MONOTONIC AND BLOCK NUMBERS AND THE EXISTENCE OF DISCRETE LOGARITHMS

R. Blecksmith*, M. Filaseta**, and C. Nicol

Dedicated to Heini Halberstam, on the occasion of his retirement.

1. Introduction

Let $\mathcal{M}$ denote the set of all positive integers m such that the digits of m weakly increase when read left to right and let $\mathcal{B}$ denote the set of all positive integers m such that if two digits of m are the same, say d, then every intermediate digit between these two digits is also d. Elements of the first set we call *monotonic* and elements of the second set we call *block*. The number 22377789, for example, is a monotonic and hence a block number, whereas 32245 is a block number but is not monotonic. The digits in these examples and throughout this introduction are *decimal* digits; however, obvious extensions of these definitions to other bases exist and will be used in subsequent sections. The purpose of this paper is to discuss various results about monotonic and block numbers, as well as to describe a general algorithm for determining the existence of certain discrete logarithms, an essential tool for investigating divisibility properties of monotonic (and block) numbers.

Monotonic numbers were first introduced in [1], where we found infinite classes of monotonic numbers base b whose products are monotonic, as long as the base is not one more than a prime. (See [1, Monontonic Product Theorem].) In this paper we investigate the question of which positive integers m have monotonic or block multiples. If $m = 2^r \cdot 5^s \cdot m'$, where m' is relatively prime to 10 and r and s are non-negative integers, then $10^{\max\{r,s\}}(10^{k\phi(9m')} - 1)/9$ is a multiple of m consisting of a string of 1's followed by a (possibly empty) string of 0's. This shows that every positive integer has a block multiple. Moreover, if m is relatively prime to 10, so that $r = s = 0$, then m has infinitely many multiples all of whose digits are 1. If 10 divides m, then 10 divides every multiple of m, so that no monotonic multiples of m exist. For monotonic multiples, therefore, it remains to consider positive integers m which are divisible by 2 or 5, but not 10. Although all such m have block multiples, it is still unclear whether they have block multiples which do not end in the digit 0 or whether they have block multiples which do not contain the digit 0 at all. In order to deal with these last two questions, we consider the subsets $\mathcal{B}_0$ and $\mathcal{B}_1$ of $\mathcal{B}$, where $\mathcal{B}_0$ is the set of block numbers not ending in the digit 0 and $\mathcal{B}_1$ is the set of block numbers not containing the digit 0.

We observed early on that the number $5^4 = 625$ did not divide any monotonic number. The argument is not difficult and will be discussed, along with similar results, in the next section. This example gave the above questions some substance since we then knew that there existed numbers not divisible by 10 which had no monotonic multiples. This also suggested that perhaps there was a power of 2 which had no monotonic multiples. Our first proof of this conjecture was a computational one involving a search tree. Later a theoretical proof was obtained which implied analogous results for block numbers. Further computations led to the following result:

Theorem 1. *The numbers 5^4 and 2^{22} do not divide any monotonic numbers. The numbers 5^{13} and 2^{53} do not divide any block numbers not ending in 0. The numbers 5^{13} and 2^{51} do not divide any block numbers not containing the digit 0.*

*Research was supported in part by the NSF under grant number DMF-8902258.
**Research was supported in part by the NSF under grant number DMS-8903123.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

The exponents above are best possible. In Section 2, we first prove the existence of such exponents. We obtain Theorem 1 from a more general result (Theorem 3) for an arbitrary base. We then discuss the computations leading to the actual exponents given in Theorem 1.

Now, we had partial anwers to our queries mentioned above. In fact, we had infinitely many examples at our disposal. We knew, for example, that not just 625 but any multiple of 625 did not have a monotonic multiple. Other examples were to come. A side comment in Section 4 (see Example 4) shows that 1616 has no monotonic multiples, and this example does not follow, at least directly, from Theorem 1.

We do not attempt to tabulate "all" numbers without monotonic multiples. The task seems tedious and difficult, and the analogous problem for block numbers is, we believe, out of computational range. However, we will demonstrate in Section 4 that although there are infinitely many positive integers without monotonic multiples, we have the following:

Theorem 2. *There are only a finite number of monotonic numbers m which do not have a monotonic multiple $> m$. There are only a finite number of block numbers m not ending with the digit 0 which do not have a block multiple $> m$.*

Although the second sentence in Theorem 2 implies the first, we state them both since our interests in Section 4 are more associated with monotonic numbers. We show in Section 4 how Theorem 2 is actually a consequence of Theorem 1. We also discuss some computations which lead to a complete list of the monotonic numbers referred to in Theorem 2—there are exactly 13 of them. The computations became quite involved, and we expect that listing the block numbers referred to in Theorem 2 is a non-trivial task. In particular, we found ourselves needing to establish whether, for certain choices of the integers a, b, and n, the congruence $a^x \equiv b \pmod{n}$ has solutions. One such congruence is

$$10^x \equiv -8 \pmod{212987265163}.$$

For the case in which n is prime, determining whether such congruences have solutions is easy. In the above example, $n = 212987265163 = 109 \cdot 787 \cdot 2482861$, and so the problem becomes a bit more difficult (especially since one can readily determine that solutions to the congruence exist if the modulus is restricted to any one of $109, 787$, or 2482861). We discuss an algorithm in Section 3 which determines whether discrete logarithms exist for a composite modulus. The algorithm is based on factoring n and on factoring $p-1$ for each prime factor p of n. The remainder of the algorithm can be shown heuristically to almost always run in polynomial time. The algorithm enabled us to complete the finite list of monotonic numbers, advertised in Theorem 2, which have no monotonic multiples bigger than themselves.

Section 5 contains a summary of other results, conjectures, and open questions about monotonic and block numbers.

2. The Proof of Theorem 1

For convenience, we introduce the notation (k) in a superscript to denote a string of k digits each equal to the digit before the superscript. Thus, $16^{(5)}78$ represents the monotonic number 16666678. Define the *number of blocks* base b for a positive integer m to be the smallest positive integer r for which we may represent m in the form $m = d_r^{(k_r)} d_{r-1}^{(k_{r-1})} \dots d_1^{(k_1)}$, where for each $j \in \{1, 2, \dots, r\}$, d_j is a digit base b (i.e., $d_j \in \{0, 1, \dots, b-1\}$) and k_j is a positive integer. If no reference is given to a base, then we will understand that the base is 10. For example, 8037776589 has 8 blocks. We begin by considering a version of Theorem 1 in which the exponents of 5 and 2 are not specified. For this purpose, it suffices to show that there is a positive integer r such that there are no block numbers not ending in the digit 0 which are divisible by 5^r or 2^r. We are able to show something stronger, namely that as r tends to infinity, the minimal number of blocks of a multiple of 5^r or 2^r, which does not end in 0, tends to infinity. This is an immediate consequence of

Theorem 3. *Let b be an integer which is not a prime power and let p be a prime divisor of b. Then as r tends to infinity through the positive integers, the minimum number of blocks base b of a multiple of p^r not ending in the digit 0 base b also tends to infinity.*

The elementary proof, which appears in [2, pp. 338-9], is an existence argument and does not aid in estimating the precise exponents given in Theorem 1. A modified proof can be given which produces bounds for such exponents, but the bounds we obtained from such a proof were poor and of no help in obtaining the exponents in Theorem 1.

