Annales Univ. Sci. Budapest., Sect. Comp. 55 (2023) 49–75

BASE N EXPRESSIBLE NUMBERS

Gary Michalek (Philadelphia, USA)

Communicated by Jean-Marie De Koninck

(Received December 6, 2022; accepted January 2, 2023)

Abstract. We present a new proof that the set of numbers expressible in base N with coefficients in a set A is a group, in the case where N is a real integer and A is a set of representatives of the congruence classes modulo N. We present results for the case where N is a Gaussian integer with a conjecture that the set of expressible numbers is a group in that situation as well.

1. Statement of main theorem

Most of this material applies equally to the integers $\mathbb{Z}$ and the Gaussian integers $\mathbb{Z}[i]$, the set of all complex numbers $a+bi$ with a and b in $\mathbb{Z}$. In cases where something is valid for both settings, both sets will be referred to as G. The word *integer* will mean either real integer or Gaussian integer when both cases are considered. If we are referring to only one case, we use the terms *real integer* and *complex integer*. In assertions where there are differences among the two cases, this will always be pointed out. The paper ends with a summary of the main results and conjectures.

Let the set A consist of one representative from each of the congruence classes modulo N, where the base N is an integer of modulus or absolute value greater than 1. The size of A is $|N|$ in the real case and $||N||^2$ in the complex case. (The canonical choice for members of A in the complex case are the complex integers in the parallelogram defined by the vectors N and Ni, though here we consider all possible A.) We call (A,N) a *system*.

Key words and phrases: Number systems, just touching covering systems.
2010 Mathematics Subject Classification: 11A67.

https://doi.org/10.71352/ac.55.049

Let B be the set A–A, that is, the set of all a - a' where a and a' are in A. We call an integer *expressible* if it can be written in the form $\sum_{j=0}^{k} b_j N^j$ where k in $\mathbb{Z}$ is nonnegative, and where each b_j is in B. Let E denote the set of all expressible integers.

Theorem 1.1. *E is a group under addition.*

This theorem will be proven in Section 5 of the paper for G = $\mathbb{Z}$. For G = $\mathbb{Z}$[i], the theorem is only conjectured to be true but will be proven under certain conditions to be explained later. Obviously 0 is a member of E, and if x is in E than so is –x, since the set B = -B. To establish Theorem 1.1, we need only show that E is closed under addition, and this is the main result proven in this paper, for $\mathbb{Z}$ in general and for $\mathbb{Z}$[i] under certain conditions. Much of the forthcoming proof applies to both cases equally. The one important difference, that necessitates special conditions for $\mathbb{Z}$[i], comes at the very end of the proof of Lemma 4.1 in Section 4.

This theorem was conjectured in the real setting for N = 3 by Imre Kátai [1]. The basic set up of number systems and of the maps we shall shortly discuss are included there. Other consequences of the theorem appear in papers by Indlekofer, Kátai, and Racskó [2], [3]. The case for N=3 was proven by the author in 1997 [4]. A proof applicable to any real integer N of absolute value greater than 1 was published in 2001 by the author [5]. The proof presented here is a substantial improvement on the proof in [5], being much more illuminating, and with some additional conjectures and results for the $\mathbb{Z}$[i] case.

An important note on A: Given the original choice of A, we may replace A by the set A-x, where x is in G. This does not change the set B or the set E. In particular we can choose x to be in A itself so that 0 is in A-x, and A-x is a subset of B. *We will always assume this replacement has been done so a system (A,N) will always have 0 as a member of A and A as a subset of B.* Consider the example of N = 3, $A_1 = \{1, -1, 3\}$ and $A_2 = \{0, -2, 2\}$. Since $A_2 = A_1 - 1$, the set B is the same for both A_1 and A_2. In fact, $B = \{0, -2, 2, -4, 4\}$ and E is obviously the set of all multiples of 2. Notice $2 = \gcd(B) = \gcd(A_2)$ but 2 is not $\gcd(A_1)$, which is why we would prefer (A_2,3) as the underlying system, as the gcd(B) is important in what follows in the real case.

If Theorem 1.1 is established, the group E can be described as follows in the next theorem:

Theorem 1.2. *Assume E is a group under addition. Then E is the smallest additive subgroup of G that contains B and that is closed under multiplication by N. We may also say E is the smallest additive subgroup of G containing A that is closed under multiplication by N.*

Note: In the real case, there is a much simpler way to describe this group as seen in the next corollary. However, the description given is the one that holds in the $\mathbb{Z}$[i] case as well, again assuming E is a group.

Proof. E is assumed to be an additive subgroup of G. Since E is the set of all integers of the form $\sum_{j=0}^{k} b_j N^j$ where k≥0, and where each b_j is in B, E obviously contains B. It is also obvious that E is closed under multiplication by N. Any other subgroup of G with these properties would also contain E. ■

Of special interest is the case where E is the entire set G, in which case (A,N) is called a *Just Touching Covering System*. This term reflects a connection with fractal geometry (explained in [1], [2], and [3]). This was the result of [5] which follows from Theorems 1.1 and 1.2:

Corollary 1.1. *In the case where G = $\mathbb{Z}$, the set E consists of all multiples of gcd(B), which is the same as gcd(A). In particular, (A,N) is a Just Touching Covering System iff gcd(B) = 1.*

Proof. Obviously the smallest additive subgoup of $\mathbb{Z}$ containing B consists of all multiples of gcd(B). The property that that set of multiples is closed under multiplication by N is automatically satisfied. ■

The property of closure under multiplication by N is only essential in the conjecture for the complex case $\mathbb{Z}$[i]. In that case, the smallest additive group containing B may not be closed under multiplication by N, and therefore may not be E which *is* closed under multiplication by N.

A nonzero additive subgroup of $\mathbb{Z}$[i] is a lattice. It is either a one-dimensional lattice <x> consisting of all *real* integer multiples of some nonzero Gaussian integer x, or it is a two-dimensional lattice <x,y> consisting of all $ax+by$ where a and b are *real* integers, and x and y are Gaussian integers that are linearly independent when viewed as vectors in $\mathbb{R}^2$. In this situation x may be chosen as a member of the lattice of minimal modulus. Then y can be chosen as a nonzero member of the lattice that is not a real multiple of x and which is of minimal modulus among all such.

The set E can be shown to be a *two-dimensional* lattice in $\mathbb{Z}$[i] *if it is in fact a group*. To see this, consider first the case where N = $c+di$ with d nonzero. In this case it is easy to find two nonzero expressible numbers that are independent as vectors in $\mathbb{R}^2$: consider any nonzero a in A and its multiple Na for one example. In the case where d is 0, it is again impossible for E to be a one-dimensional lattice <x> because then E would not contain A. This is because Nx ≡ 0 modulo N, so <x> , the set of all *real* integral multiples of x, contains representatives of at most |N| congruence classes modulo N, whereas A has representatives of all $||N||^2 = N^2$ classes in the complex integer setting.

The structure of E in the $\mathbb{Z}$[i] setting is discussed more fully in Section 6 of the paper.

2. Maps and trees

We now examine the tree of an integer x and properties of such trees when integers are added and subtracted. An illustration is provided at the end of this section.

Given an integer x, we form its B-tree as follows. In this tree, a number x is connected by arrows to |A| descendants. These descendants are computed using the maps F_a where a is a member of A. That is, x connects to $F_a(x) = (x\text{-}a+a')/N$, where a' is the unique member of A so that the division results in an integer. The |A| descendants are obtained by letting a range over A. If these descendants are added together, the various a and a' both range over all members of A and therefore their sums cancel. The sum of the descendants in the real case where A has |N| members is then $|N|\cdot x/N$, which is x or -x depending on whether N is positive or negative. In the complex case where A has $||N||^2$ members, the sum is $||N||^2\cdot x/N = \bar{N}\cdot x$.

In considering the B-tree of x, we define generation-0 to be the number x itself, generation-1 to be the |A| numbers obtained by applying the maps described above, generation-2 to be the $|A|^2$ numbers obtained by following the |A| branches off the generation-1 members, and so on. Generation-k consists of $|A|^k$ numbers (not necessarily distinct).

For any positive integer k, define A^k to be the set of representatives of the congruence classes modulo N^k consisting of the $|A|^k$ sums $\sum_{j=0}^{k-1} a_j N^j$ where each a_j is a member of A. Note that these sums are in fact from distinct congruence classes. (If $\sum_{j=0}^{k-1} a_j N^j = \sum_{j=0}^{k-1} a_j' N^j$ modulo N^k, then it easily follows that $a_j = a_j'$ for all j.)

