JOURNAL OF MATHEMATICAL ANALYSIS AND APPLICATIONS 83, 264–274 (1981)

Radix Representations of Quadratic Fields

WILLIAM J. GILBERT

University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

Submitted by G.-C. Rota

Let ρ be an algebraic integer in a quadratic number field whose minimum polynomial is $x^2 + p_1 x + p_0$. Then all the elements of the ring $\mathbb{Z}[\rho]$ can be written uniquely in the base ρ as $\sum_{k=0}^{m} a_k \rho^k$, where $0 \leqslant a_k < |p_0|$, if and only if $p_0 \geqslant 2$ and $-1 \leqslant p_1 \leqslant p_0$.

1. INTRODUCTION

Various bases have been proposed for writing complex numbers in positional notation as a single string of digits, without separating the real and imaginary parts. Such representations are analogous to the binary and decimal representations of the positive real numbers using base two or ten, respectively. The complex numbers can be represented in binary form using the base $-1 + i$; that is, every complex number can be written as $\sum_{k=-\infty}^{m} a_k(-1+i)^k$, where $a_k = 0$ or 1. We denote this representation by $(a_m a_{m-1} \cdots a_1 a_0 \cdot a_{-1} \cdots)_{-1+i}$. The Gaussian integers correspond to the integer parts of these representations in which $a_k = 0$ for all $k < 0$. For example, $2 + 3i = (1011)_{-1+i}$ and $(-1 + 7i)/5 = (11.010101 \cdots)_{-1+i}$. Another representation is the "quater-imaginary" system using $2i$ as base and 0, 1, 2 and 3 as digits. In this case the integer parts of the representation correspond to the Gaussian integers with even imaginary part, $\mathbb{Z}[2i]$. To represent all the Gaussian integers, it is necessary to use, in addition, one negative radix place; for example, $1 + 5i = (31.2)_{2i}$. See Knuth [3; §4.1] for further information on all these bases.

Katai and Szabo [2] proved that the only numbers which are suitable bases for all the Gaussian integers, using $0, 1, 2, \ldots, N-1$ as digits, are $-n \pm i$ where n is a positive integer. The number $N = n^2 + 1$, the norm of $-n \pm i$. We generalize their work to find all the bases for quadratic number fields, using natural numbers as digits. Our work subsumes all the above examples.

We restrict our attention here to only considering the numbers $0, 1, 2, \ldots, N-1$ as digits. This appears to be the natural generalization of the usual number systems and it allows addition, subtraction and multiplication

0022-247X/81/090264-11$02.00/0

to be performed in these quadratic fields in the same way as ordinary arithmetic in base N, except for a change in the carry digits. It is possible to allow negative or even certain complex numbers as digits, as long as they form a complete residue system modulo the base. In such cases, the results on the valid bases will differ slightly from our results.

2. Radix Representations in Algebraic Number Fields

Let ρ be an algebraic integer whose minimum polynomial is $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0$, where the coefficients are integers. Let $N = |\text{Norm}(\rho)| = |p_0|$. We are interested in using the base ρ with natural numbers as digits to represent elements in some number field that contains ρ. The largest subset that we could hope to represent, without using negative powers of the base, is the ring $\mathbb{Z}[\rho]$.

We say that ρ is the *base* (or *radix*) of a *full radix representation* of $\mathbb{Z}[\rho]$ if each element $z \in \mathbb{Z}[\rho]$ can be written in the form $z = \sum_{k=0}^{m} a_k \rho^k$, where the *digits* a_k are natural numbers such that $0 \leqslant a_k < N$. We denote this representation by $z = (a_m a_{m-1} \cdots a_1 a_0)_\rho$.

The reason that the norm N yields the correct number of digits is due to the fact that the quotient ring $\mathbb{Z}[\rho]/(\rho)$ is isomorphic to $\mathbb{Z}_N$ by the map which takes a polynomial in ρ to its constant term modulo N. Hence the allowable digits for the units place, a_0, must form a complete set of representatives for $\mathbb{Z}_N$.

Any such radix representation will be unique. Suppose $A(x), B(x) \in \mathbb{Z}[x]$ are polynomials whose coefficients are integers in the range from 0 to $N-1$. If $A(\rho)$ and $B(\rho)$ represent the same element of $\mathbb{Z}[\rho]$ then $A(x) - B(x)$ is in the ideal generated by $P(x)$ in $\mathbb{Z}[x]$. Since the coefficients of $A(x) - B(x)$ lie between $-N+1$ and $N-1$ and the constant term of $P(x)$ is $\pm N$, it follows that $A(x) - B(x)$ must be the zero polynomial; hence $A(x)$ and $B(x)$ have the same coefficients.

