41$$

If we consider β to be an element of $Q(2^{\frac{1}{4}})$ then

$$\beta_1 = 3 - 5\sqrt{2} ,$$

$$\beta_2 = 3 + 5\sqrt{2} = \beta ,$$

$$\beta_3 = 3 - 5\sqrt{2} = \beta_1 ,$$

$$h_2(x) = x^4 - 12x^3 - 46x^2 + 492x + 1681$$

$$= (f(x))^2$$

and $$N_2(\beta) = 1681 = (N_1(\beta))^2$$ //

An algebraic integer is an algebraic number whose minimal polynomial has integer coefficients. Consequently the norm of an algebraic integer is a rational integer.

Theorem 1.5.

The algebraic integers of an algebraic number field, $Q(\alpha)$, form an integral domain (denoted by $Z(\alpha)$). $Z(\alpha)$ is often referred to as the ring of algebraic integers of $Q(\alpha)$. //

Recalling h as defined in theorem 1.4 we have that for $\beta \in Q(\alpha)$,

$\beta \in Z(\alpha) \Leftrightarrow$ h has integer coefficients.

This fact is used when we determine the form of the algebraic integers of a particular $Q(\alpha)$.

The only rational numbers which are also algebraic integers are the rational integers, Z, and for any ring of algebraic integers, $Z(\alpha)$, we have $Z \subseteq Z(\alpha)$.

An integral basis of $Q(\alpha)$ is a set of elements $\theta_1, \theta_2, \ldots, \theta_k \in Z(\alpha)$ such that every $\beta \in Z(\alpha)$ can be written uniquely in the form $\beta = m_1\theta_1 + m_2\theta_2 + \ldots + m_k\theta_k$ where $m_1, m_2, \ldots, m_k \in Z$. Every $Z(\alpha)$ has an integral basis and an integral basis of $Z(\alpha)$ is also a basis of $Q(\alpha)$.

If $\theta_1, \theta_2, \ldots, \theta_n$ is a basis of $Q(\alpha)$ and if θ_j has conjugates $\theta_j^{(1)}, \theta_j^{(2)}, \ldots, \theta_j^{(n-1)}$ then the discriminant of the basis is the determinant,

$$\Delta = \begin{vmatrix} \theta_1 & \theta_2 & \theta_3 & \cdots & \theta_n \\ \theta_1^{(1)} & \theta_2^{(1)} & \theta_3^{(1)} & \cdots & \theta_n^{(1)} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \theta_1^{(n-1)} & \theta_2^{(n-1)} & \theta_3^{(n-1)} & \cdots & \theta_n^{(n-1)} \end{vmatrix}^2$$

The discriminant of a basis of $Q(\alpha)$ is a rational number. If the basis is also an integral basis of $Q(\alpha)$ then the discriminant of the basis is a rational integer. Each integral basis of $Q(\alpha)$ has the same discriminant. Thus the discriminant of any integral basis of $Q(\alpha)$ is also called the discriminant of the field $Q(\alpha)$.

Example 1.2

Let $\alpha = \sqrt{d}$, d a square-free integer. In chapter two we will see that

i) $1, \sqrt{d}$ forms an integral basis when $d \equiv 2, 3 \pmod 4$

ii) $1, (1 + \sqrt{d})/2$ forms an integral basis when $d \equiv 1 \pmod 4$

Thus when $d \equiv 2, 3 \pmod 4$

$$\Delta = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$

and when $d \equiv 1 \pmod 4$

$$\Delta = \begin{vmatrix} 1 & (1+\sqrt{d})/2 \\ 1 & (1-\sqrt{d})/2 \end{vmatrix}^2 = d$$

Units of the Ring of Algebraic Integers of $Q(\alpha)$

If $\beta \in Z(\alpha)$ and $\beta \neq 0$ then $\beta^{-1} \in Q(\alpha)$. If we also have that $\beta^{-1} \in Z(\alpha)$, then β is called a unit of $Z(\alpha)$.

Theorem 1.6

$\beta \in Z(\alpha)$ is a unit $\Leftrightarrow$ $N(\beta) = \pm 1$.

Proof

Let the minimal polynomial for β be

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0, \quad a_j \in Z$$

Then $a_0 \neq 0$ (otherwise f would not be minimal) and $f(\beta) = 0$. Thus we have

$$0 = 1/a_0 + a_{m-1}\beta^{-1}/a_0 + \ldots + a_1(\beta^{-1})^{m-1}/a_0 + (\beta^{-1})^m$$

The polynomial

$$f_1(x) = x^m + a_1 x^{m-1}/a_0 + \ldots + 1/a_0$$

is the minimal polynomial for β^{-1} and clearly $\beta^{-1} \in Z(\alpha)$ precisely when $a_0 = \pm 1$. The theorem now follows since $N(\beta)$ is a power of a_0 multiplied by ± 1. (Theorem 1.4 v)). //

The inverse of β is given by

$$\beta^{-1} = \beta_1\beta_2 \ldots \beta_{m-1}(N(\beta))^{-1}$$

where the β_j are as defined in (1).

If β and γ are algebraic integers of $Q(\alpha)$ and (β/γ) is a unit then we say that β and γ are associates.

The units of $Z(\alpha)$ form a multiplicative group whose structure is described in the following theorem due to Dirichlet.

Theorem 1.7

Let α be an algebraic number and f its minimal polynomial. Suppose that f has r real roots and 2s non-real roots, that is $\deg(\alpha) = r + 2s$. Then there exist units $\eta_1, \eta_2, \ldots, \eta_t$, where $t = r + s - 1$, such that every unit, η, of $Z(\alpha)$ may be written as

$$\eta = \xi\eta_1^{a_1}\eta_2^{a_2} \ldots \eta_t^{a_t}, \quad a_j \in Z$$

where ξ is some root of unity contained in $Z(\alpha)$.

Proof

[Samuel, 1970, p60], [Delone and Faddeev, 1964, p28] //

The number of possible values for ξ is finite and in the case that α is real or α has real conjugates the only values for ξ are ± 1.

The set of units $\eta_1, \eta_2, \ldots, \eta_t$ is referred to as a fundamental system of units of $Z(\alpha)$. Such a system is not unique since if $\eta_1, \eta_2, \ldots, \eta_t$ is a fundamental system then so is $\eta_1^{-1}, \eta_2, \ldots, \eta_t$.

When $t = 1$, we can write any unit of $Z(\alpha)$ as $\xi\eta_1^{a_1}$ for some unit $\eta_1 \in Z(\alpha)$. In such a case we call η_1 a fundamental unit. It is easily shown that η_1 must be such that there is no unit whose magnitude lies between 1 and $|\eta_1|$, and that the only other fundamental units are of the form $\xi\eta_1^{\pm 1}$. Consequently there are only a finite

number of fundamental units when $t = 1$. (If α is real or has a real conjugate then there are four fundamental units). It is usual to define precisely one of these units as the fundamental unit of $Z(\alpha)$.

Example 1.3

Let α be a real quadratic irrational, then $t = 1$ and there is one unit in any fundamental system. Let $\eta_1 \in Z(\alpha)$ be the smallest unit greater than unity.

Then each of η_1, η_1^{-1}, $-\eta_1$ and $-\eta_1^{-1}$ is a fundamental unit. We take η_1 as the fundamental unit. //

When t is greater than one, the situation is more complex. Firstly, there are always units whose magnitudes are arbitrarily close to unity and, secondly, from any given fundamental system of units it is possible to derive an infinite number of distinct fundamental systems. For example, the set $\eta_1, \eta_2, \ldots, \eta_t$ give rise to the systems $\eta_1\eta_2^p, \eta_2, \ldots, \eta_t$, where p is any integer. Consequently, a fundamental system cannot be characterised when $t > 1$ in a manner similar to the case when $t = 1$.

In the following three chapters we shall confine our attention to cases where $t = 0, 1$.

The problem of finding all the units of $Z(\alpha)$ is effectively solved by finding a fundamental system of units. Dirichlet's theorem offers no help in this area and we have to look to other areas of mathematics (for example, continued fractions) to find algorithms which can be used to calculate units in algebraic number

fields and theory which enables us to determine whether or not a system of units is fundamental.

2 UNITS OF QUADRATIC FIELDS

An algebraic number field of degree two is called a quadratic field. If $Q(\alpha)$ is a quadratic field then α is the root of polynomial, f, of degree two -

$$f(x) = x^2 + a_1x + a_0,\ a_1,\ a_0 \in Q.$$

Thus α is of the form

$$\alpha = (-a_1 \pm \sqrt{D})/2,\ D = a_1^2 - 4a_0,\ \sqrt{D} \notin Q.$$

Since D is a rational number we can write $D = p/q$ where $p, q \in Z$ and $(p, q) = 1$. Furthermore, we can write $pq = s^2d$ where $s, d \in Z$ and d is square-free.

Thus
$$\alpha = -a_1/2 \pm (s/2q)\sqrt{d}$$
$$= b_0 + c_0\sqrt{d},\ b_0 = -a_1/2,\ c_0 = \pm s/2q.$$

Since b_0 and c_0 are rational we have $Q(\alpha) = Q(\sqrt{d})$. Consequently we need only consider those fields of the form $Q(\sqrt{d})$ where $d \in Z$, $d \neq 0, 1$ and d is square-free. In so doing we cover all possible quadratic fields.

The Algebraic Integers of $Q(\sqrt{d})$

If β is any element of $Q(\sqrt{d})$ then $\beta = a + b\sqrt{d}$, $a, b \in Q$. The quadratic polynomial for β is

$$g(x) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d}))$$
$$= x^2 - 2a + (a^2 - b^2d).$$

Thus the norm of β with respect to the field $Q(\sqrt{d})$ is $N(\beta) = a^2 - b^2d$. β will be an algebraic integer of $Q(\sqrt{d})$ (a quadratic integer) if and only if 2a and $N(\beta)$ are rational integers. Clearly $a = k/2$ for some integer k. Letting $b = \ell_0/q$ where ℓ_0 and q are relatively prime integers, we

obtain $k^2/4 - \ell_0^2 d/q^2 = m \in Z$

$$\Rightarrow k^2q^2 - 4\ell_0^2 d = 4q^2 m.$$

Consequently $q^2 | 4\ell_0^2 d$ and so $q = 1, 2$ (since d is square-free and $(q, \ell_0) = 1$). Therefore we may write $b = \ell/2$ where ℓ is some rational integer.

We also have the following conditions which are consequences of the fact that $k^2 - \ell^2 d \equiv 0 \pmod 4$

i) $k \equiv \ell \equiv 0 \pmod 2$ when $d \equiv 2, 3 \pmod 4$

ii) $k \equiv \ell \pmod 2$ when $d \equiv 1 \pmod 4$.

These necessary conditions for β to be an algebraic integer are also sufficient conditions and so the ring of integers of $Q(\sqrt{d})$ is

i) $Z(\sqrt{d}) = \{(k + \ell\sqrt{d})/2 \mid k, \ell \in Z, k \equiv \ell \pmod 2\}$

when $d \equiv 1 \pmod 4$.

ii) $Z(\sqrt{d}) = \{(k + \ell\sqrt{d})/2 \mid k, \ell \in Z, k \equiv \ell \equiv 0 \pmod 2\}$

when $d \equiv 2, 3 \pmod 4$. (1)

Units of $Z(\sqrt{d})$

The structure of the group of units of $Z(\sqrt{d})$ may be determined by Dirichlet's theorem. The minimal polynomial for $\sqrt{d}$ over Q is $f(x) = x^2 - d$. When d is positive f has two real roots while when d is negative both roots are non-real. By theorem 1.7 we expect the following

a) $d < 0$ - $Z(\sqrt{d})$ has a finite number of units - each unit is a root of unity.

b) $d > 0$ - $Z(\sqrt{d})$ has an infinite number of units - each unit may be written as $\pm \eta_0^n$ $(n \in Z)$ where η_0 is a fundamental unit.

The norm of a quadratic unit gives rise to the diophantine equation

$$k^2 - \ell^2 d = \pm 4. \tag{2}$$

To find units of $Z(\sqrt{d})$ we seek solutions of (2) with k, ℓ subject to the restrictions in (1).

a) $\underline{d < 0}$

Since $k^2 - \ell^2 d \geq 0$, it is obvious that any solution of (2) must have $|k|, |\ell| \leq 2$. Thus the solutions of (2) are

$k = \pm 2, \quad \ell = 0$ for each d,

$k = \pm 1, \quad \ell = \pm 1$ for $d = -3$,

and $k = 0, \quad \ell = \pm 2$ for $d = -1$.

These solutions meet the restrictions given in (1) and so the units of $Z(\sqrt{d})$ are

for $d = -1$ the units are $\pm 1, \pm i$ - the fourth roots of unity,

for $d = -3$ the units are $\pm 1, (\pm 1 \pm \sqrt{-3})/2$ - the sixth roots of unity,

for $d \neq -1, -3$ the units are ± 1 - the square roots of unity.

b) $\underline{d > 0}$

As already noted, all units of $Z(\sqrt{d})$ may be expressed as $\pm \eta^n (n \in Z)$ where η is one of the four fundamental units of $Z(\sqrt{d})$. Since exactly one of these four units is greater than one we can uniquely define <u>the</u> fundamental unit to be the smallest unit greater than one. Henceforth η_d will denote <u>the</u> fundamental unit of $Z(\sqrt{d})$.

<u>Some Properties of Real Quadratic Units</u>

If $\eta = (k + \ell\sqrt{d})/2$ is any unit of $Z(\sqrt{d})$ then so are

$$N(\eta)(k - \ell\sqrt{d})/2 = \eta^{-1},$$

$$N(\eta)(-k + \ell\sqrt{d})/2 = -\eta^{-1},$$

and

$$(-k - \ell\sqrt{d})/2 = -\eta .$$

When $\eta \neq \pm 1$ exactly one of these four units is greater than one and so we have

<u>Lemma 2.1</u>

If $\eta = (k + \ell\sqrt{d})/2$ is a unit then $\eta > 1$ if and only if $k, \ell \geq 1$. //

Thus if $\eta_d = (k + \ell\sqrt{d})/2$, then k, ℓ is the minimum positive solution of (2). That is, k and ℓ are positive and if m, n is any other positive solution of (2) then $k \leq m$ and $\ell \leq n$.

<u>Lemma 2.2</u>

If $d \equiv 1 \pmod 8$ and $\eta = (k + \ell\sqrt{d})/2$ is a unit of $Z(\sqrt{d})$ then $k \equiv \ell \equiv 0 \pmod 2$. That is $\eta \in Z[1, \sqrt{d}]$.

Proof

If $k \equiv \ell \equiv 1 \pmod 2$ then $k^2 - \ell^2 d \equiv 0 \pmod 8$. //

Using these two lemmas we can obtain a lower bound on the size of η_d. When $d \equiv 5 \pmod 8$ $\eta_d \geq (1 + \sqrt{d})/2$ and in all other cases $\eta_d \geq 1 + \sqrt{d}$.

Lemma 2.3

Let $d \equiv 5 \pmod 8$ and $\eta = (k + \ell\sqrt{d})/2 \neq \pm 1$ be a unit such that $k \equiv \ell \equiv 1 \pmod 2$. Then $\eta^3 \in Z[1, \sqrt{d}]$ but $\eta^2 \notin Z[1, \sqrt{d}]$.

Proof

$$\eta^2 = ((k^2 + \ell^2 d) + 2k\ell\sqrt{d})/4$$

and
$$\eta^3 = ((k^3 + 3k\ell^2 d) + (3k^2\ell + \ell^3 d)\sqrt{d})/8.$$

We have
$$k^2 + \ell^2 d \equiv 2k\ell \equiv 2 \pmod 4$$

and so
$$\eta^2 \notin Z[1, \sqrt{d}].$$

However
$$k^3 + 3k\ell^2 d \equiv k(k^2 + 7\ell^2) \pmod 8$$
$$\equiv k(1 + 7) \pmod 8$$
$$\equiv 0 \pmod 8.$$

Similarly $3k^2\ell + \ell^3 d \equiv 0 \pmod 8$ and thus $\eta^3 \in Z[1, \sqrt{d}]$. //

From the norm of a unit we have

$$(k - \ell\sqrt{d}) = \pm 2/\eta \qquad (3)$$

Supposing $\eta > 1$ we obtain

i) $$k = \ell\sqrt{d} \pm 2/\eta \qquad (4)$$

ii) $$\eta = (k + \ell\sqrt{d})/2 = k \pm 1/\eta$$

and so
$$|\eta - k| = 1/\eta .$$

Thus, when η is large, $\ell\sqrt{d}$ and η are close approximations to the integer

k. In fact, for $\eta > 4$, knowledge of one of the values k, ℓ or η uniquely determines the values of the two integers k and ℓ. In particular $k = [\ell\sqrt{d} + 1/2]$ and $\ell = [k/\sqrt{d} + 1/2]$.

Example 1

$$\eta = (5564523 + 1543321\sqrt{13})/2 \text{ is a unit of } Z(\sqrt{13})$$

and has norm $N(\eta) = (5564523^2 - 1543321^2 \times 13)/4$.

We have $k = 5564523,$

$$\ell\sqrt{d} = 5564523.0000003594 \ldots,$$

and $\eta = 5564523.0000001797 \ldots$ //

If (3) is multiplied through by $2/\ell$ we obtain the most important form of approximation involving the coefficients k and ℓ,

$$(k/\ell - \sqrt{d}) = \pm 2/\ell\eta$$

$$= 4/\ell(k + \ell\sqrt{d}). \qquad (5)$$

Thus k/ℓ is a rational approximation to the irrational number $\sqrt{d}$. The following theorem shows that the closeness of approximation may be considered to be a function of $1/\ell^2$.

Theorem 2.1

Let $\eta = (k + \ell\sqrt{d})/2 > 1$ be a unit of $Z(\sqrt{d})$.

i) For $k \equiv \ell \equiv 0 \pmod 2$, set $k_0 = k/2$, $\ell_0 = \ell/2$.

Then $\eta = k_0 + \ell_0\sqrt{d}$

and $|k_0/\ell_0 - \sqrt{d}| < 1/2\ell_0^2$.

ii) For $k \equiv \ell \equiv 1 \pmod 2$

we have $|k/\ell - \sqrt{d}| < 1/2\ell^2$,

except for $d = 5, 13$.

Proof

i) $|k_0/\ell_0 - \sqrt{d}| = 1/\ell_0(k_0 + \ell_0\sqrt{d})$ from (5)

$\leq 1/\ell_0(2\ell_0\sqrt{d} - 1/\eta)$ from (4)

But $d \geq 2$ and $\eta \geq 1 + \sqrt{d}$ and so

$(2\ell_0\sqrt{d} - 1/\eta) > 2\ell_0$

ii) $|k/\ell - \sqrt{d}| = 4/\ell(k + \ell\sqrt{d})$ from (5)

$\leq 4/\ell(2\ell\sqrt{d} - 2/\eta)$ from (4)

$< 1/2\ell^2$ when $d \geq 21$.

From Lemma 2.2, the only values of $d < 21$ for which $k \equiv \ell \equiv 1 \pmod 2$ may occur are $d = 5$ and $d = 13$. //

When this theorem is viewed alongside the theory of simple continued fractions, we find that the problem of finding the fundamental unit of $Z(\sqrt{d})$ is solved.

Simple Continued Fractions(s.c.f.)

The following material (up to theorem 2.2) is covered by Chrystal [1959, II, pages 423 - 452], McCoy [1965, pages 96 - 119], Hardy and Wright [1960, pages 129 - 140], and Jones [1955, pages 76 - 91]. McCoy, Chrystal, and Jones also cover much of the material beyond theorem 2.2 with McCoy being the easiest to follow. However Chrystal covers more ground, especially on the form of the s.c.f. expansion of $\sqrt{d}$. Pettofrezzo and Byrkit [1970, pages 149 - 205] give an easy to read introduction to this material but some of the later results are only stated without proof.

A finite s.c.f. is an expression of the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}} \qquad (6)$$

Where $a_n \in Z$ and $a_n \geq 1$ for $n \geq 2$. The a_n are called the partial quotients or terms of the s.c.f. For convenience, the s.c.f. (6) is written as $(a_1, a_2, a_3, \ldots, a_m)$.

Any rational number can be represented as a finite s.c.f. and, conversely, any finite s.c.f. represents a rational number.

The convergents of (6) are the rational numbers

$$c_n = (a_1, a_2, \ldots, a_n), \quad n = 1, 2, \ldots, m.$$

Clearly c_m is equal to the value of the s.c.f. (6).

An infinite s.c.f. is an expression similar to (6) which does not terminate. The convergents of an infinite s.c.f. are defined in the same manner as those of a finite s.c.f.