Given a member z of A^k for any positive integer k, we define the map F_z by $F_z(x) = (x\text{-}z+z')/N^k$, where z' is the unique member of A^k so that the division results in an integer. It is easy to see that the generation-k members of the B-tree of x are given precisely by the $F_z(x)$ as z ranges over A^k. In the real case, the sum of the numbers in generation-k is then x if N is positive and $(-1)^k x$ if N is negative. In the complex case the sum is $\bar{N}^k x$. Also note that, for $z = \sum_{j=0}^{k-1} a_j N^j$, in addition to $F_z(x)$ being a member in generation-k of the B-tree of x, the map F_z describes *a specific path* through the B-tree to that descendant, namely the composition of single generation maps F_{a_0} followed by F_{a_1}, and so on up to $F_{a_{k-1}}$. For shorthand we can refer to "the z-path" through the tree of x. An example is in the illustration at the end of this section. Since all the members of A^k have a unique expansion in the form $z = \sum_{j=0}^{k-1} a_j N^j$,

the z-path is unambiguous. However, the A^k that we are considering z to be a member of does need to be specified. In the illustration that follows, where N=3 and A = {0, 25, 5}, the number z =25 is both a member of A and of A^2, in which it has the form $25+0\cdot3^1$. Considering 25 as a member of A means the map and path we are considering is from x to its first generation, given by $F_{25}(x) = (x-25+a)/3$ for some a in A. However, when considering 25 to be in A^2, the map and path is from x to a member of its second generation, namely $F_{25}(x) = (x-25+z')/9$ where z' is in A^2. Since $25 = 25+0\cdot3^1$, the 25-path in this case is in two steps and first connects x to $y = (x-25+a)/3$ and then connects y to $(y-0+a')/3$ in the second generation. Here $z' = a+a'\cdot3^1$.

The main point of trees as regards E is that, if x is expressible, then $x = z_1-z_2$ for some z_1 and z_2 in A^k for some k, so that $F_{z_1}(x) = (x-z_1+z_2)/N^k = 0$. Therefore there is a zero in generation-k of the tree of x specifically located by following the z_1-path through the tree. Conversely the appearance of 0 in the tree of x shows that x is expressible, with the path to that 0 specifying the map and hence the expression.

2.1. The interval I

It is a simple matter of checking the inequalities to show that for any integers x and m, if $|x|>|m|/(|N|-1)$ then $|(x-m)/N|<|x|$. Also, if $|x|\leq|m|/(|N|-1)$ then $|(x-m)/N|\leq|m|/(|N|-1)$ as well. In particular this applies to the case where m is in B, as in the F_a maps above where $F_a(x)$ is of the form (x-m)/N. Let M be the absolute value of the largest member of B divided by |N|-1. Then from the inequalities, if $|x|>M$ then $|F_a(x)|<|x|$ and if $|x|\leq M$ then $|F_a(x)|\leq M$ too. (In the complex case this is still true, using modulus instead of absolute value.) Define I to be the disk of radius M about 0 in the complex case, or the interval [-M,M] in the real case. (Actually we can say I consists just of the integers inside the interval or disk.) By the inequalities above, repeated applications of maps of the form F_a with a in A give a sequence of descendants of x which decrease in modulus until the result is inside I. Further descendants of members of I all lie inside I. We will call I the "interval for B", though technically in the complex case it is a disk not an interval.

Notice it is possible to determine whether *all* integers are expressible by simply checking whether all the integers in I are expressible, since the tree of every x has a generation all of whose members belong to I.

2.2. Adding and subtracting trees

If w = x + y, for integers x, y, and w, the paths in the tree of x add to the paths in the tree of y to produce paths in the tree of w. Specifically, with any z in A^k and $F_z(x)$ describing the z-path in the tree of x, there will be a path given by $F_{z'}(y)$ where z' is also in A^k so that adding the descendants of x

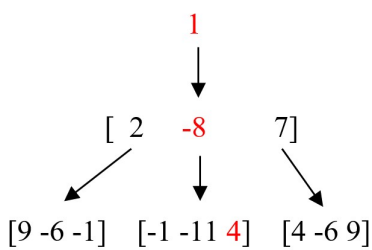
and y along those paths *at each one-generation step* produces the descendants in a specific path in the tree of w, namely the path corresponding to $F_z(w)$. The *same* z is associated with the x path as with the w path. The path for the y tree is from the z´ that makes $F_{z'}(y) = (x\text{-}z\text{+}z')/N^k$ integral. (There are also other ways paths can add, but this is the one we will use going forwards.) This is clear because $F_z(x) + F_{z'}(y) = (x\text{-}z\text{+}z')/N^k + (y\text{-}z'\text{+}z'')/N^k = (w\text{-}z\text{+}z'')/N^k = F_z(w)$, where z´ and z´´ are chosen in the only way that makes the results integers. Conversely, given any path in the tree of w, we can find paths in the trees of x and y that add to that path: indeed just choose the same z-path for x as you were given for w. The path in the tree of y is the z´-path where z´ is chosen to make $(x\text{-}z\text{+}z')/N^k$ integral.

If $w = x - y$, we can subtract paths in the trees of x and y to produce paths in the tree of w. Specifically if we choose any z in any A^k and then consider the *same* z-path in both the x and the y trees, then subtracting those paths produces a path in the tree of w. This is shown as follows: $F_z(x) - F_z(y) = (x\text{-}z\text{+}z')/N^k - (y\text{-}z\text{+}z'')/N^k = (w\text{-}z''\text{+}z')/N^k = F_{z''}(w)$. The path produced is the z´´-path in the w tree, where z´´ is the member of A^k that makes $(y\text{-}z\text{+}z'')/N^k$ integral. Conversely, any path in the w tree (say the z´´ path) can be seen as a path in the y tree subtracted from a path in the x tree by again using the z that makes $(y\text{-}z\text{+}z'')/N^k$ integral and choosing the z path in both the x and y trees.

The properties described above are illustrated in the simple example below.

2.3. Illustration 1: Properties of trees

Consider $N = 3$ and $A = \{a_0, a_1, a_2\} = \{0, 25, 5\}$. The maps to create the tree will be given in this order from left to right: $F_0(x) = (x\text{-}0\text{+}a)/3$ and $F_{25}(x) = (x\text{-}25\text{+}a')/3$ and $F_5(x) = (x\text{-}5\text{+}a'')/3$ where $\{a, a', a''\}$ are the unique members of A that give integral descendants for x. For example, the first two generations of descendants of $x = 1$ are shown. For clarity, only one arrow connects a number to its first generation descendants. Notice the sum of terms in any generation will equal the root number 1.



The second generation can also be computed directly by using $A^2 = 3A+A = \{0, 75, 15, 25, 100, 40, 5, 80, 20\}$, written in the order that creates the second generation from left to right. For example F_z with $z = 40 = 3(5)+25$ is the composition $F_5 \circ F_{25}$: $F_{40}(1) = (1\text{-}40\text{+}75)/9 = 4$ (which is 6th in the second generation) and the two steps to that 4 are given as $F_{25}(1) = (1\text{-}25\text{+}0)/3 = -8$ and then $F_5(-8) = (-8\text{-}5\text{+}25)/3 = 4$. (The z-path for $z = 40$ is shown in red in the tree.)

In the trees below, we again show only two generations (omitting the arrows). We show an example of an expressible number with 0 in its tree, as well as the adding and subtracting of paths in trees. Notice the following three points about the examples below:

a) A path leading to 0 in the tree for x corresponds to an expression for x. For example, in the tree for 5 below there is a path to 0 (shown in red). The first step is an application of F_{25}, the middle map, which takes 5 to $(5\text{-}25\text{+}5)/3 = -5$. This is followed by an application of F_0, the left map, which takes -5 to $(-5\text{-}0\text{+}5)/3 = 0$. The resulting expression is $5 = 3(0\text{-}5)+(25\text{-}5)$. The red numbers in this expression indicate the maps and paths used, and come from seeing which numbers were subtracted by the application of the two maps. The path may be described as the z-path for z in A^2 given by $z = 3(0)+25 = 25$, where $F_{25}(5) = (5 - 25 + 20)/9 = 0$. Note the 25 that was subtracted is the 4th member in the list of A^2 above, and the 0 in the tree is the 4th in its generation. This F_{25} is an A^2 map whereas the F_{25} mentioned earlier in this paragraph was an A map, an ambiguity that was explained earlier.

b) A particular path is chosen in the tree of 1, and a path is then found in the tree of 4 which will add to it, producing a path in the tree of 5. The path in the tree of the sum can be chosen to be the same as for one of the summands. In this example I chose it to match the path in the tree for 1 but it can be done in other ways. Notice that the paths in the trees of 1 and 5 are the same: they take the leftmost descendant in the first step and the center descendant in the second. At each step the numbers on the paths add up to the number in the path of the tree of 5. The paths are in blue.

c) Note also if the *same* path is chosen in the two trees for 1 and 4, and the paths are subtracted, the result is a path in the tree of the difference -3. The route of the difference path is not necessarily the same as for the trees that were subtracted. The paths are in blue, and for the 1 tree and the 4 tree connect to the rightmost descendant followed by the leftmost.

