Can. Math. Bull. Vol. **39** (1), 1996 pp. 47–54

THE DIVISION ALGORITHM IN COMPLEX BASES

WILLIAM J. GILBERT

ABSTRACT. Complex numbers can be represented in positional notation using certain Gaussian integers as bases and digit sets. We describe a long division algorithm to divide one Gaussian integer by another, so that the quotient is a periodic expansion in such a complex base. To divide by the Gaussian integer w in the complex base b, using a digit set D, the remainder must be in the set $wT(b,D) \cap \mathbb{Z}[i]$, where $T(b,D)$ is the set of complex numbers with zero integer part in the base. The set $T(b,D)$ tiles the plane, and can be described geometrically as the attractor of an iterated function system of linear maps. It usually has a fractal boundary. The remainder set can be determined algebraically from the cycles in a certain directed graph.

1. **Complex bases.** A Gaussian integer b, together with a digit set D, of Gaussian integers containing zero, is called a *valid base for the complex numbers* if every Gaussian integer, z, can be represented uniquely in the form

$$z = \sum_{j=0}^{s} a_j b^j, \quad \text{where } a_j \in D.$$

Such a representation will be denoted by $z = (a_s a_{s-1} \cdots a_1 a_0)_b$ and the valid base will be denoted by (b, D). It can be shown, using arguments similar to [6, Theorem 2] or [8, Theorem 10], that every complex number $z \in \mathbb{C}$ has an infinite radix expansion in the valid base (b, D) of the form

$$z = \sum_{j=-\infty}^{s} a_j b^j, \quad \text{where } a_j \in D.$$

This will be denoted by $z = (a_s a_{s-1} \cdots a_1 a_0 . a_{-1} a_{-2} \cdots)_b$. As in the standard bases, these infinite expansions are not necessarily unique. The digits to the left of the radix point, $(a_s a_{s-1} \cdots a_1 a_0)_b$, constitute the *integer part* of the representation.

Knuth [7, Section 4.1] describes many positional number systems, including the binary expansion of the complex numbers in the base $-1+i$ using the digits 0 and 1. For example, in this base, $(-2-i)/2$ can be written as $(110.01)_{-1+i}$. If (b, D) is a valid base, then the digit set D must be a complete residue system modulo b, and the number of digits must be $b\bar{b} = \text{Norm}(b)$ [2]. The most obvious generalizations from the real bases to the complex bases occur if we choose the digit set to be the set of natural numbers $\{0, 1, 2, \ldots, \text{Norm}(b) - 1\}$. In this case, Kátai and Szabó [6] show that the only valid bases for the complex numbers are $-n \pm i$, where n is a positive integer, and the digit

Received by the editors June 24, 1994; revised March 2, 1995.
AMS subject classification: 11A63, 58F08.

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

set is $\{0, 1, 2, \ldots, n^2\}$. However if the digits are allowed to be complex, there are many valid bases.

Each complex base (b, D), gives rise to a tile

$$T(b,D) = \{(0.a_1a_2\cdots)_b \mid a_i \in D\} \subset \mathbb{C}$$

consisting of the complex numbers expressible in the base with zero integer part. If the base is valid, then $T(b,D)$ is a closed set with unit area that tiles the plane by translations using the group $\mathbb{Z}[i]$. The translate of $T(b,D)$ by a Gaussian integer z consists of those complex numbers with integer part z. For example, $T(-1+i, \{0, 1\})$, shown in Figure 1(a), is the space-filling twin dragon curve [7, Section 4.1]. The boundary of the tiles $T(-n+i, \{0, 1, 2, \ldots, n^2\})$ are all fractal curves. Points on the boundary of $T(b,D)$ also lie on the boundary of two (or more) translated regions and correspond to complex numbers with two (or more) expansions in the base (b,D) with different integer parts [3].