If we define

$$p_1 = a_1, \qquad q_1 = 1,$$

$$p_2 = a_2p_1 + 1, \qquad q_2 = a_2,$$

and $$p_n = a_np_{n-1} + p_{n-2}, \qquad q_n = a_nq_{n-1} + q_{n-2}, \qquad (7)$$

for $n \geq 3$

then $$c_n = p_n/q_n \; \forall \; n \in Z^+$$

A proof by induction shows that

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^n$$

and consequently we have $(p_n, q_n) = 1$. That is p_n/q_n is the n^{th} convergent expressed in its lowest terms.

For any s.c.f. the convergents c_{2n+1} form a monotonic increasing sequence of rational numbers and the convergents c_{2n} form a monotonic decreasing sequence of rational numbers. Every odd numbered convergent is less than every even numbered convergent and if the s.c.f. is infinite the convergents tend to a limit as $n \to \infty$. Thus any infinite s.c.f. defines a unique irrational number. Conversely, any irrational number, x, can be represented as a unique infinite s.c.f. whose partial quotients are given by

$$x_1 = x, \; a_n = [x_n], \; x_{n+1} = 1/(x_n - a_n), \; n = 1,2,3, \ldots, \qquad (8)$$

x_n is called the n^{th} complete quotient and $x_n = (a_n, a_{n+1}, a_{n+2}, \ldots.)$ as a s.c.f.

The convergents of the s.c.f. for a real number, x, form a sequence of increasingly better rational approximations to x. All

convergents satisfy the inequality $|x - p_n/q_n| < 1/q_n^2$ and of every successive pair of convergents at least one satisfies the inequality $|x - p_n/q_n| < 1/2q_n^2$. The last inequality is, in fact, a sufficient condition to guarantee that a given rational number, p/q, is a convergent of the s.c.f. for x.

Theorem 2.2

If $p, q \in Z$ and $|x - p/q| < 1/2q^2$ then p/q is a convergent of the s.c.f. for x.

Proof

[Hardy and Wright, 1960, page 153], [McCoy, 1965, pages 119 - 122]. //

Theorems 2.1 and 2.2 give us the connection between the coefficients of a quadratic unit and simple continued fractions.

Theorem 2.3

Let $\eta = (k + \ell\sqrt{d})/2 > 1$ be a unit of $Z(\sqrt{d})$ such that either

i) $x \equiv y \equiv 0 \pmod 2$

or ii) $x \equiv y \equiv 1 \pmod 2$ but $d \neq 5, 13$.

Then $k/\ell = p_n/q_n$ where p_n/q_n is a convergent of the s.c.f. for $\sqrt{d}$. Moreover, if k and ℓ are odd then $k = p_n$ and $\ell = q_n$, and if k and ℓ are even then $k = 2p_n$ and $\ell = 2q_n$.

Proof

The theorem follows immediately from theorems 2.1 and 2.2 //

In particular, the coefficents of the fundamental unit are to be found amongst the convergents of the s.c.f. for $\sqrt{d}$, except in the cases when $d = 5$ and $d = 13$. However, by lemma 2.3, we can be assured of finding η_d^3 in these two cases.

Further theory will tell us which convergents of the expansion will give units but first we look at the form of the s.c.f. expansion of real quadratic surds of which $\sqrt{d}$ is a special case.

Periodic s.c.f.s and the Expansion of Quadratic Surds

A quadratic surd is an irrational number of the form $(a + b\sqrt{e})/c$, where a, b, c and e are rational numbers with $e > 0$. Such a number can always be rewritten in the form $(m + b\sqrt{d})/n$ where m, n, d and b are integers and $m^2 \equiv b^2 d \pmod{n}$.

A periodic s.c.f. is an infinite s.c.f. for which there exist fixed integers r and m such that $a_n = a_{n+r}$ for each $n \geq m$. We will assume that r and m are the minimum such integers. Such a s.c.f. is denoted by

$$(a_1, a_2, \ldots, a_{m-1}, \overline{a_m, a_{m+1}, \ldots, a_{m+r-1}}) \qquad (9)$$

The set of terms $a_m, a_{m+1}, \ldots, a_{m+r-1}$ is called the period and r is the length of the period. The set of terms $a_1, \ldots, a_{m-1}$ is called the pre-period. For any $n \geq m$, the n^{th} and $(n + r)^{th}$ complete quotients have the same expansion as s.c.f. and hence we have

$$x_n = x_{n+r}, \quad \forall\ n \geq m. \qquad (10)$$

Quadratic surds and periodic s.c.f. are linked by the following theorem.

Theorem 2.4

A s.c.f. is periodic if and only if it is the expansion of a real quadratic surd.

Proof

[Hardy and Wright, 1960, page 144]. //

It is also possible to characterize those quadratic surds whose s.c.f. expansion is purely periodic, that is, the value of m in (9) is one. Firstly we define a reduced quadratic surd to be a quadratic surd, $(a + b\sqrt{d})/c$, with the property that $(a + b\sqrt{d})/c > 1$ and $-1 < (a - b\sqrt{d})/c < 0$.

Theorem 2.5

A s.c.f. is purely periodic if and only if it is the expansion of a reduced quadratic surd.

Proof

[McCoy, 1965, page 133] //

The expansion of an irrational number is, in general, calculated by (8), but in the case of quadratic surds we have the following algorithm which simplifies the calculations.

Algorithm 2.1 [Hendy, 1975, page 1]

Let $\alpha = (a + b\sqrt{d})/c$ be an algebraic number of $Q(\sqrt{d})$, where $a, b, c, d \in Z$. Assume $b^2 d \equiv a^2 \pmod{c}$, $0 \leq a < \sqrt{d}/2$, and $d > 0$ is not a perfect square. Then in the s.c.f. expansion of α we have

$$a_n = [(P_n + b\sqrt{d})/Q_n] \qquad n = 1, 2, \ldots,$$

where $$P_n = a_{n-1} Q_{n-1} - P_{n-1} \qquad n = 2, 3, \ldots,$$

$$Q_n = (b^2 d - P_n^2)/Q_{n-1} \qquad n = 2, 3, \ldots,$$

and $$P_1 = a, \quad Q_1 = c. \qquad //$$

It is easily shown that P_n and Q_n are always rational integers. [Chrystal, 1959, II, page 455]. Recalling the n^{th} complete quotient x_n we have

$$x_n = (P_n + b\sqrt{d})/Q_n .$$

That is, the algorithm retains the n^{th} complete quotient in the form of a quadratic surd.

It is not always possible to recognize the end of the period by observation of the values of a_n alone. This is because the period or pre-period may be periodic to some extent.

However from (10) we have, when $n = m$,

$$(P_m + b\sqrt{d})/Q_m = (P_{m+r} + b\sqrt{d})/Q_{m+r} .$$

Thus $P_m = P_{m+r}$ and $Q_m = Q_{m+r}$ (otherwise we would have $\sqrt{d}$ equal to some rational number). Alternatively if $P_s = P_{s+t}$ and $Q_s = Q_{s+t}$ for some integers s and t then $s \geq m$ and $r \mid t$. If this was not so we could show that r or m was not minimal. Thus from the first occurrence of a

repetition of a pair P_n, Q_n we can determine the exact form (9) of the s.c.f. expansion.

We also have the following connection between P_{n-1}, q_{n-1} and Q_n.

Theorem 2.6

Let α and Q_n be as defined in Algorithm 2.1.
Set $\beta_n = p_n - \alpha q_n (n \geq 1)$ where p_n/q_n is the n^{th} convergent of α.

Then $Q_n = (-1)^{n-1} c\, N(\beta_{n-1})$, $n = 2, 3, 4, \ldots$

Proof

[Hendy, 1975, pages 1, 2]. //

This theorem will enable us to recognize which convergents of the s.c.f. for $\sqrt{d}$ give the coefficients of a unit without actually having to calculate the value of $p_{n-1}^2 - q_{n-1}^2 d$.

(For $\alpha = \sqrt{d}$, $N(\beta_{n-1}) = N(p_{n-1} - q_{n-1}\sqrt{d}) = N(p_{n-1} + q_{n-1}\sqrt{d})$)

The Simple Continued Fraction Expansion of $\sqrt{d}$

If we now take $a = 0$, $c = b = 1$ in Algorithm 2.1, we obtain the s.c.f. for $\sqrt{d}$. Chrystal [1959, II, pages 460 - 467] proves the following properties of the s.c.f. for $\sqrt{d}$.

i) The preperiod contains exactly one term, a_1. (This may also be proved from the fact that $\sqrt{d} + [\sqrt{d}]$ is a reduced quadratic surd).

ii) The sequences P_n, Q_n, a_n exhibit the following symmetries. ($p(d)$ is the length of the period of $\sqrt{d}$).

n	1	2	3 . . .	$p(d)-1$	$p(d)$	$p(d)+1$	$p(d)+2$	$p(d)+3$ . . .
P_n	0	P_2	P_3 . . .	P_4	P_3	P_2	P_2	P_3 . . .
Q_n	Q_1	Q_2	Q_3 . . .	Q_3	Q_2	Q_1	Q_2	Q_3 . . .
a_n	a_1	a_2	a_3 . . .	a_3	a_2	$2a_1$	a_2	a_3 . . .

and so $\sqrt{d} = (a_1, \overline{a_2, a_3, a_4, \ldots, a_4, a_3, a_2, 2a_1})$ //

iii) $0 \le P_n < \sqrt{d}$, $0 < Q_n < 2\sqrt{d}$, $0 < a_n < 2\sqrt{d}$. $P_n = 0$ only when $n = 1$.

iv) The middle of the period may be recognized by the first occurrence of either of the following conditions.

a) $P_n = P_{n+1}$

in which case $P_{n-1} = P_{n+2}$, $Q_{n-1} = Q_{n+1}$, $a_{n-1} = a_{n+1}$

$P_{n-2} = P_{n+3}$, $Q_{n-2} = Q_{n+2}$, $a_{n-2} = a_{n+2}$

etc.,

and the length of the period is even.

b) $Q_n = Q_{n+1}$ and $a_n = a_{n+1}$

in which case $P_n = P_{n+2}$

$P_{n-1} = P_{n+3}$, $Q_{n-1} = Q_{n+2}$, $a_{n-1} = a_{n+2}$

$P_{n-2} = P_{n+4}$, $Q_{n-2} = Q_{n+3}$, $a_{n-2} = a_{n+3}$

etc.,

and the length of the period is odd.

The advantage algorithm 2.1 has over (8) lies in the fact that at all times we are dealing with integers in the range 0 to $2\sqrt{d}$. If (8) is used to obtain the expansion of $\sqrt{d}$ it is not unusual to require the decimal value of $\sqrt{d}$ correct to at least $\sqrt{d}$ decimal digits. For

example, to calculate the expansion of $\sqrt{94}$ requires $\sqrt{94}$ correct to 13 decimal places.

Thus using (8), we often require multiprecision arithmetic for values of d larger than 100. However using algorithm 2.1 and a small calculator we can handle values of d as large as 10^8 (on an eight digit calculator).

An added bonus is that in view of iv) above we can recognize the expansion at its midpoint and no further work is required to obtain the complete expansion.

The Fundamental Unit of $Z(\sqrt{d})$

In view of theorem 2.6 the convergent p_n/q_n of $\sqrt{d}$ gives the coefficients of a unit if and only if $Q_{n+1} = 1$ or $Q_{n+1} = 4$. The values of n for which $Q_n = 1$ follow a precise pattern.

Theorem 2.7

$Q_n = 1$ if and only if $n = t\,p(d) + 1$, where t is some non-negative integer.

Proof

If $n = t\,p(d) + 1$ then $a_n = 2a_1$ from (11)

$= [(P_n + \sqrt{d})/Q_n]$.

Since $P_n \leq a_1$ and $[\sqrt{d}] = a_1$ it is clear that we must have $P_n = a_1$ and $Q_n = 1$.

Suppose that $Q_n = 1$. If $n = 1$ the result is trivial. Thus assume $n \geq 2$. Since $\sqrt{d} - P_n < Q_n < \sqrt{d} + P_n$ for $n \geq 2$ [Hickerson, 1973, page 430] it follows that $P_n = a_1$ and thus $a_n = 2a_1$. Now $P_{n+1} = a_n Q_n - P_n = a_1$

and $Q_{n+1} = (d - P_{n+1}^2)/Q_n = d - a_1^2$. But $P_2 = a_1$ and $Q_2 = d - a_1^2$. Thus $P_{n+j} = P_{1+j}$ and $Q_{n+j} = Q_{1+j}$, $\forall\ j \in Z^+$, and so $(n + j) - (1 + j) = n - 1$ is a multiple of the period length i.e. $n - 1 = t\ p(d)$ where t is some positive integer. //

The only time $Q_n = 4$ can occur is when $d \equiv 5 (\mathrm{mod}\ 8)$. However there is no way in which we can forecast if the value $Q_n = 4$ will appear in the expansion of a particular $\sqrt{d}$.

We now have enough information to outline the way in which the fundamental unit of $Z(\sqrt{d})$ may be obtained.

i) $d \equiv 2, 3 (\mathrm{mod}\ 4)$, $d \equiv 1 (\mathrm{mod}\ 8)$.

In this case $\eta_d \in Z[1, \sqrt{d}]$ and so we look for those convergents which give $p_n^2 - q_n^2 d = \pm 1$. From theorems 2.6 and 2.7 this occurs precisely when $n = t\ p(d)$ where $t \in Z^+$. (β_0 is not defined so we disregard the fact that $Q_1 = 1$). Since the coefficients of the fundamental unit are the minimum positive solution of $k_0^2 - \ell_0^2 d = \pm 1$, and since the integers p_n, q_n increase in size as n increases, it follows that

$$\eta_d = p_{p(d)} + q_{p(d)}\sqrt{d}$$

The positive powers of η_d are given by

$$\eta_d^t = p_{tp(d)} + q_{tp(d)}\sqrt{d}\ . \qquad (12)$$

Thus the coefficients k_0, ℓ_0 of η_d may be obtained by first obtaining the expansion of $\sqrt{d}$ from algorithm 2.1, then calculating $\ell_0 = q_{p(d)}$ by (7) and finally obtaining k_0 by (4), that is, by setting $k_0 = [\ell_0\sqrt{d} + 1/2]$ (except when $\eta < 4$). Using (4) to obtain k_0, instead of actually calculating $p_{p(d)}$ by (7), saves much work when p(d) is large.

ii) $d \equiv 5 \pmod 8$ and $d \neq 5, 13$.

There are two possibilities,

a) $\eta_d = k_0 + \ell_0\sqrt{d}$, $k_0, \ell_0 \in Z$,

b) $\eta_d = (k + \ell\sqrt{d})/2$, $k, \ell \in Z$.

If a) is the case then the coefficients of the fundamental unit will be given by the $p(d)^{th}$ convergent of the expansion of $\sqrt{d}$. If b) is the case then the $p(d)^{th}$ convergent will give the coefficients of η_d^3. By considering

$$\eta_d = (k + \ell\sqrt{d})/2,$$

$$\eta_d^2 = ((k^2 + \ell^2 d) + 2k\ell\sqrt{d})/4 = (k_1 + \ell_1\sqrt{d})/2,$$

and

$$\eta_d^3 = ((k^3 + 3k\ell^2 d) + (3k^2\ell + \ell^3 d)\sqrt{d})/8 = k_0 + \ell_0\sqrt{d},$$

we have that $k < k_1 < k_0$ and $\ell < \ell_1 < \ell_0$ (since $k \geq 4$ by (4)). Consequently $k/\ell = p_a/q_a$, $k_1/\ell_1 = p_b/q_b$, and $k_0/\ell_0 = p_{p(d)}/q_{p(d)}$, where $a < b < p(d)$ and $Q_{a+1} = Q_{b+1} = 4$.

Since we are not able to tell in advance whether a) or b) is the case, the fundamental unit is found by expanding $\sqrt{d}$ by algorithm 2.1 and noting the successive values of Q_n. The first occurrence of $Q_n = 4$ or $Q_n = 1$ $(n > 1)$ will give

$$\eta_d = (p_{n-1} + q_{n-1}\sqrt{d})/\sqrt{Q_n}\ .$$

When $\eta_d \in Z[1, \sqrt{d}]$, the positive powers of η_d are given by (12), otherwise we have

$$\eta_d^{3t+1} = (p_{a+t\,p(d)} + q_{a+t\,p(d)}\sqrt{d})/2, \quad t = 0, 1, 2, \ldots,$$

$$\eta_d^{3t+2} = (p_{b+t\,p(d)} + q_{b+t\,p(d)}\sqrt{d})/2, \quad t = 0, 1, 2, \ldots,$$

and

$$\eta_d^{3t} = p_{tp(d)} + q_{tp(d)}\sqrt{d}, \quad t = 1, 2, 3, \ldots,$$

To complete this section we note that

$$\eta_5 = (1 + \sqrt{5})/2,$$

and

$$\eta_{13} = (3 + \sqrt{13})/2.$$

The Length of the Period of $\sqrt{d}$

The amount of work required to calculate a particular η_d depends on the length of the period of $\sqrt{d}$. We have already seen that the period is of finite length and hence η_d is obtainable in a finite number of steps. However it has long been known that the period is not only finite but is also bounded by some function of d.

Chrystal [1959, II, page 457] shows that $p(d) < 2d$ in the following manner. In algorithm 2.1, the number of possible distinct pairs P_n, Q_n $(n > 1)$ is $[\sqrt{d}]\,[2\sqrt{d}] < 2d$, since $0 < P_n < \sqrt{d}$ and $0 < Q_n < 2\sqrt{d}$. The p(d) pairs of integers P_2, Q_2; P_3, Q_3; . . . ; $P_{p(d)}, Q_{p(d)}$; $P_{p(d)+1}, Q_{p(d)+1}$ must all be distinct and hence we have $p(d) < 2d$.

Recently several papers have been published which give much sharper bounds on the length of the period.

Hickerson [1973, pages 429 - 432] refines the argument of Chrystal by taking into consideration the fact that $Q_n \mid (d - P_n^2)$. Thus

we have that the number of pairs P_n, Q_n that can occur when expanding $\sqrt{d}$ is bounded by the cardinality of the set

$$T(d) = \{(p, q) | p, q \in Z^+, 0 < p < \sqrt{d}, q | (d - p^2)\} .$$

A result of Srinivasa Ramanujan enables Hickerson to obtain a bound on the cardinality of T(d), which is

$$d^{\frac{1}{2}} + \log 2/\log\log d + O(\log\log\log d/(\log\log d)^2) \qquad (13)$$

Thus p(d) is also bounded by this expression. This result best describes the behaviour of the maximum length of the period as $d \to \infty$. That is, given a $\delta > 0$, $\exists\, D_\delta \in Z^+$ such that $d > D_\delta$ implies $p(d) < d^{\frac{1}{2}} + \delta$.

For a more precise bound we turn to Stanton, Sudler and Williams [1976, pages 525 - 536]. A bound in terms of $L(1, \chi) = \sum_{n \geq 1} (\Delta | n) n^{-1}$ is obtained as

$$p(d) < \mu\sqrt{\Delta}\, L(1, \chi)/(2h \log \alpha)$$

where Δ is the discriminant of $Q(\sqrt{d})$

$(\Delta | n)$ is the Kronecker symbol

h is the class number of $Q(\sqrt{d})$

$\alpha = (1 + \sqrt{5})/2$

$\mu = 1$ if $\eta_d \in Z[1, \sqrt{d}]$

$\quad\; 3$ otherwise .

This is achieved as follows. Let $\eta = p_{p(d)} + q_{p(d)}\sqrt{d}$. It is easily shown that $\eta > \alpha^{p(d)}$. Consequently $p(d) < \log \eta / \log \alpha$. However $\eta = \eta_d^{\mu}$ and so $p(d) < \mu \log \eta_d / \log \alpha$. The bound is then obtained by using the result $\log \eta_d = \sqrt{\Delta}\, L(1, \chi)/2h$. Since $L(1, \chi) < A \log d$, we have $p(d) < Bd^{\frac{1}{2}} \log d$. The bulk of the paper is then concerned with finding numerical values for the constants A and B. The resulting bound is

$$p(d) < 0.72\, d^{\frac{1}{2}} \log d, \text{ for } d > 7 \tag{14}$$

Cohn [1977, pages 21 - 32] attacks the problem of finding an upper bound for p(d) by considering primitive classes of solutions of the equations

$$x^2 - y^2 d = N \ , \quad \text{where } |N| < 2\sqrt{d}. \tag{15}$$

A class of solutions is a set $(\pm X \pm Y\sqrt{d})\eta_1^n$, where $X + Y\sqrt{d}$ is a solution of (15), η_1 is the smallest positive power of η_d contained in $Z[1, \sqrt{d}]$ such that $N(\eta_1) = 1$, and n is any integer. A primitive class is one in which $(X, Y) = 1$. (It is shown that this is well-defined - that is, if $X_1 + Y_1\sqrt{d}$ and $X_2 + Y_2\sqrt{d}$ are in the same class then $(X_1, Y_1) = (X_2, Y_2)$). From theorem 2.6 we know that each convergent p_n/q_n gives a primitive solution, and it is easily shown that each $p_n + q_n\sqrt{d}$, $1 \le n \le p(d)$, is in a distinct primitive class. Consequently the number of distinct primitive classes of solutions of (15) is an upper bound for p(d).