To prove Theorem 1 with the specific exponents given, a different approach was used. The results concerning powers of 5 actually can be verified in a direct manner. To prove that 5^{13} does not divide any $m \in \mathcal{B}_0$, we begin by writing m in the form $10^{13}q + r$, where q and r are non-negative integers with $r < 10^{13}$. It is not difficult to establish that there is an $m \in \mathcal{B}_0$ which is divisible by 5^{13} if and only if there is an $r \in \mathcal{B}_0$ with ≤ 13 digits which is divisible by 5^{13}. Thus, we need only check the $2^{12} = 4096$ odd multiples of 5^{13} which are $\leq 10^{13}$. None of these are in $\mathcal{B}_0$, and the desired result follows. A similar argument works to show that 5^4 does not divide any monotonic numbers and 5^{13} does not divide any numbers in $\mathcal{B}_1$. The latter is, of course, a consequence of the $\mathcal{B}_0$ result, since $\mathcal{B}_1 \subseteq \mathcal{B}_0$.

As mentioned in the introduction, these exponents are best possible. In fact, one can show that 5^3 divides a monotonic number m if and only if $m = 1^{(k)}25$ where k is a positive integer, that 5^{12} divides an $m \in \mathcal{B}_0$ if and only if m is a block number ending in 336669921875 or 663330078125, and that 5^{12} divides an $m \in \mathcal{B}_1$ if and only if m is a block number not containing the digit 0 and ending in 336669921875.

The results in Theorem 1 involving powers of 2 are more complicated. An argument as above shows, for example, that for block numbers not ending in the digit 0, we need to consider the multiples of 2^{53} not ending in 0 which have ≤ 53 digits. There are $4 \cdot 5^{52}$ such multiples, and this is much too large for the computational approach suggested above. To complicate matters further, keep in mind that initially the exponent 53 was unknown to us. To obtain our results in this case, we construct four search trees as follows. For each successive positive integer k, we construct every block number not ending in 0 with $\leq k$ digits which is divisible by 2^k. Theorem 3 implies that eventually this process must stop; in other words, for k sufficiently large, there will be no block numbers not ending in 0 which are divisible by 2^k. Note that once we obtain a k for which no $m \in \mathcal{B}_0$ with $\leq k$ digits is divisible by 2^k, we needn't consider larger values of k for they too will have this property. We begin with $k = 1$ and find that 2, 4, 6, and 8 are the numbers in $\mathcal{B}_0$ with ≤ 1 digits which are divisible by 2. The four numbers 2, 4, 6, and 8 each begin a search tree. When we pass to the case $k = 2$, each block number considered must end in one of these four digits. Thus, 2 (in the case $k = 1$) branches to 12, 32, 52, 72, and 92 (in the case $k = 2$), while 4 (in the case $k = 1$) branches to 04, 24, 44, 64, and 84 (in the case $k = 2$). Each of the numbers in the case $k = 2$ then branches to numbers in the case $k = 3$. For example, 32 branches to 032, 432, 632, and 832. Note that 232 is not a block number and, hence, does not appear in this list. In branching from the k digit number m, we attach an *odd* digit in front of m if 2^k exactly divides m, otherwise we attach an *even* digit. In either case, we do *not* attach any digit used in a previous block of m. The authors repeated this process as long as we encountered block numbers divisible by 2^k. The program was encoded in Pascal and ran for about an hour on an IBM AT compatible personal computer. There were a total of 14358898 vertices. The largest power of 2 dividing the number corresponding to each vertex was checked, and, thus, it was established that 2^{53} does not divide m for every $m \in \mathcal{B}_0$. A similar computation was done to show that 2^{22} does not divide any monotonic numbers and 2^{51} does not divide any numbers in $\mathcal{B}_1$. The only monotonic numbers divisible by 2^{21} are 112222333344677888 and 122233333345555557888; the only numbers in $\mathcal{B}_0$ divisible by 2^{52} are $3^{(9)}7^{(16)}0049^{(6)}6^{(11)}88512$ and $76^{(9)}2^{(16)}9950^{(6)}3^{(11)}11488$; and the only number in $\mathcal{B}_1$ divisible by 2^{50} is $7^{(9)}2^{(15)}4^{(6)}3^{(7)}9^{(3)}5116^{(4)}88$. Observe that these last numbers form finite lists whereas the analogous numbers for powers of 5 mentioned above form infinite lists. There are only two monotonic numbers divisible by 2^{21}, but there are infinitely many monotonic numbers divisible by 5^3. It can be shown that finite lists always occur with powers of 2 in the analogous problem for a base $b \equiv 2 \pmod 4$. More specifically, if k is the smallest positive integer such that 2^k does not divide any monotonic numbers in a given base b (with $b \equiv 2 \pmod 2$), then only finitely many monotonic numbers base b are divisible by 2^{k-1}. We do not know the general situation for powers of primes different from 2. Finally, it is interesting to note that our computations produced the number $1122662^{(4)}5^{(10)}9^{(3)}744$, a block number not containing 0 which has only 26 digits but is divisible by 2^{45}.

3. The Existence of Discrete Logarithms

In this section we describe a general algorithm for determining whether the discrete logarithm base a of b exists modulo m. Equivalently, can we solve the exponential congruence

$$a^x \equiv b \pmod{m}, \tag{1}$$

where the modulus m is relatively prime to a? We need two lemmas.

Lemma 1. *Given integers a and b, let p be an odd prime such that p does not divide a and let e be a positive integer. Then the congruence $a^n \equiv b \pmod{p^e}$ has a solution in n if and only if $b^k \equiv 1 \pmod{p^e}$ where k is the order of a modulo p^e.*

Proof. Given the notation above, suppose first that there is an n such that $a^n \equiv b \pmod{p^e}$. Then clearly $b^k \equiv \left(a^k\right)^n \equiv 1 \pmod{p^e}$. Conversely, suppose that we know $b^k \equiv 1 \pmod{p^e}$. Then b is a root of the polynomial $f(x) = x^k - 1$ modulo p^e. We wish to prove that there is an integer n for which $a^n \equiv b \pmod{p^e}$. So we invesitigate the roots of $f(x)$ modulo p^e. Let g be a generator for the reduced residue system modulo p^e and let $w = \phi(p^e) = p^{e-1}(p-1)$. At most k of the numbers $1, g, g^2, \dots, g^{w-1}$ satisfy $f(x) = x^k - 1 \equiv 0 \pmod{p^e}$; otherwise, there exist integers u and v with $0 \le u < v \le w-1$ and $v - u < w/k$ such that $g^{uk} - 1 \equiv 0 \equiv g^{vk} - 1 \pmod{p^e}$, which implies that $g^{(v-u)k} \equiv 1 \pmod{p^e}$, contradicting that the order of g modulo p^e is $w > (v-u)k$. Thus, the polynomial $f(x)$ has at most k incongruent roots modulo p^e. By the definition of k, these roots are $1, a, a^2, \dots, a^{k-1}$. Since b is a root of $f(x)$, it follows that b is power of a modulo p^e. □