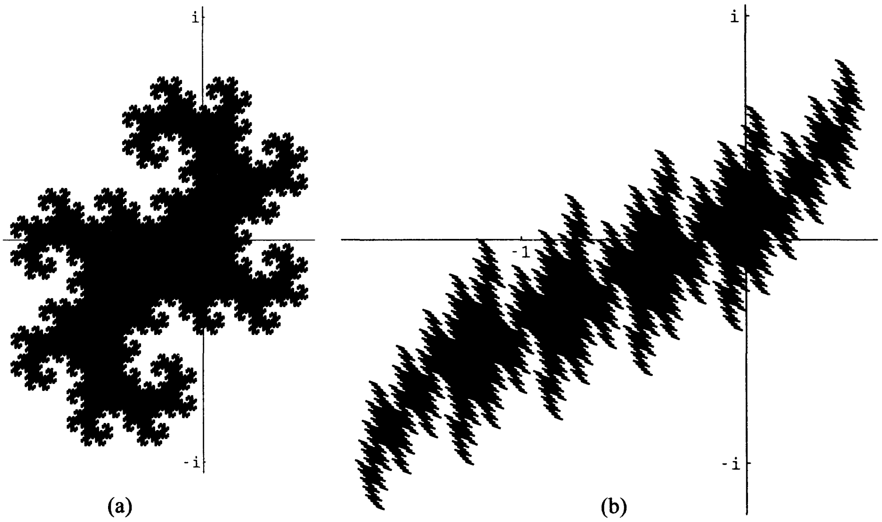

FIGURE 1: The tiles (a) $T(-1+i, \{0, 1\})$ and
(b) $T(-2+i, \{0, 1, 2, 3, 4\})$ lie in the complex plane and have unit area with fractal boundaries.

2. **Iterated function systems.** The tile $T(b,D)$ can also be viewed as the attractor of an iterated function system, where the number of functions is the number of digits in the base. For each digit $a \in D$ in the base (b,D), define the function $f_a\colon \mathbb{C} \longrightarrow \mathbb{C}$ by $f_a(z) = (z+a)/b$. These are linear contraction maps and, if $z = (0.a_1a_2\cdots)_b \in T(b,D)$, then $f_a(0.a_1a_2\cdots)_b = (0.aa_1a_2\cdots)_b \in T(b,D)$. Hence

$$T(b,D) = \bigcup_{a \in D} f_a\big(T(b,D)\big)$$

and $T(b,D)$ is the unique invariant (or attractor) set determined by Hutchinson's Theorem [5] applied to the set of functions $\{f_a \mid a \in D\}$. Moreover, the set $T(b,D)$ is self-similar

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

with respect to these functions. The set $\{f_a \mid a \in D\}$ forms an iterated function system as defined in [1, Section 3.7].

Each function f_a maps $T(b,D)$ into itself. Moreover, for each $z \in T(b,D)$ there exists $a \in D$ such that $f_a^{-1}(z) \in T(b,D)$. If $z = (0.a_1a_2a_3\cdots)_b$, then $f_{a_1}^{-1}(z) = (0.a_2a_3\cdots)_b$ is the Bernoulli shift on the sequence of digits to the right of the radix point. Therefore, for any $z \in T(b,D)$, there exists an infinite sequence $a_1, a_2, \ldots$ of elements of D such that

$$f_{a_j}^{-1} \circ \cdots \circ f_{a_2}^{-1} \circ f_{a_1}^{-1}(z) \in T(b,D)$$

for all j. This idea will be used in the Escape Time Algorithm in the next section. The elements of the sequence $a_1, a_2, \ldots$ are precisely the digits in a base (b,D) expansion of z.

3. **The long division algorithm.**

In [4], we showed how to add, subtract, and multiply numbers in complex bases. We also gave examples of division, but gave no general division algorithm.

The only problem in generalizing the usual long division algorithm to complex bases is to determine what the remainders should be when a Gaussian integer v is divided by the Gaussian integer w. We now show that the long division algorithm will remain bounded if and only if the remainders all lie in the set $wT(b,D) \cap \mathbb{Z}[i]$, that we call the *remainder set* and denote by $\mathrm{RemSet}(b,D,w)$.

LONG DIVISION ALGORITHM. *Let (b,D) be a valid base for the complex numbers. If v and $w \neq 0$ are Gaussian integers, then there exists a Gaussian integer A and digits $a_j \in D$ such that*

$$\begin{aligned} v &= Aw + r_0 \\ br_0 &= a_1w + r_1 \\ br_1 &= a_2w + r_2 \\ &\vdots \end{aligned}$$

where each remainder $r_j \in \mathrm{RemSet}(b,D,w) = wT(b,D) \cap \mathbb{Z}[i]$.