The major part of the paper is then concerned with finding an upper bound for the number of distinct primitive classes of solutions of (15). The resulting bound is

$$(7/(2\pi^2))\, d^{\frac{1}{2}} \log d + O(d^{\frac{1}{2}}), \tag{16}$$

which is also the bound for p(d).

In arriving at their result Stanton et al show that $p(d) < .52\, d^{\frac{1}{2}} \log d$ for $d > D_1$ where D_1 is a computable constant ($D_1 \approx 10^{2434.25}$). However Cohn's result implies that

$$p(d) < (7/(2\pi^2))\, d^{\frac{1}{2}} \log d + A\, d^{\frac{1}{2}}, \quad A \text{ a constant}$$

$$= d^{\frac{1}{2}} \log d\, ((7/(2\pi^2)) + A/\log d)$$

Therefore, for $d > e^{A/0.165}$, Cohn's result is a sharper bound, and for sufficiently large d, Cohn's result gives the bound on p(d) as

$$p(d) < .355\, d^{\frac{1}{2}} \log d \qquad (17)$$

Consequently as $d \to \infty$, the best bound we have for p(d) is given by (17). (For large d, (13) is greater than $d^{\frac{1}{2}} \log d$). Lehmer [1969, page 139] has suggested that p(d) may be as large as $0.3\, d^{\frac{1}{2}} \log d$ for large d and so Cohn has noted that it is possible that (16) cannot be significantly improved upon.

It should be remembered that although we have these upper bounds for p(d), the actual value of p(d) may lie anywhere in the range 1 to $A\, d^{\frac{1}{2}} \log d$. (A depending on which bound is appropriate).

Example 2

i) For d = 1726 we have

$$p(d) = 88 \quad \text{[Hickerson, 1973, page 429]}$$

$$\approx .265\, d^{\frac{1}{2}} \log d\ .$$

ii) For $d = 1722 = 41^2 + 41$ we have

$$\sqrt{1722} = (41, \overline{2, 82}) \qquad \text{and } p(d) = 2. \qquad //$$

Thus it can be seen that the bound is not necessarily an indication of

the size of p(d).

The bounds so far obtained are for arbitrary d. However, in many cases it is possible to lower the bound considerably.

Stanton et al show that for $d > 1.27 \times 10^6$ (14) may be multiplied by 2^{-t}, where t is defined as

$$t = \begin{cases} r - 1 \text{ if } d \text{ is the sum of two squares} \\ r - 2 \text{ otherwise} \end{cases}$$

and r is the number of distinct prime factors of Δ.

Example 3

Let $d = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 = 9{,}699{,}690$. Then $d \equiv 2 \pmod 4$ and so $\Delta = 4d$, $r = 8$ and $t = 6$ since d is not the sum of two squares. Thus (14) would initially give

$$p(d) < .72\, d^{\frac{1}{2}} \log d \approx 36074.7 ,$$

but multiplying by 2^{-t} gives

$$p(d) < 563.7$$

In fact $p(d) = 36$. //

Of course if we are to employ this fact in obtaining a sharper bound on p(d), extra work is required to factor d, and if d has few prime factors, little or no improvement on the bound will be obtained.

In many special cases it is possible to give the exact form of the s.c.f. expansion of $\sqrt{d}$, and hence the exact value of p(d). For example, letting $d = a_1^2 + r$, where $a_1 = [\sqrt{d}]$, we have

i) If $r = 1$, then $\sqrt{d} = (a_1, \overline{2a_1})$ and $p(d) = 1$.

ii) If $r \mid 2a_1$, $r \neq 1$, then $\sqrt{d} = (a_1, 2a_1/r, 2a_1)$ and $p(d) = 2$.

iii) If $\exists$ $m, n \in Z^+$ such that $a_1 = n(4m^2 + 1) + m$ and $r = 4mn + 1$, then $\sqrt{d} = (a_1, 2m, 2m, 2a_1)$ and $p(d) = 3$

These are easily verified by expanding the various forms of d by algorithm 2.1. The list can be extended to larger values of p(d).

Finally it should be noted that there are infinitely many values of d for which the last two approaches offer no extra information about the size of p(d) and in these cases the only information we have is given by (14) and (16).

An Alternative Approach for $d \equiv 1 \pmod 4$

In this section we assume that $d \equiv 1 \pmod 4$. An integral basis for $Z(\sqrt{d})$ is $1, \omega = (1 + \sqrt{d})/2$. Thus $Z(\sqrt{d}) = \{k + \ell\,\omega \mid k, \ell \in Z\}$. The norm of any integer $\beta = k + \ell\,\omega \in Z(\sqrt{d})$ is now given by

$$N(\beta) = (k + \ell\,\omega)(k + \ell\,\bar{\omega}) \text{ where } \bar{\omega} = (1 - \sqrt{d})/2 \qquad (18)$$

Suppose that $\eta = (k_1 + \ell\sqrt{d})/2 > 1$ is a unit of $Z(\sqrt{d})$. Then $N(\eta)\eta^{-1} = (k_1 - \ell\sqrt{d})/2$ is also a unit of $Z(\sqrt{d})$ and may be written in terms of the integral basis as

$$(k_1 - \ell\sqrt{d})/2 = (k - \ell\,\omega) \quad \text{where } k = (k_1 + \ell)/2 \in Z$$

Since k_1 and ℓ are both positive it follows that k is positive. From (18)

$$|k - \ell\omega| = 1/(k - \ell\bar{\omega}) .$$

Since $|k - \ell\omega| \leq 2/(1 + \sqrt{d})$

we have $k - \ell\bar{\omega} \geq \ell\omega - 2/(1 + \sqrt{d}) - \ell\bar{\omega}$

$= \ell\sqrt{d} - 2/(1 + \sqrt{d})$

$> 2\ell$, except when $d = 5$ and $\ell = 1, 2$.

This gives us a parallel to theorem 2.3.

Theorem 2.8

Suppose $d \neq 5$. If $\eta = (k_1 + \ell\sqrt{d})/2 > 1$ is a unit of $Z(\sqrt{d})$, then letting $k = (k_1 + \ell)/2$ we have that $k - \ell\omega = N(\eta)\eta^{-1}$ is a unit and

$$|k/\ell - \omega| < 1/2\ell^2 .$$

Since $(k, \ell) = 1$ we have $k = p_n$, $\ell = q_n$ for some convergent p_n/q_n of the s.c.f. for ω. //

The Expansion of ω

Since $d \equiv 1 \pmod 2$, ω can be expanded without adjustment by algorithm 2.1. To obtain some idea of the form of the expansion we firstly look at reduced quadratic surds associated with ω.

Let $a_1 = [\sqrt{d}]$ and suppose that a_1 is even. Then $(a_1 - 1 + \sqrt{d})/2$ is a reduced quadratic surd and consequently it has a purely periodic s.c.f.

Thus $$(a_1 - 1 + \sqrt{d})/2 = (\overline{\hat{a}_1, a_2, \ldots, a_r}), \qquad (19)$$

where $\hat{a}_1 = [(a_1 - 1 + \sqrt{d})/2] = a_1 - 1$. We can rewrite (19)

as $$(a_1 - 2)/2 + \omega = (a_1 - 1, \overline{a_2, \ldots, a_r, a_1 - 1})$$

and thus, since $(a_1 - 2)/2 \in Z$,

$$\omega = (a_1/2, \overline{a_2, \ldots, a_r, a_1 - 1}).$$

In a similar manner we can derive

$$\omega = ((a_1 + 1)/2, \overline{a_2, \ldots, a_r, a_1}) \qquad (20)$$

for the case where a_1 is odd. Thus the period starts after the first term (except for $d = 5$ where $(1 + \sqrt{5})/2 = (\bar{1})$).

By slightly modifying Chrystal's proofs [1959, II, pages 460 - 467] it is easily shown that when ω is expanded by algorithm 2.1 P_n, Q_n and a_n exhibit almost exactly the same relationships as they do in the expansion of $\sqrt{d}$.

We have i) letting r be the length of the period and $a = [\omega]$.

n	1	2	3 . . .	$r-1$	r	$r+1$	$r+2$	$r+3$
P_n	$P_1=1$	P_2	P_3 . . .	P_4	P_3	P_2	P_2	P_3
Q_n	$Q_1=2$	Q_2	Q_3 . . .	Q_3	Q_2	Q_1	Q_2	Q_3
a_n	a	a_2	a_3 . . .	a_3	a_2	$2a-1$	a_2	a_3

ii) $1 \le P_n < \sqrt{d}$, $1 \le Q_n < 2\sqrt{d}$, $1 \le a_n < 2\sqrt{d}$, $\forall\, n \in Z^+$

iii) the middle of the period may be recognised in precisely the same manner as for $\sqrt{d}$.

Recalling theorem 2.5 we have

$$Q_n = 2(-1)^{n-1} N(p_{n-1} - q_{n-1}\omega) . \qquad (21)$$

Since $(p_{n-1} - q_{n-1}\omega) \in Z(\sqrt{d})$, $N(\beta_{n-1})$ must be a rational integer and so Q_n is always even. Consequently P_n is always odd (since $Q_n \mid (d - P_n^2)$),

and ii) above may be modified to give $0 < a_n < \sqrt{d}$, $\forall$ n.

Obtaining Units from the Expansion of ω

From (21) we have that $p_{n-1} - q_{n-1}\omega$ is a unit if and only if $Q_n = 2$. The values of n for which $Q_n = 2$ follow exactly the same pattern as the one that was found for the values of n for which $Q_n = 1$ in the expansion of $\sqrt{d}$.

Theorem 2.9

Let r be the length of the period of ω. Then $Q_n = 2$ if and only if $n = tr + 1$, $t = 0, 1, 2, \ldots$

Proof

Let $a_1 = [\sqrt{d}]$ and assume that a_1 is odd. Suppose $Q_n = 2$ and $n \neq 1$. By extending a theorem of Hickerson [1973, page 430] we have $\sqrt{d} - P_m < Q_m < \sqrt{d} + P_m$ for $m > 1$. Thus $\sqrt{d} - P_n < Q_n$ and since we must have $P_n < \sqrt{d}$ and P_n odd it follows that $P_n = a_1$. $P_n = a_1$ and $Q_n = 2$ implies $a_n = [(a_1 + \sqrt{d})/2] = a_1$. Therefore $P_{n+1} = 2a_1 - a_1 = a_1$ and $Q_{n+1} = (d - a_1^2)/2$. However, since $P_1 = 1$, $Q_1 = 2$ and $a = (a_1 + 1)/2$, it follows that $P_{n+1} = P_2$ and $Q_{n+1} = Q_2$. Thus $(n + 1) - 2 = n - 1$ is a multiple of r.

Conversely, if $n = tr + 1 > 1$, then from (20) we have $a_n = a_1$. If $Q_n \neq 2$ then $Q_n \geq 4$ and $a_n \leq [(a_1 + \sqrt{d})/4] = [a_1/2] < a_1$. Thus we must have $Q_n = 2$.

Noting that $Q_1 = 2$ completes the proof for the case a_1 odd.

The case where a_1 is even is proved in a similar manner. //

In view of this theorem we have that $(p_{tr} - q_{tr}\omega)$ is a unit for each $t \in Z^+$. The r^{th} convergent gives

$$\eta_d^{-1} N(\eta_d) = p_r - q_r\omega ,$$

and so from theorem 2.8 we have

$$\eta_d = (2p_r - q_r + q_r\sqrt{d})/2$$

In fact the positive powers of η_d are given by

$$\eta_d^t = (2p_{tr} - q_{tr} + q_{tr}\sqrt{d})/2 .$$

Comparison

For $d \equiv 1 \pmod 4$ we now have two ways in which η_d can be calculated. That is, we can use the expansion of $\sqrt{d}$ or the expansion of ω. The question which naturally arises is whether one method is more efficient than the other. A comparison of the number of terms of the s.c.f. which must be calculated in order to obtain η_d for $5 \leq d \leq 100005$, $d \equiv 5 \pmod 8$ gives the following results.

i) For 24.65% of the values of d the number of terms which must be calculated is the same.

ii)

	Average No.terms using $\sqrt{d}$	Average No.terms using ω
$5 \leq d \leq 25005$	21.80	22.06
$5 \leq d \leq 50005$	29.66	29.95
$5 \leq d \leq 75005$	35.48	35.75
$5 \leq d \leq 100005$	40.12	40.40

These results suggest that there is slightly less work involved if the expansion of $\sqrt{d}$ is used. However the difference is so marginal that we can ignore it unless we wish to produce tables of η_d for a large number of d.

3 UNITS OF PURE CUBIC FIELDS

$Q(\alpha)$ is called a cubic field if the minimal polynomial for α is a cubic. If α is also the cube root of a rational number then $Q(\alpha)$ is called a pure cubic field. We can assume without loss of generality that α is the cube root of a positive cube-free rational integer, d.

The Integers of $Q(d^{1/3})$

Let d be a positive cube-free rational integer and let $\delta = d^{1/3}$. We shall assume $\delta \in R$ and thus $Q(\delta)$ will be a real field. We can write $d = pq^2$ where p, q are two distinct relatively prime positive square-free integers. Any $\beta \in Q(\delta)$ can be written as

$$\beta = a + b\delta + c_0\delta^2 \quad a, b, c_0 \in Q .$$

However, since $\delta^2 = (p^2 q^4)^{1/3} = q(p^2 q)^{1/3}$, β is more conveniently written as

$$\beta = a + b\delta + c\emptyset$$

where $\emptyset = (p^2q)^{1/3}$ and $c = c_0 q$.

The conjugates of β are

$$\beta_1 = a + b\delta\mu + c\emptyset\mu^2 ,$$

and $$\beta_2 = a + b\delta\mu^2 + c\emptyset\mu , \qquad (1)$$

where $\mu = (-1 + \sqrt{-3})/2$.

Thus the cubic polynomial for β is

$$g(X) = (X - \beta)(X - \beta_1)(X - \beta_2)$$

$$= X^3 - 3aX^2 + 3(a^2 - pqbc)X - N(\beta)$$

where $N(\beta) = a^3 + b^3pq^2 + c^3p^2q - 3abcpq$

Theorem 3.1

The integers of $Q(\delta)$, $\delta^3 = pq^2$, are the numbers

$$\beta = (x + y\delta + z\emptyset)/3 , \quad x, y, z \in Z,$$

with $x \equiv y \equiv z \equiv 0 \pmod 3$ when $pq^2 \not\equiv \pm 1 \pmod 9$ (type I fields), and $x \equiv py \equiv qz \pmod 3$ when $pq^2 \equiv \pm 1 \pmod 9$ (type II fields).

Proof

Sved [1970, page 142] gives $1, \delta, \emptyset$ as an integral basis for the integers of type I fields, and $(1 + p\delta + q\emptyset)/3, \delta, \emptyset$ as an integral basis for the integers of type II fields.

For type I fields the statement in the theorem is obviously equivalent to that given by Sved.

For type II fields we note

i) $\beta = (x + y\delta + z\emptyset)/3 = x(1 + p\delta + q\emptyset)/3 +$

$+ \delta(y - px)/3 + \emptyset(z - qx)/3, \quad x \equiv yp \pmod 3 \Rightarrow xp \equiv y \pmod 3$

(since $3 \nmid p$) and so $(y - px)/3$ is an integer. Similarly $(z - qx)/3$ is an integer and so β can be expressed in terms of the integral basis given by Sved.

ii) Let $a, b, c \in Z$.

Then $a(1 + p\delta + q\emptyset)/3 + b\delta + c\emptyset = (a + (ap + 3b)\delta + (aq + 3c)\emptyset)/3$

Letting $x = a$, $y = ap + 3b$, $z = aq + 3c$ we have $py \equiv ap^2 \equiv a \equiv x \pmod 3$ and $qz \equiv aq^2 \equiv a \equiv x \pmod 3$. Thus the statement in the theorem is again equivalent to that given by Sved. //

Units of $Z(\delta)$

The minimal polynomial for δ is $f(X) = X^3 - d$. Since f has one real root and two non-real roots we have, by theorem 1.7, that there exists a unit $\eta \in Z(\delta)$ such that any unit of $Z(\delta)$ can be expressed in the form $\xi\eta^n$, where ξ is a root of unity and n is an integer. Since f has one real root we have that $\xi = \pm 1$. Thus there are four units which we could take as fundamental. Of these four units only one is greater than unity. We shall denote this unit by η_d.

In many works η_d^{-1} is taken as <u>the</u> fundamental unit. (For example, Sved [1970] and Beach, Williams and Zarnke [1971]). One reason for doing this is that the coefficients of η_d^{-1} are of the order of the square root of the coefficients of η_d. However Shanks [1975, page 330] notes that for applications involving the fundamental unit of $Z(\delta)$ it is usually preferable to use η_d as the fundamental unit. Since many of the results to be presented in this chapter involve units $\eta > 1$ we shall take η_d as <u>the</u> fundamental unit.

We now develop some of the properties of cubic units. For the rest of this chapter we shall assume that η is a unit of $Z(\delta)$ such that

$$\eta = (x + y\delta + z\emptyset)/3 > 1.$$

When η is a unit of a type I field we shall sometimes write η in the form

$$\eta = x_0 + y_0\delta + z_0\emptyset \ , \ x_0, y_0, z_0 \in Z$$

where $x = 3x_0$, $y = 3y_0$ and $z = 3z_0$.

From (1) the conjugates of η are

$$\eta' = (x + y\delta\mu + z\emptyset\mu^2)/3$$

and $$\eta'' = (x + y\delta\mu^2 + z\emptyset\mu)/3, \ \mu = (-1 + \sqrt{-3})/2 \qquad (2)$$

Thus $$N(\eta) = \eta\eta'\eta''$$

$$= (x^3 + y^3pq^2 + z^3p^2q - 3xyzpq)/27 .$$

The norm of η may be rewritten as

$$N(\eta) = \eta((x^2 - pqyz) + (pz^2 - xy)\delta + (qy^2 - xz)\emptyset)/9$$

$$= \eta((x - y\delta)^2 + (y\delta - z\emptyset)^2 + (z\emptyset - x)^2)/18 \qquad (3)$$

Since the second term of (3) is positive definite we have that η and $N(\eta)$ have the same sign. Thus we have

Lemma 3.1

If η is a unit of $Z(\delta)$ such that $\eta > 1$ then $N(\eta) = 1$ //

Thus $$\eta^{-1} = \eta'\eta'' = ((x^2 - pqyz) + (pz^2 - xy)\delta + (qy^2 - xz)\emptyset)/9$$

We now prove a theorem from which many of the later results of this chapter will be derived.

Theorem 3.2

Let $\eta = (x + y\delta + z\emptyset)/3 > 1$ be a unit of $Z(\delta)$, $\delta^3 = d > 0$, d cube free.

Then i) $|x - y\delta| \leq \sqrt{3}(A\sqrt{3} + B)/\eta^{\frac{1}{2}} < 3.47/\eta^{\frac{1}{2}}$

ii) $|x - z\emptyset| \leq \sqrt{3}(A\sqrt{3} + B)/\eta^{\frac{1}{2}} < 3.47/\eta^{\frac{1}{2}}$

iii) $|z\emptyset - y\delta| = 2\sqrt{3}B/\eta^{\frac{1}{2}} < 3.47/\eta^{\frac{1}{2}}$

iv) $|\eta - x| \leq 2(A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}} < 2.31/\eta^{\frac{1}{2}}$

v) $|\eta - y\delta| \leq (A\sqrt{3} + B)/\eta^{\frac{1}{2}} \leq 2/\eta^{\frac{1}{2}}$

vi) $|\eta - z\emptyset| \leq (A\sqrt{3} + B)/\eta^{\frac{1}{2}} \leq 2/\eta^{\frac{1}{2}}$

where $A, B \geq 0$ and $A^2 + B^2 = 1$.

Proof

From (2) we have

$$\eta' = (x + y\delta\mu + z\emptyset\mu^2)/3, \quad \mu = (-1 + \sqrt{-3})/2$$

$$= (x - (y\delta + z\emptyset)/2)/3 + i(\sqrt{3}\delta y - \sqrt{3}\emptyset z)/6 . \qquad (4)$$

Similarly $\eta'' = (x - (y\delta + z\emptyset)/2)/3 - i(\sqrt{3}y\delta - \sqrt{3}z\emptyset)/6$

Thus $|\eta'| = |\eta''|$, and since $\eta\eta'\eta'' = 1$ we also have $|\eta'| = 1/\eta^{\frac{1}{2}}$.