Adding: 1+4 = 5

1

[**2** -8 7]

[9 **-6** -1] [-1 -11 4] [4 -6 9]

4

[3 -7 **8**]

[1 1 1] [6 -9 -4] [11 -4 **1**]

5

[**10** **-5** 0]

[5 **-5** 10] [**0** -10 5] [0 0 0]

(We follow the same path in 1 as in the sum 1+4, and a different path in the tree of 4.)

Subtracting: 1-4 = -3

1

[2 -8 **7**]

[9 -6 -1] [-1 -11 4] [**4** -6 9]

4

[3 -7 **8**]

[1 1 1] [6 -9 -4] [**11** -4 1]

-3

[-1 **-1** -1]

[8 -7 -2] [8 **-7** -2] [8 -7 -2]

(We follow the same path in both 1 and 4, a different path in 1-4.)

Note: The first step in the tree for 1 is to (1-5+25)/3 and in the tree of 4 to (4-5+25)/3. In subtracting 1-4 this corresponds to 1-4 connecting to (1-5+25)/3 - (4-5+25)/3 = (-3 -25 +25)/3 = -1. This is $F_{25}(-3)$ which is why the *middle* -1 is in blue in the first generation of the tree of -3.

3. Omniexpressible numbers

A key part of the proof of Theorem 1.1 is the existence of *omniexpressible numbers*, that is, integers x for which every descendant of x is expressible. There are an infinite number of ways to express such x in the form $z_1 - z_2$ with z_1 and z_2 in some A^k, since the initial path through the tree of x can be arbitrary and still one would be able to extend the path to a descendant 0. That means you can "start expressing" an integer x with *any* expression of the form $\sum_{j=0}^{k} b_j N^j$ where k≥0, provided x is congruent to this expression modulo N^{k+1}. You can then add on higher power terms to make the completed expression equal to x.

Let K be the set of omniexpressible integers. It is unclear at first that such numbers exist (apart from 0, for which all descendants are equal to 0). In fact, finding nonzero omniexpressible integers is the key to the proof of Theorem 1.1. That omniexpressibility is important to the proof is not surprising. From the proof we will present in Section 5, it becomes clear that *all* expressible integers are in fact omniexpressible in the real case. (In the complex case, if one or two expressible numbers are omniexpressible then they all are.)

This is especially easy to see *in the real case* because Corollary 1.1 asserts that the set of expressible numbers E is the set of all multiples of d = gcd(B). The multiples of d are all omniexpressible due to the fact that all descendants of a multiple of d are also multiples of d. See for example the tree of 5 in the illustration in Section 2 above. A short proof of this is presented here as a corollary of Theorems 1.1 and 1.2:

Corollary 3.1. *In the $\mathbb{Z}$ case, every expressible number is also omniexpressible.*

Note: This is also conjectured in the $\mathbb{Z}[i]$ case.

Proof. Let gcd(B) = gcd(A) = d. Let a be the member of A that is congruent to 1 modulo N, and write a = sd for some integer s. Then sd+rN =1 for some integer r, so that d and N are relatively prime.

Then if x is a multiple of d, any descendant of x is of the form $(x\text{-}z_1+z_2)/N^k$ where z_1 and z_2 are in some A^k, the members of which are all multiples of d. Then a descendant of x is a multiple of d divided by N^k which is still a multiple of d. ■

That any expressible number in the real setting is omniexpressible will also be seen to be a direct result of the proof of Theorem 1.1 that we will present in Section 5, so Corollary 3.1 above is only presented here to show that in the real setting that fact is quite directly seen to be true.

Most important though are the following results, true in both the $\mathbb{Z}$ and the $\mathbb{Z}[i]$ setting. We refer to both sets $\mathbb{Z}$ and $\mathbb{Z}[i]$ simultaneously as G, which is in either case a group under addition.

Lemma 3.1. *The set K is a subgroup of G.*

Proof. Obviously 0 is a member of K since all its descendants are 0.

If x and y are omniexpressible, then so is w = x+y: Any descendant of w can be expressed as x´+y´ where x´ and y´ are descendants of x and y, and where the path from x to x´ in the tree of x adds to the path from y to y´ in the tree of y to produce the path from w to x´+y´. Since x´ is expressible, there is a path from x´ to 0 in the x tree, and a path from y´ to some y´´ in the y tree that will add to it, extending the path in the w tree from x´+y´ to 0+y´´. Since y´´ is expressible, there is a path connecting 0+y´´ to 0+0 in the w tree. Therefore the arbitrary descendant x´+y´ in the tree of w is expressible, and w is omniexpressible.

Finally, since B = –B, if a number is expressible so is its opposite. Since the members of the tree of –x consist of the opposites of the members of the tree of x, for any integer x, if x is omniexpressible so is -x. In other words, K = –K. This establishes that K is a subgroup of G under addition. ■

There is an obvious corollary to Lemma 3.1:

Corollary 3.2. *A system (A,N) for $\mathbb{Z}$ is a Just Touching Covering System iff the number 1 is omniexpressible. A system (A,N) for $\mathbb{Z}[i]$ is a Just Touching Covering System iff the numbers 1 and i are omniexpressible.*

The importance of this concept of omniexpressibility is made clear by the following:

Theorem 3.1. *E is a subgroup of G if and only if K = E. That is, E is a group if and only if every expressible number is omniexpressible.*

Proof. Obviously if K= E, then E is a group by Lemma 3.1. On the other hand, say E is a group under addition. Let x be in E. Then we need to show that x is in K, i.e. that x is omniexpressible. It suffices to show that all the first-generation descendants of x are expressible, since x is an arbitrary member of E. These descendants are of the form $F_a(x) = (x\text{-}a+a')/N$ where a and a' are in A. Since E is a group and x, a and a' are in E, it follows that $w = x\text{-}a+a'$ is expressible. But w is a multiple of N, and its entire first generation consists of the same repeated number w/N: $F_{a''}(w) = (w\text{-}a''+a'')/N = w/N$ for any a''. Since w is expressible, it must mean $w/N = (x\text{-}a+a')/N$ is expressible as well. ■

4. The existence of a nonzero omniexpressible number in the real case

We show that, for the real case $\mathbb{Z}$, E contains a nonzero omniexpressible number, which will be the key fact in proving Theorem 1.1 in Section 5. We record this as:

Lemma 4.1. *For any system (A,N) for $\mathbb{Z}$, there exists a nonzero omniexpressible number.*

We also mention at this point a conjecture for the complex $\mathbb{Z}$[i] case, that if true will provide a proof for Theorem 1.1 in that situation as well, also presented in Section 5.

Conjecture 1. *Given any system (A,N) for $\mathbb{Z}$[i]:*

a) *Assume Im(N) $\neq$ 0. Then there exists a nonzero omniexpressible integer.*

b) *Assume Im(N) = 0. Then there are two omniexpressible integers, independent as vectors in $\mathbb{R}^2$.*

Note: As we shall see in Section 5, if these conditions are met then E is a group, in fact a two-dimensional lattice, and all expressible numbers are omniexpressible. This conjecture was tested in numerous computer examples, albeit for relatively small N. In all examples, the conjectured one or two omniexpressible numbers were found. A computer program was also used to generate and plot all the members of E in the disk I and in all cases the plot was consistent with E being a two-dimensional lattice.

Before proceeding with the proof of Lemma 4.1, we need the following definition of *nonemerging sets*.

Consider an ordered set of integers, say D = $\{s_1, s_2, ..., s_k\}$, of size k greater than 0, where it is possible that numbers may be repeated. One may form a tree for the entire set D by applying the various maps F_a to the individual members of the set. An example is shown in the illustration below. The set D is called a *merging set* if it has a descendent set which contains duplicate numbers. If *all* descendent sets of D feature k distinct numbers, we say D is a *nonmerging set*. A set of size one is an example of a nonmerging set. As remarked earlier, applying the same F_z to two members of a set corresponds to a path on the tree of the *difference* of those two numbers. Thus another way of defining a nonmerging set D is as a set where all the differences of pairs $\{s_i, s_j\}$ of members of the set are inexpressible: if such a difference did map to 0, then s_i and s_j would have the same image under some map F_z.