There may be choices in the algorithm, but for each choice,

$$\frac{v}{w} = A + (0.a_1a_2\cdots)_b.$$

The integer part A can be expanded in the base (b,D) and therefore each choice yields a base (b,D) expansion of v/w. Moreover every such expansion can be obtained in this way.

PROOF. Since $T(b,D)$ tiles the complex plane using translations from $\mathbb{Z}[i]$, the magnified set $wT(b,D)$ will tile the plane using translations from $w\mathbb{Z}[i]$. Hence, for any $v \in \mathbb{Z}[i]$, there exists $A \in \mathbb{Z}[i]$ such that $v = Aw + r_0$, where $r_0 \in wT(b,D)$. Since v, A and w are Gaussian integers, $r_0 \in wT(b,D) \cap \mathbb{Z}[i]$.

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

To prove the long division algorithm, we shall convert the problem to one involving iterated function systems. The tile $T(b,D)$ is the attractor of the iterated function system $\{f_a \mid a \in D\}$ where $f_a(z) = (z+a)/b$. Consider the conjugate iterated function system obtained by multiplication by w. The conjugate function to f_a is $g_a \colon \mathbb{C} \longrightarrow \mathbb{C}$ where

$$g_a(z) = wf_a(w^{-1}z) = \frac{z+aw}{b}.$$

The magnified set $wT(b,D)$ must be the attractor for the iterated function system $\{g_a \mid a \in D\}$. Each function g_a has an inverse $g_a^{-1} \colon \mathbb{C} \longrightarrow \mathbb{C}$, which is the expansion map defined by $g_a^{-1}(z) = bz - aw$. The general term in the division algorithm is $br_{j-1} = a_jw + r_j$, which is equivalent to

$$r_j = br_{j-1} - a_jw = g_{a_j}^{-1}(r_{j-1}).$$

Hence the division algorithm can be viewed as a dynamical system that starts with the remainder r_0 and produces the system of remainders $r_1, r_2, \ldots$ corresponding to a choice of digits $a_1, a_2, \ldots$, where $r_j = g_{a_j}^{-1}(r_{j-1})$.

By the Escape Time Algorithm in [1, Section 7.1], or the repelling method in [9], there exists a sequence of maps $g_{a_1}^{-1}, g_{a_2}^{-1}, \ldots$, such that the successive terms $r_1, r_2, \ldots$ remain bounded if and only if the initial term r_0 is in the attractor $wT(b,D)$. Moreover, if the sequence of remainders does remain bounded, then all the complex numbers r_j lie in $wT(b,D)$. If a remainder r_j were to lie outside $wT(b,D)$ then $r_{j+s} \longrightarrow \infty$ and $r_{j+s}b^{-j-s} \not\longrightarrow 0$ as $s \longrightarrow \infty$. Since r_0 was constructed to lie in $wT(b,D)$, there exists digits $a_1, a_2, \ldots$ satisfying the long division algorithm with each remainder $r_j \in wT(b,D) \cap \mathbb{Z}[i]$.

For any choice of the digits $a_1, a_2, \ldots$ for which the remainders are bounded

$$\begin{aligned}\frac{v}{w} &= A + \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots + \frac{a_s}{b^s} + \frac{r_s}{wb^s} \\ &= A + (0.a_1a_2\cdots a_s)_b + \frac{r_s}{wb^s} \longrightarrow A + (0.a_1a_2\cdots)_b \quad \text{as } s \longrightarrow \infty.\end{aligned}$$

Furthermore any base b expansion of v/w yields a sequence of bounded remainders and therefore can be obtained in this way. ∎

We show in the next section that the remainder set, $\mathrm{RemSet}(b,D,w)$, is a finite set of Gaussian integers, and so the remainders $r_0, r_1, r_2, \ldots$ must eventually repeat. This implies, as in real bases, that the Long Division Algorithm will eventually be periodic, or will terminate with zero remainder.

4. **The remainder set algorithm.** As the boundary of the tile $T(b,D)$ is usually a fractal, the set $wT(b,D) \cap \mathbb{Z}[i]$ could be difficult to calculate directly. You cannot determine geometrically which integers lie on the fractal boundary. We therefore give an algebraic algorithm for determining the remainder set for division by w in the base b. This Remainder Set Algorithm uses a directed graph on the Gaussian integers, derived from the maps of an iterated function system. The remainder set will be the Gaussian integers in the cycles in this graph.