Lemma 2. *Let a and b be integers. Let $p_1^{e_1}$ and $p_2^{e_2}$ be distinct odd prime powers relatively prime to a such that for some integers n_1 and n_2 we have $a^{n_1} \equiv b \pmod{p_1^{e_1}}$ and $a^{n_2} \equiv b \pmod{p_2^{e_2}}$. Then the congruence $a^n \equiv b \pmod{p_1^{e_1}p_2^{e_2}}$ has a solution if and only if $n_1 \equiv n_2 \pmod{\gcd(k_1, k_2)}$ where k_1 is the order of a modulo $p_1^{e_1}$ and k_2 is the order of a modulo $p_2^{e_2}$.*

Proof. The conditions of the lemma imply that $a^n \equiv b \pmod{p_1^{e_1}p_2^{e_2}}$ has a solution if and only if a solution exists to the simultaneous congruences

$$n \equiv n_1 \pmod{k_1} \quad \text{and} \quad n \equiv n_2 \pmod{k_2}.$$

By the Chinese Remainder Theorem, this is equivalent to the statement of the lemma. □

We are now ready to describe an algorithm to check whether congruences of the form given in (1) have a solution. We begin with a somewhat weaker form of the algorithm.

Problem. *Given prime powers $p_1^{e_1}$ and $p_2^{e_2}$ and integers a and b with $e_1 > 0$, $e_2 > 0$, and $\gcd(a, p_1p_2) = 1$, determine whether*

$$a^x \equiv b \pmod{p_1^{e_1}p_2^{e_2}} \tag{2}$$

has a solution.

Algorithm. *[The existence of the discrete logarithm of b base a modulo $m = p_1^{e_1}p_2^{e_2}$.]*

1. Compute $A = \operatorname{ord}_{p_1^{e_1}}(a)$ and $B = \operatorname{ord}_{p_2^{e_2}}(a)$.

2. Check to see if $b^A \equiv 1 \pmod{p_1^{e_1}}$ and $b^B \equiv 1 \pmod{p_2^{e_2}}$. If either of these is not true, then stop; there is no solution to (2).

3. Compute $D = \gcd(A, B)$.

4. Factor D in the form $D = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$, where the q_j are distinct primes and the f_j are positive integers.

5. For $j = 1$ to s, consider $d_j = q_j^{f_j}$. Find $k_1, k_2 \in \{0, 1, \dots, d_j - 1\}$ satisfying

$$\left(b \cdot a^{-k_1}\right)^{A/d_j} \equiv 1 \pmod{p_1^{e_1}} \quad \text{and} \quad \left(b \cdot a^{-k_2}\right)^{B/d_j} \equiv 1 \pmod{p_2^{e_2}}.$$

Lemma 1 and Step 2 guarantee that k_1 and k_2 exist. If there is a j such that $k_1 \neq k_2$, then stop; there is no solution to (2). If for each j, we find that $k_1 = k_2$, then there is a solution to (2).

To explain why the algorithm works, Lemma 2 implies that we only need to see if $x \equiv y \pmod{D}$, where $D = \gcd(A, B)$ and x and y are the least positive integers satisfying

$$a^x \equiv b \pmod{p_1^{e_1}} \quad \text{and} \quad a^y \equiv b \pmod{p_2^{e_2}}.$$

We want to avoid having to compute the actual values of x and y. By the Chinese Remainder Theorem, in order to determine whether x and y are congruent modulo D, we need merely check to see if $x \equiv y \pmod{d_j}$ for each prime power divisor $d_j = q_j^{f_j}$ of D. In other words, we just want to know how to get the values of x and y modulo d_j. This is the purpose of k_1 and k_2 in Step 5. We only concern ourselves here with x since an analogous procedure works with y. The algorithm is justified by the following:

Claim. *For $d = d_j$, there is a unique $k \in \{0, 1, \dots, d - 1\}$ such that*

$$\left(b \cdot a^{-k}\right)^{A/d} \equiv 1 \pmod{p_1^{e_1}}. \tag{3}$$

Furthermore, $x \equiv k \pmod{d}$.

Proof. We know that

$$a^x \equiv b \pmod{p_1^{e_1}} \quad \text{and} \quad a^A \equiv 1 \pmod{p_1^{e_1}}.$$

Since d divides A, we can write $A = du$, where u is some positive integer. Let ℓ be the least non-negative integer such that $x \equiv \ell \pmod{d}$. Clearly, $\ell \in \{0, 1, \dots, d - 1\}$. Then $x = \ell + dv$ for some integer v. We have that

$$a^\ell a^{dv} = a^{\ell + dv} = a^x \equiv b \pmod{p_1^{e_1}}$$

so that

$$\left(b \cdot a^{-\ell}\right)^u \equiv \left(a^{dv}\right)^{A/d} \equiv \left(a^A\right)^v \equiv 1 \pmod{p_1^{e_1}}.$$

This proves most of the Claim. Next, we prove that the solution $k = \ell$ for (3) is unique.

Assume that $k \neq \ell$ and $k \in \{0, 1, \dots, d - 1\}$ is as in (3). Then since $a^x \equiv b \pmod{p_1^{e_1}}$, we get that

$$1 \equiv \left(b \cdot a^{-k}\right)^{A/d} \equiv \left(a^{x-k}\right)^u \equiv a^{(x-k)u} \pmod{p_1^{e_1}}.$$

Since $k \neq \ell$ and $x \equiv \ell \pmod{d}$, it follows that d does not divide $x - k$. Thus, $A = du$ does not divide $(x - k)u$. Since $A = \operatorname{ord}_{p_1^{e_1}}(a)$, this contradicts the above congruence, completing the proof. $\square$

Remark 1. If the congruence in (1) involves more than two primes, the stated algorithm seemingly does not apply. However, it is not difficult to check that the explanation of the algorithm following its statement above leads to a simple way to check for the existence of solutions to $a^x \equiv b \pmod{n}$ when $n = p_1^{e_1} \dots p_r^{e_r}$ with $r > 2$. One simply needs to apply the algorithm with the modulus $p_i^{e_i} p_j^{e_j}$ for every combination of i and j with $1 \leq i < j \leq r$. A solution to the congruence will exist modulo n if and only if a solution exists modulo every $p_i^{e_i} p_j^{e_j}$.