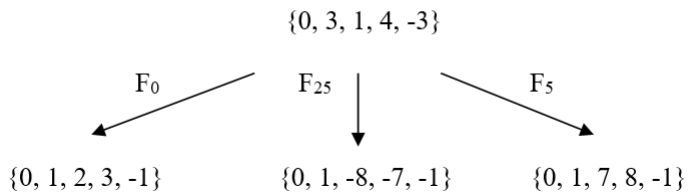
Notice that any set containing more than |I| members will be a merging set. Repeatedly applying F_0, where $F_0(x) = (x\text{-}0+a)/N$ with a in A, will eventually

lead to a set with at most |I| distinct members, because eventually all the images of the members of the set will be in I. It then makes sense to define a *Maximal Nonmerging Set (MNM Set)* to be a nonmerging set of maximal cardinality. Note that any descendant in the tree of a MNM Set is also a MNM Set, since it is obviously the same size.

4.1. Illustration 2

As earlier consider N = 3 and A = $\{a_0, a_1, a_2\}$ = {0, 25, 5}. The maps to create the tree are in this order from left to right: $F_0(x) = (x\text{-}0+a)/3$ and $F_{25}(x) = (x\text{-}25+a')/3$ and $F_5(x) = (x\text{-}5+a'')/3$ where $\{a, a', a''\}$ are the unique members of A that give integral descendants for x. For example, the first two generations of descendants of x = 1 was shown earlier in Illustration 1.

We can form the tree of a set of numbers in the same way, as we do below for D = {0, 3, 1, 4, -3}. With these same F maps in the order given above, we have the first generation of the tree of D shown below. Recall as a computational check that the sum of the sets in any generation, when treated as vectors, will equal D, since this is the real case with N positive.



The set D is clearly a nonmerging set since the differences of distinct members of {0, 3, 1, 4, -3} are not multiples of 5, and in fact D is a MNM Set, as are all its descendent sets.

4.2. Proof of Lemma 4.1

To prove Lemma 4.1 we need:

Lemma 4.2. *Let $M = \{m_1, m_2, ..., m_k\}$ and $M' = \{m_1', m_2', ..., m_k'\}$ be MNM Sets. If $m_i = m_i'$ for all $i > 1$, and $m_1 \neq m_1'$, then $m_1 - m_1'$ is a nonzero omniexpressible number.*

Proof. Consider the set $M \cup \{m_1'\} = \{ m_1, m_2, ..., m_k, m_1' \}$. Consider any descendent set in its tree. Write this set as $D = \{n_1, n_2, ..., n_k, n_1'\}$ where each n_i is the image of m_i, and n_1' is the image of m_1'. Note that $n_1 - n_1'$ is an arbitrary descendant of $m_1 - m_1'$ since D is an arbitrary descendant in the tree. The proof is by contradiction. Assume $n_1 - n_1'$ is not expressible. Then

the images of n_1 and $n_1{}'$ will be different in any further application of maps to the set D. Moreover, the image of n_i for $i > 1$ will not equal the images of n_1 and $n_1{}'$ since M and M′ are nonmerging sets. Then D is a nonmerging set of k+1 members, contradicting the maximality of M and M′. ■

The proof of Lemma 4.1 is then as follows:

Proof. For the proof of Lemma 4.1, we need to find two MNM Sets which differ in exactly one of their members. If T is a MNM Set of size 1, say $T = \{x\}$, then we are done: for y unequal to x, the set $T' = \{y\}$ is also a MNM Set, so x-y is a nonzero omniexpressible number. We may thus assume T is a MNM Set of size greater than 1. Notice that if an integer x is added to each member of T, the result, denoted T+x, is a MNM Set. This is clear since the differences between members of T are the same as the differences between members of T+x. By choosing x to be the opposite of the largest member of T, we see there exists an MNM Set M = T+x that contains 0 with all other members being negative integers. Write $M = \{0, m_2,..., m_k\}$ and assume the numbers are listed in descending order with m_k being the smallest number in the set.

Let S be the set of integers in the interval $[m_k, |m_k|]$. If this interval lies *inside* I, the interval for B, then let S be the integers in I instead. Then any F_z is a map from S to S. Any map F_z creates a directed graph on S connecting each s in S to its image $F_z(s)$. There are at most $|S|^{|S|}$ possible graphs. Choose k so that the size of A^k is larger than $|S|^{|S|}$. Consider the maps F_z with z in A^k. Since there are more maps than there are graphs on S, there are two different z and z′ in A^k where the maps F_z and $F_{z'}$ have the same graph on S. In particular, $F_z(M) = F_{z'}(M)$. It is impossible that these two maps have the same images on all members of $\mathbb{Z}^+$:

Lemma 4.3. *If z and z′ are in A^k and $F_z(x) = F_{z'}(x)$ for all x in $\mathbb{Z}^+$, then $z = z'$.*

Proof. Assume $F_z(x) = F_{z'}(x)$ for all x in $\mathbb{Z}^+$. For any given x in $\mathbb{Z}^+$ we have $(x\text{-}z+z_2)/N^k = (x\text{-}z'+z_3)/N^k$, where z_2 and z_3 are in A^k . Then $z_2–z = z_3–z'$ so that $z–z' = z_2–z_3$. Then $F_{z_2}(z\text{-}z') = (z\text{-}z'\text{-}z_2+z_3)/N^k = 0$. As x ranges over the members of $\mathbb{Z}^+$, the numbers z_2 (which are congruent to z–x modulo N^k) range through all congruence classes modulo N^k. That is, $F_{z''}(z\text{-}z') = 0$ for all z′′ in A^k. Then generation-k of the tree for z–z′ consists entirely of zeroes. Since the sum of the numbers in generation-k is z–z′ (or possibly its opposite if N is negative), we get $z–z' = 0$, proving Lemma 4.3. ■

We can now complete the proof of Lemma 4.1.

By Lemma 4.3, there is some *smallest* positive integer r greater than $|m_k|$ where F_z and $F_{z'}$ have different images on r. Consider the MNM Set r+M with

M above: r+M = {r, r+m_2,.., r+m_k}. All numbers in r+M are positive, with r being the largest. If we look at the images of r+M under F_z and $F_{z'}$ we get two MNM Sets which agree in all their members apart from $F_z(r)$ and $F_{z'}(r)$. Thus by Lemma 4.2 we have proven Lemma 4.1, the existence of a nonzero omniexpressible number for the real case. ■

Note: In the complex case, the proofs of Lemmas 4.2 and 4.3 work as well. We would replace intervals by disks in that setting but things work in basically the same way. In the last step of the proof of Lemma 4.3 in the complex case the sum of the members of generation-k of the tree of z–z´ is $\bar{N}^k \cdot$ (z–z´), so again if $\bar{N}^k \cdot$ (z–z´) = 0 then z = z´. This same proof nearly works to establish Conjecture 1 for the complex case as recorded above, at least in the case for N with nonzero imaginary part where we need find only one nonzero omniexpressible number. The only problem that comes up (a significant one) is that $\mathbb{Z}$ is nicely ordered by size, whereas $\mathbb{Z}$[i] is not, so that the final step of translating M by r does not work. I have other techniques for proving the existence of a nonzero omniexpressible in the real case, but they all rely at some point on the ordering of $\mathbb{Z}$.

5. The proof of Theorem 1.1 if some nonzero omniexpressible numbers exist

By Lemma 4.1, in the real case, K will always contain a nonzero integer. As remarked earlier, the existence of nonzero omniexpressible integers is the key to the proof of Theorem 1.1. The analogous requirements for the proof in the complex setting are only conjectured (Conjecture 1 above) and not proven. Nevertheless, the theorem is still very useful if we can find one or two nonzero omniexpressibles in the $\mathbb{Z}$[i] setting in specific examples (Section 6). We rewrite Theorem 1.1 from Section 1 of this paper in ways appropriate to the two settings, and in addition will incorporate the facts about omniexpressible numbers that emerge from the proof. As part of the proof it will turn out that all expressible numbers are omniexpressible, but we saw in Section 3 that this condition is equivalent to E being a group, so it is not surprising that this emerges in the proof we are about to present. The proofs for the real and the complex cases are quite similar, but in Section 5.1 we present an alternate version of the proof that is even more unified. Each proof has its merits.

Theorem 5.1. *If (A,N) is a system for $\mathbb{Z}$, then E is a group under addition. Consequently E has the description given in Theorem 1.2, that E is the smallest subgroup of $\mathbb{Z}$ containing A that is closed under multiplication by N. In addition, every expressible number is omniexpressible.*

Theorem 5.2. *Assume (A,N) is a system for $\mathbb{Z}$[i] that satisfies these conditions:*

(1) *If Im(N) $\neq$ 0, there exists an omniexpressible integer other than 0,*

(2) *If Im(N) = 0, there are two omniexpressible integers, independent as $\mathbb{R}^2$ vectors.*

Then it follows that E is a group under addition. Consequently E has the description given in Theorem 1.2, that E is the smallest subgroup of $\mathbb{Z}$[i] containing A that is closed under multiplication by N. In addition, every expressible number is omniexpressible.