We can extend the definition of radix representation to include elements of $\mathbb{Q}(\rho)$ by using negative powers of the base. We say that the element $z \in \mathbb{Q}(\rho)$ has the radix representation $z = (a_m a_{m-1} \cdots a_1 a_0 \cdot a_{-1} a_{-2} \cdots)_\rho$ if it can be written as the convergent series $\sum_{k=-\infty}^{m} a_k \rho^k$, where $0 \leqslant a_k < N$, and the digits are eventually periodic or terminating. The number $(a_m a_{m-1} \cdots a_1 a_0)_\rho$ is called the *integer part* of the representation. As in the decimal system, these representations are not necessarily unique; a few numbers even have three expansions. For example, if $\rho = (-1 + \sqrt{7}i)/2$ with minimum polynomial $x^2 + x + 2$ then $(-3 - \sqrt{7}i)/8 = (0.\overline{001})_\rho = (1.\overline{010})_\rho = (11.\overline{100})_\rho$, where a bar over a string of digits indicates that they are to be repeated indefinitely.

We shall prove the following results that completely determine the

quadratic elements that yield good bases. We will also obtain some partial results on elements of higher degree.

THEOREM 1. *Let ρ be a quadratic integer with minimum polynomial $x^2 + p_1 x + p_0$ and let $N = |p_0|$. Then ρ is the base of a full radix representation of $\mathbb{Z}[\rho]$ with digits $0, 1, 2, \ldots, N-1$ if and only if $p_0 \geqslant 2$ and $-1 \leqslant p_1 \leqslant p_0$.*

As the structure of the quadratic fields is well-known we obtain the following.

COROLLARY 2. *For each quadratic field there is a full radix representation using a base ρ whose integer parts $\mathbb{Z}[\rho]$ are precisely the algebraic integers in the field.*

The following list gives such bases of smallest norm for each quadratic field.

Field	Smallest Norm	Bases of smallest norm
$\mathbb{Q}(i)$	2	$-1 \pm i$
$\mathbb{Q}(\sqrt{3}i)$	3	$\dfrac{-3 \pm \sqrt{3}i}{2}$
$\mathbb{Q}(\sqrt{mi})$ for $-m \equiv 1 \pmod 4$	$\dfrac{m+1}{4}$	$\dfrac{\pm 1 \pm \sqrt{mi}}{2}$ for $m \geqslant 7$
$\mathbb{Q}(\sqrt{mi})$ for $-m \equiv 2, 3 \pmod 4$	m	$\pm\sqrt{mi}$ for $m \geqslant 2$
$\mathbb{Q}(\sqrt{m})$ for $m \equiv 1 \pmod 4$	$\dfrac{\alpha^2 - m}{4}$	$\dfrac{-\alpha \pm \sqrt{m}}{2}$ where $\alpha = 2\left\lfloor \dfrac{1+\sqrt{4+m}}{2} \right\rfloor + 1$
$\mathbb{Q}(\sqrt{m})$ for $m \equiv 2, 3 \pmod 4$	$\beta^2 - m$	$-\beta \pm \sqrt{m}$ where $\beta = \lfloor \sqrt{m+1} \rfloor + 1$

For the sake of completeness, we mention that the only rational integers that provide a full radix representation of $\mathbb{Z}$ are those whose minimum polynomials are of the form $x + p_0$ with $p_0 \geqslant 2$. That is, the only integral bases that will represent all the rational integers, without using a sign as prefix, are the negative integers less than or equal to -2.

3. The Clearing Algorithm

The ring $\mathbb{Z}[\rho]$ is isomorphic to the quotient ring $\mathbb{Z}[x]/(P(x))$. Given any integer polynomial, we now describe an algorithm for finding an equivalent polynomial modulo $P(x)$ whose digits lie in the range from 0 to $N-1$. Whenever this algorithm terminates it yields a radix representation for the corresponding element of $\mathbb{Z}[\rho]$.