Remark 2. In the introduction, we made a comment about the running time of such an alogorithm. Basically, the algorithm runs quickly (after some initial factorizations) since D in this algorithm can usually be expected to be small. More specifically, we never encountered a $D > 20$. One explanation for this is that if one views the values of A and B as being random numbers $\le x = \max\{p_1^{e_1}, p_2^{e_2}\}$, then it is not too difficult to show that on average $\gcd(A,B)$ has order $\log x$. Another explanation can be given as follows. Fix $z \ge 1$. The number of A and B both $\le x$ which are both divisible by a given positive integer d is $[x/d]^2 \le x^2/d^2$, where $[\,]$ denotes the greatest integer function. Thus, the number of pairs $(A,B) \in (\mathbb{Z} \cap [1,x])^2$ with both A and B divisible by some $d \ge z$ is bounded above by

$$\sum_{d \ge z} \frac{x^2}{d^2} \le \frac{x^2}{z^2} + x^2 \int_z^{\infty} \frac{1}{t^2}\,dt \le \frac{2x^2}{z}.$$

This implies that there are $\le 2x^2/z$ pairs $(A,B) \in (\mathbb{Z} \cap [1,x])^2$ with $\gcd(A,B) \ge z$. Thus, we shouldn't expect that $\gcd(A,B)$ is of order greater than $\log\log x$ very often.

4. The Proof of Theorem 2 using Exponential Congruences

We begin by explaining how Theorem 2 can be viewed as a consequence of Theorem 1. We will only concern ourselves with monotonic numbers as the statement for block numbers is proved in essentially the same way. Let m be a monotonic number. It suffices to show that if m has ≥ 21 digits, then m has a monotonic multiple $> m$. Write $m = 2^r \cdot 5^s \cdot m'$, where m' is relatively prime to 10 and r and s are non-negative integers. Theorem 1 implies that $r \le 21$ and $s \le 3$. Consequently, $t = t(m) = \max\{r, s\}$ is ≤ 21. If m has t' digits and $t' \ge t$, then for every positive integer k, m divides $m + 10^{t'}(10^{k\phi(9m')} - 1)/9$, a monotonic number formed by attaching a string of 1's in front of m. Since this number is clearly $> m$, Theorem 2 (for monotonic numbers) follows.

For the remainder of this section, we concern ourselves with listing the monotonic numbers m which do not have a monotonic multiple $> m$. The above proof of Theorem 2 implies that m has $\le t(m) - 1$ digits. Note also that with r and s as above, either $r = 0$ or $s = 0$. Assume $r = 0$. Then $m \ge 5^s$, $s \le 3$, and $t(m) = s$ all imply that m has $\ge t(m)$ digits, giving a contradiction. Thus, $r \ge 1$ and $s = 0$. Hence, $t(m) = r$ and m has $\le r - 1$ digits. Recall that the set of vertices for the search trees described at the end of Section 2 corresponded to all the monotonic numbers divisible by 2^k with $\le k$ digits where k denotes an arbitrary positive integer. The monotonic m without monotonic multiples $> m$ form a subset of the numbers associated with these vertices. Therefore, from the search trees, we are able to determine all the elements of the set

$$\mathcal{S} = \{m : m \text{ is monotonic and } m \text{ has } \le t(m) - 1 \text{ digits}\}.$$

This gives us a relatively small set from which we can find all the desired monotonic numbers. In fact, $|\mathcal{S}| = 220$. Next, we go through each element m of $\mathcal{S}$ and determine whether it has a monotonic multiple greater than itself.

Some elementary arguments eliminate over a third of the elements in $\mathcal{S}$. If the number of digits in m is $t(m) - 1$ and the leading digit of m is ≥ 2, then we can attach a string of $\phi(9m')$ 2's in front of m, where $m = 2^{t(m)} \cdot m'$. This expanded number is divisible by m, since we gain an extra factor of 2 by using a string of 2's instead of 1's. For example, the 17 digit number 23333334555557888, which is exactly divisible by 2^{18}, can be handled this way. We can even allow the number of digits to be $t(m) - 2$ if the leading digit is ≥ 4. For example, 466688 is a six digit monotonic number divisible by 2^8. In this case, we prefix a leading string of 4's in front of the number. This simple attachment method finds monotonic multiples for 68 of the 220 numbers in $\mathcal{S}$. Looking at the right side of a monotonic number, we notice that a montonic number whose unit digit is ≤ 4 has an easily determined monotonic multiple, namely, its double. The eleven digit number 11122233344, divisible by 2^{12}, clearly divides the monotonic 22244466688. This "doubling rule" settles 8 more elements in $\mathcal{S}$, leaving exactly 144 numbers to consider. These numbers are listed in Table 1 at the end of this section. The table is broken into 3 categories: (I) the easy cases, (II) the medium difficult cases, and (III) the hard cases. Most of the cases in the first two categories were obtained by a direct search program on an IBM AT compatible computer. For the cases in category III, along with several of the more difficult cases in category II, we implemented the algorithm of Section 3 in Maple on a Sun workstation.

We state our results and give a few examples which demonstrate the procedures we used to complete Table 1. We found that exactly 13 monotonic numbers m do not have monotonic multiples $> m$. These numbers are (listed in order of the largest power of 2 dividing each number, in parenthesis next to the number, and then by size):

1.	55666688 (11)	8.	223346688 (20)
2.	1111666688 (12)	9.	11222555557888 (20)
3.	114455666688 (13)	10.	1122233444466688 (20)
4.	1123355557888 (15)	11.	111222333335666688 (20)
5.	111111134445568 (16)	12.	112222333344677888 (21)
6.	11133344677888 (17)	13.	122233333334555557888 (21)
7.	11223456677888 (17)		

The examples below fall into 2 categories: (i) those $m \in \mathcal{S}$ for which a monotonic multiple $> m$ exists, and (ii) those $m \in \mathcal{S}$ for which a monotonic multiple $> m$ does not exist. We deal with the examples for (i) first.

Example 1. [Case #142 in Table 1.] The number $m = 223333334555557888$ is in $\mathcal{S}$, and we describe how we showed that m has a monotonic multiple $> m$. First, observe that the prime factorization of m is given by

$$m = 2^{20} \cdot 212987265163 = 2^{20} \cdot 109 \cdot 787 \cdot 2482861.$$

Checking the search trees of Section 2 we find that the only monotonic numbers $> m$ which are divisible by 2^{20} are of the form $1^{(n)}2^{(1)}0^{(18)} + m$, and furthermore, any such monotonic number is divisible by 2^{20}. Hence, in order for m to have a monotonic multiple $> m$, it is necessary and sufficient that there exists a non-negative integer n such that

$$1^{(n)}2^{(1)}0^{(18)} \equiv 1^{(n)}2^{(1)}0^{(18)} + m \equiv 0 \pmod{212987265163}. \tag{4}$$

Since

$$1^{(n)}2^{(1)}0^{(18)} = \frac{10^n - 1}{9}10^{19} + 2 \cdot 10^{18},$$

the congruence in (4) reduces to

$$10^{n+19} \equiv -18 \cdot 10^{18} + 10^{19} \equiv -8 \cdot 10^{18} \pmod{9 \cdot 212987265163}.$$

To simplify the above congruence, we use that 10 is relatively prime to the modulus so that we can divide by 10^{18} on both sides of the congruence. It is easy to see that for any integer n, we have that $10^{n+1} \equiv -8 \pmod 9$. Thus, we wish to determine if there is a solution to the congruence

$$10^x \equiv -8 \pmod{212987265163}. \tag{5}$$

This is the congruence mentioned in the introduction. By Remark 1 at the end of Section 2, in order to use the algorithm in Section 2 to determine whether there is an integer x satisfying (5), we consider the prime divisors of the modulus, namely 109, 787, and 2482861, two at a time. Applying the algorithm for each pair, we discover that a solution to congruence (5) exists.