We first prove Theorem 5.1 (the Real case):

Proof. By Lemma 4.1, we know a nonzero omniexpressible integer exists. Let x be the smallest positive member of K. Since K = -K, -x is the largest negative omniexpressible. Consider the set D = {0, x, ..., (|N|-2)x, (|N|-1)x}. These numbers are all omniexpressible because K is a group under addition. If two members of D were equivalent modulo N, then subtracting would yield a nonzero integer k where kx is omniexpressible and divisible by N, with 0< k< |N|. Then kx/N is also a positive omniexpressible (being a descendant of kx) and is smaller than x, which is a contradiction. Thus each member of the set D is congruent to a different member of A and in fact D contains one member from each congruence class modulo N.

If jx is the member of D congruent to a modulo N for a in A, then jx has descendant F_a(jx) = (jx - a+0)/N, which is omniexpressible. Hence jx-a is also omniexpressible: its first-generation descendants are all the same number, (jx-a)/N. Therefore a is omniexpressible, since a = (jx) - (jx-a) which is a difference of omniexpressible numbers. This is true for any a in A. Then A is a subset of K which means d = gcd(A) is also a member of K. It follows that <d>, the set of all real integer multiples of d, is a subset of K.

On the other hand, any expressible number is a sum with coefficients in B = = A–A and is therefore divisible by d, so we have E $\subseteq$ <d> $\subseteq$ K $\subseteq$ E. Therefore E = K = <d> proving the theorem. ■

We now prove Theorem 5.2 (the Complex case):

Proof. In this proof the members of $\mathbb{Z}$[i] are referred to interchangeably as numbers or integers, or as vectors depending on how they are being viewed.

Case 1: Im(N) $\neq$ 0

Here we assume there exists an omniexpressible integer x other than 0. The set K is a subgroup of $\mathbb{Z}$[i] under addition (Lemma 3.1) and hence contains this number x and all its real integral multiples. Then Nx is also in K, since all

its first-generation descendants equal x. If N = r+s**i**, for real integers r and s, then Nx=rx+**i**sx. Since rx is in K, it follows that **i**sx = Nx-rx is as well. Then K contains both nonzero sx and **i**sx. Let z be a smallest nonzero integer for which z and **i**z are both in K. Then K contains the ideal <z>, the set of all complex integer multiples of z.

We show z and N are relatively prime: Assume z = mn and N = mt where m, n, and t are complex integers with ||m|| > 1. Consider y = mnt. Then y = tz is in <z> and is thus in K. On the other hand, y/N = n is then also in K, being a descendant of y. Also, **i**y = **i**mnt = **i**tz is in K as it is a multiple of z. Then **i**y/N = **i**n is also in K. Since n and **i**n are both in K and n has norm less than the norm of z, we have a contradiction. Therefore z and N are relatively prime.

Since z and N are relatively prime, there is a complex integer w such that wz $\equiv$ 1 modulo N. If a is any member of A, we have $a$wz $\equiv$ a modulo N, where $a$wz is in K. Then the descendant ($a$wz-a)/N is also in K. Again this implies $a$wz-a is also omniexpressible, as its first-generation descendants all equal the omniexpressible ($a$wz-a)/N. Then a = $a$wz - ($a$wz-a) is omniexpressible too, for any a in A.

We then have that A is contained in K. Since B = A–A, we have that B is also a subset of K. Since K is an additive group that is closed under multiplication by N, and since K contains B, it is clear that K contains E, the set of all numbers in the form $\sum_{j=0}^{k} b_j N^j$ where k$\geq$0, and where each b_j is in B. We have E $\subseteq$ K $\subseteq$ E , and so E = K, proving Theorem 5.2 in Case 1.

Case 2: Im(N) = 0

Here we assume there are two omniexpressible integers independent as R^2 vectors. Denote these numbers as X = x_1+**i**x_2 and Y = y_1+**i**y_2, where x_1, x_2, y_1, and y_2 are real integers. Since K is an additive group, it follows that y_1X-x_1Y is a nonzero vector in K with real part zero. (Nonzero since X and Y are independent and clearly y_1 and x_1 cannot both be zero, and in K since y_1 and x_1 are real integers). Write this vector as **i**r where r is a nonzero real integer. Similarly, s = y_2X-x_2Y is a nonzero vector in K with imaginary part zero. Then z = rs is a nonzero real integer, in K since r is a real integer and s is in K. Also **i**z is in K since **i**z = s·**i**r where **i**r is in K and s is a real integer. The proof given in Case 1 follows as before, since K contains both z and **i**z for some nonzero z, which is what was needed subsequent to the first paragraph of that proof. ■

Note that both cases of the proof are essentially the same but the proof clarifies why in Case 1 we only needed the existence of the one omniexpressible number.

5.1. An alternative proof of Theorem 1.1 if nonzero omniexpressible numbers exist

We present an alternative proof for Theorems 5.1 and 5.2 with an interesting method that works basically the same way in either $\mathbb{Z}$ or $\mathbb{Z}$[i]. We combine the two settings into one proof, though the requirements about the existence of omniexpressibles in the complex cases are still the same as above. As before denote the setting as G to cover both cases, where G can be either the group $(\mathbb{Z},+)$ or the group $(\mathbb{Z}[i],+)$.

Proof. By Lemma 3.1, K is an additive subgroup of G. We first establish that G/K is a finite group.

In the real case, K is a subgroup of $\mathbb{Z}$ and K is not $\{0\}$, so K is the set $<a>$ consisting of all multiples of some nonzero integer a. Therefore $\mathbb{Z}/K = G/K$ is a finite group.

In the complex case, the additive subgroup K of $\mathbb{Z}$[i] is a lattice. If we have an omniexpressible nonzero integer x, then we have a second omniexpressible integer Nx that is independent of x (considered as vectors in $\mathbb{R}^2$) if Im(N) is nonzero. If Im(N) = 0, we are already assuming that we have two independent omniexpressible numbers. In either case, since K contains two linearly independent complex integers, we have that K is a two-dimensional lattice, namely a set <x,y> consisting of all ax+by where a and b are *real* integers, and x and y are Gaussian integers that are linearly independent when viewed as vectors in $\mathbb{R}^2$. Again we have that $\mathbb{Z}$[i]/K = G/K is a finite group. For the remainder of the proof we consider the real and complex cases at the same time.

In any coset g+K, members of the coset are either all expressible or are all inexpressible. If g is *expressible*, then so is g+k for any k in K: Take any path from g to 0. There is a complementary path from k to some k´ such that 0+ k´ is a descendant of g+k. Since k´ is expressible, because k is omniexpressible, we then have 0 is a descendant of g+k. Thus if g is expressible, so is any member of g+K. On the other hand, if g is *inexpressible*, so is any member of g+K: Assume g+k connects to 0. Then g+k connects to g´+k´ = 0 , where g´ is a descendant of g and k´ is a descendant of k. Then g´ = -k´ is expressible, and then so is g, which is a contradiction. We may thus speak of 'expressible cosets' and 'inexpressible cosets'.

If F is *any* map of the type described earlier, say F_z with z in A^t for some t, then F(g+K) = F(g) + K. In other words, any F maps cosets to cosets. The proof is as follows: For any k in K, F(g+k) = F(g)+F´(k) for some map F´= $F_{z'}$ where z´ is also in A^t by the additive property in trees. Since F´(k) is in K, we have F(g+K) $\subseteq$ F(g)+K.

On the other hand, any F(g)+k can be written as F(g+N^tk), since F(g+N^tk) = F(g)+F´(N^tk) for some map F´= $F_{z'}$ with z´ in A^t. Then F´(N^tk) =

$= (N^t k\text{-}z' + z')/N^t = k$ no matter what z' is. This also shows $N^t k$ is omniexpressible since k is the only number in generation-t of its tree. Thus $F(g)+K \subseteq F(g+K)$ and we conclude that $F(g+K) = F(g) + K$.

Furthermore, F is a bijection from G/K to G/K. That F is onto follows from the fact that, for any g in G, $g+K = F(N^t g+K)$. That F is one-to-one then follows from the fact that G/K is a *finite* group.