It is useful to view polynomials in $\mathbb{Z}[x]$ as finite strings in the ring of strings introduced in [1]. The algorithm we describe will, in these terms, be a clearing algorithm for conversion to base ρ. In [1] the authors mainly concentrated on the base 2, but their work generalizes to any base ρ by changing their carry constant from $K(x)=x-2$ to our minimum polynomial $P(x)$.

The polynomial $E(x)=\sum_{k=0}^{m} e_k x^k$ will be called *clear* for the base ρ if $0 \leqslant e_k < N$ for all k. We say that the polynomial $A(x) \in \mathbb{Z}[x]$ can be *cleared* if $A(x)$ is congruent modulo $P(x)$ to a clear polynomial. We shall also say that $A(\rho)=\sum_{k=0}^{m} a_k \rho^k \in \mathbb{Z}[\rho]$ can be cleared if $\sum_{k=0}^{m} a_k x^k \in \mathbb{Z}[x]$ can be cleared. Since $\mathbb{Z}[\rho]$ is isomorphic to $\mathbb{Z}[x]/(P(x))$ this concept is well defined.

Any element of $\mathbb{Z}[\rho]$ can be written as $A(\rho)=\sum_{k=0}^{d-1} a_k \rho^k$, since the minimum polynomial of ρ has degree d. This element can be cleared if and only if there exists a polynomial $C(x) \in \mathbb{Z}[x]$ such that

$$A(x)+P(x)\,C(x)=E(x) \tag{1}$$

where $E(x)$ is clear. That is

$$a_k + p_0 c_k + p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d} = e_k \tag{2}$$

for all $k \geqslant 0$, where $0 \leqslant e_k < N$, and $c_i = 0$, if $i < 0$. Since $|p_0| = N$, the congruence

$$e_k \equiv a_k + p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d} \pmod{N}$$

defines e_k uniquely. Furthermore there is a unique integer c_k satisfying (2).

We can rewrite (2) as the nonlinear difference equation

$$p_0 c_k + p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d} = e_k \tag{3}$$

for $k \geqslant 0$ with the initial values $c_{-1}, c_{-2}, \ldots, c_{-d}$ being given by

$$\begin{pmatrix} 1 & p_{d-1} & p_{d-2} & \cdots & p_1 \\ 0 & 1 & p_{d-1} & \cdots & p_2 \\ 0 & 0 & 1 & \cdots & p_3 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} c_{-d} \\ c_{-d+1} \\ c_{-d+2} \\ \vdots \\ c_{-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{d-1} \end{pmatrix}$$

and where $0 \leqslant e_k < N$. Since the coefficient matrix has determinant 1, there is a one-to-one correspondence between the integer points $(a_0, a_1, \ldots, a_{d-1})$ and the integer initial values $(c_{-d}, c_{-d+1}, \ldots, c_{-1})$. Equation (3) can be rewritten as

$$c_k = \frac{e_k}{p_0} - \frac{(p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d})}{p_0} \tag{4}$$

$$= \begin{cases} \left\lceil \dfrac{p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d}}{-p_0} \right\rceil & \text{if } p_0 > 0 \\ \left\lfloor \dfrac{p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d}}{-p_0} \right\rfloor & \text{if } p_0 < 0 \end{cases}$$

where $\lceil x \rceil$ is the ceiling function of x (the least integer greater than or equal to x) and $\lfloor x \rfloor$ is the floor function of x (the greatest integer less then or equal to x). The nonlinear part of the difference equation (3) is the "saw-tooth function"

$$e_k = N \left\{ \frac{p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d}}{N} \right\} \tag{5}$$

where $\{x\} = x - \lfloor x \rfloor$, the fractional part of x.

The problem of whether the number ρ is a good base now becomes a question about the stability of the nonlinear difference equation (3). The algebraic integer ρ is the base for a full radix representation of $\mathbb{Z}[\rho]$ if and only if equation (3) converges to zero for all integral initial values.

4. Divergence of the Clearing Algorithm

The nonlinear part, e_k, of the difference equation (3) is bounded and we would expect the behaviour of (3) to be similar to the corresponding linear equation

$$p_0 c_k + p_1 c_{k-1} + \cdots + p_{d-1} c_{k-d+1} + c_{k-d} = 0, \tag{6}$$

at least for large values of the variables. We now use this idea to prove that whenever the linear equation (6) diverges then so does the clearing algorithm (3) and hence ρ cannot be a good base.