We make three further observations before finishing this example. First, in this example we made use of the above algorithm merely to describe how we can deal with a large number of the elements in $\mathcal{S}$. For this particular example, one needn't make use of the algorithm, and in general, if the modulus has only one relatively large prime factor, one can get away with simply using Lemma 1. In this case, one can easily find that $10^9 \equiv -8 \pmod{109}$ and $10^{126} \equiv -8 \pmod{787}$. The orders of 10 modulo 109 and 787 are 108 and 393 respectively. Using the Chinese Remainder Theorem, we get that $10^x \equiv -8 \pmod{109 \cdot 787}$ if and only if $x = 1305 + 14148\ell$ for some integer ℓ. We multiply both sides of (5) by 10^{-1305}. Observe that $10^{-1305} \equiv 625208 \pmod{2482861}$ and $10^{14148} \equiv 2242218 \pmod{2482861}$. One easily gets that (5) has a solution if and only if there is an integer ℓ such that

$$2242218^{\ell} \equiv -8 \cdot 625208 \equiv 2446919 \pmod{2482861}.$$

Now, one simply uses Lemma 1 with $a = 2242218$ and $p = 2482861$.

Secondly, we note that with a bit more work Lemma 1 or the algorithm can often aid in actually solving a congruence such as (5). Thus, we were able to show that $\ell = 106172$ and hence the smallest monotonic multiple of $m = 223333334555557888$ greater than itself is a number with over one and a half billion digits, namely $1^{(1502122760)}2^{(3)}3^{(6)}45^{(5)}78^{(3)}$.

Finally, we note that in all the cases in which we made use of the algorithm, the only prime which appeared in the modulus raised to a power > 1 was 3. Thus, it is worth observing that the order of 10 modulo 3^{r+1} is 3^{r-1} for every positive integer r, a fact which is easily established by elementary considerations.

Example 2. [Case #137 in Table 1.] We now set $m = 111333334555557888 = 2^{19} \cdot 3 \cdot 33997 \cdot 2082061$ which is in $\mathcal{S}$, and we describe how we showed that m has a monotonic multiple $> m$. In the previous example, it was only necessary to consider multiples of the form $1^{(n)}2^{(3)}3^{(6)}45^{(5)}78^{(3)}$; in this case, one can readily use the algorithm as described above to show that m has no multiples of this form. However, by considering numbers of the more general form $1^{(n)}2^{(k)}3^{(6)}45^{(5)}78^{(3)}$, one does arrive at a monotonic multiple of m greater than itself. We simply used the above algorithm as in the previous example successively with $k = 1, 2, \ldots$ until we found a value of k which gave rise to an n leading to a multiple of m. The smallest such k was 81 and the smallest such n given that $k = 81$ was 2629434378.

We note that whenever we investigated an element in $\mathcal{S}$ which was large and had a monotonic multiple greater than itself, the multiple had the form $1^{(n)}2^{(k)}3^{(6)}45^{(5)}78^{(3)}$. In particular, this was true of every element of $\mathcal{S}$ divisible by 2^{16}, except case #126. On the other hand, this example does not explain how we knew when to stop checking values of k when we encountered an element of $\mathcal{S}$ which had no monotonic multiples of the form $1^{(n)}2^{(k)}3^{(6)}45^{(5)}78^{(3)}$. Since a priori we did not know such an element had this property, we needed some mechanism for stopping such a search. We did nothing elegant here; we simply stopped searching for k when we had checked up to $k = 500$. The largest k we encountered was 335 (see Case #131 in Table 1.) If we could not determine such a multiple with $k \le 500$, we tried other forms; and if they also failed in producing multiples, we then simply sought to establish that no monotonic multiples exist, using k-trees as discussed below in Example 4.

Example 3. [Case #110 in Table 1.] The number $1122455666688 = 2^{14} \cdot 3 \cdot 97 \cdot 311 \cdot 757 \in \mathcal{S}$ gave us more trouble than most. To aid anyone wishing to verify our results, we simply note that using the algorithm, it is possible to show that 1122455666688 has a multiple of the form $1^{(n)}2^{(1757)}3^{(16)}45^{(5)}78^{(3)}$.

Example 4. [Case #80 in Table 1.] We now set $m = 1111666688 = 2^{12} \cdot 11^2 \cdot 2243 \in \mathcal{S}$. We show that m has no monotonic multiples $> m$. To do this, we introduce the notion of k-trees where k is relatively prime to 10. The vertices of the k-trees help to form a description of the monotonic numbers which are divisible by k. We begin by describing how we construct $k-$trees. First, one finds the smallest number of the form $1^{(n)}$ which is divisible by k. Then one begins with 0 or a monotonic multiple of k which is $< 1^{(n)}$, constructing one tree for each such number. Subsequent numbers are formed by successively adding numbers of the form $1^{(n)} \times 10^j$ (where j weakly increases as one proceeds). The exponent j is increased in such a way as to keep all the numbers considered monotonic. A vertex of such a tree is formed each time one encounters a number m with its final r digits distinct from the final r digits of all previous vertices, where r is defined to be the largest positive integer for which m is divisible by 2^r. As a simple example, consider the number $k = 101$. Here, $n = 4$, and there are no monotonic multiples of 101 which are < 1111. Hence, we begin with 0, which branches to the four vertices 2222, 4444, 6666, and 8888. There four vertices, together with 0, form the complete set of vertices for the 101-tree. There is a simple method for testing to see if a monotonic number m is divisible by 101; just subtract numbers of the form $1111 \cdot 10^j$ from the left-most digits of m. For example, if $m = 1122223444$, one first subtracts $1111 \cdot 10^6$ from m to get the number 11223444. Since 101 divides 1111, we see that m is divisible by 101 if and only if 11223444 is divisible by 101. Continuing in this manner we obtain successively 113444, 2344, 1233, and 122. We stop here as we now have a number which is < 1111. Since 122 is not divisible by 101, neither is m. Note that each time we do a subtraction and obtain a new number, the new number is monotonic. If we reverse the steps, we find ourselves beginning with a number < 1111 and adding numbers of the form $1111 \cdot 10^j$. This is precisely how we constructed our tree (beginning with 0 or monotnic multiples of m). It is easy to see from the 101-tree then that every monotonic multiple of 101 must end in 2222, 4444, 6666, or 8888. Since every such number is not divisible by 16, we get that $1616 = 16 \cdot 101$ has no monotonic multiples, as mentioned in the introduction.