If g is inexpressible, so is its descendant F(g). Therefore F will map the inexpressible cosets to inexpressible cosets. Since there are a finite number of cosets, it follows that the expressible cosets must map to the expressible cosets. Thus if g is expressible, so is F(g) for the arbitrary map F. Thus g is in fact omniexpressible if it is expressible. (Note also that the only expressible coset is K itself.) All expressible integers are therefore in K, so we have $E \subseteq K \subseteq E$, proving Theorems 5.1 and 5.2 that E = K is a group, and that all expressible numbers are omniexpressible. ■

6. The application of Theorem 5.2 for the complex case

In this section we discuss the use of Theorem 5.2 in finding the group E in the complex setting in examples of (A,N) where the assumptions of Theorem 5.2 are satisfied. First, to verify that the assumptions of Theorem 5.2 are satisfied, we would need to find nonzero omniexpressible numbers. The approach discussed below explains how to tell if E is a group, and importantly if it is not, and then describes how to determine what that group is. We are using this revised version of Theorem 5.2 that incorporates the comments on the structure of E when it is a group, covered in Section 1:

Theorem 6.1. *Let N be a Gaussian integer of modulus greater than 1, and A a set of representatives of the congruence classes modulo N containing 0. Let E be the set of all Gaussian integers expressible in the form* $\sum_{j=0}^{k} b_j N^j$ *where* $k \geq 0$, *and where each* b_j *is in* $B = A - A$. *If there is a nonzero Gaussian integer that is omniexpressible or, in the case where Im(N) = 0, if there are two such omniexpressible numbers that are independent as vectors in* $\mathbb{R}^2$, *then E is a group. In addition, all expressible numbers are omniexpressible. Specifically, E is the smallest additive subgroup of* $\mathbb{Z}[i]$ *that contains A which is closed under multiplication by N. E is a two-dimensional lattice generated by a member of E of minimal modulus, and a second member of E that is independent of the first and that has minimal modulus among all such.*

In an example, the first task is to establish that E is a group by finding the requisite omniexpressible numbers. If E is a group then all expressible numbers are omniexpressible by Theorem 3.1, including of course the members of A. So the obvious approach would be to take a smallest nonzero member x

of A (or of B if it contains smaller numbers than A) and write out its tree for enough generations to check for omniexpressibility. This is possible because the distinct members of any tree are finite in number and some generation will contain exclusively members of I. After examining the tree of x we see that either some descendant of x is not expressible, in which case E is not a group, or all descendants of x do connect to 0, in which case we have found one nonzero omniexpressible. We have then established E is a group by Theorem 6.1 if $\mathrm{Im}(N) \neq 0$. In the case where $\mathrm{Im}(N) = 0$, we would need to find a second omniexpressible number which is independent of x as a vector in $\mathbb{R}^2$. We may be lucky and have already found the needed second omniexpressible number as a descendant of x. If we are not lucky, in Section 1 we showed that, when $\mathrm{Im}(N) = 0$, it is not possible that all members of A lie on the same line through the origin in $\mathbb{R}^2$. So we can look for a second omniexpressible by examining any member of A that is independent of x. There is no luck involved in the choice, other than that for some numbers you may need to examine fewer generations of the tree. If E is a group, then all members of A are omniexpressible. If this second member of A is also omniexpressible then we know E is a group by Theorem 6.1, and if it is not omniexpressible, then E is not a group. Therefore, in total, to determine if E is a group requires checking at most two members of A for omniexpressibility.

A drawback here is that nonzero members of A could all be quite large. In reality one need only examine the trees of the integers in I, for each nonzero x in A has a generation contained entirely in I and these descendants cannot all be 0. Thus there is a nonzero member of E in I if E is a group. If $\mathrm{Im}(N) = 0$, there are two independent members of E in I: If x and y are independent in A, with their kth generations in I, it is not possible that all those descendants lie on the same line through the origin, since the sum of the generation-k members are $N^k x$ and $N^k y$. So a possible shorter approach would take two independent members of A, and then find two independent descendants of them in I to check for omniexpressibilty. E is a group if and only if they are both omniexpressible.

Assuming you have found the one or two omniexpressible numbers needed to establish that E is a group, the next task would be to identify the group. As discussed in Section 1 of the paper, E is a two-dimensional lattice <x,y> consisting of all $ax+by$ where a and b are *real* integers and x and y are Gaussian integers that are independent as vectors in $\mathbb{R}^2$. We need to find a pair of generators x and y of E where x is a nonzero member of E of minimal modulus and y is a member of E that is independent of x and that has minimal modulus among all such members of E. We can first easily identify x as it must be a member of I. The tree-examination is much simpler now: we only need to establish x is expressible, as omniexpressibility is guaranteed since E is a group. In general there will therefore be fewer generations in the tree of x to check. We would examine the different members of I in order of increasing modulus,

and x would be the first *expressible* number we find. There is no guarantee that y will be found within I. If Im(N) $\neq$ 0, Nx will be expressible and independent of x, so Nx is a possible candidate for y (and a bound on how big y could be). In the case where Im(N) = 0 we have less guidance, but in this case we can fall back on the fact that A contains vectors independent of x as pointed out in Section 1. So there is a member of A that is expressible and independent of x, which gives a candidate for y (and a bound on how big y could be). It may still take a bit of work to find the smallest expressible number independent of x. A computer is recommended. The following rather simple examples were done using just a spreadsheet that displays the first generation of a number x.

Example 6.2. N = 1+2i and A = {0, -2+2i, -1, -3+2i, 4i}

Note: The canonical A is in the quadrilateral defined by the vectors N and iN and consists of {0, i, 2i, -1+i, -1+2i}. The other possible A are shifts of the canonical members by adding aN +biN where a and b are any real integers.

The radius of the disk I is $\sqrt{17}/(\sqrt{5}-1)$ where $\sqrt{17}$ is the modulus of a largest member of B = A–A, namely 1+4i, and where $\sqrt{5}$ is the modulus of N. This is less than $\sqrt{12}$ so a biggest member of I is 1+3i, to give some idea of how large a set may be involved as the descendants of a number x in I.

We need only find one nonzero omniexpressible and we will check the smallest member of A which is x = -1. (There is no smaller member of B, which is important to check in general. However there is no real reason to assume you would have to look less deeply into the tree of -1 to confirm omniexpressibility than you would in testing any other member of I in A.)

In the tree of -1 you need only check the first generation of each new member of the tree you encounter, to see if there are any new numbers encountered. Since -x is omniexpressible if x is, you can skip checking the opposites of numbers you have previously checked. We see that generation-1 of -1 contains 0 (twice), 1, -2 and 2i. The 1 will have a 0 in its first generation since -1 does. The numbers -2 and 2i have -1 as a descendant so they are expressible. In generation-2 of the tree of -1, the only new encounter is with 1+2i (apart from opposites of previously encountered numbers). The first generation of 1+2i features only the number 1 which is expressible. Thus all members of the tree are expressible and we have determined E is a group. We now look for small numbers as generators for E = <x,y>. Obviously -1 is a smallest nonzero member of E so we can choose x to be -1. Within the tree of -1, 2i is expressible and is a candidate for y, being independent of -1. But there may be a smaller number as well. Examining the tree of the number i up to generation-3 shows it is not expressible. Similarly neither 1+i nor 1-i are expressible. Therefore 2i is a smallest member of E independent of -1 and E = <-1, 2i>.

Example 6.3. N= 2 and A = {0, 1+2i, 2+i, 3+i}. The largest member of B is 3+i so the disk I has radius $\sqrt{10}$ / (2-1) = $\sqrt{10}$. So a largest member of

I is 3+i. The set B contains (3+i) – (2+i) = 1, so we examine the tree of 1. Its first generation includes 0 obviously as it is in B. The other generation-1 members are 1, -i, and 1+i. The first generations of both -i and 1+i include 1 so they are expressible. The second generation of 1 contains only 2+i and 1-i as unchecked numbers (ignoring repeated numbers or their opposites). Both have 0 as a first-generation descendant so they are expressible. The only unchecked number in the third generation of the 1-tree is the number 2, which has 1 as its only first-generation descendant, and is therefore expressible. Therefore 1 is omniexpressible. For an omniexpressible number independent of 1 we saw already that -i is omniexpressible. Therefore E is a group and is obviously $\langle 1,-i\rangle = \mathbb{Z}[i]$. In this example (A,N) is a Just Touching Covering System.

Example 6.4. Again with N = 2 and A = {0, 5+2i, 2+i, 3-3i}. A largest member of B is 5+2i so I has radius $\sqrt{29}$ / (2-1) = $\sqrt{29}$ with a largest member of I being 5+2i. I chose to examine the tree of 2+i which is in A. It required going through to generation-6 until no new numbers were encountered, but there were not many distinct descendants and they all were expressible. Since 1 featured in the tree of 2+i, we already have found the second independent omniexpressible, so E is a group. Since i was also in the tree, we see E = = $\langle 1,i\rangle = \mathbb{Z}[i]$ and (A,N) is again a Just Touching Covering System.