Proposition 3. *Let $X_k = QX_{k-1} + f(X_{k-1})$ be a real non-linear difference equation with $X_k, X_{k-1} \in \mathbb{R}^d$. If the matrix Q is diagonalizable with an eigenvalue of modulus larger than one and $f(X_{k-1})$ is bounded for*

all vectors X_{k-1}, then there exists some initial integral vector $X_0 \in \mathbb{Z}^d$ for which the solution of the difference equation is unbounded.

Proof. Let μ be the spectral radius of Q. Since Q is diagonalizable there is a consistent matrix norm $\|\cdot\|$ for which $\|Q\| = \mu$. Explicitly, change the basis of $\mathbb{C}^d$ so as to diagonalize Q and then take the row sum norm. Let M be an upper bound of $\|f(X_{k-1})\|$ for all $X_{k-1} \in \mathbb{R}^d$.

Suppose Q has a real eigenvalue λ with modulus μ. We shall show that if the initial value X_0 is large enough and sufficiently close to an eigenvector U_0 corresponding to λ then the solution X_k of the difference equation will be close to $Q^k U_0 = \lambda^k U_0$ and so will diverge. There are infinitely many initial integral vectors $X_0 \in \mathbb{Z}^d$ and eigenvectors $U_0 \in \mathbb{R}^d$ with eigenvalue λ such that $\|X_0 - U_0\| \leqslant 1$. This follows from Minkowski's Theorem in the geometry of numbers applied to the symmetric convex sets in $\mathbb{R}^{d+1}$ defined by $|x_i - x_{d+1} u_i| \leqslant h$, for $i = 1, 2, \ldots, d$, and $|x_{d+1}| \leqslant L$, where $(u_1, \ldots, u_d)^T$ is one fixed eigenvector, L is an arbitrarily large number and h is a fixed small number.

If there are no real eigenvalues with modulus μ there will be a pair of complex conjugate eigenvalues λ, $\bar{\lambda}$ of modulus μ with eigenvectors S, $\bar{S} \in \mathbb{C}^d$. Write $S = V + iW$ where $V, W \in \mathbb{R}^d$ and let $U_0 = \alpha V + \beta W \in \mathbb{R}^d$ be in the plane spanned by V and W. Then $U_0 = \gamma S + \bar{\gamma}\bar{S}$, where $\gamma = (\alpha - i\beta)/2$ and $\|U_0\| = |\gamma|$, the maximum length of the component of U_0 along the eigenvectors. Now $QU_0 = \lambda\gamma S + \bar{\lambda}\bar{\gamma}\bar{S}$ is also in the subspace spanned by V and W. Hence $\|QU_0\| = |\lambda\gamma| = \mu \|U_0\|$ and $\|Q^k U_0\| = \mu^k \|U_0\|$. As in the case of the real eigenvalues, we can find infinitely many initial integral vectors $X_0 \in \mathbb{Z}^d$ such that $\|X_0 - U_0\| \leqslant 1$ where U_0 is in the plane spanned by V and W.

The solution to the difference equation $X_k = QX_{k-1} + f(X_{k-1})$ is

$$X_k = Q^k X_0 + Q^{k-1} f(X_0) + Q^{k-2} f(X_1) + \cdots + f(X_{k-1}).$$

Now if $\|X_0 - U_0\| \leqslant 1$ then

$$\begin{aligned} \|X_k - Q^k U_0\| &\leqslant \|Q^k (X_0 - U_0)\| + \|Q^{k-1} f(X_0)\| + \cdots + \|f(X_{k-1})\| \\ &\leqslant \mu^k + \mu^{k-1} M + \cdots + M \\ &= \mu^k + M\left(\frac{\mu^k - 1}{\mu - 1}\right). \end{aligned}$$

Since $\|Q^k U_0\| = \mu^k \|U_0\|$,

$$\begin{aligned} \frac{\|X_k - Q^k U_0\|}{\|Q^k U_0\|} &\leqslant \frac{1}{\|U_0\|}\left(1 + \frac{M}{\mu - 1}\left(1 - \frac{1}{\mu_k}\right)\right) \\ &< \frac{1}{\|U_0\|}\left(1 + \frac{M}{\mu - 1}\right). \end{aligned}$$

Now choose the initial value X_0 so that $\|U_0\| > 2(1 + M/(\mu - 1))$ and then $\|X_k - Q^k U_0\| < \|Q^k U_0\|/2$ for all k. Hence $\|X_k\| \geqslant \|Q^k U_0\| - \|X_k - Q^k U_0\| > \|Q^k U_0\|/2 = \mu^k \|U_0\|/2$. Therefore $\|X_k\|$ tends to infinity as k tends to infinity and the solution is unbounded. ∎