Consequently we can set

$$|(x - (y\delta + z\emptyset)/2)/3| = A/\eta^{\frac{1}{2}} \qquad (5)$$

and

$$|\sqrt{3}(y\delta - z\emptyset)/6| = B/\eta^{\frac{1}{2}} \qquad (6)$$

and then from (4) we have

$$|\eta'| = (A^2/\eta + B^2/\eta)^{\frac{1}{2}} = (A^2 + B^2)^{\frac{1}{2}}/\eta^{\frac{1}{2}}$$

Thus $A^2 + B^2 = 1$ and $A, B \geq 0$.

Rewriting (6) gives $|y\delta - z\emptyset| = 2\sqrt{3}\, B/\eta^{\frac{1}{2}}$ which is iii) of the theorem.

To obtain i) we note that

$$x - (y\delta + z\emptyset)/2 = x - (y\delta + y\delta \pm 2\sqrt{3}\, B/\eta^{\frac{1}{2}})/2$$

$$= x - y\delta \pm \sqrt{3}\, B/\eta^{\frac{1}{2}}$$

and thus from (5) we have

$$|x - (y\delta + z\emptyset)/2| = 3A/\eta^{\frac{1}{2}}$$

$$\Rightarrow \quad |x - y\delta| \leq 3A/\eta^{\frac{1}{2}} + \sqrt{3}\, B/\eta^{\frac{1}{2}}$$

We obtain ii) in a similar manner.

Using i) and ii) we now have

$$\eta = (x + y\delta + z\emptyset)/3$$

$$\geq x/3 + (x/3 - (A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}}) + (x/3 - (A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}})$$

$$= x - 2(A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}}$$

In a similar manner we have

$$\eta \leq x + 2(A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}},$$

and so

$$|\eta - x| \leq 2(A\sqrt{3} + B)/\sqrt{3}\eta^{\frac{1}{2}}.$$

v) and vi) are obtained in the same manner as iv).

To find an upper bound for $A\sqrt{3} + B$ we set $A = \cos\theta$, $B = \sin\theta$ (since $A^2 + B^2 = 1$) and then maximize $\sqrt{3}\cos\theta + \sin\theta$ for $\theta \in [0, \pi/2]$. Differentiating with respect to θ and setting the result equal to zero produces

$$\cos\theta = \sqrt{3}\sin\theta \Rightarrow \tan\theta = 1/\sqrt{3}$$

Thus $\theta = \pi/6$ and the corresponding maximum is $\sqrt{3}\cos\pi/6 + \sin\pi/6 = 2$. The right hand side of each inequality now follows. //

Thus when η is large the four numbers η, x, $y\delta$, and $z\emptyset$ will be close approximations to each other. In particular we note that η is a

close approximation to a rational integer. (Compare the quadratic case where a similar result was obtained).

Example 3.1

Let $\delta = 21^{1/3}$. From Sved [1970, page 144],

$$\eta = (5115 + 1854\delta + 672\emptyset)/3$$

is a unit of $Z(\delta)$.

We have $x = 5115$,

$y\delta = 5115.0454 \ldots$,

$z\emptyset = 5115.0372 \ldots$, $(3.47/\eta^{\frac{1}{2}} = 0.048 \ldots)$

and $\eta = 5115.0275 \ldots$

$(2.31/\eta^{\frac{1}{2}} = 0.0322 \ldots$ and $2/\eta^{\frac{1}{2}} = 0.0279 \ldots)$ //

It is fairly obvious from theorem 3.2 that when η is large, x, y and z will all be positive integers. In fact this is true for any unit $\eta > 1$.

Theorem 3.3

Let $\eta = (x + y\delta + z\emptyset)/3$ be a unit of $Z(\delta)$. Then $\eta > 1$ if and only if $x, y, z > 0$.

Proof

Clearly $x, y, z > 0$ implies $\eta > 1$. To show that the converse is true we firstly show that for $\eta > 1$ the coefficients x, y and z are non-zero.

If at least one of x, y, z is zero then from theorem 3.1 we have $x \equiv y \equiv z \equiv 0 \pmod 3$ and so we can write $x/3 = x_0$, $y/3 = y_0$,

$z/3 = z_0,\ x_0,\ y_0,\ z_0 \in Z$.

Suppose $x = 0$. Then $N(\eta) = y_0^3pq^2 + z_0^3p^2q = 1$ which implies $pq \mid 1$. However $pq^2 > 1$ and so $pq \nmid 1$. Thus x cannot be zero. If $y = z = 0$ then $\eta = 1$ which has been excluded from consideration. Thus the only cases left to consider are $x, z \neq 0$, $y = 0$ and $x, y \neq 0$, $z = 0$.

Suppose $y = 0$. Then $N(\eta) = x_0^3 + z_0^3p^2q = 1$. Since x_0 and z_0 are non-zero they must differ in sign and so

$$x_0^3z_0^3p^2q < 0 \Rightarrow x_0z_0\emptyset < 0 \tag{7}$$

However
$$\eta^3 = x_0^3 + z_0^3p^2q + 3x_0z_0\emptyset(x_0 + z_0\emptyset)$$
$$= 1 + 3x_0z_0\emptyset\eta$$

and so (7) implies $\eta^3 < 1$. This contradicts the fact that $\eta > 1$. Thus $y \neq 0$.

If $z = 0$ then a similar argument leads to a contradiction. Thus x, y, z are non-zero.

We now show that $x, y, z > 0$. From v) of theorem 3.2 we have $|\eta - y\delta| < 2$ (since $\eta^{\frac{1}{2}} > 1$). Thus $y\delta > -2 + \eta > -1$ and so $y > -1$ since $\delta > 1$. Since y is non-zero it follows that y must be positive. Using vi) of theorem 3.2 shows that z must also be positive.

From iv) of theorem 3.2 we now have

$$x \geq -2.31 + \eta$$
$$\Rightarrow \quad x > -1.31$$

Thus $x = -1$ or $x > 0$. If $x = -1$ then we must have $pq^2 \equiv \pm 1 \pmod 9$ and thus $pq \geq 10$. Remembering that $y, z > 0$, we have

$$N(\eta) = (-1 + y^3pq^2 + z^3p^2q + 3yzpq)/27$$

$$\geq (-1 + 10 + 10 + 30)/27$$

$$> 1$$

Thus $x = -1$ is impossible and so $x > 0$. //

Using theorems 3.2 and 3.3 we can obtain a lower bound for η_d. The method is shown in the following example.

Example 3.2

a) Let $d = 2$. Then $p = 2$, $q = 1$ and $Q(\delta)$ is a type I field. From theorem 3.2 vi) we have

$$|\eta_d - z\emptyset| \leq 2/\eta_d^{\frac{1}{2}}$$

Theorem 3.3 shows that $z > 0$ and since $z \equiv 0 \pmod 3$ we have $z \geq 3$. Thus

$$\eta_d \geq 3\emptyset - 2/\eta_d^{\frac{1}{2}}$$

Since $\eta_d^{\frac{1}{2}} > 1$ we obtain

$$\eta_d \geq 3 \times 4^{1/3} - 2 > 2.76 .$$

However this implies $\eta_d^{\frac{1}{2}} > 1.66$ and so we have

$$\eta_d \geq 3 \times 4^{1/3} - 2/1.66 > 3.55$$

Continuing in this iterative manner we obtain

$$\eta_d > 3.7$$

b) Let d = 10. Then p = 10, q = 1 and $Q(\delta)$ is a type II field. We have $z \geq 1$ and so from vi) of theorem 3.2

$$\eta_d \geq \emptyset - 2/\eta_d^{\frac{1}{2}}$$

Starting with $\eta_d = 1$ we iterate as in the previous case and after 4 steps obtain $\eta_d > 3.6$. //

Pure Cubic Units and Simple Continued Fractions

In chapter two we found that the problem of obtaining units of $Q(\sqrt{d})$ was solved by the use of simple continued fractions. That we were able to do this depended upon the fact that the coefficients of any unit greater than one gave a good rational approximation to $\sqrt{d}$. Although theorem 3.2 shows that x/y is a rational approximation to δ, x/z is a rational approximation to $\emptyset$, and y/z is a rational approximation to $\emptyset/\delta$, the closeness of approximation is not good enough to guarantee that x/y, x/z and y/z are convergents of the simple continued fraction for δ, $\emptyset$ and $\emptyset/\delta$ respectively, except in cases where x, y, z are 'small'. The following theorem defines what is meant by x, y, z 'small'.

Theorem 3.4

Let $\eta = (x + y\delta + z\emptyset)/3 > 1$ be a unit of $Z(\delta)$. For type I fields we can write $\eta = x_0 + y_0\delta + z_0\emptyset$ ($x_0, y_0, z_0 \in Z$, $x = 3x_0$, $y = 3y_0$, $z = 3z_0$), and we have

$$z_0 < 9\delta^2\emptyset/16 - 1 \Rightarrow y_0/z_0 \text{ is a convergent of the s.c.f. expansion of } \emptyset/\delta .$$

For type II fields, except when d = 289,361, we have

$z < \delta^2\phi/48 - 1 \Rightarrow y/z$ is a convergent of

the s.c.f. expansion of ϕ/δ.

Proof

From theorem 3.2 we have

$$|z\phi - y\delta| < 2\sqrt{3}/\eta^{\frac{1}{2}} ,$$

and thus

$$|\phi/\delta - y/z| < 2\sqrt{3}/z\delta\eta^{\frac{1}{2}} \qquad (8)$$

For type I fields

$$z_0 < 9\delta^2\phi(1 - 2/3z_0\phi)/16$$

$$\Rightarrow \quad z_0 < 9\delta^2\phi(1 - 2/3z_0\phi\eta^{\frac{1}{2}})/16 \quad \text{since } \eta > 1$$

$$\Rightarrow \quad 16z_0^2 < 3\delta^2(3z_0\phi - 2/\eta^{\frac{1}{2}})$$

$$\Rightarrow \quad 16z_0^2 < 3\delta^2\eta \qquad \text{from theorem 3.2}$$

$$\Rightarrow \quad 4z_0 < \sqrt{3}\delta\eta^{\frac{1}{2}}$$

$$\Rightarrow \quad 4z_0^2 < \sqrt{3}z_0\delta\eta^{\frac{1}{2}}$$

$$\Rightarrow \quad 2/\sqrt{3}z_0\delta\eta^{\frac{1}{2}} < 1/2z_0^2 \qquad (9)$$

From (8), (9) and theorem 2.2 we now have

$$z_0 < 9\delta^2\phi(1 - 2/3z_0\phi)/16 \Rightarrow |y_0/z_0 - \phi/\delta| < 1/2z_0^2$$

$$\Rightarrow y_0/z_0 \text{ is a convergent of}$$

the s.c.f. for ϕ/δ .

When $d \neq 2$ we have $3\delta^2/8 < 9\delta^2\phi/16 - 1$ and thus

$$z_0 < 9\delta^2\phi/16 - 1 \Rightarrow z_0 \leq 3\delta^2/8 \text{ or } 3\delta^2/8 < z_0 < 9\delta^2\phi/16 - 1$$

However $3\delta^2/8 < z_0 \Rightarrow 3\delta^2/8z_0 < 1$, and so

$$z_0 < 9\delta^2\emptyset/16 - 1 \quad \Rightarrow z_0 \leq 3\delta^2/8 \text{ or } 3\delta^2/8 < z_0 < 9\delta^2\emptyset/16 - 3\delta^2/8z_0$$

$$\Rightarrow z_0 < 9\delta^2\emptyset/16 - 3\delta^2/8z_0$$

$$\Rightarrow z_0 < 9\delta^2\emptyset(1 - 2/3z_0\emptyset)/16$$

Thus the result is now clear for $d \neq 2$. When $d = 2$ the result is trivial since $9\delta^2\emptyset/16 - 1 \approx 0.42$.

For type II fields we can show (in a manner similar to the type I field case)

$$z < \delta^2\emptyset/48 - \delta^2/24z \Rightarrow y/z \text{ is a convergent of the s.c.f. for } \emptyset/\delta \ .$$

To complete the proof we must show that when $d \neq 289,361$

$$z < \delta^2\emptyset/48 - 1 \Rightarrow z < \delta^2\emptyset/48 - \delta^2/24z \qquad (10)$$

When $\delta^2 < 24$ (10) clearly holds. (10) also holds when $\delta^2/24 < \delta^2\emptyset/48 - 1$ since

$$z < \delta^2\emptyset/48 - 1 \Rightarrow z < \delta^2/24 \text{ or } \delta^2/24 < z < \delta^2\emptyset/48 - 1$$

$$\Rightarrow z < \delta^2/24 \text{ or } \delta^2/24 < z < \delta^2\emptyset/48 - \delta^2/24z$$

$$\Rightarrow z < \delta^2\emptyset/48 - \delta^2/24z \ .$$

Consequently the only values of d for which (10) may not hold are those d for which $\delta^2 > 24$ and $\delta^2/24 > \delta^2\emptyset/48 - 1$.

We find by exhaustive testing of all possibilites that 289 and 361 are the only values of d that satisfy these inequalities. Thus when $d \neq 289, 361$ (10) is true. //

The other two approximations (x/y to δ and x/z to $\emptyset$) give similar results. However, of the three, the approximation of y/z to $\emptyset/\delta$ is the best for our purposes and so we shall confine our attention to this one approximation.

It must be pointed out that we do not necessarily have $(y, z) = 1$ (nor $(y_0, z_0) = 1$ for type I fields). Thus it is possible that $y = kp_n$, $z = kq_n$ where p_n/q_n is a convergent of $\emptyset/\delta$. However this extra complicating factor is easily taken care of as will be shown in example 3.3.

If any units are found by the use of s.c.f. (with the z coefficient satisfying the inequality in theorem 3.4) then, clearly, the first one found will be η_d. An example in which η_d is found by using s.c.f. will follow theorem 3.5.

S.c.f. do not give a general method of obtaining cubic units but they can be used to obtain a lower bound for η_d in those cases where units are not obtained. The bound obtained is in general much better than the bound obtained by the method shown in example 3.2.

Theorem 3.5

For type I field we write $\eta_d = x_0 + y_0\delta + z_0\emptyset$.

Let $$z_1 = [9\delta^2\emptyset/16 - 1]$$

Then either $z_0 \leq z_1$ and thus y_0/z_0 is a convergent of the s.c.f. for $\emptyset/\delta$

or $$\eta_d > 3(z_1 + 1)\emptyset - 2/(3(z_1 + 1)\emptyset - 2)^{\frac{1}{2}}.$$

For type II fields we have $\eta_d = (x + y\delta + z\emptyset)/3$.

Suppose $d \neq 289,361$ and let

$$z_2 = [\delta^2 \emptyset/48 - 1]$$

Then either $z \leq z_2$ and thus y/z is a convergent of the s.c.f. for $\emptyset/\delta$

or $$\eta_d > (z_2 + 1)\emptyset - 2/((z_2 + 1)\emptyset - 2)^{\frac{1}{2}}.$$

Proof

The theorem follows immediately from theorems 3.2, 3.4. //

The following example illustrates the results of the last two theorems.

Example 3.3

a) Let $d = 52$. Then $Q(\delta)$ is a type I field and $p = 13$, $q = 2$, $\emptyset = \delta^2/2$. Let $\eta_{52} = x_0 + y_0\delta + z_0\emptyset$. The value of z_1 in theorem 3.5 is 53 and thus if $z_0 \leq 53$ we will find $y_0 = kp_n$, $z_0 = kq_n$ where p_n/q_n is a convergent of $\emptyset/\delta$ ($k \in Z^+$). k is further restricted in that we must have

$$|\emptyset/\delta - p_n/q_n| < 1/2(kq_n)^2 \qquad (11)$$

The first few terms of the expansion of $\emptyset/\delta$, together with the corresponding convergents are given below.

($\emptyset/\delta = 1.866255 \ldots$)

n	1	2	3	4	5
a_n	1	1	6	2	10
p_n	1	2	13	28	293
q_n	1	1	7	15	157

We now check all pairs kp_n, kq_n ($kq_n \leq 53$) satisfying (11) by first calculating the third coefficient x_0' using theorem 3.2 i) ($|x - y_0\delta| < 1.16/\eta^{\frac{1}{2}}$). Since $\eta_{52} > 3\emptyset - 2 \approx 18.89$ we have $x_0' = [kp_n\delta + \frac{1}{2}]$. We then calculate $N(x_0' + kp_n\delta + kq_n\emptyset)$ as the conclusive check. The results are set out below.

$n = 1$ - kp_1, kq_1 do not satisfy (11) for any value of k.

$n = 2$ - kp_2, kq_2 satisfy (11) when $k = 1$. We have

$x_0' = 7$ and $N(7 + 2\delta + \emptyset) = 5$.

$n = 3$ - kp_3, kq_3 satisfy (11) when $k = 1$, $x_0' = 49$ and

$N(49 + 13\delta + 7\emptyset) = 25$.

$n = 4$ - kp_4, kq_4 satisfy (11) when $k = 1, 2$.

$k = 1$ - $x_0' = 105$ and $N(105 + 28\delta + 15\emptyset) = 79$

$k = 2$ - $x_0' = 209$ and $N(209 + 56\delta + 30\emptyset) = 1$

Thus $\eta_{52} = 209 + 56\delta + 30\emptyset$.

b) Let $d = 167$. Then $p = 167$, $q = 1$ and $Q(\delta)$ is a type I field. We have $z_1 = 516$ and $\emptyset/\delta = (167)^{1/3} = 5.506878\ldots$ The first few terms and convergents of the s.c.f. for $\emptyset/\delta$ are

n	1	2	3	4	5	6	7
a_n	5	1	1	35	1	5	2
p_n	5	6	11	391	402	2401	5204
q_n	1	1	2	71	73	436	945

The calculations for those kp_n, kq_n, with $kq_n \leq 516$, which satisfy (11) are set out below

n	k	x'_0	$N(x'_0 + kp_n\delta + kq_n\emptyset)$
2	1	33	700
3	1	61	28
3	2	121	25
3	3	182	35
3	4	242	200
5	1	2214	349
6	1	13222	7

Thus none of the possibilities with $kq_n \leq 516$ give a unit and so we can conclude that $z_0 \geq 517$. Thus from theorem 3.5 we have

$$\eta_{167} > 3 \times 517\emptyset - 2/(3 \times 517\emptyset - 2)^{\frac{1}{2}} > 47035$$

If we had used the method of example 3.2 we would have obtained $\eta_{167} > 90.7$ //

As can be seen from part b) of example 3.3, the lower bound obtained using s.c.f. is in general much better than the bound obtained using the method of example 3.2 (Although for type II fields with small d the bound obtained will be the same by either method). The extra work involved in obtaining the larger bound is small and the importance of being able to obtain a large lower bound for η_d will be seen in the last section of this chapter.

Obtaining Pure Cubic Units

Since simple continued fractions do not give a general method of obtaining pure cubic units, other algorithms have been developed for this purpose. Among these we have the Szekeres, Voronoi, Billevich and Jacobi-Perron algorithms. All four algorithms attempt to locate units lying between 0 and 1. The following comments relate to pure cubic fields, although all four algorithms can be used to obtain units in other algebraic number fields.

Szekeres' algorithm [Szekeres, 1970] and the Jacobi-Perron algorithm [Bernstein, 1971] are generalizations of the idea of continued fractions to higher dimensions. Neither algorithm is guaranteed to locate units of $Z(\delta)$ although in practice both algorithms are quite successful in this respect. In practice it appears likely that Szekeres' algorithm will almost always locate η_d^{-1}. Sved [1970] used this algorithm to calculate units for $2 \leq d < 200$, d cube-free. In all cases η_d^{-1} was obtained. Sved also used the algorithm to obtain as many powers of each η_d^{-1} as was practical. Only in a few cases were powers of η_d missed. The Jacobi-Perron algorithm is, in general, less efficient than Szekeres' algorithm.

Billevich's algorithm [Steiner and Rudman, 1976] is very inefficient when the coefficients of the fundamental unit are large and thus the algorithm is of little use in many cases. However the algorithm is guaranteed to locate η_d^{-1} which is not true of the Jacobi-Perron algorithm and Szekeres' algorithm, but this advantage is greatly outweighed by the inefficiency of the algorithm in the cases where η_d is large.

Over the past century a number of tables of (fundamental) pure cubic units have been published. Markoff [1892] produced a table of fundamental units for $2 \leq d \leq 70$. However subsequent tables have shown that in two cases ($d = 28, 55$) Markoff obtained η_d^2 and not η_d. Markoff's table of units is reproduced in Delone and Faddeev [1964, page 304]. In the following 70 years, tables of fundamental units were published by Nagell [1923], Wolfe [1923] (for $d = 85$ Wolfe gives η_d^2 and not η_d), Cassels [1950] and Selmer [1955]. Selmer's table is the most extensive of those so far mentioned. He gives a fundamental unit for each cube-free integer d with $2 \leq d \leq 100$.

In recent years the calculation of fundamental units has been aided by the use of computors and consequently the tables published over the past few years have been more extensive than the earlier tables.