7. Programmable computation of an expression: replacing a Just Touching Covering System by an equivalent Number System

We make an observation about the computation of an expression for an expressible number in either any real case example, or in complex case examples where the conditions of Theorem 5.2 are met. This is a consequence of Theorem 3.1, that expressible numbers are omniexpressible. Choose a map F of the type described above, so that F(I) is minimal in size. If F(I) contains any expressible nonzero number x, then you can pick a map F′ so that F′(x) = 0. Then (F′∘ F)(I) will be strictly smaller than F(I) which was assumed impossible. Therefore F maps every expressible number in I to 0. (Theorem 3.1 matters here since we need to know an expressible number cannot map to an inexpressible number.) Then repeated application of F will map *any expressible number* to 0, since eventually the image will lie in I and *will be expressible by Theorem 3.1.* Then at most one more application of F will result in a connection to 0.

Note: In finding an F that makes F(I) of minimal size there is more guidance in the real case. One can keep composing various maps until the image of I contains 0 as the only multiple of d = gcd(A). In fact one could stop here without making F(I) minimal and that would be sufficient. (If you wanted to

make F(I) minimal you would keep applying maps until the image contains at most one representative of each congruence class modulo d). In the complex case there is less guidance but finding out what the lattice E is would be a first step, as in the examples of Section 6. As we see below, we need F(I) to have 0 as the only member of E.

Say the map chosen to minimize the size of F(I) is $F = F_z$ with z in A^t. Then any expressible x can be written as $\sum_{j=0}^{k}(z-z_j')N^{tj}$ for some nonnegative integer k, with the same z as in the definition of F and with various $z_j{}'$ in A^t. We have a specific expression for an expressible number that can be computed using F, by keeping track of which numbers are subtracted in each application of F. Notice also that the same path through the trees of any two expressible numbers x and y will connect to 0. (It may be that the path for x connects to 0 earlier, but continuing to follow the z-path from 0 connects back to 0, so the paths in the trees of x and y can be chosen to be the same length). We call the expression obtained from this map F *the canonical expression defined by z.* (There are others of course, for other z also work). An example of this is provided below. Importantly, this gives us a simple programmable way to find an expression for an expressible number.

[Note: This is certainly not the only way to define such a programmable method. For example it is also possible to apply F_0 repeatedly to an expressible number until the result is in I and then follow with one final application of the map F discussed above. That this works is also due to Theorem 3.1.]

To get more perspective on what we are doing here, we review the initial set up of the problem. The set G is either $\mathbb{Z}$ (the real integers case) or $\mathbb{Z}$[i] (the complex integers case). Consider the system (A,N) where N of modulus greater than 1 is in G and A is a set of representatives of the classes modulo N. Let B = A–A. Let E be the set of all integers that are expressible using B, i.e. all integers that can be written in the form $\sum_{j=0}^{k-1} b_j N^j$ with b_j in B and k some positive integer. *We will consider E to be not only the set of expressible numbers x, but also all the different expressions those x may have.* Note for convenience we may replace A by A-a with a in A. Of course (A-a)–(A-a) = B is unchanged, as is E, both in its members and their expressions. We do this so we can assume the new A contains 0 and is thus a subset of B.

If all numbers are expressible, i.e. E = G, we say (A,N) is a *Just Touching Covering System.* But if each member of G has an expression (necessarily unique) using only coefficients in A, we say (A,N) is a *Number System.* In expressing numbers using just A there is no tree, and there is only one map to consider: F_A, mapping x to (x-a)/N for the appropriate a in A. A number x is expressible in A-coefficients if $F_A{}^k(x) = 0$ for some positive integer k.

For t a positive integer, let A^t be the set of all $\sum_{j=0}^{t-1} a_j N^j$ with a_j in A. This A^t is a set of representatives of all the congruence classes modulo N^t. Then

we can consider the system (A^t,N^t) and $\widetilde{B} = A^t - A^t$. The same set E for (A,N), *including all its expressions*, can also be seen as the set of all numbers in the form $\sum_{j=0}^{k-1} b_j (N^t)^j$ with b_j in $\widetilde{B}$ and k any positive integer. (We are just grouping the expressions into strings of length t, but the expressions are not changing, only the way they are viewed. If you replace members of $A^t - A^t$ by their original strings of length t with coefficients in A–A, the expressions are identical to those for the original system (A,N).) For any z in A^t, we can also consider the system $(\widetilde{A}, \widetilde{N})$ where $\widetilde{A}$ = z - A^t and $\widetilde{N} = N^t$. Here $\widetilde{A}$ is still a set of representatives of the classes modulo $\widetilde{N}$, $\widetilde{A} - \widetilde{A}$ is the same $\widetilde{B}$, and the set E is unchanged, both in its members and their expressions. Since 0 is still a member of $\widetilde{A}$, we have that $\widetilde{A}$ is a subset of $\widetilde{B}$. If we define $\widetilde{A}$ = z - A^t using the z that came from the choice of F_z for the canonical expression defined above, then each member of E has, as one of its expressions, an expression in the form $\sum_{j=0}^{k-1} a_j \widetilde{N}^j$ for some positive integer k with a_j in $\widetilde{A}$. This is the canonical expression for a member of E given by z. Consider the map $F_{\widetilde{A}}$ given by $F_{\widetilde{A}}$ (x) = (x-a)/ $\widetilde{N}$ where a is the unique member of $\widetilde{A}$ for which the result is integral. Note $F_{\widetilde{A}}$ is the same map as F_z for the original system (A,N) and the special z as chosen above. The canonical expression for a member of E can be found simply by applying the map $F_{\widetilde{A}}$ repeatedly until the result is 0, and observing which members of $\widetilde{A}$ were subtracted along the way.

In the case where E is the entire set of integers, as mentioned above, we have a nice vocabulary for what we are doing. If E is the set of expressible numbers using coefficients in B for a system (A,N), then, since E contains all integers, we say (A,N) is a Just Touching Covering System. This result says that there is another system $(\widetilde{A}, \widetilde{N})$ for which it is also true that all integers are in the E for this system (i.e. expressible using $\widetilde{A} - \widetilde{A}$ coefficients) and such that all the expressions using $\widetilde{A} - \widetilde{A}$ coefficients are identical to those of the original system using A–A (though terms of the expression are grouped together in strings of length t). But importantly the latter system $(\widetilde{A}, \widetilde{N})$ is also a Number System: one of the expressions for each x uses only coefficients in $\widetilde{A}$. Thus every Just Touching Covering System provides a Number System by an appropriate replacement of A by $\widetilde{A}$ = z-A^t. Again, that this works is due to the fact that all expressible numbers are omniexpressible. We can say the Number System is an equivalent replacement for the original Just Touching Covering System in that it produces all the same expressions including the canonical one given by $F_{\widetilde{A}}$. We summarize these observations as a theorem:

Theorem 7.1. *Let G be either the set of integers $\mathbb{Z}$ or the set of Gaussian integers $\mathbb{Z}[i]$. Consider a system (A,N) for G. In the Gaussian integer setting assume also there exists an omniexpressible number other than 0, or in the case of N having imaginary part equal to 0, assume there are two omniexpressible numbers, independent as vectors in $\mathbb{R}^2$. Let B = A–A. Let E be the set of*

all integers that are expressible using B, i.e. all integers that can be written in the form $\sum_{j=0}^{k-1} b_j N^j$ *with* b_j *in B and k any positive integer. Consider E to be not just the expressible numbers but all the expressions those numbers have in this form. Then there is a system* $(\widetilde{A}, \widetilde{N})$ *for which the associated E is identical in that the same numbers are expressible, and all the expressions using* $\widetilde{A} - \widetilde{A}$ *are essentially the same as those using A–A coefficients. However, any expressible number in E has one expression where the coefficients all lie in* $\widetilde{A}$*. (Whereas it may not be true that there is such an expression with all coefficients in A.) In the special case where E = G, i.e. all numbers are expressible, then we can say that while (A,N) is a Just Touching Covering System, there is a* Number System *(*$\widetilde{A}, \widetilde{N}$*) for which all* $\widetilde{A} - \widetilde{A}$ *coefficient expressions of a number are essentially the same as the A–A coefficient expressions that come from the system (A,N).*

7.1. Illustration 3

Here is a simple illustration of this idea. Consider the real case of N= 3 and A = {0, 4, 2}. Here B= {-4, -2, 0, 2, 4} and it is obvious E consists of all the even integers. The interval I = [-2,2] ∩ ℤ. If you consider z in A^2 where z = 6 = 0 + 2(3^1) and the map F= F_z, then F({-2, -1, 0, 1, 2}) = {0, 1} which is obviously minimal since 1 is inexpressible.