COROLLARY 4. *If ρ or any of its conjugates have a modulus smaller than one then there are some elements of $\mathbb{Z}[\rho]$ that have no radix representation in the base ρ.*

Proof. The clearing algorithm (3) can be written in the matrix form $X_k = QX_{k-1} + f(X_{k-1})$ where $X_{k-1} = (c_{k-d}, c_{k-d+1}, \ldots, c_{k-1})^T$,

$$f\begin{pmatrix} c_{k-d} \\ c_{k-d+1} \\ \vdots \\ c_{k-2} \\ c_{k-1} \end{pmatrix} = N\left\{\frac{p_1 c_{k-1} + \cdots + c_{k-d}}{N}\right\}\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

and

$$Q = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & & & 1 \\ \dfrac{-1}{p_0} & \dfrac{-p_{d-1}}{p_0} & & \cdots & \dfrac{-p_1}{p_0} \end{pmatrix},$$

the companion matrix of the reciprocal polynomial to $P(x)$. Since $P(x)$ is irreducible with one root of modulus smaller than one, Q is diagonalizable with an eigenvalue of modulus larger than one. It follows from Proposition 3 that there are some elements of $\mathbb{Z}[\rho]$ for which the clearing algorithm is unbounded. These elements have no radix representation in base ρ with the digits lying between 0 and $N - 1$. ∎

5. CONVERGENCE OF THE CLEARING ALGORITHM

We now investigate some conditions under which the clearing algorithm is convergent. These will be sufficient to determine practically all the numbers that are good bases for quadratic fields.

PROPOSITION 5. *The clearing algorithm* (3) *converges to a nonzero*

equilibrium position for some initial values if and only if the minimum polynomial $P(x)$ satisfies $|P(1)| < N$.

Proof. The clearing algorithm (3) converges to the equilibrium position $c \in \mathbb{Z}$ if $c_k = c$ for all $k \geqslant k_0$. From (3) and (5) this happens if and only if

$$c(p_0 + p_1 + \cdots + p_{d-1} + 1) = N \left\{ \frac{c(p_1 + p_2 + \cdots + p_{d-1} + 1)}{N} \right\}.$$

Since $|p_0| = N$, this is equivalent to $cP(1)/N = \{cP(1)/N\}$. The only solution to $x = \{x\}$ is $0 \leqslant x < 1$, so c is an equilibrium position if and only if $0 \leqslant cP(1) < N$. Hence there is a nonzero equilibrium position if and only if $|P(1)| < N$. ∎

If there is a nonzero equilibrium position then either $c = 1$ or $c = -1$ is also an equilibrium position. Hence either $A(\rho)$ or $-A(\rho)$ cannot be cleared where $A(\rho) = \sum_{k=0}^{d-1} \left(\sum_{i=k+1}^{d} p_i\right) \rho^k$.

PROPOSITION 6. *If $P(x)$ has a positive real root then ρ cannot be the base for a complete radix representation of $\mathbb{Z}[\rho]$. This always happens when p_0, the constant term of the minimum polynomial, is negative.*

Proof. Let ρ_1 be a conjugate of ρ which is real and positive. Suppose -1 could be represented in the base ρ as $-1 = \sum_{k=0}^{m} a_k \rho^k$. Applying the $\mathbb{Q}$-isomorphism that takes ρ to ρ_1 we would obtain $-1 = \sum_{k=0}^{m} a_k \rho_1^k$, which is impossible since the right-hand side is positive. ∎

So far we have found conditions under which the number ρ does not yield a good base. We now give a condition under which the clearing algorithm does terminate for all initial values. The following proof is essentially a generalization of Katai and Szabo's for the Gaussian integer case given in [2].

PROPOSITION 7. *Suppose ρ has minimum polynomial $P(x)$ whose coefficients are nonnegative. If N can be represented in base ρ as $(r_m r_{m-1} \cdots r_1 0)_\rho$, where $r_m + r_{m-1} + \cdots + r_1 = N$, then ρ is the base of a full radix representation of $\mathbb{Z}[\rho]$.*

Proof. Let $R(x) = \sum_{k=1}^{m} r_k x^k$. Since $R(\rho) = N$ and $R(1) = N$ we can write $R(x) - N = P(x)\, C(x)$ for some polynomial $C(x)$ satisfying $C(1) = 0$.