For the purposes of this example, we use the 11-trees. Here, $n = 2$, and there is only one 11-tree and it begins with 0. The 11-tree, pictured below, is more complicated than the 101-tree described above, with its five vertices. Branching happens in two ways: (1) when we increase the leading digits of m or (2) when we append digits in front of m. The tree is given in Figure 1. A vertex obtained by increasing the leading digits of m is drawn immediately below node m. Branching to a new number obtained by appending digits in front of m is indicated by using an arrow and placing the new number to the right of the arrow. The value of the largest power of 2 dividing each number in the tree is placed between parentheses to the immediate right of the number. Note that we cannot extend a vertex m to the right if the number in parenthesis is $<$ the number of digits of m.

0 (∞)				
22 (1)				
44 (2) $\to$	1144 (3)			
	3344 (4) $\to$	113344 (6) $\to$	11113344 (7)	
66 (1)		333344 (5)		
88 (3) $\to$	2288 (4) $\to$	112288 (5)		
	4488 (3)			
	6688 (5) $\to$	226688 (7) $\to$	22226688 (8) $\to$	1122226688 (9)
	8888 (3)	446688 (5)		
		666688 (6) $\to$	11666688 (8) $\to$	1111666688 (12) $\to$ 111111666688 (10)
			33666688 (7)	
			55666688 (10) $\to$	2255666688 (9)
				4455666688 (10) $\to$ 114455666688 (13)
				334455666688 (11)

Figure 1. The 11-Tree

The tree reveals some interesting information about monotonic numbers divisible by 11. First, it should be observed that there are no monotonic numbers divisible by $2^{14} \cdot 11$ and 114455666688 is the only monotonic number divisible by $2^{13} \cdot 11$. This does not help with the present case of $m = 1111666688$. But Figure 1 also shows that the only monotonic numbers $> m$ which are divisible by $2^{12} \cdot 11$ are of the form $1^{(2n)}4^{(2)}5^{(2)}6^{(4)}8^{(2)}$ where n is a postive integer. Thus, to show that m has no monotonic multiple $> m$ it suffices to show that no number of this form can be divisible by 2243. Letting $x = 2n + 10$, it is easy to check that it suffices to establish that the congruence

$$10^x \equiv -9 \cdot (4455666688) + 10^{10} \equiv 1490 \pmod{2243}$$

has no solution. This can be done by using Lemma 1 or by noting that 10 is a quadratic residue modulo 2243 and 1490 is not.

Before leaving this example, we observe that the figure suggests that a monotonic number is divisible by 11 if and only if every digit occurs an even number of times. This is in fact the case and can easily be proven by elementary methods.

Example 5. [Case #125 in Table 1.] Consider now $m = 111111134445568 \in \mathcal{S}$. In the previous example, we made use of an 11-tree. The only other k-trees we needed to construct to obtain the finite list of monotonic numbers referred to in Theorem 2 were 37-trees. Since 37 divides 111 and 37 is the only monotonic multiple of 37 which is < 111, we get two 37-trees, one beginning with 0 and the other beginning with 37. The construction of the 37-trees is done in a direct manner as in the previous example; therefore, we will not display the trees here. The trees reveal that there are no monotonic multiples of $2^{17} \cdot 37$ and that $m = 111111134445568$ is the only monotonic number divisible by $2^{16} \cdot 37$. Thus, m cannot have any monotonic multiples $> m$.

Example 6. [Case #119 in Table 1.] Consider $m = 1123355557888 = 2^{15} \cdot 37 \cdot 67 \cdot 13829 \in \mathcal{S}$. Using the 37-tree, one obtains that the only monotonic numbers divisible by $2^{15} \cdot 37$ are m and numbers of the form $1^{(n)}34445568$ (with $n \geq 7$ and $n \equiv 1 \pmod 3$). Using Lemma 1, it is easy to establish that there are no multiples of 67 of the form $1^{(n)}34445568$. Since 67 divides m, there are no monotonic multiples of m greater than m.

Example 7. [Cases #143 and #144 in Table 1.] Finally we note that the last two numbers in Table 1, 112222333344677888 and 12223333334555557888 do not have monotonic multiples bigger than themselves because they are the only monotonic numbers divisible by 2^{21} and neither one divides the other.

Table 1. The Complete List for $\mathcal{S}$

List the monotonic numbers m for which the power of 2 dividing m exceeds the number of digits of m, not including cases which can readily be resolved by attaching strings of 2's or 4's in front, or by using the doubling rule. We search for the thirteen numbers listed above without monotonic multiples greater than themselves. (For readability, we drop the parentheses around the superscripts in forming strings of digits.)

Part I. The Easy Cases. Here we just search for the smallest monotonic multiple.

	Power of 2 is 4	
1.	16	48
	Power of 2 is 5	
2.	288	3456
3.	1248	113568
4.	1568	377888
5.	1888	237888
	Power of 2 is 6	
6.	448	1344
7.	2368	37888
8.	11456	1122688
9.	13888	22234688
	Power of 2 is 7	
10.	128	256
11.	2688	1346688
12.	3456	1133568
13.	11136	233666688
14.	24448	146688
15.	34688	1244466688
16.	111488	33557888
17.	112256	11113344
18.	117888	23356677888
19.	125568	1144677888

	Power of 2 is 8	
20.	256	5888
21.	5888	1477888
22.	13568	1234688
23.	133888	1335666688
24.	146688	23455557888
25.	223488	1122222235557888
26.	333568	222236677888
27.	1157888	11112223346688
28.	1224448	12335555666688
29.	1234688	111122223456677888
30.	1477888	112333344677888
	Power of 2 is 9	
31.	45568	16677888
32.	122368	14456677888
33.	357888	3355557888
34.	1125888	33355557888
35.	2226688	11135666688
36.	2277888	111111335666688
37.	2344448	112344555557888
38.	3557888	333555557888
39.	11237888	$112^{14}3456677888$
40.	12333568	3333333334444455666688
41.	12466688	123333333455555555557888
42.	15666688	1133344444445555557888

Part II. The Medium Difficulty Cases. Here we just search for the monotonic multiples, using exponential congruences to determine the correct number of leading 1's. We list the multiples in exponential string notation. Note that cases 65, 80, 100, and 119 are the only cases without monotonic multiples greater than themselves. Note also that case 110 is resolved by the algorithm in Section 3 while case 122 is resolved by Lemma 1.