As already mentioned, Sved [1970] used Szekeres' algorithm to calculate η_d^{-1} for $2 \leq d < 200$. Wada [1970] gives a table of η_d for $2 \leq d < 250$. The most recent, and also the most extensive table produced so far, is that of Beach, Williams and Zarnke [1971]. The units in this table were calculated by Voronoi's algorithm and η_d^{-1} is given for each cube-free d with $2 \leq d < 1000$.

Algorithm for Determining the Fundamental Unit of $Z(\delta)$ given any Unit of $Z(\delta)$

One of the drawbacks of Szekeres' algorithm is that there is no guarantee that the first unit obtained by the algorithm is in fact fundamental. Thus an algorithm which can determine whether or not a given pure cubic unit is fundamental would greatly enhance the value of

Szekeres' algorithm. In this section we shall develop such an algorithm. In addition, the algorithm will produce the fundamental unit in those cases where the given unit is not fundamental. Thus if the algorithm was used in conjuction with Szekeres' algorithm we could be sure that any unit obtained by the combined algorithm was indeed fundamental. The amount of work required to test whether or not a unit is fundamental is small when compared with the amount of work required to obtain the unit by the use of Szekeres' algorithm.

Before developing our algorithm we note that Delone and Faddeev[1964, pages 88-95] give an algorithm which can be used to determine whether or not a given cubic integer, β, is an integral power of some other cubic integer. However this algorithm is of most use when $N(\beta) \neq \pm 1$. The algorithm also involves factoring of integers which are related to the coefficients of the cubic polynomial for β. When β is small this does not pose much difficulty but for large β the integers which must be factored will also be large and so the algorithm is not particularly efficient in the cases in which we will be interested. (see the examples at the end of this chapter which deal with $\eta_{167} \approx 10^{96}$ and $\eta_{23}^{6} \approx 10^{59}$).

Determining whether or not η is fundamental is accomplished by determing whether or not there exists an integer, $n > 1$, such that $\eta^{1/n}$ is a unit. We have seen that it is possible to obtain a lower bound, L, for η_d such that $\eta_d > L > 1$. Thus we need only consider those n for which

$$\eta^{1/n} > L$$

$$\Rightarrow \quad n < \log \eta / \log L$$

Thus it is desirable that we can easily obtain a value for L which is as large as possible. Furthermore, it clearly suffices to check only those $\eta^{1/n}$ where n is a prime integer. Thus the number of checks which must be performed is finite.

For a given integer, n, we check whether $\eta^{1/n}$ is a unit as follows. Firstly we calculate $\eta^{1/n}$ as a real number. Secondly we test to see if there exists an integer x such that $|x - \eta^{1/n}| < 2.31/\eta^{1/2n}$ (theorem 3.2 iv)). If no such integer exists then $\eta^{1/n}$ is not a unit. If the test is positive then it is possible that $\eta^{1/n}$ is a unit and the conclusive step is to calculate y and z from the inequalities of theorem 3.2 and then calculate $N((x + y\delta + z\emptyset)/3)$.

Thus if η is not fundamental we will obtain a new unit η_a such that $\eta = \eta_a^n$ (n prime). Although η_a will not necessarily be fundamental it is clear that a finite number of repetitions of the above process will lead to η_d.

The algorithm is now stated in full.

Algorithm 3.1

Let $\eta > 1$ be a unit of the pure cubic field $Q(\delta)$, $\delta^3 = d \in Z^+$, d cube-free. Then η_d is obtained from η as follows.

1 Obtain a lower bound, L, for η_d such that $\eta_d > L \geq 1$. (Use either the method of example 3.2 or the method of example 3.3b)).

2 Set $r = 2$

3 Set $N = [\log \eta / \log L + 1]$

4 If $r \geq N$ go to 11

5 Set $\eta(r) = \eta^{1/r}$

6 If $\nexists\, x \in Z$ such that $|x - \eta(r)| < 2{,}31/(\eta(r))^{\frac{1}{2}}$ go to 9

7 Calculate y and z using theorem 3.2

8 If $N((x + y\delta + z\emptyset)/3) = 1$ go to 10

9 Increment r to the next largest prime, go to 4

10 Reset $\eta = \eta(r)$, go to 3

11 The current value of η is fundamental.
Stop.

Notes

a) At steps 6 and 7 multiple values of x, y and z are possible when $\eta(r)$ is small. However when $\eta(r) > 21.4$ only one value of x, one value of y and one value of z is possible.

b) The value of N calculated in step 3 is the minimum integer, N, such that $\eta^{1/N} < L$.

c) In step 8 we need only test if the norm is equal to + 1. This is because units greater than one have positive norm (Lemma 3.1) //

Practical Use of the Algorithm

To satisfactorily perform the test at step 6 we need to calculate $\eta(r)$ to $[3\log_{10} \eta(r)/2 + 2]$ decimal digits, and to calculate the norm of a suspected unit we must perform integer arithmetic with approximately $[2\log_{10} \eta(r)]$ digits. (Using the expression

$N(\eta) = (x(x^2 - pqyz) + pqy(y^2q - xz) + zpq(z^2p - xy))/27)$.

Thus to use the algorithm we must be able to calculate to at least $[\log_{10} \eta]$ decimal digits (in the case where $\eta(2)$ is a suspected unit) and consequently multiprecision arithmetic computor programs * are necessary (for example, $\eta_{167} \approx 10^{96}$ - see example 3.5). Of course to obtain η, by the use of an algorithm such as Szekeres', we must be able to work with this number of digits and thus the algorithm does not call for any extra computational precision. In fact the amount of precision required decreases as the value of r increases (see example 3.4).

The probability that a non-unit value of $\eta(r)$ will satisfy the test at step 6 would appear to be of the order $1/(\eta(r))^{\frac{1}{2}}$. Thus, when $\eta(r)$ is large, we expect that the test at step 6 will very rarely be satisfied when $\eta(r)$ is not a unit. In practice we find that this is indeed so. (In the two examples at the end of the chapter we see that only those $\eta(r)$ which are units satisfy the test at step 6). Thus the amount of work required to shown that $\eta(r)$ is not a unit is usually very small.

When $\eta(r)$ does satisfy the test at step 6 of the algorithm we must then calculate y, z and finally $N((x + y\delta + z\emptyset)/3)$. This involves a considerable amount of computation and it would be desirable to avoid such computation where possible. (When $\eta(r)$ is a unit this computation cannot be avoided since the ultimate test for a unit is the computation of the norm). To make the algorithm more economic with regard to the amount of computation required we can add the following steps.

---

* See Appendix 1

i) From the norm equation for a positive unit we have

$$x^3 + pq(y^3q + z^3p - 3xyz) = 27N(\eta) = 27$$

and so $x^3 \equiv 27 \pmod{pq}$.

Thus we add between steps 6 and 7.

6a If $x^3 \not\equiv 27 \pmod{pq}$ go to 9.

(This step would be achieved by first calculating x_{pq} where $0 \leq x_{pq} < pq$ and $x_{pq} \equiv x \pmod{pq}$ and then testing the congruence of x_{pq}^3 and 27 modulo pq).

ii) Step 7 can be expanded using inequalities of theorem 3.2

7a If $\nexists\, y \in Z$ such that $|y\delta - \eta(r)| \leq 2/(\eta(r))^{\frac{1}{2}}$ go to 9.

7b If $\nexists\, z \in Z$ such that $|z\emptyset - \eta(r)| \leq 2/(\eta(r))^{\frac{1}{2}}$ go to 9.

The addition of 6a is particularly effective when $\eta(r)$ is small (less than 1000) since the probability that step 6 is satisfied by non-unit values of $\eta(r)$ is relatively high in these cases. As a final point it should be noted that the computational economies introduced above are only of importance (that is, save some computation) in a small number of cases. This is because step 6 filters out almost all non-unit values of $\eta(r)$ and thus steps 6a, 7a and 7b are rarely executed when $\eta(r)$ is not a unit.

We now give two examples which illustrate the use of the algorithm and indicate the amount of work involved when it is applied to specific examples. The calculations were done on a B6700 computer using the multiprecision programs listed in Appendix 1.

Example 3.4

Let d = 23. Then $Q(\delta)$ is a type I field, $\eta = x_0 + y_0\delta + z_0\emptyset$

is a unit of $Q(\delta)$, where

$$x_0 = 251401129\ \ 6271379187\ \ 9829592761$$
$$7258440514\ \ 3510195116\ \ 6439999601$$
$$y_0 = 88401156\ \ 3861048459\ \ 5086024628$$
$$7875956789\ \ 8501378224\ \ 5618425660$$
$$z_0 = 31084842\ \ 2280000275\ \ 0405930152$$
$$0668641067\ \ 2496635313\ \ 4343732220$$
$$\eta \approx 754203388\ \ 8814137563\ \ 9488778285$$
$$1775321543\ \ 0530585349\ \ 9319998803$$
$$.0000000000\ \ 0000000000\ \ 0000000004$$
$$\approx 7.542 \times 10^{58}$$

(This η is obtained by taking the reciprocal of the sixth power of the unit given by Sved [1970]). Applying the algorithm we obtain

$$L = 873.3$$

(This bound is obtained in a manner similar to that of example 3.3b)). Consequently $N = [\log(7.542 \times 10^{58})/\log(873.3) + 1]$

$$= 21$$

Firstly we test $\eta(2)$, the square root of η.

$$\eta(2) = 2746276367\ \ 8869134462\ \ 7557332202$$
$$.9999999999\ \ 9999815705,$$

and $$2.31/(\eta(2))^{\frac{1}{2}} \approx 4.41 \times 10^{-15}$$

Thus the test at step 6 is positive and so we take

$$x = 2746276367\ \ 8869134462\ \ 7557332203$$

For the test at step 6a we note that

$$x \equiv 3 \pmod{23}$$

and thus $x^3 \equiv 3^3 \equiv 27 \pmod{23}$. Therefore we proceed to calculate

$$\eta(2)/\delta \approx 965683833\ \ 7882646905\ 0995173039$$

$$.9999999999\ 9999930631,$$

$$\eta(2)/\emptyset \approx 339567160\ \ 0078384044\ \ 8684822730$$

$$.0000000000\ 0000047179$$

Noting that $2/(\eta(2))^{\frac{1}{2}} \approx 3.8 \times 10^{-15}$ we see that

$$y = 965683833\ \ 7882646905\ \ 0995173040,$$

and $$z = 339567160\ \ 0078384044\ \ 8684822730,$$

satisfy the inequalities of steps 7a and 7b respectively. The final test is to calculate $N((x + y\delta + z\emptyset)/3$ which we find is unity. Thus $\eta(2)$ is a unit of $Q(\delta)$. Consequently we replace η by $\eta(2)$ and return to step 3 of the algorithm.

N now takes the value 11. r still has the value 2 and so we calculate

$$\eta(2) \approx 52404\ \ 9269428640.024917 \qquad (12)$$

This is clearly not a unit since the test at step 6 is negative. r is incremented to 3 and

$$\eta(3) \approx 6500020803.0000191071,$$

$$2.31/(\eta(3))^{\frac{1}{2}} \approx 0.0000286$$

Thus the test at step 6 is positive, so we take

$$x = 6500020803 ,$$

and note that $x \equiv 3 \pmod{23}$. Thus the test in step 6a is positive and we calculate

$$\eta(3)/\delta \approx 2285627579.9999918228,$$

$$\eta(3)/\emptyset \approx 803704110 .0000005128,$$

and $$2/(\eta(3))^{\frac{1}{2}} \approx 0.0000248$$

Thus we take

$$y = 2285627580,$$

$$z = 803704110$$

and the calculation of the norm confirms that $\eta(3)$ is a unit. Thus $\eta(3)$ replaces η.

N now takes the value 4. r has the value 3. (At (12), $\eta(2)$ was not a unit and so r = 2 need not be considered again)

$$\eta(3) \approx 1866.257 \quad \text{and} \quad 2.31/(\eta(3))^{\frac{1}{2}} \approx 0.053$$

and thus $\eta(3)$ is not a unit. r is now incremented to 5 which is greater than N. Thus we can stop and conclude that

$$\eta \approx 6500020803.0000191071$$

is the fundamental unit of $Q(\delta)$. //

Example 3.5

Let d = 167. $Q(\delta)$ is a type I field and from Sved [1970] we have

$$\eta \approx 621050\ 0640303132\ 6161103562\ 8827556350\ 7362478867\ 5341597327\ 4816722532\ 9679837287\ 8103562731\ 1528000987\ .0000000000\ 0000000000\ 0000000000\ 0000000000\ 0000000200\ 1896095838$$

$$\approx 6.21 \times 10^{95}$$

is a unit of $Q(\delta)$. (This is the reciprocal of the unit given by Sved).

From example 3.3b) we have L = 47035.

Thus $N = [\log \eta / \log(47035) + 1]$

$= 21$

The values of $\eta(r)$ which need checking are set out below. Clearly, none of these $\eta(r)$ satisfy the test at step 6 of the algorithm.

$\eta(2) \approx 78806729\ 6637992244\ 0050104080\ 3056469673\ 0335831406\ .2371560251,$

$\eta(3) \approx 85\ 3183020141\ 7547364081\ 5443829075\ .5805448903,$

$\eta(5) \approx 1440871735\ 3864111266\ .2999492424,$

$\eta(7) \approx 4838\ 7409603319\ .6430345357,$

$\eta(11) \approx 511053133\ .\ 5546616359,$

$\eta(13) \approx 23372332\ .\ 0124097584,$

$\eta(17) \approx 431409.595,$

$\eta(19) \approx 110088.893.$

The next value of r, 23, is greater than N so we can stop and conclude that

$$\eta \approx 6.21 \times 10^{95}$$

is the fundamental unit of $Q(\delta)$. //

4 Units of $Q(d^{1/4})$, $d < 0$, d square -free

The third and final type of field, $Q(\alpha)$, in which the units of the ring of integers can be expressed as powers of a fundamental unit occurs when α is of degree four and α and its conjugates are non-real. A special case of this type of field is when α is the fourth root of a square-free negative integer.

The Integers of $Q(d^{1/4})$

Let d be a square-free negative integer and let $\delta = d^{1/4}$.

Then $Q(\delta) = \{x + y\delta + z\delta^2 + t\delta^3 \mid x, y, z, t \in Q\}$.

Let $\beta = x_1 + y_1\delta + z_1\delta^2 + t_1\delta^3$. Then the conjugates of β

are $$\beta_1 = x_1 + y_1\delta i - z_1\delta^2 - t_1\delta^3 i,$$

$$\beta_2 = x_1 - y_1\delta + z_1\delta^2 - t_1\delta^3,$$

and $$\beta_3 = x_1 - y_1\delta i - z_1\delta^2 + t_1\delta^3 i.$$

The quartic polynomial for β is

$$f(X) = (X - \beta)(X - \beta_1)(X - \beta_2)(X - \beta_3)$$

$$= X^4 - AX^3 + BX^2 - CX + N \qquad (1)$$

where $$A = 4x_1, \qquad (2)$$

$$B = 6x_1^2 - 2dz_1^2 - 4dy_1t_1, \qquad (3)$$

$$C = 4(x_1(x_1^2 - z_1^2d) + d(z_1(y_1^2 + t_1^2d) - 2x_1y_1t_1)), \qquad (4)$$

and $$N = (x_1^2 + d(z_1^2 - 2y_1t_1))^2 - d(2x_1z_1 - y_1^2 - t_1^2d)^2. \qquad (5)$$

Theorem 4.1

The ring of integers of $Q(\delta)$ is given by

$$Z(\delta) = \{(x + y\delta + z\delta^2 + t\delta^3)/4 \mid x, y, z, t \in Z\}$$

with the following restrictions on x, y, z, t.

i) $d \equiv 1 \pmod 8$ $\quad x \equiv y \equiv z \equiv t \pmod 2$, $x \equiv z \pmod 4$, $y \equiv t \pmod 4$.

ii) $d \equiv 5 \pmod 8$ $\quad x \equiv y \equiv z \equiv t \equiv 0 \pmod 2$ $x \equiv z \pmod 4$, $y \equiv t \pmod 4$.

iii) $d \equiv 2, 3 \pmod 4$ $\quad x \equiv y \equiv z \equiv t \equiv 0 \pmod 4$

Proof

Let $\beta = x_1 + y_1\delta + z_1\delta^2 + t_1\delta^3$, $x_1, y_1, z_1, t_1 \in Q$ be an integer of $Q(\delta)$. Then A, B, C and N above must be integers. Furthermore $\beta_2 = x_1 - y_1\delta + z_1\delta^2 - t_1\delta^3$ is also an integer of $Q(\delta)$ since it satisfies the same polynomial as β and is clearly an element of $Q(\delta)$. Consequently

$$\beta\beta_2 = (x_1^2 + z_1^2 d - 2y_1 t_1 d) + (2x_1 z_1 - y_1^2 - t_1^2 d)\delta^2$$

$$= E + F\delta^2 \qquad (6)$$

is also an algebraic integer. However $\beta\beta_2 \in Q(\sqrt{d})$ and is therefore a quadratic integer. From (1) of chapter 2 we have that E and F must be integers when $d \equiv 2, 3 \pmod 4$, and when $d \equiv 1 \pmod 4$ 2E and 2F must be integers. In either case we have from (6)

$$2(x_1^2 + z_1^2 d - 2y_1 t_1 d) \in Z \qquad (7)$$

and

$$2(2x_1 z_1 - y_1^2 - t_1^2 d) \in Z \qquad (8)$$

Also, from (3) we have

$$6x_1^2 - 2dz_1^2 - 4dy_1 t_1 \in Z \qquad (9)$$

From (2) we have $x_1 = x/4$ where $x \in Z$.

Let $y_1 = y_0/p$, $z_1 = z_0/q$, $t_1 = t_0/r$ where y_0, z_0, t_0, p, q, $r \in Z$, $(y_0, p) = (z_0, q) = (t_0, r) = 1$ and $p, q, r > 0$. We shall show that $p|4$, $q|4$, and $r|4$ and hence it will follow that we may write $z_1 = z/4$, $y_1 = y/4$, $t_1 = t/4$ where y, z and t are integers.

From (7)

$$2(x^2/16 + z_1^2 d - 2y_1 t_1 d) \in Z$$

and so
$$x^2 + 16z_1^2 d - 32y_1 t_1 d \in 8Z^* \tag{10}$$

From (9)
$$3x^2 - 16z_1^2 d - 32y_1 t_1 d \in 8Z \tag{11}$$

Subtracting (11) from (10) gives $-2x^2 + 32z_1^2 d \in 8Z$ and thus $32z_1^2 d \in 2Z$. Dividing by two gives $16z_0^2 d/q^2 \in Z$ and since $(z_0, q) = 1$ we must have $q^2|16d$. Since d is square-free it follows that $q|4$.

From (10) we now have that $32y_1 t_1 d$ is an integer. Thus

$$32^2 y_1^2 t_1^2 d^3 \in Z \tag{12}$$

From (8)
$$xz - 8y_1^2 - 8t_1^2 d \in 4z$$

$$\Rightarrow 8y_1^2 + 8t_1^2 d \in Z \tag{13}$$

$$\Rightarrow 32dy_1^2 + 32t_1^2 d^2 \in 4dz \tag{14}$$

(12) and (14) imply that $32dy_1^2$ and $32t_1^2 d^2$ are both integers since their sum and product are both integers. Substituting for y_1 gives $32dy_0^2/p^2 \in Z$. Thus $p^2|32d$ and so $p|8$. Multiplying (13) by 8 gives $64y_0^2/p^2 + 64t_1^2 d \in Z$. Since $p|8$ it follows that $64y_0^2/p^2 \in Z$ and so $64t_1^2 d$ must also be an integer. Thus $64t_0^2 d/r^2$ is an integer which implies that $r|8$ (since d is square-free and $(r, t_0) = 1$).

---

* $8Z = \{0, \pm 8, \pm 16, \ldots\}$

We now show that $r = 8$ or $p = 8$ is impossible. Suppose $p = 8$. From (13) we have $64y_0^2/p^2 + 64t_0^2 d/r^2 \equiv 0 \pmod 8$. Since $p^2 | 32d$ we must have $2|d$ and from $(p, y_0) = 1$ we have that y_0 is odd. Thus $64y_0^2/p^2 \equiv 1 \pmod 8$. Consequently $64t_0^2 d/r^2 \equiv -1 \pmod 8$. However the last congruence is impossible when $r|8$ and $2|d$. Thus $p \neq 8$ and so $p|4$.

This now gives $64y_0^2/p^2 = 4m$, $(m \in Z)$, and so from (13) we have $4m + 64t_0^2 d/r^2 \equiv 0 \pmod 8$. Thus $64t_0^2 d/r^2 \equiv 0 \pmod 4$. This congruence cannot hold when $r = 8$, $(r, t_0) = 1$, and d is square-free. Therefore $r \neq 8$ and so $r|4$.

Consequently we now have $\beta = (x + y\delta + z\delta^2 + t\delta^3)/4$ with $x, y, z, t \in Z$.