Let $A(x) \in \mathbb{Z}[x]$ be any polynomial that is to be cleared. Add suitable multiples of $P(x)$ to $A(x)$ so that the coefficients are all positive. The resulting polynomial is $B(x) = A(x) + P(x)\, S(x)$, for some $S(x) \in \mathbb{Z}[x]$. Since $P(\rho) = 0$, $B(\rho) = A(\rho) \in \mathbb{Z}[\rho]$. We now clear $B(x)$ by adding suitable

positive multiples of $P(x)\,C(x)$ to it. Define the sequence of polynomials $B_k(x) \in \mathbb{Z}[x]$, for $k \geqslant 0$, by $B_0(x) = B(x)$ and

$$B_k(x) + \lfloor B_k(0)/N \rfloor\, P(x)\, C(x) = xB_{k+1}(x) + e_k, \qquad \text{for} \quad k \geqslant 0.$$

Since $P(0)\,C(0) = -N$, $0 \leqslant e_k < N$. As the other coefficients of $P(x)\,C(x)$ are nonnegative, all the coefficients of $B_{k+1}(x)$ must be nonnegative. Note that $B_k(\rho) = \rho B_{k+1}(\rho) + e_k$. Now $B_k(1) = B_{k+1}(1) + e_k \geqslant B_{k+1}(1)$; that is, the sum of the coefficients of $B_{k+1}(x)$ is less than or equal to the sum of the coefficients of $B_k(x)$. As k increases, the sequence $B_k(1)$ is a decreasing sequence of nonnegative integers and so must eventually be constant. If $B_m(1) = 0$, for some m, then $B_m(x) = 0$ and $A(\rho) = B(\rho) = (e_{m-1} e_{m-2} \cdots e_1 e_0)_\rho$ which is a clear representation in base ρ.

If $B_k(1) = B_{k+1}(1) \neq 0$, for all $k \geqslant m$, then $e_k = 0$ and so $B_k(\rho) = \rho B_{k+1}(\rho)$. Hence $B_m(\rho) = \rho^l B_{m+l}(\rho)$ for all $l \geqslant 0$. But the only element of $\mathbb{Z}[\rho]$ divisible by all powers of ρ is the zero element. Hence $B_m(\rho) = 0$ and, as before, $A(\rho) = B(\rho) = (e_{m-1} e_{m-2} \cdots e_1 e_0)_\rho$.

Therefore, if $C(1) = 0$, any element of $\mathbb{Z}[\rho]$ can be cleared and ρ is the base of a full radix representation of $\mathbb{Z}[\rho]$. ∎

Note that the digits $r_m r_{m-1} \cdots r_1$ are the carry digits for arithmetic in the base ρ. In the proof of the above proposition, elements were cleared using $P(x)\,C(x) = r_m x^m + \cdots + r_1 x - N$ but in practice it is more efficient to clear elements by just using the minimum polynomial $P(x)$.

6. Quadratic Fields

We are now in a position to prove Theorem 1 and find the bases for all the quadratic fields. Let $P(x) = x^2 + p_1 x + p_0$ be the minimum polynomial of the quadratic integer ρ. For ρ to be a good base, it follows from Proposition 6 that $p_0 = N$. Now if $p_1 < -N - 1$ or $p_1 > N + 1$, $P(x)$ has a root of modulus smaller than one and so, by Corollary 4, the clearing algorithm diverges. If $-N - 1 \leqslant p_1 < -1$, by Proposition 5, the clearing algorithm has a nonzero equilibrium state.

Since $(x-1)\,P(x) = x^3 + (p_1 - 1)\,x^2 + (N - p_1)\,x + N$, whenever $1 \leqslant p_1 \leqslant N$, the number N has the representation $(1\ p_1 - 1\ N - p_1\ 0)_\rho$ which satsifies the conditions of Proposition 7. If $p_1 = 0$, $(x^2 - 1)\,P(x) = x^4 + (N-1)\,x^2 - N$ and $N = (1\,0\,N-1\,0\,0)_\rho$ also satisfies Proposition 7. Therefore ρ is the base of a full radix representation whenever $0 \leqslant p_1 \leqslant N$. When $p_1 = N + 1$, $P(x)$ is reducible and so the only case remaining is $p_1 = -1$.