We first show how to find the remainder set when w and b are coprime. We shall use the functions $g_a \colon \mathbb{C} \longrightarrow \mathbb{C}$ defined by $g_a(z) = (z+aw)/b$, but restrict them to the Gaussian integers.

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

THEOREM. *If w and b are coprime Gaussian integers, define the function $g\colon \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$ by*

$$g(z) = g_a(z) = \frac{z + aw}{b}$$

where a depends on z and is chosen so that $z+aw \equiv 0 \pmod{b}$. Then z is in the remainder set $\mathrm{RemSet}(b, D, w)$ *if and only if $g^p(z) = z$ for some positive integer p.*

PROOF. Let z be a Gaussian integer. The set of digits, D, forms a complete residue system modulo the base b. Since w and b are coprime integers, $\{aw \mid a \in D\}$ and $\{z + aw \mid a \in D\}$ also form complete residue systems modulo b. Hence there exists a unique digit $a \in D$ with $z + aw \equiv 0 \pmod{b}$. Therefore, for each Gaussian integer z, $g(z) = g_a(z)$ is well defined and is also a Gaussian integer.

The map g is a contraction, when the modulus of z is large. Let M be the largest modulus of the digits in D and let $R = M|w|/(|b| - 1)$. Then, under iterations of g, the orbit of every Gaussian integer z must end up inside the circle of radius R, since

$$|g(z)| = \left|\frac{z + aw}{b}\right| \leq \frac{|z| + M|w|}{|b|} < |z|, \quad \text{whenever } |z| > R.$$

Since there are only a finite number of Gaussian integers with modulus less that R, the orbit of every Gaussian integer z must eventually cycle (or end up at a fixed point).

It follows from the Long Division Algorithm that r_0 is in the remainder set $\mathrm{RemSet}(b, D, w)$ if and only if there exists an infinite sequence of digits $a_1, a_2, \ldots$ from D, and Gaussian integers $r_1, r_2, \ldots,$ such that $r_j = g_{a_j}^{-1}(r_{j-1})$. We can write $r_{j-1} = g(r_j)$, since a_j is the unique digit with $g_{a_j}(r_j) \in \mathbb{Z}[i]$. Hence $\ldots, r_2, r_1, r_0$ is part of an orbit under iterations of g, and $r_j = g^k(r_{j+k})$ for all positive k. Therefore each Gaussian integer r_j has modulus less than R, and two of the remainders must be the same. This implies that r_0 must lie in a cycle; that is, there exists an integer p such that $r_0 = g^p(r_0)$. Conversely if r_0 lies in a cycle then it lies in the remainder set. ■

The function g determines an infinite directed graph whose vertices are the Gaussian integers. Each vertex has exactly one edge departing from it and $\mathrm{Norm}(b)$ edges entering it. The vertices lying in the cycles form the remainder set $\mathrm{RemSet}(b, D, w)$. These cycles can be found as follows.

REMAINDER SET ALGORITHM. *The remainder set* $\mathrm{RemSet}(b, D, w)$*, for division by w in the base (b, D), can be computed as follows, whenever w and b are coprime Gaussian integers. Systematically look at all the Gaussian integers, z, with modulus less than $R = M|w|/(|b| - 1)$, where M is the largest modulus of the digits in D. If it is not known whether z lies in the remainder set, calculate the iterates under the function g defined in the previous theorem, i.e. z, $g(z)$, $g^2(z)$, $g^3(z) \cdots$, until they cycle. If they start cycling at $g^h(z)$ with $g^h(z) = g^{h+p}(z)$, then $g^h(z)$, $g^{h+1}(z), \ldots, g^{h+p-1}(z)$ all lie in the remainder set, and z, $g(z), \ldots, g^{h-1}(z)$ do not.*