We now develop the relationships between x, y, z, t modulo 4.

1) $d \equiv 2, 3 \pmod 4$.

Since E and F of (6) must be integers

we have $$x^2 + z^2 d - 2ytd \equiv 0 \pmod{16} \qquad (15)$$

and $$2xz - y^2 - t^2 d \equiv 0 \pmod{16} \qquad (16)$$

a) $d \equiv 2 \pmod 4$ - since $2|d$ we must have $x^2 \equiv 0 \pmod 2$ from (15). Thus $2|x$. This implies that $x^2 - 2ytd \equiv 0 \pmod 4$ and therefore $z^2 d \equiv 0 \pmod 4$. Since $4 \nmid d$ we must have $2|z$. From (16) we now have $y^2 + t^2 d \equiv 0 \pmod 8$ and since $2|d$ we must have $2|y$ and consequently $2|t$. Since y, z, t, d are all even we now have, from (15), $x^2 \equiv 0 \pmod 8$ and so $4|x$. This then implies that $z^2 d \equiv 0 \pmod 8$ and so $4|z$. Similarly $4|y$ and $4|t$.

b) $d \equiv 3 \pmod 4$ - from (15) we have $x^2 + z^2 d \equiv 0 \pmod 2$ and so $x \equiv z \pmod 2$. Similarly $y \equiv t \pmod 2$. If y and t are both even then from (15) $x^2 + z^2 d \equiv 0 \pmod 8$ and so x and z must be even. Similarly x, z even implies y, t even. Thus $x \equiv y \equiv t \equiv z \pmod 2$. However from (16) we have $2xz - y^2 - t^2 d \equiv 0 \pmod 4$ and this congruence is impossible when x, y, z, t are odd. Therefore we must have $x \equiv y \equiv z \equiv t \equiv 0 \pmod 2$.

Suppose neither x nor z is divisible by 4. Then $x^2 + z^2 d \equiv 0 \pmod{16}$ and so $2ytd \equiv 0 \pmod{16}$. This is only possible if $4 \mid y$ or $4 \mid t$. Thus we can be sure that at least one of x, y, z, t must be divisible by 4. However from (15) and (16) it follows that if one of x, y, z, t is divisible by 4 then the other three must also be divisible by 4.

Thus for $d \equiv 2, 3 \pmod 4$, $x \equiv y \equiv z \equiv t \equiv 0 \pmod 4$.

2) $d \equiv 1 \pmod 4$.

In this case we only require 2E and 2F of (6) to be integers and so we have

$$x^2 + z^2 d - 2ytd \equiv 0 \pmod 8 \qquad (17)$$

and

$$2xz - y^2 - t^2 d \equiv 0 \pmod 8 \qquad (18)$$

From (17) $x^2 + z^2 \equiv 0 \pmod 2$ and thus $x \equiv z \pmod 2$. Similarly from (18) we have $y \equiv t \pmod 2$. Suppose y, t are even. Then from (17) $x^2 + z^2 d \equiv 0 \pmod 8$ and this can only be true when x, z are even. In a similar manner we have x, z even implies y, t even (from (18)). Thus $x \equiv y \equiv z \equiv t \pmod 2$.

a) $d \equiv 1 \pmod 8$ - suppose $x \equiv y \equiv z \equiv t \equiv 1 \pmod 2$. Then from (17) $0 \equiv x^2 + z^2 d - 2ytd \equiv 1 + 1 - 2yt \pmod 8$. Thus $yt \equiv 1 \pmod 4$ and so $y \equiv t \pmod 4$. Similarly $x \equiv z \pmod 4$. Suppose x, y, z, t are even. Then, from (17), $x^2 + z^2 \equiv 0 \pmod 8$ and so $x \equiv z \pmod 4$. Similarly $y \equiv t \pmod 4$.

b) $d \equiv 5 \pmod 8$ - suppose that x, y, z, t are odd. Then, from (17), $0 \equiv x^2 + z^2 d - 2ytd \equiv 1 + 5 - 2yt \pmod 8$. Thus $yt \equiv 3 \pmod 4$ and so $y \equiv -t \pmod 4$. Similarly $x \equiv -z \pmod 4$. If β is an integer then so is $\beta_m = (x_m + y_m\delta + z_m\delta^2 + t_m\delta^3)/4$, where $x_m, y_m, t_m, z_m \in \{-1, 1\}$ and $x_m \equiv x \pmod 4$, $y_m \equiv y \pmod 4$, etc. (This follows since $1, \delta, \delta^2, \delta^3$ are integers). By replacing β_m with $-\beta_m$ if necessary we can assume that $x_m = 1$ and consequently $z_m = -1$. Since $y \equiv -t \pmod 4$ we will have $y_m t_m = -1$. For the integer β_m we have (from (4))

$$x_m(x_m^2 - z_m^2 d) + dz_m(y_m^2 + t_m^2 d) - 2x_m y_m t_m d \equiv 0 \pmod{16}$$

Substituting, we obtain

$$1(1 - d) + d(1 + d) - 2d \equiv 1 - d^2 \equiv 0 \pmod{16}$$

However, $d \equiv 5 \pmod 8$ implies $1 - d^2 \equiv 8 \pmod{16}$. Thus x, y, z, t all odd leads to a contradiction. Consequently $x \equiv y \equiv z \equiv t \equiv 0 \pmod 2$.

$$\text{From (17) } x^2 + 5z^2 - 10yt \equiv 0 \pmod 8$$

$$\Rightarrow \quad x^2 + 5z^2 \equiv 0 \pmod 8$$

$$\Rightarrow \quad x \equiv z \pmod 4.$$

Similarly, from (18), $y \equiv t \pmod 4$.

Thus the necessity of the conditions given in the theorem has been shown.

For $d \equiv 2, 3 \pmod 4$ it is obvious that the conditions are sufficient.

For $d \equiv 5 \pmod 8$ $(2 + 2\delta^2)/4$ and δ are clearly integers of $Q(\delta)$. $((2 + 2\delta^2)/4$ is in fact a quadratic integer). All of the numbers described in part ii) of the theorem can be obtained from these two integers by using the operations of addition and multiplication. Thus the conditions given in ii) are sufficient.

When $d \equiv 1 \pmod 8$ we can obtain all the numbers described in i) of the theorem by additions and multiplications of the numbers $(1 + \delta + \delta^2 + \delta^3)/4$, $(1 + \delta^2)/2$, and δ. It is easily verified (using (2), (3), (4), (5)) that these numbers are integers of $Q(\delta)$ and thus the conditions given in i) are sufficient. //

(At no stage in this theorem did we make any assumptions on the sign of d and therefore the result given in the theorem also describes the integers of $Q(d^{1/4})$ when d is a positive square-free integer).

Units of $Z(\delta)$ ($\delta^4 = d < 0$, d a square-free integer)

The norm of any integer $\beta = (x + y\delta + z\delta^2 + t\delta^3)/4$ is given by

$$N(\beta) = (x^2 + z^2d - 2ytd)^2/256 - d(y^2 + t^2d - 2xz)^2/256.$$

Thus the norm of any integer is non-negative and consequently any unit, η, has norm $N(\eta) = 1$.

Let $\eta = (x + y\delta + z\delta^2 + t\delta^3)/4$ be a unit of $Z(\delta)$. Then $\eta' = (x - y\delta + z\delta^2 - t\delta^3)/4$ is a conjugate of η and is also a unit of $Z(\delta)$ since $N(\eta) = N(\eta')$. Therefore the product

$$\eta\eta' = (x^2 + z^2d - 2ytd)/16 + \delta^2(2xz - y^2 - t^2d)/16$$

is also a unit. However, as previously noted, the product $\eta\eta'$ is a quadratic integer and hence it is a unit of $Z(\delta^2)$. Recalling the units of $Z(\delta^2)$ from chapter 2 we have

i) for $d = -1$ $\eta\eta' = \pm 1, \pm i$ and so

either $x^2 + z^2d - 2ytd = \pm 16$ and $2xz - y^2 - t^2d = 0$

or $x^2 + z^2d - 2ytd = 0$ and $2xz - y^2 - t^2d = \pm 16$

ii) for $d = -3$ $\eta\eta' = \pm 1, (\pm 1 \pm \sqrt{-3})/2$ and so

either $x^2 + z^2d - 2ytd = \pm 16$ and $2xz - y^2 - t^2d = 0$

or $x^2 + z^2d - 2ytd = \pm 8$ and $2xz - y^2 - t^2d = \pm 8$.

iii) for $d \neq -1, -3$ $\eta\eta' = \pm 1$ and thus

$$x^2 + z^2d - 2ytd = \pm 16 \text{ and } 2xz - y^2 - t^2d = 0 \qquad (19)$$

Since the product $\eta\eta'$ is always a root of unity, ξ, we have $\eta^{-1} = \xi^{-1}\eta'$. Thus $|\eta^{-1}| = |\eta'|$ and $|\eta\eta'| = 1$ for any unit of $Z(\delta)$.

In the following sections we will need to express η and η' in the form $a + bi$, $a, b \in R$. To do this we must fix the value of δ as one particular 4^{th} root of d. Henceforth we shall assume that $\delta = (1 + i)|d^{\frac{1}{4}}|/\sqrt{2}$.

Lemma 4.1

Let $\eta = (x + y\delta + z\delta^2 + t\delta^3)/4$ be a unit of $Z(\delta)$, $\delta^4 = d < 0$, d square-free. Then

$$\eta = (x + yD_1 - tD_3)/4 + i(yD_1 + zD_2 + tD_3)/4,$$

and $\eta' = (x - yD_1 + tD_3)/4 + i(zD_2 - yD_1 - tD_3)/4,$

where $D_1 = |d^{\frac{1}{4}}|/\sqrt{2}$; $D_2 = |d^{\frac{1}{2}}|$, and $D_3 = |(d^3)^{\frac{1}{4}}|/\sqrt{2}$.

Proof

$$\eta = (x + y\delta + z\delta^2 + t\delta^3)/4$$

$$= (x + y|d^{\frac{1}{4}}|(1 + i)/\sqrt{2} + z|d^{\frac{1}{2}}|i + t|(d^3)^{\frac{1}{4}}|(-1 + i)/\sqrt{2})/4$$

$$= (x + yD_1 + yD_1 i + zD_2 i - tD_3 + tD_3 i)/4$$

$$= (x + yD_1 - tD_3)/4 + i(zD_2 + yD_2 + tD_3)/4$$

The expression for η' is obtained in a similar manner. //

The conditions given in (19) enable us to prove the following property of the polynomial for η.

Lemma 4.2

Suppose $d \neq -1, -3$. Then in the polynomial (1) for the unit $(x + y\delta + z\delta^2 + t\delta^3)/4 \in Z(\delta)$ we have $C = \pm A$. The sign taken agrees with the sign of $x^2 + z^2d - 2ytd$.

Proof

$$C = (x(x^2 - z^2d) + dz(y^2 + t^2d) - 2xytd)/16$$

$$= (x(x^2 + z^2d - 2ytd) + dz(-2xz + y^2 + t^2d))/16$$

$$= A(x^2 + z^2d - 2ytd)/16 + dz(-2xz + y^2 + t^2d)/16.$$

From (19) we have $x^2 + z^2d - 2ytd = \pm 16$ and $-2xz + y^2 + t^2d = 0$. Thus $C = \pm A$ and the sign taken agrees with the sign of $x^2 + z^2d - 2ytd$. //

From theorem 1.7 we know that any unit of $Z(\delta)$ can be written

as $\xi\eta_d^n$ where η_d is a fundamental unit of $Z(\delta)$, $n \in Z$ and ξ is a root of unity. Since δ has non-real conjugates there is the possibility of roots of unity other than ± 1.

Roots of Unity in $Z(\delta)$

Theorem 4.2

Let $\delta^4 = d$ be a square-free negative integer. The only roots of unity in $Z(\delta)$ are

i) $\pm 1, \pm i, \pm \delta, \pm \delta^3$ when $d = -1$, the eighth roots of unity,

ii) $\pm 1, (\pm 1 \pm \sqrt{-3})/2$ when $d = -3$, the sixth roots of unity,

iii) ± 1 when $d \neq -1, -3$.

Proof

Let $\eta = (x + y\delta + z\delta^2 + t\delta^3)/4$ be a root of unity of $Z(\delta)$. Then from lemma 4.1 we have

$$\eta = (x + yD_1 - tD_3)/4 + i(zD_2 + yD_1 + tD_3)/4$$

Since $|\eta| = 1$ for a root of unity we have

$$|(x + yD_1 - tD_3)/4| \leq 1, \quad |(zD_2 + yD_1 + tD_3)/4| \leq 1.$$

η' must also be a root of unity when η is and so we also have, from lemma 4.1,

$$|(x - yD_1 + tD_3)/4| \leq 1, \quad |(zD_2 - yD_1 - tD_3)/4| \leq 1.$$

From the two pairs of inequalities we obtain $|x/2| \leq 2$ and $|zD_2/2| \leq 2$, that is $|x| \leq 4$ and $|zD_2| \leq 4$, for any root of unity. Since $|zD_2| \leq 4$ the possible values for z are $0, \pm 1, \pm 2, \pm 3, \pm 4$.

If $z = \pm 4$ then $D_2 \leq 1$ and so the only possible value of d is -1. This leads to the roots of unity $\pm \delta^2 = \pm i$.

$z = \pm 3$ is a possibility only when $d \equiv 1 \pmod 8$. However we must also have $3D_2 \leq 4$ and no value of d satisfies both these requirements.

If $z = \pm 2$ then $d \equiv 1 \pmod 4$ and $D_2 \leq 2$. Thus $d = -3$ is the only possibility. Since $x \equiv z \pmod 4$, $x = \pm 2$ and we obtain the units $(\pm 1 \pm \sqrt{-3})/2$. These units are sixth roots of unity. Four other units with $x = -z = \pm 2$ are also obtained but they are not roots of unity. (see example 4.5 ii)).

If $z = \pm 1$ then $d \equiv 1 \pmod 8$ and $D_2 \leq 4$. Thus the possibilities are $d = -7, -15$. We must also have $x = \pm 1, \pm 3$ with $x \equiv z \pmod 4$. The only units satisfying these conditions are $\pm(3 - \delta - \delta^2 - \delta^3)/4$ and $\pm(3 + \delta - \delta^2 + \delta^3)/4$ when $d = -7$. However these are not roots of unity.

If $z = 0$ then $x = 0$ or $x = \pm 4$. With $x = \pm 4$ we get the roots of unity ± 1(for each d). With $x = 0$ we obtain the units $\pm \delta, \pm \delta^3$ when $d = -1$. These are eighth roots of unity. //

Algorithm to Determine the Fundamental Unit of $Z(\delta)$ given any Unit of $Z(\delta)$

The main purpose of this chapter is to show that an algorithm similar to algorithm 3.1 can be developed for the quartic case. The remainder of this chapter will move in this direction.

For the rest of this chapter we will assume that η is a unit of $Z(\delta)$ such that $|\eta| > 1$.

We now prove a theorem around which we will build the algorithm.

Theorem 4.3

Let $d = \delta^4$ be a square-free negative integer.
If $\eta = (x + y\delta + z\delta^2 + t\delta^3)/4$ is a unit of $Z(\delta)$, $|\eta| > 1$, then we have $\eta = H + Ii$, $H, I \in R$, and

$$|x/2 - H| \leq 1/|\eta|,$$

and $$|zD_2/2 - I| \leq 1/|\eta| .$$

Proof

From lemma 4.1 we have $H = (x + yD_1 - tD_3)/4$ and $I = (zD_2 + yD_1 + tD_3)/4$. We also have

$$|(x - yD_1 + tD_3)/4 + i(zD_2 - yD_1 - tD_3)/4| = |\eta'| = 1/|\eta|$$

Thus $$|x - yD_1 + tD_3|/4 \leq 1/|\eta|, \qquad (20)$$

and $$|zD_2 - yD_1 - tD_3|/4 \leq 1/|\eta| \qquad (21)$$

Rewriting the last two inequalities we have

$$|2x/4 - (x + yD_1 - tD_3)/4| \leq 1/|\eta|,$$

and $$|2zD_2/4 - (zD_2 + yD_1 + tD_3)/4| \leq 1/|\eta|$$

The result is now clear. //

Corollary

For any unit, $\eta = (x + y\delta + z\delta^2 + t\delta^3)/4 \in Z(\delta)$, $|\eta| > 1$, we have

i) $|I| \geq |z|D_2/2 - 1/|\eta|$

ii) $|H| \geq |x|/2 - 1/|\eta|$.

Proof

From theorem 4.3 we have $|zD_2/2 - I| \leq 1/|\eta| < 1$. If $z \neq 0$ then $|z|D_2 > 2$ (since $|z| = 1$ implies $|d| \geq 7$). Thus z and I must have the same sign and so $|zD_2/2 - I| = ||z|D_2 - |I||$ and i) follows. If $z = 0$ the inequality is trivial.

Similarly if $|x| > 2$ or $x = 0$, inequality ii) holds. If $|x| = 1$, then from $|x/2 - H| \leq 1/|\eta|$ we see that either x and H are of the same sign or else $|\eta| < 2$. If x and H are of the same sign then the inequality holds and if $|\eta| < 2$ then the inequality is trivial (since the right-hand side will be negative). //

Thus the real and imaginary part of η are very closely related to the integers x and z. Furthermore, $\gamma = (x + izD_2)/2 = (x + z\delta^2)/2$ is an integer of $Q(\delta^2)$ and

$$|\eta - \gamma| = |(H - x/2) + i(I - zD_2/2)|$$

$$\leq 1/|\eta| + 1/|\eta| = 2/|\eta|$$

Thus η is a close approximation to an integer of $Q(\delta^2)$. This compares with the previous cases (chapters 2 and 3) where the units were close approximations to rational integers.

Example 4.1

Let $d = -10$. Then $\eta = (5756 + 2832\delta + 432\delta^2 - 552\delta^3)/4$ is a unit of $Z(\delta)$.

We have $\eta \approx 2877.999671 + 683.052053i$,

$|\eta^{-1}| \approx .000338$,

$x/2 = 2878$,

and $zD_2/2 \approx 683.051975$.

Also $|\eta - (x/2 + zD_2 i/2)| \approx .000414$

$\leq 2|\eta^{-1}|$ //

Before defining the fundamental unit of $Z(\delta)$ we need the following lemma.

Lemma 4.3

Let $\eta = H + Ii$ be a unit of $Q(\delta)$, $|\eta| > 1$, $H, I \in R$. Then $H = 0$ implies $d = -1$.

Proof

Suppose $H = 0$. Then from theorem 4.3 we have $|x/2| < 1$. Thus $x = 0$ or $x = \pm 1$.

If $x = 0$ then since $H = 0 = (x + yD_1 - tD_3)/4$ we have $tD_3 = yD_1$ and thus $y/t = |d^{\frac{1}{2}}|$. Since $y, t \in Z$ and d is square-free this can only be true when $d = -1$.

Suppose $x = \pm 1$. Then $d \equiv 1 \pmod 8$ and so $|d| \geq 7$. If $|z| \geq 3$ then from the corollary to theorem 4.3, $|I| > |z|D_2/2 - 1$

$\geq 3\sqrt{7}/2 - 1 > 2.96$, and thus $|\eta| > 2.96$. However from theorem 4.3 we also have $x = \pm 1$ implies $|1/2 - 0| \leq 1/|\eta|$ and thus $|\eta| \leq 2$. Consequently $|z| \geq 3$ is impossible and so $z = \pm 1$. Substituting $x = z = \pm 1$ in (19) gives $1 + d - 2ytd = \pm 16$ and so $d|17$ or $d|15$. Since $d \equiv 1 \pmod 8$ the only possibility is $d = -15$. However there is no unit in $Z(\delta)$, $d = -15$, with $x = z = \pm 1$. Thus $x = \pm 1$ and $H = 0$ is impossible. //

When $d \neq -1, -3$ there are four fundamental units in $Z(\delta)$. If one of these units is η then the other three are $-\eta$, η^{-1} and $-\eta^{-1}$. Of these units precisely one has both a positive real part and magnitude greater than one. We shall arbitrarily choose this unit to be <u>the</u> fundamental unit and denote it by η_d.

When $d = -1$ there are sixteen units which would serve as a fundamental unit and when $d = -3$ there are twelve units which would serve as a fundamental unit. (In each case twice the number of roots of unity in $Z(\delta)$). We shall not define η_d for these two cases.

As in the previous case (algorithm 3.1) the algorithm is based on the approximation to an integer by η. (In this case the approximation is to a quadratic integer). We use the inequalities given in theorem 4.3 to pick out possible units from the complex numbers $\eta^{1/p}$, $p = 2, 3, 5, 7, \ldots$. The coefficients x, y, z, t of any possible unit can be calculated as follows.

1) x and z are obtained from the inequalities of theorem 4.3

2) adding (20) to (21) we have

$$|x + zD_2 - 2yD_1|/4 \leq 2/|\eta| \qquad (22)$$

and so y can be obtained.