		1	2	3	4	5	6	7	8
	Power of 2 is 10								
43.	37888	1	4	0	0	0	2	0	2
44.	1133568	5	2	4	0	0	0	0	3
45.	1266688	0	3	2	0	0	2	2	3
46.	11557888	7	4	4	6	2	4	0	2
47.	12223488	10	6	0	0	5	0	1	3
48.	14445568	3	7	3	7	5	0	1	3
49.	16677888	3	3	3	0	4	0	1	3
50.	23333888	2	3	6	6	5	0	1	3
51.	111111168 $\times$ 2 = 222222336								
52.	111123456	129	6	8	0	4	0	1	3
53.	111346688	31	4	0	6	2	4	0	2
54.	112677888	67	6	3	6	5	0	1	3
55.	113445888	0	10	7	8	5	0	1	3
56.	122344448	17	6	9	4	0	3	0	2
57.	135666688	161	10	6	2	0	1	2	3
58.	144677888	10	1	5	4	0	3	0	2
	Power of 2 is 11								
59.	677888	2	0	3	2	0	1	2	3
60.	4466688	0	2	3	4	0	3	0	2
61.	11122688	6	2	2	1	5	0	1	3
62.	11245568	9	0	4	0	1	4	0	2
63.	13477888	10	3	0	0	5	0	1	3
64.	33445888	9	3	7	1	5	0	1	3
65.	55666688	Solution 1. [11-tree]							
66.	122226688	2	19	6	0	1	4	0	2
67.	123557888	96	12	4	2	0	1	2	3
68.	222222336	95	3	10	2	2	4	0	2
69.	256677888	304	7	4	1	5	0	1	3
70.	333477888	31	1	5	1	5	0	1	3
71.	1111144448	527	6	4	4	0	3	0	2
72.	1223333888	111	6	1	0	3	0	1	3
73.	1335666688	1	5	23	2	2	4	0	2
74.	1344677888	1064	8	8	1	5	0	1	3
	Power of 2 is 12								
75.	12288	0	1	1	0	0	4	0	2
76.	1445888	2	0	8	0	1	4	0	2
77.	11112448	2	8	1	1	1	2	2	3
78.	122277888	6	22	1	0	3	0	1	3
79.	224677888	39	10	1	2	2	4	0	2
80.	1111666688	Solution 2. [11-tree]							
81.	1115557888	11	8	6	2	0	1	2	3
82.	1444466688	18	1	13	2	0	1	2	3
83.	2334445568	50	19	0	3	0	3	0	2

		1	2	3	4	5	6	7	8
	Power of 2 is 12 (cont.)								
84.	11223666688	289	2	6	1	5	0	1	3
85.	11355557888	4054	1	14	2	0	1	2	3
86.	12222222336	4933	7	7	0	1	4	0	2
87.	12256677888	591	13	1	0	3	0	1	3
88.	12333477888	1485	9	36	0	1	4	0	2
89.	14555557888	775	23	21	2	0	1	2	3
	Power of 2 is 13								
90.	23666688	14	5	5	1	5	0	1	3
91.	155557888	36	7	2	4	0	3	0	2
92.	2336677888	843	26	4	2	0	1	2	3
93.	11112357888	1958	17	21	1	5	0	1	3
94.	13335666688	21594	48	1	0	3	0	1	3
95.	13344677888	2118	1	7	1	5	0	1	3
96.	22244466688	523	31	17	1	5	0	1	3
97.	111136677888	5884	4	9	1	5	0	1	3
98.	112222445568	24114	27	22	1	5	0	1	3
99.	112223346688	5	1	2	0	4	0	1	3
100.	114455666688	Solution 3. [11-tree]							
101.	134555557888	7154	18	8	1	5	0	1	3
	Power of 2 is 14								
102.	114688	0	1	1	1	1	2	2	3
103.	222445568	14	12	15	1	5	0	1	3
104.	3355557888	57	15	0	1	1	0	0	3
105.	34455666688	2242	8	34	1	5	0	1	3
106.	111255666688	2267	17	15	1	5	0	1	3
107.	1111233445888	3716	5	1	0	3	0	1	3
108.	1112224677888	13279	4	8	1	5	0	1	3
109.	1113444466688	60628	9	0	1	1	0	0	3
110.	1122455666688	n	1757	16	1	5	0	1	3
111.	1334555557888	47539	34	12	1	5	0	1	3
	Power of 2 is 15								
112.	1133477888	1	0	11	1	5	0	1	3
113.	2455666688	1	22	20	1	5	0	1	3
114.	11111333888	81	19	5	1	5	0	1	3
115.	22555557888	375	6	15	1	5	0	1	3
116.	23456677888	1	7	40	1	5	0	1	3
117.	122334445568	384	24	4	2	0	1	2	3
118.	222235557888	5751	27	10	1	5	0	1	3
119.	1123355557888	Solution 4. [37-tree]							
120.	1222244466688	2555	38	10	1	5	0	1	3
121.	2222222245888	43561	33	11	1	5	0	1	3
122.	11133335666688	n	2	6	1	5	0	1	3
123.	13334555557888	32765	11	27	1	5	0	1	3

Part III. The Hard Cases. Here we search for the ending digits of any monotonic multiple, using Lemma 1 and the algorithm to settle the existence of a solution for n leading 1's. There are nine more numbers m which do not have monotonic multiples $> m$.

Power of 2 is 16

124. $1111456677888 = 2^{16} \cdot 3^3 \cdot 79 \cdot 7951 \mid 1^n 2^4 3^6 45^5 78^3$
125. $111111134445568 = 2^{16} \cdot 37 \cdot 45822199$ Solution 5. [37-tree]

Power of 2 is 17

126. $1124466688 \times 9901 = 11133344677888$
127. $2233444466688 = 2^{17} \cdot 3 \cdot 5679943 \mid 1^n 2^3 3^6 45^5 78^3$
128. $11133344677888 = 2^{17} \cdot 23 \cdot 373 \cdot 9901$ Solution 6. [The only possible multiples are $1^n 2^k 3^6 45^5 78^3$, $1^n 2^5 35^3 78^3$, $1^n 3^5 45^5 78^3$, $1^n 2^3 3^5 56^4 8^2$, $1^n 2^4 3^4 4^2 67^2 8^3$, which all fail modulo 9901.]
129. $11223456677888 = 2^{17} \cdot 7 \cdot 13 \cdot 43 \cdot 79 \cdot 277$ Solution 7. [The only possible multiples are $1^n 2^k 3^6 45^5 78^3$, $1^n 2^5 35^3 78^3$, $1^n 3^5 45^5 78^3$, $1^n 2^3 3^5 56^4 8^2$, $1^n 2^4 3^4 4^2 67^2 8^3$, which fail modulo 91, 79, 7, 13, and 43, respectively.]
130. $22333335666688 = 2^{17} \cdot 1249 \cdot 136421 \mid 1^n 2^4 3^6 45^5 78^3$
131. $133334555557888 = 2^{17} \cdot 17 \cdot 5081 \cdot 11777 \mid 1^n 2^{335} 3^6 45^5 78^3$
132. $1111122336677888 = 2^{17} \cdot 61 \cdot 138970339 \mid 1^n 2^{104} 3^6 45^5 78^3$
133. $1111234455666688 = 2^{17} \cdot 131 \cdot 719 \cdot 90011 \mid 1^n 2^8 3^6 45^5 78^3$

Power of 2 is 18

134. $122222222245888 = 2^{18} \cdot 409 \cdot 883 \cdot 1291 \mid 1^n 2^3 73^6 45^5 78^3$
135. $11112222235557888 = 2^{18} \cdot 3^4 \cdot 1619 \cdot 323243 \mid 2^k 3^6 45^5 78^3$