When $P(x) = x^2 - x + N$, any element of $\mathbb{Z}[\rho]$ can be written as $A = a_1\rho + a_0$ whose modulus is $|a_1\rho + a_0| = (a_0^2 + a_0a_1 + Na_1^2)^{1/2}$. Let $a_0 = kN + e_0$ where $0 \leqslant e_0 < N$. Then the first step of the clearing algorithm (2) produces the element $B = -k\rho + a_1 + k$ where $A = B\rho + e_0$ and $|B| = (a_1^2 + a_1k + Nk^2)^{1/2}$. It can be checked that $|B| < |A|$ in all cases except when $A = \rho - 1$, $-\rho - 1$ or a_0 for $-\sqrt{N} \leqslant a_0 \leqslant 0$. Therefore after a finite number of applications of the clearing algorithm we obtain

$$A = C\rho^r + e_{r-1}\rho^{r-1} + \cdots + e_1\rho + e_0$$

where $0 \leqslant e_i < N$ and $C = \rho - 1$, $-\rho - 1$ or a_0 for $-\sqrt{N} \leqslant a_0 \leqslant 0$. However, all these exceptional elements can be cleared since $\rho - 1 = (1\ 0\ N-1)_\rho$, $-\rho - 1 = (1\ 0\ N-2\ N-1)_\rho$ and $a_0 = (1\ 0\ N-1\ N+a_0)_\rho$ for $-\sqrt{N} \leqslant a_0 \leqslant -1$.

Therefore the clearing algorithm always terminates when $P(x) = x^2 - x + N$. This completes the proof of Theorem 1.

7. Conjectures for Other Bases

Most of our results give some information on bases for number fields of degree three and higher. We conjecture that the cubic integer ρ is the base for a full radix representation of $\mathbb{Z}[\rho]$ if and only if its minimum polynomial $x^3 + p_2x^2 + p_1x + p_0$ satisfies (i) $p_0 = N \geqslant 2$, (ii) $p_2 \geqslant 0$, (iii) $p_1 + p_2 \geqslant -1$, (iv) $p_1 - p_2 \leqslant N - 2$ and (v) $p_2 \leqslant N - 2$ (if $p_1 \leqslant 0$) or $p_2 \leqslant N - 1$ (if $1 \leqslant p_1 \leqslant N - 1$) or $p_2 \leqslant N$ (if $p_1 \geqslant N$). These are the only cubics satisfying Corollary 4 and Propositions 5 and 6 and for which N and $-N$ are representable. The clearing algorithm applied to N using any other cubic diverges or eventually cycles with a period ranging from 1 to 13.

It is also possible to consider nonintegral algebraic numbers as bases. Suppose ρ has a minimum polynomial $p_dx^d + \cdots + p_1x + p_0 \in \mathbb{Z}[x]$ where $GCD(p_d,\ldots,p_1,p_0) = 1$. Then the results of Corollary 4 and Propositions 5, 6 and 7 still hold with $N = |p_0|$.

The only rational numbers which are good bases are those of the form $-p_0/p_1$ where $-p_0/p_1 < -1$. All rational numbers of the form $\mathbb{Z}[1/p_1]$ can be represented in the base $-p_0/p_1$ using digits $0, 1,\ldots, |p_0| - 1$. This follows from Corollary 4 and Propositions 6 and 7 (cf. the solution to Problem E2604 in the *American Mathematical Monthly* **84** (1977), p. 821, which was essentially to calculate the length of the base 3/2 expansion of the even positive integers.)

We conjecture that the non-integral quadratic bases that yield a full radix representation must have minimum polynomial $p_2x^2 + p_1x + p_0 \in \mathbb{Z}[x]$ where (i) $p_0/p_2 > 1$ and (ii) $-1 \leqslant p_1/p_2 < (p_0/p_2) + 1$.

REFERENCES

1. F. FALTIN, N. METROPOLIS, B. ROSS, AND G.-C. ROTA, The real numbers as a wreath product, *Adv. in Math.* **16** (1975), 278–304.
2. I. KATAI AND J. SZABO, Canonical number systems for complex integers, *Acta Sci. Math. (Szeged)* **37** (1975), 255–260.
3. D. E. KNUTH, "The Art of Computer Programming," Vol. 2, "Seminumerical Algorithms," Addison–Wesley, Reading, Mass., 1969.