3) t is obtained from (20)

The norm of a suspected unit can then be calculated and a conclusive result obtained. Thus we now have a method by which a complex number may be tested to see whether or not is is a unit of $Z(\delta)$.

To make the algorithm workable we need a lower bound, L, for the magnitude of η_d such that $L > 1$. The following examples show how this may be done.

Example 4.2

Let $d = -2$ and $\eta_d = (x + y\delta + z\delta^2 + t\delta^3)/4 = H + Ii$, $H, I \in R$. We have $x \equiv z \equiv 0 \pmod 4$. If $x = 0$ or $z = 0$ then from (19) we have $y^2 + t^2 d = 0$. This is only possible when $d = -1$ or when $y = t = 0$ (and hence $\eta = \pm 1, \pm i$). Thus $x, z \neq 0$. (In fact we have the general result that $x, z \neq 0$ for any η where $|\eta| \neq 1$ and $d \neq -1$).

From the corollary to theorem 4.3 we have

$$|x/2| - 1/|\eta_d| \leq |H| ,$$

and

$$|zD_2/2| - 1/|\eta_d| \leq |I| .$$

Since $|\eta_d| > 1$ and $|x|, |z| \geq 4$ we obtain $|H| > 1$, $|I| > 1.828$ and thus $|\eta_d| > 2.08$. We can now use the new lower bound for $|\eta_d|$ in an iterative manner to give $|H| > 1.519$, $|I| > 2.347$ and thus $|\eta_d| > 2.795$. Several further iterations give $|\eta_d| > 3$. //

This method works well for $d \equiv 2, 3 \pmod 4$ but cannot be used successfully for $d \equiv 1 \pmod 4$ when $|d|$ is small. However in that case

a bound can be obtained as follows.

Example 4.3

Let $d = -15$ and $\eta_d = (x + y\delta + z\delta^2 + t\delta^3)/4 = H + Ii$, $H, I \in R$. Suppose $|\eta_d| < 3$. Then $|H| < 3$ and $|I| < 3$. From the corollary to theorem 4.3 we have $|x| \leq 2(|H| + 1/|\eta_d|) < 8$ and from (19) we have $x^2 \equiv \pm 1 \pmod{15}$. Thus $|\eta_d| < 3$ implies $x = \pm 1, \pm 4$. From the corollary to theorem 4.3 we also have $|z| < 2.07$ and so $|z| = \pm 1, \pm 2$. (In the previous example it was shown that $z = 0$ is not possible).

Since $x \equiv z \pmod 4$ we are left with the possibilities $x = z = \pm 1$. Neither possibility leads to η_d and so we conclude that $|\eta_d| > 3$. //

Before presenting the algorithm we must consider one problem which arises in the quartic case which we did not have to contend with in the pure cubic case. Suppose we were given the unit $\eta = -\eta_d^2$ and had to determine the fundamental unit. Merely testing $\eta^{1/p}$ for $p = 2, 3, 5, \ldots$, would not be sufficient since $\eta^{1/2} = \pm i\eta_d$ is not a unit of $Z(\delta)$ unless $d = -1$. When $d = -1, -3$ the problem is further compounded by the presence of eighth and sixth roots of unity. Consequently we shall exclude $d = -1, -3$ from the following algorithm. (However a fundamental unit for each of these cases will be given in the examples at the end of the chapter.

When $d \neq -1, -3$ we can overcome the problem by testing both $\eta^{1/2}$ and $(-\eta)^{1/2}$. When $p > 2$, p prime, there is no problem since $(-\eta)^{1/p} = -(\eta^{1/p})$. However it is possible that we would end up with $-\eta_d$ rather

than η_d. (Assuming that $|\eta| > 1$).

Algorithm 4.1

Assume $d \neq -1, -3$. Let η be any unit of $Z(\delta)$ such that $|\eta| > 1$. Then the fundamental unit of $Z(\delta)$ may be obtained as follows. (If $\eta = H + Ii$ then $Re(\eta) = H$, $Im(\eta) = I$).

1. Obtain a lower bound, L, for the magnitude of η_d such that $L > 1$

2 Set $\eta(2) = \eta^{\frac{1}{2}}$

3 If $|\eta(2)| < L$ go to 26

4 If $\nexists\, x \in Z$ such that $|x/2 - Re(\eta(2))| < 1/|\eta(2)|$ go to 8

5 If $\nexists\, z \in Z$ such that $|zD_2/2 - Im(\eta(2))| < 1/|\eta(2)|$ go to 8

6 Calculate y, t from (20) and (22)

7 If $N((x + y\delta + z\delta^2 + t\delta^3)/4) = 1$ then set $\eta = \eta(2)$ and go to 2

8 Set $\eta(2) = (-\eta)^{\frac{1}{2}}$

9 If $\nexists\, x \in Z$ such that $|x/2 - Re(\eta(2))| < 1/|\eta(2)|$ go to 13

10 If $\nexists\, z \in Z$ such that $|zD_2/2 - Im(\eta(2))| < 1/|\eta(2)|$ go to 13

11 Calculate y, t from (20) and (22)

12 If $N((x + y\delta + z\delta^2 + t\delta^3)/4) = 1$ then set $\eta = \eta(2)$ and go to 2

13 Set p = 3

14 Set $N = [\log|\eta|/\log L + 1]$

15 If $p \geq N$ go to 26

16 Set $\eta(p) = \eta^{1/p}$ (any one of the p p^{th} roots)

17 Set $\mu(p) = 1^{1/p}$ (any primitive p^{th} root of unity)

18 Set j = 1

19 If $\nexists\, x \in Z$ such that $|x/2 - Re(\eta(p))| < 1/|\eta(p)|$ go to 23

20 If $\nexists\, z \in Z$ such that $|zD_2/2 - Im(\eta(p))| < 1/|\eta(p)|$ go to 23

21 Calculate y, t from (20) and (22)

22 If $N((x + y\delta + z\delta^2 + t\delta^3)/4) = 1$ then set $\eta = \eta(p)$, go to 14

23 If $j \geq p$ then increment p to the next largest prime, go to 15

24 Set $j = j + 1$

25 Set $\eta(p) = \eta(p).\mu(p)$, go to 19

26 If $Re(\eta) < 0$ then set $\eta = -\eta$

27 Stop, η is the fundamental unit .

Notes

i) When $|\eta(p)|$ is small there is the possibility of several values of x, y, z, t at steps 4, 5, 6, 9, 10, 11, 19, 20 and 21. All possibilities must be checked. However when $|\eta(p)| > 4$ only one value of x and one value of z are possible, and when $|\eta(p)| > 10$ only one value of y and one value of t are possible.

ii) Since the units of $Z(\delta)$ will, in general, be non-real numbers we must check all p p^{th} roots of η. Steps 17, 18, 23, 24, 25 of the algorithm ensure that this is done. //

We now give an example to illustrate the use of the use of the theorem.

Example 4.4

Using algorithm 4.1 we show that the following units are fundamental.

d	η_d
-2	$1 - \delta^2 - \delta^3$
-5	$2 + 2\delta + \delta^2$
-6	$1 - 4\delta - 4\delta^2 - 2\delta^3$
-7	$(3 + \delta - \delta^2 + \delta^3)/4$
-10	$27 + 12\delta + \delta^2 - 3\delta^3$

(These units were obtained by exhaustive testing of small values of x, y, z, t).

<u>d = -2</u>

$$1 - \delta^2 - \delta^3 \approx 2.189 - 2.603i,$$

and $$|1 - \delta^2 - \delta^3| \approx 3.402$$

From example 2 we have L = 3. Thus $1 - \delta^2 - \delta^3$ is the fundamental unit since $|1 - \delta^2 - \delta^3|^{\frac{1}{2}} < L$ and $\mathrm{Re}(1 - \delta^2 - \delta^3) > 0$.

<u>d = -5</u>

$$2 + 2\delta + \delta^2 \approx 4.115 + 4.351i,$$

and $$|2 + 2\delta + \delta^2| \approx 5.989$$

In a manner similar to example 2 we obtain L = 4.6 and thus $2 + 2\delta + \delta^2$ is the fundamental unit.

<u>d = -6</u>

$$1 - 4\delta - 4\delta^2 - 2\delta^3 \approx 1.995 - 19.646i,$$

and $$|1 - 4\delta - 4\delta^2 - 2\delta^3| \approx 19.747$$

We have L = 5.03 and since $|\eta^{\frac{1}{2}}| < L$ we have $\eta_{-6} = 1 - 4\delta - 4\delta^2 - 2\delta^3$.

d = -7

$$(3 - \delta - \delta^2 - \delta^3)/4 \approx 1.223 - 1.710i$$

and $$|(3 - \delta - \delta^2 - \delta^3)/4| \approx 2.102$$

In the manner of example 3 we will obtain a lower bound L. Suppose $|\eta_d| < 1.5$. Then from the corollary to theorem 4.3 we have $|x| < 5$. However from (19) we have $x^2 \equiv \pm 16 \equiv \pm 2 (\text{mod } 7)$. Thus $|x| = 3, 4$. From the corollary to theorem 3.4 we also have that $|z| < 1.89$ and so $|z| = 1$. ($z = 0$ is only possible when $d = -1$). Therefore the only possibility is $|z| = 1$ and $|x| = 3$ (since $x \equiv z (\text{mod } 4)$). This leads to the unit we started with (and its associates) and so we can conclude $|\eta_{-7}| > 1.5$. Thus we can take L = 1.5. Since $(2.102)^{\frac{1}{2}} < 1.5$ we conclude that $(3 - \delta - \delta^2 - \delta^3)/4$ is the fundamental unit.

d = -10

$$27 + 12\delta + \delta^2 - 3\delta^3 \approx 54.018 + 6.322i,$$

and $$|27 + 12\delta + \delta^2 - 3\delta^3| \approx 54.387 .$$

We have L = 6.4 and thus we must check $\eta^{\frac{1}{2}}$ and $(-\eta)^{\frac{1}{2}}$.

$$\eta^{\frac{1}{2}} \approx 7.362 + 0.429i \text{ and } |\eta^{\frac{1}{2}}| \approx 7.374$$

For d = -10 we must have $x = 0 (\text{mod } 4)$ and clearly no $x \equiv 0 (\text{mod } 4)$ satisfies step 4 of the algorithm. Thus $\eta^{\frac{1}{2}}$ is not a unit.

$$(-\eta)^{\frac{1}{2}} \approx -0.429 + 7.362i \text{ and } |(-\eta)^{\frac{1}{2}}| \approx 7.374$$

No value of $x \equiv 0 (\text{mod } 4)$ satisfies step 9 of the algorithm and so $(-\eta)^{\frac{1}{2}}$ is not a unit. Step 14 of the algorithm sets N = 3 and so we stop. Thus $\eta_{-10} = 27 + 12\delta + \delta^2 - 3\delta^3$. //

Finally we give a fundamental unit for each of the cases d = -1 and d = -3.

Example 4.5

i) A unit of $Z((-1)^{\frac{1}{4}})$ is $\delta + \delta^2 + \delta^3$. If $\delta + \delta^2 + \delta^3$ is not a fundamental unit then there must exist a unit, η, such that

$$1 < |\eta| \leq |\delta + \delta^2 + \delta^3|^{\frac{1}{2}} < 1.554$$

Thus letting $\eta = H + Ii$, we have from the corollary to theorem 4.3

$$1.554 > |H| \geq |x/2| - 1,$$

and

$$1.554 > |I| \geq |z|D_2/2 - 1.$$

Thus η must have $|x|, |z| < 5.108$ and so the possibilities are $|x| = 0, \pm 4$ and $|z| = 0, \pm 4$. However the only units we are led to are roots of unity or associates of $\delta + \delta^2 + \delta^3$, and so no such η exists. Thus $\delta + \delta^2 + \delta^3$ is a fundamental unit of $Z((-1)^{\frac{1}{4}})$.

ii) In a similar manner to i) it can be shown that $(1 - \delta - \delta^2 - \delta^3)/2$ is a fundamental unit of $Z((-3)^{\frac{1}{4}})$. //

APPENDIX 1

Multiprecision Arithmetic Computer Programs

Many computational problems arising in number theory require considerably more precision than is normally available on a calculator or computer. Consequently it is necessary to develop multiprecision arithmetic computer programs to handle the calculations encountered in problems such as examples 3.4 and 3.5.

The algol procedures listed in this appendix, which were developed on a B6700 computer, were written in order that the calculations required by algorithm 3.1 could be performed. The procedures listed cover all the basic arithmetic operations and can easily be extended to cope with other multiprecision computations which arise in number theory.

For these procedures multiprecision numbers are stored in one dimensional integer arrays. The procedures use two types of multiprecision numbers

a) Multiprecision Integers (m.p. integers)

An m.p. integer, x,is stored in an integer array, X, according to the equation

$$x = X[-2](X[0] + X[1] \times 10^{10} + X[2] \times 10^{20} + \ldots + X[n] \times 10^{10n})$$

where $X[-2] = \pm 1$ and $0 \leq X[j] < 10^{10}$. X[-1] is set equal to n. That is, X[-2] contains the sign of x, X[-1] contains the number $n = [\log_{10}|x|/10]$ (the 'length' of x), and X[0], X[1], . . . , X[n] contain the magnitude of x in base 10^{10} 'digits'.

Example 1

The integer x = -1234567892 1234567891 1234567890 would be stored in the array, X, as follows

X[-2] ← -1 ; X[-1] ← 2 ;

X[0] ← 1234567890 ;

X[1] ← 1234567891 ;

X[2] ← 1234567892 ; //

b) Multiprecision floating point numbers (m.p.f.p. numbers)

An m.p.f.p. number, y, is stored in an integer array Y according to the equation

$y = Y[-2](Y[0] \times 10^{-10(n+1)} + Y[1] \times 10^{-10n} + \ldots + Y[n] \times 10^{10})10^{10Y[n+1]}$

where $Y[-2] = \pm 1$, $0 \leq Y[j] < 10^{10}$, and $Y[-1] = n$.

Example 2

i) The integer of example 1 is converted to a m.p.f.p. number by setting X[3] ← 3.

ii) The number y = 126.2539286742 0397627891 is stored in an integer array Y as follows

Y[-2] ← 1 ; Y[-1] ← 2 ;

Y[0] ← 397627891 ;

Y[1] ← 2539286742 ;

Y[2] ← 126 ;

Y[3] ← 1 ; //

Zero is stored as an m.p. integer as

$$X[-2] = 1;\ X[-1] = X[0] = 0\ ;$$

For the floating point representation of zero we add $X[1] = 0$.

We now briefly describe the procedures. (The procedures assume that the array which is to hold the result of an operation has been declared large enough to hold the result). Unless otherwise stated the arrays which are parameters of the procedures need not be distinct.

TRANS (X, Y, F):

X, Y are m.p. integers. F is an integer which is set equal to 1 when X is an m.p.f.p. number and zero otherwise.

Result : $Y \leftarrow X$

ADD(Y, Z);

Y, Z are m.p. integers of the same sign.

Result: $Z \leftarrow Y + Z$

MULTIADD (X, Y, Z);

X, Y are m.p. integers, Z is an integer array.

Result: $Z \leftarrow X + Y$

SIMPLEMULT (SMALL, BIG, PRODUCT):

SMALL is a single precision integer and BIG is an m.p. integer. PRODUCT is an integer array.

Result: PRODUCT ← BIG * SMALL

MULTIMULT (NUM1 , NUM2 , PRODUCT);

NUM1 , NUM2 are m.p. integers and PRODUCT is an integer array.

Result: PRODUCT ← NUM1 .* NUM2

SIMPLEDIV (I, A, Q, REM);

A is an m.p. integer. Q is an integer array. I is a single precision integer and REM is an integer identifier. REM and I must be distinct.

Result Q ← [|A|/|I|] * sign (A/I)

REM ← A - Q * I

SD (D, A, Q);

Used by MULTIDIV to produce 1 'digit' of QUOT.

MULTIDIV (DIVS, DIVD, QUOT, REM);

DIVS and DIVD are m.p. integers, QUOT and REM are integer arrays. All four arrays should be distinct.

Result: QUOT ← [|DIVD|/|DIVS|] * sign (DIVD/DIVS)

REM ← DIVD - QUOT * DIVS

CHOP (X, N);

X is an m.p.f.p. number. N is a positive single precision integer.

Result: X is chopped to N base 10^{10} digits.

(No change if X[-1] ≤ N - 1).

FPADD (X, Y, Z);

X, Y are m.p.f.p. numbers and Z is an integer array.

Result: Z ← X + Y (exact)

SFPMULT (I, A, PROD);

Floating point equivalent of SIMPLEMULT (exact result)

SFPDIV (I, A, Q);

I is a single precision integer and A is a m.p.f.p. number.

Q is an integer array.

Result: Q ← A/I (to A[-1] + 1 base 10^{10} digits)

FDIV (D, A, Q, N);

D, A are m.p.f.p. numbers, Q is an integer array. D, A, Q should be distinct arrays. N is a positive single precision integer.

Result: Q ← A/D (to N base 10^{10} digits)

FMULT (X, Y, PROD);

Floating point equivalent of MULTIMULT. Result is exact.

NR (N, D, S, X);

N, S are positive single precision integers, D is an m.p.f.p. number and X is an integer array.

Result: X ← $D^{1/N}$ (to S base 10^{10} digits)

Using Newton-Raphson iteration.