Power of 2 is 19

136. $222333344677888 = 2^{19} \cdot 424067201 \mid 2^k 3^6 45^5 78^3$
137. $111333334555557888 = 2^{19} \cdot 3 \cdot 33997 \cdot 2082061 \mid 1^{2629434378} 2^{81} 3^6 45^5 78^3$

Power of 2 is 20

For 138 - 142 the only possible solution is $1^n 2^3 3^6 45^5 78^3$

138. $223346688 = 2^{20} \cdot 3 \cdot 71$ Solution 8. [Lemma 1 modulo 71.]
139. $11222555557888 = 2^{20} \cdot 1583 \cdot 6761$ Solution 9. [Lemma 1 modulo 6761.]
140. $1122233444466688 = 2^{20} \cdot 1070245213$ Solution 10. [Lemma 1 modulo 10702663.]
141. $111222333335666688 = 2^{20} \cdot 3 \cdot 23 \cdot 1537244677$ Solution 11. [Lemma 1 modulo 1537244677.]
142. $223333334555557888 = 2^{20} \cdot 109 \cdot 787 \cdot 2482861 \mid 1^{1502122760} 2^3 3^6 45^5 78^3$

Power of 2 is 21

143. 112222333344677888 Solution 12. [search tree]
144. 12223333334555557888 Solution 13. [search tree]

5. Miscellaneous Results and Questions

In this section, we state a few brief facts about monotonic and block numbers without offering proofs and pose some problems about these numbers which we have been unable to resolve.

Theorem 3 of Section 2 implies that the number of blocks in 2^n tends to infinity with n. Thus, if $B(k)$ denotes the number of blocks in the positive integer k, then $\lim_{n\to\infty} B(2^n) = \infty$. Let a be a positive integer which is not a power of 10. Then we have been able to show that $\lim_{n\to\infty} B(a^n) = \infty$. (See [2, Thm. 1].) In particular, for every positive integer n which is not a power of 10, there is a positive integer k such that n^k is not a block integer.

In Section 4 we dealt with the case in which the product of a monotonic number with a positive integer is monotonic. One can consider the analog for addition; but it is not difficult to show that for every monotonic m, there is a positive integer k for which $k + m$ is monotonic. For example, if $m = 123456789$, take $k = 999999989$. On the other hand, if one requires k also to be monotonic, one can show that the conclusion is different. In fact, for any number $m = 1^{(n)}23456789$, with n a positive integer, and for any monotonic number k, the sum $k + m$ is not monotonic. The analogous situation with block numbers is that for every block number b, there exists a block number b' such that $b + b'$ is a block number.

In [1] we were able to determine all monotonic numbers m such that m^2 is also monotonic. We can generalize to other powers of monotonic numbers. The main result is

Theorem 4. *The only numbers for which m and m^2 are monotonic lie in the four families $16^{(n)}7$, $3^{(n)}4$, $3^{(n)}5$, and $3^{(k)}6^{(n)}7$, where n and k are arbitrary non-negative integers, together with the spurious solutions 1, 2, 3, 6, 12, 13, 15, 16, 38, 116, and 117. The only numbers for which m and m^3 are monotonic are 1, 2, 3, and 5. The only numbers for which m and m^4 are monotonic are 1, 2, and 4.*

The proof of Theorem 4 for squares of monotonic numbers is based on computations and an intricate induction on the number of digits of m. Unlike the situation with squares, there are no infinite lists of monotonic numbers with monotonic cubes or fourth powers. The short list of fourth powers was found rather readily by first doing a search to show that there are no monotonic integers a with 11 digits such that a^4 is monotonic in its rightmost 11 digits. The cubic case was slightly more difficult. A preliminary search showed that if $a \notin \{1, 2, 3, 5\}$ and a and a^3 are monotonic, then the 5 right-most digits of a must each be 9. Then a search was done to rule out these possible "exceptions."

It would be nice to obtain similar results theoretically. In particular, we conjecture that for each integer $r > 2$, there are only finitely many monotonic numbers m for which m^r is also monotonic. Another curious question also arose during our computations: Is it true that every integer $m > 125167$ for which m^2 is monotonic, is itself monotonic?

In the general case of base b arithmetic, we conjecture that if $b-1$ is squarefree, then there are only a finite number of monotonic numbers a base b for which a^2 is also monotonic base b. More generally, we conjecture that if $b-1$ is k-free, then there are only a finite number of monotonic numbers a base b for which a^k is also monotonic base b. These conjectures may be true even if a is not required to be monotonic base b. We are far from being able to establish such a result.

We were able to come up with a complete list of block numbers whose squares are block numbers. The list was somewhat long (with 51 families of numbers) and we do not include it. However, we note the example $26733^2 = 714653289$ arose in which the digits of the square form a permutation of $1, 2, \ldots, 9$.

It is easy to show that the density of monotonic as well as the more abundant block numbers is very small. More specifically, for any positive integer n, there are $\binom{n+8}{8}$ monotonic numbers with exactly n digits and there are

$$9 \sum_{k=1}^{\min\{10,n\}} (k-1)! \binom{9}{k-1} \binom{n-1}{k-1}$$

block numbers with exactly n digits. This is strong enough to imply that the sum of the reciprocals of the block numbers converges and even that $\displaystyle\sum_{b \in \mathcal{B}} \frac{1}{(\log b)^{10} \log\log b}$ converges.

Every arithmetic progression of block numbers is finite. Every geometric progression of block numbers with the ratio between consecutive terms not a power of 10 is finite. In fact, there exists an absolute constant C such that every arithmetic progression of block numbers has $\leq C$ terms. We do not know if such a C exists for geometric progressions.

For every integer $n > 3$, there is an integer b such that $2 \leq b < n$ and n is not monotonic in base b.

Given a base $b \geq 2$, are there infinitely many monotonic or block primes? For $b = 2$, this is equivalent to asking whether there are infinitely many Mersenne primes. For $b = 10$, the largest known monotonic prime or block prime is $1^{(1031)}$.

In parting, the authors thank (blame) J. L. Selfridge for getting us started on looking at such questions and for (un)helpful discussions. Paul Erdős was the first to point out the connection between Theorems 1 and 2. We also thank Greg Manning who partially aided in some of the programming associated with this paper; in particular, the list of block numbers whose squares are block numbers, which we alluded to earlier in this section, would not have come about without his help.

References

1. Richard Blecksmith and Charles Nicol, *Montonic Numbers*, Math. Mag. **66** (1993), 257–262.
2. R. Blecksmith, M. Filaseta, and C. Nicol, *A result on the digits of a^n*, Acta. Arith. **64** (1993), 331–339.

Department of Mathematical Sciences
Northern Illinois University
DeKalb, IL 60115

Department of Mathematics
University of South Carolina
Columbia, SC 29208

Department of Mathematics
University of South Carolina
Columbia, SC 29208