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

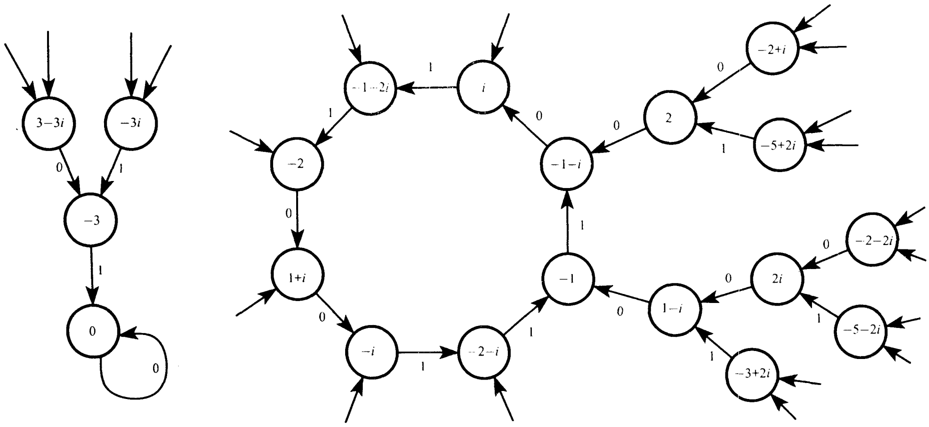

FIGURE 2: The directed graph for division by 3 in the base $(-1+i, \{0,1\})$.

For example, Figure 2 shows part of the graph determined by division by 3 in the base $-1+i$ with digit set $D = \{0,1\}$. Each edge $z \longrightarrow g(z)$ is labeled by the digit $a \in D$, where $z + aw \equiv 0 \pmod{b}$, so that $g(z) = g_a(z)$. The graph contains two cycles, an 8-cycle, and the origin as a fixed point. Hence the remainder set for division by 3 in the base $(-1+i, \{0,1\})$ is $\{0, -1, -2, i, -i, 1+i, -1-i, -2-i, -1-2i\}$. This remainder set can be used to show, for example, that $2i/3 = (11.\overline{00110111})_{-1+i}$, where the bar over a sequence of digits indicates that the sequence is to be repeated indefinitely.

If w and b are not coprime, we can write $v/w = vu/w_1b^k$, where w_1 and b are coprime, and apply the Division Algorithm to vu/w_1.

It is also possible to construct a more complicated directed graph on the Gaussian integers to determine the remainder set when w and b are not coprime. For each digit $a \in D$ define $g_a^{-1}\colon \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$ by $g_a^{-1}(z) = bz - aw$. This defines an infinite directed graph on the Gaussian integers. There are Norm(b) edges leaving each vertex v, corresponding to each digit $a \in D$, and they point to the vertices $g_a^{-1}(v)$. The remainder set for division by w in the base b consists of the periodic vertices lying in the cycles in this graph, plus any pre-periodic vertices, lying in a path that eventually cycles.

Figure 3 shows some examples of remainder sets, when w and b are coprime, that were computed using the Remainder Set Algorithm. Compare Figure 3 with Figure 1. The remainder sets consist of the Gaussian integers lying in the magnified set $wT(b,D)$, or equivalently, the Gaussian integers z for which z/w lies in $T(b,D)$.

Since the tile $T(b,D)$ has unit area, the region $wT(b,D)$ has area Norm(w). If the remainder set, RemSet(b,D,w) contains exactly Norm(w) members, then the set will be a complete residue system modulo w and there will be no choice in the Long Division Algorithm. However, if the remainder set contains more than Norm(w) elements, then there will sometimes be a choice for division by w in the base b. In this case, some of the elements of the remainder set must lie on the boundary of $wT(b,D)$. Each boundary

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press

element must be congruent modulo w to some other boundary element, since $wT(b, D)$ tiles the plane by translations in $w\mathbb{Z}[i]$.