The arrays declared at the beginning of the listing which follows are working arrays for some of the procedures. They are not for general use.

```
     INTEGER ARRAY XXX,ZZZ,YYY,VVV[-2:150];
PROCEDURE TRANS(X,Y,F);INTEGER F;INTEGER ARRAY X,Y[-2];
   BEGIN INTEGER I;
         FOR I:=-2 STEP 1 UNTIL X[-1] DO Y[I]:=X[I];
         IF F=1 THEN Y[I]:=X[I]
    END OF TRANS;
PROCEDURE ADD(Y,Z); INTEGER ARRAY Y,Z[-2];
    BEGIN INTEGER I ,J;
     J:=SIZE(Z)-3;
         IF J GTR Z[-1] THEN FOR I:=(Z[-1]+1) STEP 1 UNTIL J
                                  DO Z[I]:=0;
         J:=Y[-1];
         FOR I:=0 STEP 1 UNTIL J DO
              BEGIN
                   Z[I]:=Z[I] + Y[I];
                IF Z[I] GTR 9999999999
                     THEN BEGIN
                            Z[I]:=Z[I]-10000000000;
                            Z[I+1]:=Z[I+1]+1
                          END
              END;
     J:=MAX(Z[-1],Y[-1])+1;
     IF Z[J] NEQ 0 THEN Z[-1]:=J ELSE Z[-1]:=J-1;
     END OF ADD;
PROCEDURE MULTIADD(X,Y,Z); INTEGER ARRAY X,Y,Z[-2];
     BEGIN INTEGER I;   LABEL L1;
     IF X[-2]=Y[-2] THEN BEGIN
              FOR I:=-2 STEP 1 UNTIL X[-1] DO ZZZ[I]:=X[I];
         ADD(Y,ZZZ)  ;   END
                    ELSE BEGIN
          FOR I:=0 STEP 1 UNTIL X[-1] DO
               ZZZ[I]:=9999999999 -X[I];
          ZZZ[0]:=ZZZ[0]+1;
          ZZZ[-1]:=X[-1];
         IF Y[-1] GTR X[-1] THEN BEGIN
               FOR I:=(X[-1]+1) STEP 1 UNTIL Y[-1] DO
                    ZZZ[I]:=9999999999;
                    ZZZ[-1]:=Y[-1] END;
         I:= ZZZ[-1]+1;
        ADD(Y,ZZZ);
          IF  ZZZ[I]=1 THEN
               BEGIN ZZZ[-1]:=ZZZ[-1]-1;
                     ZZZ[-2]:=Y[-2]    ;
                    WHILE ZZZ[ZZZ[-1]]=0 DO ZZZ[-1]:=*-1 ;
                IF ZZZ[-1]=-1 THEN BEGIN
                          ZZZ[-1]:=0;  ZZZ[-2]:=1  END
               END
                     ELSE
               BEGIN FOR I:=0 STEP 1 UNTIL ZZZ[-1] DO
                    ZZZ[I]:=9999999999 -ZZZ[I];
                    ZZZ[0]:= * +1;
                    I:=0;
L1   :              IF ZZZ[I]=10000000000
                         THEN BEGIN ZZZ[I+1]:=*+1;
                                    ZZZ[I]:=0 ;
                                    I:=* +1;
                                  GO TO L1 END;
                   ZZZ[-2]:=X[-2]     ;
                    WHILE ZZZ[ZZZ[-1]]=0 DO ZZZ[-1]:=*-1
               END
         END          ;
     TRANS(ZZZ,Z,0);
     END OF MULTIADD;
```

```
    PROCEDURE SIMPLEMULT(SMALL,BIG,PRODUCT); VALUE SMALL;
         INTEGER SMALL; INTEGER ARRAY BIG,PRODUCT[-2];
         BEGIN INTEGER I,J,CARRY; DOUBLE PROD ,M;
        CARRY:=0;
         IF SMALL = 0 OR (BIG[-1]=0 AND BIG[0]=0)
              THEN BEGIN PRODUCT[-2]:=1;
                         PRODUCT[-1]:=0;PRODUCT[0]:=0  END
              ELSE BEGIN J:= SIGN(SMALL)*SMALL;
                 FOR I:=0 STEP 1 UNTIL BIG[-1] DO BEGIN
                        PROD:= J MUX BIG[I] + CARRY;
                        CARRY:= ENTIER(PROD/10000000000);
                        M:=CARRY MUX 10000000000;
                        PRODUCT[I]:=INTEGER(SINGLE(PROD-M)) END;
                        I:= BIG[-1]+1;
                   IF CARRY=0 THEN PRODUCT[-1]:=I-1
                             ELSE BEGIN
                                  PRODUCT [I]:= CARRY;
                                  PRODUCT[-1]:=I     END;
                PRODUCT[-2]:=SIGN(SMALL)*BIG[-2]  END
       END OF SIMPLEMULT;
PROCEDURE MULTIMULT(NUM1,NUM2,PRODUCT);
              INTEGER ARRAY NUM1,NUM2,PRODUCT[-2];
    BEGIN
         INTEGER I,J,K;
              IF (NUM1[-1]=0 AND NUM1[0]=0) OR (NUM2[-1]=0 AND
                                                NUM2[0]=0)
                THEN BEGIN PRODUCT[-2]:=1;
                           PRODUCT[-1]:=0;
                           PRODUCT[0]:=0
                     END
                ELSE BEGIN
                  FOR I:= 0 STEP 1 UNTIL (SIZE(ZZZ)-3) DO ZZZ[I]:=0;
                      FOR I:=0 STEP 1 UNTIL NUM1[-1] DO
                            BEGIN
                                SIMPLEMULT(NUM1[I],NUM2,YYY);
                                FOR J:=0 STEP 1 UNTIL      YYY[-1] DO
                                    ZZZ[I+J]:=*+     YYY[J]     ;
                                 IF ENTIER(I/50)*50=I THEN BEGIN
                                      ZZZ[-1]:=I+NUM2[-1]+2;
                                      SIMPLEMULT(1,ZZZ,ZZZ) END;
                              END;
                           K:=NUM1[-1]+NUM2[-1];
                           FOR I:= 0 STEP 1 UNTIL K DO
                                 BEGIN
                                      J:=ENTIER( ZZZ[I]/10000000000);
                                   PRODUCT[I]:= ZZZ[I]-10000000000*J;
                                    ZZZ[I+1]:=*+J
                                END;
                            PRODUCT[K+1]:= ZZZ[K+1];
                            IF  ZZZ[K+1]=0 THEN PRODUCT[-1]:=K
                                           ELSE PRODUCT[-1]:=K+1;
                            PRODUCT[-2]:=NUM1[-2]*NUM2[-2]
                     END
     END OF MULTIMULT;
```

```
PROCEDURE SIMPLEDIV(I,A,Q,REM);VALUE I;INTEGER I,REM;
  INTEGER ARRAY A,Q[-2];
     BEGIN INTEGER J,K,L; DOUBLE M,N; K:=0;
           L:=I*SIGN(I);
          FOR J:=A[-1] STEP -1 UNTIL 0
                DO BEGIN M:=K MUX 10000000000+A[J];
                         Q[J]:=ENTIER(SINGLE(M/L));
                          N:=Q[J] MUX L;
                          K:= INTEGER(SINGLE(M-N))
                   END;
           REM:=K*A[-2];
          IF Q[A[-1]]=0 THEN Q[-1]:=A[-1]-1
                        ELSE Q[-1]:=A[-1];
           Q[-2]:=A[-2]*SIGN(I);
         IF Q[-1]=-1 THEN BEGIN Q[-1]:=0;Q[-2]:=1 END
    END OF SIMPLEDIV;
PROCEDURE SD(D,A,Q);INTEGER ARRAY D,A[-2];INTEGER Q;
    BEGIN DOUBLE M;INTEGER I,J;INTEGER ARRAY SAVE[-2:A[-1]];
           LABEL L1,L2;
         I:=A[-1];J:=D[-1];
          M:=(D[J-1]+1)/10000000000; M:=D[J]+M;
        IF I=J THEN M:=A[I]/M
                  ELSE M:=(A[I] MUX 10000000000 + A[I-1])/M;
         Q:=ENTIER(SINGLE(M));
           FOR J:=-2 STEP 1 UNTIL I DO SAVE[J]:=A[J];
           SIMPLEMULT(-Q,D,A);
           FOR J:=0 STEP 1 UNTIL A[-1] DO
                IF SAVE[J]<A[J] THEN BEGIN
                     SAVE[J]:=SAVE[J]+10000000000-A[J];
                     SAVE[J+1]:=*-1 END
                          ELSE SAVE[J]:=*-A[J];
                WHILE SAVE[SAVE[-1]]=0 DO SAVE[-1]:=*-1;
                IF SAVE[-1]=-1 THEN BEGIN SAVE[-1]:=0;GO TO L1 END ;
           IF (SAVE[-1]<D[-1]) OR (SAVE[-1]=D[-1] AND
                        SAVE[SAVE[-1]]<D[D[-1]])
                         THEN GO TO L1;
           FOR J:=-2 STEP 1 UNTIL SAVE[-1] DO A[J]:=SAVE[J];
        MULTIADD(A,D,A);
           IF A[-2]=-1 THEN GO TO L1;  Q:=*+1;
         FOR J:=-2 STEP 1 UNTIL A[-1] DO SAVE[J]:=A[J];
           MULTIADD(A,D,A);
           IF A[-2]=-1 THEN GO TO L1;  Q:=*+1;       GO TO L2;
L1:  FOR J:=-2 STEP 1 UNTIL  SAVE[-1] DO A[J]:=SAVE[J];
L2  :END OF SD;
```

```
PROCEDURE MULTIDIV(DIVS,DIVD,QUOT,REM);
     INTEGER ARRAY DIVS,DIVD,QUOT,REM[-2];
    BEGIN INTEGER ARRAY SAVE[-2:DIVD[-1]];
         INTEGER I,J,K,M;LABEL L1;
          IF DIVS[-1]=0 AND DIVS[0]=0 THEN BEGIN QUOT[0]:=-1;
                                               GO TO L1 END;
        IF DIVD[-1]<DIVS[-1]
              THEN  BEGIN QUOT[0]:=QUOT[-1]:=0;
                          QUOT[-2]:=1;
                          FOR K:=-2 STEP 1 UNTIL DIVD [-1]
                             DO REM [K]:=DIVD[K];
                          GO TO L1 END;
          M:=DIVS[-2]; DIVS[-2]:=-1; I:=DIVS[-1]-1; J:=DIVD[-1];
       FOR K:=-2 STEP 1 UNTIL J DO SAVE[K]:=DIVD[K];
         FOR K:=0 STEP 1 UNTIL I DO DIVD[K]:=SAVE[J-I+K];
         DIVD[-2]:=1; DIVD[-1]:=I; I:=*+1; QUOT[-1]:=J-I;
        QUOT[-2]:=M*SAVE[-2];
          FOR K:=QUOT[-1] STEP -1 UNTIL 0 DO
              BEGIN
                    FOR J:=DIVD[-1] STEP -1 UNTIL 0 DO
                         DIVD[J+1]:=DIVD[J] ;
                         DIVD[0]:=SAVE[K];
                         DIVD[-1]:=*+1;
                         IF DIVD[DIVD[-1]]=0 THEN DIVD[-1]:=*-1;
                  IF DIVD[-1] GEQ I THEN SD(DIVS,DIVD,QUOT[K])
                                    ELSE QUOT[K]:=0
             END;
          IF QUOT[QUOT[-1]]=0
              THEN BEGIN QUOT[-1]:=*-1;
                         IF QUOT[-1]=-1
                           THEN BEGIN QUOT[-1]:=0;QUOT[-2]:=1 END
                   END;
          FOR K:=-1 STEP 1 UNTIL DIVD [-1]
               DO REM[K]:=DIVD[K]; REM[-2]:=SAVE[-2];
          FOR K:=-2 STEP 1 UNTIL SAVE[-1] DO DIVD[K]:=SAVE[K];
        DIVS[-2]:=M;
L1:  END OF MULTIDIV;
PROCEDURE CHOP(X,N); VALUE N; INTEGER N; INTEGER ARRAY X[-2];
      BEGIN INTEGER I,J;
           IF X[-1] GTR (N-1)
                THEN BEGIN I:=X[-1]-N+1;
                           FOR J:=0 STEP 1 UNTIL N
                               DO X[J]:=X[J+I];
                           X[-1]:=N-1
                     END
    END OF CHOP;
```

```
PROCEDURE FPADD(X,Y,Z);INTEGER ARRAY X,Y,Z[-2];
     BEGIN INTEGER EX,EY,XO,YO,I,J,K;
         PROCEDURE AD(A,B);INTEGER ARRAY A,B[-2];
             BEGIN I:=(XO-YO)*SIGN(XO-YO);
                   FOR J:=A[-1] STEP -1 UNTIL 0
                         DO VVV[J+I]:=A[J];
                FOR J:=0 STEP 1 UNTIL (I-1)
                         DO VVV[J]:=0;
                          VVV[-2]:=A[-2]; VVV[-1]:=A[-1]+I;
                   IF VVV[-1] GEQ B[-1] THEN K:=VVV[-1]
                                        ELSE K:=B[-1];
                    MULTIADD(VVV,B,VVV);
               END OF SB;
          EX:=X[X[-1]+1]; EY:=Y[Y[-1]+1];
        XO:=EX-X[-1]; YO:=EY-Y[-1];
          IF XO=YO
               THEN BEGIN IF Y[-1] GEQ X[-1] THEN K:=Y[-1]
                                             ELSE K:=X[-1];
                          MULTIADD(X,Y,VVV);
                    END
               ELSE IF XO<YO THEN AD(Y,X)
                             ELSE AD(X,Y);
          IF EY GEQ EX THEN VVV[VVV[-1]+1]:=EY+VVV[-1]-K
                       ELSE VVV[VVV[-1]+1]:=EX+VVV[-1]-K;
          IF VVV[-1]=0 AND VVV[0]=0 THEN VVV[1]:=0;
          TRANS(VVV,Z,1);
     END OF FPADD;
PROCEDURE SFPMULT(I,A,PROD);VALUE I;INTEGER I;
   INTEGER ARRAY A,PROD[-2];
     BEGIN INTEGER K,J;K:=A[-1];J:=A[K+1];
        SIMPLEMULT(I,A,PROD);
          IF PROD[-1]=K THEN PROD[K+1]:=J
                        ELSE PROD[K+2]:=J+1;
          IF PROD[0]=0 AND PROD[-1]=0 THEN PROD[1]:=0
END OF SFPMULT;
    PROCEDURE SFPDIV(I,A,Q);VALUE I; INTEGER I;
        INTEGER ARRAY A,Q[-2];
      BEGIN INTEGER J,K ,E; K:=A[-1];E:=A[K+1];
          SIMPLEDIV(I,A,Q,J);
          IF Q[K]=0
                THEN BEGIN
                     Q[K+1]:=E-1;Q[-1]:=K;
                   FOR K:=Q[-1] STEP -1 UNTIL 1
                                DO Q[K]:=Q[K-1];
                      Q[0]:=ENTIER(SIGN(J/I)*(J/I)*10000000000)
                     END
               ELSE Q[K+1]:= E
END OF SFPDIV;
```

```
PROCEDURE FDIV(D,A,Q,N);VALUE N; INTEGER N;
      INTEGER ARRAY D,A,Q[-2];
      BEGIN INTEGER  I,P,EA;
            P:=N+D[-1];EA:=A[A[-1]+1];
            IF A[-1]<P
               THEN BEGIN IF  (SIZE(A)-3)<P
                              THEN RESIZE(A[*],P+3,RETAIN);
                          P:=*-A[-1];
                            FOR I:=A[-1] STEP -1 UNTIL 0
                              DO A[I+P]:=A[I];
                          FOR I:=(P-1) STEP -1 UNTIL 0
                              DO A[I]:=0;
                            A[-1]:=*+P          END
                    ELSE P:=0;
            MULTIDIV(D,A,YYY,ZZZ);
            IF YYY[-1]=(A[-1]-D[-1])
                 THEN BEGIN YYY[YYY[-1]+1]:=EA-D[D[-1]+1 ]+1;
                            CHOP(YYY,N) END
                 ELSE  YYY[YYY[-1]+1]:=EA-D[D[-1]+1];
            A[-1]:=*-P;
            IF P NEQ 0 THEN FOR I:=0 STEP 1 UNTIL A[-1]
                            DO A[I]:=A[I+P];
                               A[A[-1]+1]:=EA        ;
         TRANS(YYY,Q,1);
      END OF FDIV;
  PROCEDURE FMULT(X,Y,PROD);INTEGER ARRAY X,Y,PROD[-2];
    BEGIN INTEGER M,EX,EY;
            EX:=X[X[-1]+1];
            EY:=Y[Y[-1]+1];
            M:=X[-1]+Y[-1]+1;
           MULTIMULT(X,Y,PROD);
            IF PROD[-1]=M THEN PROD[PROD[-1]+1]:=EX+EY
                          ELSE PROD[PROD[-1]+1]:=EX+EY-1;
            IF PROD[-1]=0 AND PROD[0]=0 THEN PROD[1]:=0
END OF FMULT;
```

```
PROCEDURE NR(N,D,S,X); VALUE N,S; INTEGER N,S;INTEGER ARRAY D,X[-2];
     BEGIN DOUBLE POWER,APPROX,DIFF; INTEGER J,EX; LABEL LEND;
           PROCEDURE ITERATE(K);VALUE K;INTEGER K;
               BEGIN INTEGER I;
                     TRANS(X,XXX,1);
                     FOR I:=N-3 STEP -1 UNTIL 0 DO
                          BEGIN FMULT(X,XXX,XXX);
                                CHOP(XXX,K+1) END;
                     FDIV(XXX,D,XXX,K);SFPMULT(N-1,X,X);
                    FPADD(X,XXX,X);SFPDIV(N,X,X);
               END;
          IF N=1 THEN BEGIN TRANS(D,X,1);  GO TO LEND END;
        J:=D[-1];
          POWER:=D[J-1]/10000000000;POWER:=*+D[J];
          POWER:=DLOG(POWER); POWER:=*+(D[J+1]-1)*10;
         APPROX:=POWER/N;
          EX:=ENTIER((APPROX/10));
          DIFF:=APPROX-EX*10;J:=ENTIER(DIFF); DIFF:=*-J;
         X[-2]:=X[-1]:=1;
          APPROX:=10**J*DEXP(DIFF*DLN(10));
          X[1]:=ENTIER(APPROX);
          APPROX:=(APPROX-X[1])*10000000000;
     X[0]:=ENTIER(APPROX);
          X[2]:=EX+1;
          IF X[1]=0 THEN BEGIN X[0]:=1;X[1]:=EX;X[-1]:=0.END;
         J:=2;
          WHILE J+1 LEQ S  DO
                    BEGIN ITERATE(J+1); J:=J*2 END;
        CHOP(X,ENTIER(S/2+1));
         ITERATE(X[-1]+2);     ITERATE(S+1); CHOP(X,S);
LEND:END OF NR;
```

BIBLIOGRAPHY

ADAMS, W.W. and GOLDSTEIN, L.J.(1976)
Introduction to Number Theory, Prentice-Hall, New Jersey.

BEACH, B.D., WILLIAMS, H.C. and ZARNKE, C.R. (1971)
Some Computor Results on Units in Quadratic and Cubic Fields. Scientific Report 31, University of Manitoba, Winnipeg, p609 - 647.

BERNSTEIN, L.(1971)
Lecture Notes in Mathematics, Vol.207, The Jacobi-Perron Algorithm Its Theory and Application, Springer-Verlag Berlin Heidelberg.

CASSELS, J.W.S.(1950)
The rational solutions of the Diophantine Equation $Y^2 = X^3 - D$. Acta Mathematica, Vol.82, p243 - 273

CHRYSTAL, G.(1959)
Algebra : An Elementary Text-book for the Higher Classes of Secondary Schools and for Colleges, Part II., 6th ed. Chelsea Publishing Company, New York.

CLARK, A.(1971)
Elements of Abstract Algebra, Wadsworth Publishing Company, Belmont, California.

COHN, H.(1962)
A Second Course in Number Theory, John Wiley and Sons, New York.

COHN, J.H.E.(1977)
The Length of the Period of the Simple Continued Fraction of $d^{\frac{1}{2}}$. Pacific Journal of Mathematics, Vol. 71 No. 1 p21 - 32.

DELONE, B.N. and Faddeev, D.K.(1964)
The Theory of Irrationalities of the Third Degree, Translations of Mathematical Monographs, Volume 10, American Mathematical Society, Providence, R.I.

HARDY, G.H. and WRIGHT, E.M.(1960)
An Introduction to the Theory of Numbers, 4th ed. Oxford University Press, Oxford.

HENDY, M.D. (1975)
Classification of Ideals by Norm into Ideal Classes over the Integers of Real Quadratic Number Fields. Private Communication.

HICKERSON, D.R.(1973)
Length of Period of Simple Continued Fraction Expansion of $\sqrt{d}$. Pacific Journal of Mathematics, Vol. 46 No. 2 p429 - 432.

JEANS, N.S. and HENDY, M.D.(1978)
Determining the Fundamental Unit of a Pure Cubic Field Given Any Unit. Mathematics of Computation, Vol. 32.

JONES, B.W.(1955)
The Theory of Numbers, Holt, Rinehart and Winston, New York.

LEHMER, D.H.(1969)
Computor Technology Applied to the Theory of Numbers, p117 - 151. In LeVeque, W.J. ed. M.A.A. Studies in Mathematics Vol. 6, Studies in Number Theory, The Mathematical Association of America.

MARKOFF, A.(1892)
Sur les nombres entiers dépendants d'une racine cubique d'un nombre entier ordinaire. Mémoires Acad. Imp. Sci. St. Petersbourg, Vol. 38.

MAXFIELD, J.E. and MAXFIELD, M.W.(1971)
Abstract Algebra and Solution by Radicals, W.B. Saunders Company, Philadelphia.

McCOY, N.H.(1965)
The Theory of Numbers, MacMillan, New York.

NAGELL, T.(1923)
Über die Einheiten in reinen kubischen Zahlkörpern. Vid-Selsk, Skr. I. Mat. Nat. Kl., No. 11.

NIVEN, I. and ZUCKERMAN, H.S.(1972)
An Introduction to the Theory of Numbers, 3rd ed. John Wiley and Sons, New York.

PETTOFREZZO, A.J. and BYRKIT, D.R.(1970)
Elements of Number Theory, Prentice-Hall, New Jersey.

RICHMAN, F.(1971)
Number Theory : An Introduction to Algebra, Wadsworth Publishing Company, Belmont, California.

SAMUEL, P.(1970)
Algebraic Theory of Numbers, Houghton Mifflin Company, Boston. (Translation of Théorie algébrique des nombres, (1967), Hermann, Paris).

SELMER, E.S.(1955)
Tables for the purely cubic field $K(\sqrt[3]{m})$. Avhandlinger Utgitt av det Norske Videnskaps-Akademi i Oslo. I. No. 5.

SHANKS, D.(1975)
Review of Beach, Williams and Zarnke [1971]. In Mathematics of Computation, Vol. 29, p330.

STANTON, R.G. SUDLER, C. and WILLIAMS, H.C.(1976)
An Upper Bound for the Period of the Simple Continued Fraction for $\sqrt{d}$. Pacific Journal of Mathematics, Vol. 67 No. 2, p525 - 536.

STEINER, R. and RUDMAN, R.(1976)
On an Algorithm of Billevich for Finding Units in Algebraic Number Fields. Mathematics of Computation, Vol.30, p598 - 609.

SVED, M.(1970)
Units in Pure Cubic Number Fields. Annales Universitatis Scientiarum Budapestinensis De Rolando Eötyös Nominatae Sectio Mathematica, Vol. 13, p141 - 149.

SZEKERES, G.(1970)
Multidimensional Continued Fractions. Annales Universitatis Scientiarum Budapestinensis De Rolando Eötvös Nominatae Sectio Mathematics, Vol. 13, p113 - 140.

WADA, H.(1970)
A Table of Fundamental Units of Purely Cubic Fields, Proceedings of the Japan Academy, Vol. 46, p1135 - 1140.

WOLFE, C.(1923)
On the Indeterminate Cubic Equation $x^3+Dy^3+D^2z^3-3Dxyz = 1$, University of California Publications in Mathematics, Vol. 1, p359 - 364.