[The computations are as follows:

A^2 = 3A+A ={0, 2, 4, 6, 8, 10, 12, 14, 16} and F(-2) = (-2 - 6 + 8)/9 = 0, F(-1) = (-1 - 6+16)/9 = 1, F(0) = (0 − 6 +6)/9 = 0, F(1) = (1 - 6+14)/9 = 1, F(2) = (2 - 6 + 4)/9 = 0.]

Then choosing $\widetilde{A}$ to be z-A^2 = {6, 4, 2, 0, -2, -4, -6, -8, -1} for $\widetilde{N}$ =9, we have every even integer expressible as a sum of powers of 9 with unique coefficients in $\widetilde{A}$. These are the repeated applications of $F_{\widetilde{A}}$ to find an expression for 100, where $F_{\widetilde{A}}$(x) = (x-a)/9 with a the unique member of $\widetilde{A}$ that results in an integer:

100 → (100 − -8)/9 = 12→ (12 − -6)/9 = 2 → (2 − 2)/9 = 0

Or the same map viewed as F_6 for the original (A,3) system using A^2:

100 → (100 − 6+14)/9 = 12→ (12 − 6+12)/9 = 2 → (2 − 6+4)/9 = 0

Tracking which numbers were subtracted, this gives the expression in $\widetilde{A}$ to be 100 = -8 + (-6)9 + (2)9^2 or, in the F_6 version, 100 =(6-14)+(6-12)9+(6-4)9^2.

The latter expresssion can be expanded to see the expression it corresponds to in the original B= A–A. Subtracting the expansions of the A^2 terms involved (6 = 0 + 2(3^1), 14 = 2 + 4(3^1), 12 = 0 + 4(3^1), and 4 = 4 + 0(3^1)) we get:

100 = (0-2)+(2-4)3^1+(0-0)3^2+(2-4)3^3+(0-4)3^4+(2-0)3^5.

This is the canonical expression for z with z = 6 = 0 + 2(3^1). The repeated F_0 and F_2 steps are highlighted above in red.

Secondly, to illustrate that the same z-paths lead to 0 in the trees of any two expressible numbers, we compare the expression for 1000 to the expression for 100 above. The expression for 1000 using the F_6 map repeatedly is:

1000 →(1000 − 6+14)/9 =112→(112 − 6+2)/9 =12 → (12 − 6+12)/9 =2→ (2 − 6+4)/9 =0.

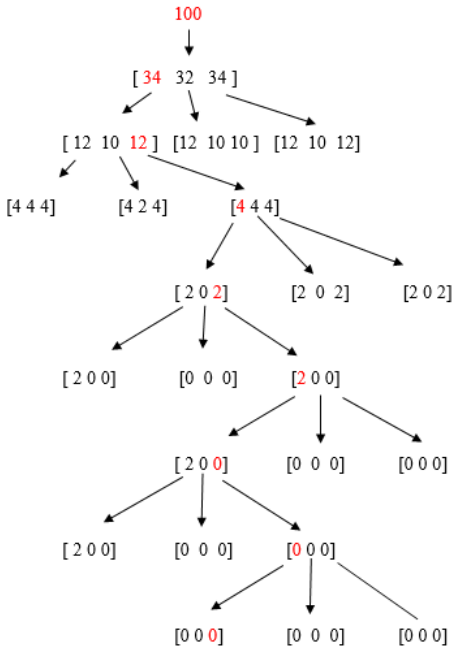
By observing which numbers were subtracted at each stage, we see that 1000 has expression:

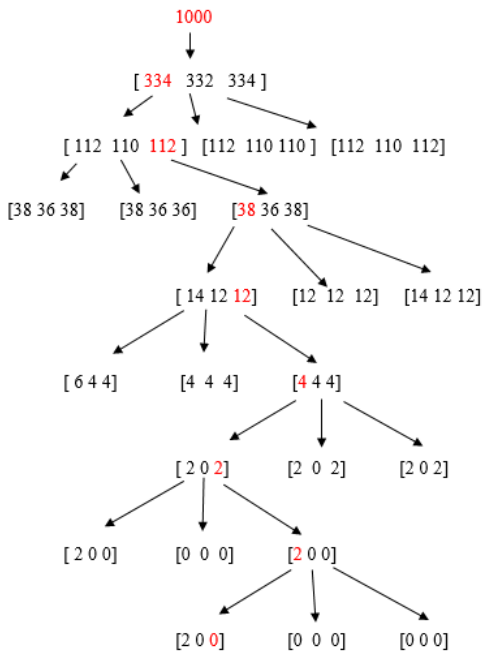
1000 = (6-14)+(6-2)9+(6-12)9^2+(6-4)9^3

Compare this to the following, where F_6 has been applied a fourth time in the computation for 100 above to make the expressions the same length:

100 = (6-14)+(6-12)9+(6-4)9^2+(6-6)9^3

These expressions represent the same paths in the tree of 100 and 1000: Still with N = 3 and A = {a_0, a_1, a_2} = {0, 4, 2}, the maps to create the tree will be given in this order from left to right: F_0(x) = (x-0+a)/3 and F_4(x) = (x-4+a')/3 and F_2(x) = (x-2+a'')/3 where {a, a', a''} are the unique members of A that give integral descendants for x. Since 6 = 0+2·3^1, F_6 is given as $F_2 \circ F_0$, namely, of the three paths from a number x, this says follow the leftmost path (F_0) to the first generation, then the rightmost path (F_2) to the next generation in the original B-tree. Repeating this two-step route leads to 0 as a descendant in all trees of expressible numbers. For example, below we show the relevant parts of the trees for 100 and 1000 where a number is connected to its three first-generation descendants by a single arrow to prevent overcrowding. We alternate choosing the leftmost of the three descendants with the rightmost, giving the expressions above in the original B. The route is shown in red.


100
[34 32 34]
[12 10 12] [12 10 10] [12 10 12]
[4 4 4] [4 2 4] [4 4 4]
[2 0 2] [2 0 2] [2 0 2]
[2 0 0] [0 0 0] [2 0 0]
[2 0 0] [0 0 0] [0 0 0]
[2 0 0] [0 0 0] [0 0 0]
[0 0 0] [0 0 0] [0 0 0]


1000
[334 332 334]
[112 110 112] [112 110 110] [112 110 112]
[38 36 38] [38 36 36] [38 36 38]
[14 12 12] [12 12 12] [14 12 12]
[6 4 4] [4 4 4] [4 4 4]
[2 0 2] [2 0 2] [2 0 2]
[2 0 0] [0 0 0] [2 0 0]
[2 0 0] [0 0 0] [0 0 0]

To recap the results in this paper we have shown:

Theorem 7.2. *Let the additive group G be either $\mathbb{Z}$ or $\mathbb{Z}[i]$. Let E be the set of all numbers expressible in $B = A - A$. In the real case, E is the smallest subgroup of G containing B that is closed under multiplication by N, and all members of E are omniexpressible. In the complex case, if there exists a nonzero omniexpressible number or, in a case with Im(N) = 0, if there exist two independent omniexpressible numbers, then the same conclusion holds: E is the smallest subgroup of G containing B that is closed under multiplication by N, and all members of E are omniexpressible.*

Notes: In the complex case, it is conjectured that the required omniexpressible numbers always exist and E is always as described. In examples above we used the theorem to find E in cases where the conjectured conditions were shown to hold. In both cases, if A is shifted to contain 0 so that A is a subset of B, we can also say E is the smallest subgroup of G containing A that is closed under multiplication by N. In the real case the group E is specifically the set of all multiples of gcd(B) = gcd(A). Finally, the fact that all expressible numbers are omniexpressible leads to a specific programmable way to find an expression for an expressible number. If E is equal to the entire set G, this is essentially a way of replacing the Just Touching Covering System by an "equivalent" Number System.

References

[1] **Indlekofer, K.-H., I. Kátai, and P. Racskó,** Number systems and fractal geometry, in: Galambos, János and Kátai, Imre (Eds.) *Probability Theory and Applications: Essays to the Memory of József Mogyoródi* Springer Netherlands, Dordrecht, 1992, 319–334.

[2] **Indlekofer, K.-H., I. Kátai, and P. Racskó,** Some remarks on generalized number systems, *Acta Sci. Math., Szeged*, **57** (1993), 543–553.

[3] **Kátai, I.,** *Generalized Number Systems and Fractal Geometry*, Monograph, Janus Pannonius University, Pécs, Hungary, 1995.

[4] **Michalek, G.,** Base three just touching covering systems, *Publ. Math. Debrecen*, **51(3-4)** (1997), 241–263.

[5] **Michalek, G.,** Base N just touching covering systems, *Publ. Math. Debrecen*, **58** (2001), 549–557.

G. Michalek
La Salle University (retired)
Philadelphia
USA
garyemichalek@gmail.com