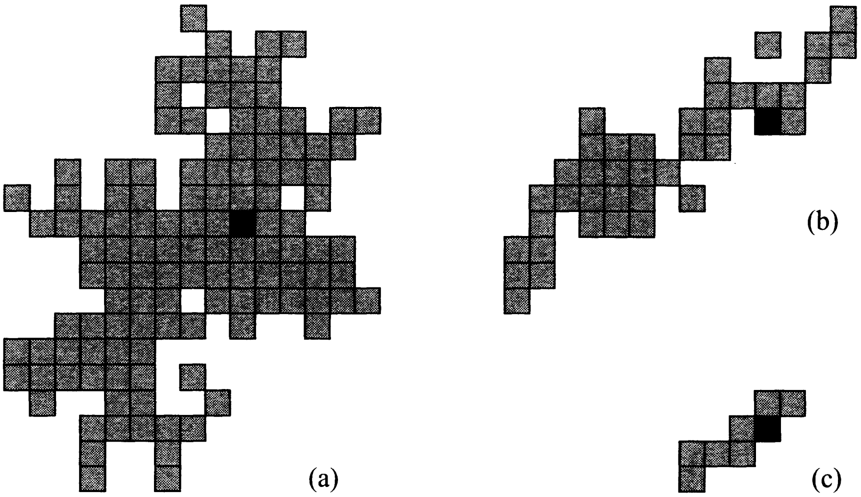

FIGURE 3: The remainder sets for (a) division by 11 in the base $(-1+i, \{0,1\})$, (b) division by 6 in the base $(-2+i, \{0,1,2,3,4\})$ and (c) division by 2 in the base $(-2+i, \{0,1,2,3,4\})$. Each small square represents one Gaussian integer. The black square is the origin.

The remainder set for division by 3 in the base $(-1+i, \{0,1\})$, computed in Figure 2, contains 9 elements and, as $\mathrm{Norm}(3) = 9$, there will be no choice in the division algorithm. Since the remainder set in Figure 3(a) has 121 elements, division by 11 in the base $(-1+i, \{0,1\})$ will also yield a unique expansion. Furthermore, this remainder set will tile the Gaussian integers by translations by elements of $11\mathbb{Z}[i]$.

The remainder sets in Figure 3(b) and 3(c) however, contain 40 and 8 elements respectively, which is more than $\mathrm{Norm}(6) = 36$ and $\mathrm{Norm}(2) = 4$. Hence sometimes there will be choices in the division algorithm for division by 6 or 2 in the base $(-2+i, \{0,1,2,3,4\})$.

Figure 3(c) can be used to show that $(1+i)/2$ has three expansions in the base $(-2+i, \{0,1,2,3,4\})$, namely $(0.\overline{041})_{-2+i}$, $(13.\overline{104})_{-2+i}$, and $(14.\overline{410})_{-2+i}$.

The analogous Long Division Algorithm holds when the base and all the digits are ordinary integers, with the norm in the real numbers being the absolute value. Matula [8] describes some unusual integer digit sets that give representations of all the real numbers. Matula gives an example of a rational number, $5\frac{3}{4}$, with three different representations in a base. The Division Algorithm and the Remainder Set Algorithm show that there are actually five representations of $5\frac{3}{4}$ in the base $(5, \{0,1,7,23,-1\})$, namely $\left(11.\overline{(-1)}\right)_5$, $\left(1(-1).\bar{7}\right)_5$, $\left(0.\overline{(23)}\right)_5$, $\left(10.\overline{(-1)(23)}\right)_5$, and $\left(1.\overline{(23)(-1)}\right)_5$. Matula lists the first three of these expansions.

References

1. M. F. Barnsley, *Fractals everywhere*, 2nd ed., Academic Press, New York, 1993.

2. W. J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl. **83**(1981), 264–274.

3. ———, *Complex numbers with three radix expansions*, Canad. J. Math. **34**(1982), 1335–1348.

4. ———, *Arithmetic in complex bases*, Math. Mag. **57**(1984), 77–81.

5. J. E. Hutchinson, *Fractals and self similarity*, Indiana Univ. Math. J. **30**(1981), 713–747.

6. I. Káiti and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged) **37**(1975), 255–260.

7. D. E. Knuth, *The art of computer programming, Vol. 2, Seminumerical algorithms*, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1981.

8. D. W. Matula, *Basic digit sets for radix representation*, J. Assoc. Comput. Mach. **29**(1982), 1131–1143.

9. P. Prusinkiewicz and G. Sandness, *Koch curves as attractors and repellers*, IEEE Comput. Graphics Appl. (6) **8**(1988), 26–40.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
N2L 3G1
e-mail: wgilbert@uwaterloo.ca

https://doi.org/10.4153/CMB-1996-006-1 Published online by Cambridge University Press