NUMBERS WITHOUT ONES

by STEVEN T. KUHN and ANDREW VOGT
Departments of Philosophy and Mathematics
Georgetown University
Washington, D. C. 20057

(Submitted February 1990)

1. INTRODUCTION

We report solutions to the following general problem:

> Fix a base b and a positive integer k. Does every set of positive integers $\{x_1,\ldots,x_k\}$ have an integer multiplier $m \geq 1$ such that none of $mx_1,\ldots,mx_k$ contains the digit 1 in various positions of its base b representation?

It has been known for more than a century ([1], p. 454) that every positive integer x has a multiple mx consisting of repetitions of any prescribed string of digits followed perhaps by zeros. But the structure of a set of numbers $\{mx_1,\ldots,mx_k\}$ is not so easy to stipulate, even if we merely require that the digits differ from 1. Related questions are discussed in [1] Chapter XX, [2] Chapter IX, and, in connection with the generation of pseudo-random numbers, [3] Section 3.2.

2. SUMMARY OF RESULTS

Let the base b be a positive integer ≥ 2, and let the variables $k,m,n,x_1,\ldots,x_k$ denote positive integers. Our results are the following:

RESULT 1: i) If $2^k < b$, then for any set $\{x_1,\ldots,x_k\}$ there is an m such that none of $mx_1,\ldots,mx_k$ has leftmost digit 1.

ii) If $2^k \geq b$, then there exist sets $\{x_1,\ldots,x_k\}$ such that for any m at least one of $mx_1,\ldots,mx_k$ has leftmost digit 1.

RESULT 2: i) If b is not a prime power, or if $b = p^n$ for some prime p and $k < n(p^n - p^{n-1})$, then for any set $\{x_1,\ldots,x_k\}$ there is an m such that none of $mx_1,\ldots,mx_k$ has rightmost nonzero digit 1.

ii) If $b = p^n$ and $k \geq n(p^n - p^{n-1})$, then there exist sets $\{x_1,\ldots,x_k\}$ such that for any m at least one of $mx_1,\ldots,mx_k$ has rightmost nonzero digit 1.

RESULT 3: If $k \leq b - 2$ when b is prime, or $k \leq$ the smallest prime factor of b when b is not prime, then for any n and any set $\{x_1,\ldots,x_k\}$ there is an m such that none of $mx_1,\ldots,mx_k$ has the digit 1 among its n rightmost nonzero digits (a string of consecutive digits the last of which is the rightmost nonzero digit of the number).

3. THE LEFTMOST DIGIT CASE

Given a set of positive integers $x_1, \ldots, x_k$, we express them in scientific notation by $x_i = a_i b^{k_i}$ with k_i in $\{0,1,2,\ldots\}$ and a_i in $[1,b)\cap Q$, and we order them so that $a_1 \leq \ldots \leq a_k$.

<u>Proposition 3.1</u>: Let b be ≥ 3. The following are equivalent:

$$\text{for each integer } m \geq 1 \text{ at least one of } mx_1, \ldots, mx_k \text{ has leftmost digit equal to 1;} \tag{3.1.1}$$

and

$$\frac{b}{2} \leq \frac{a_k}{a_1} \text{ and } \frac{a_{i+1}}{a_i} \leq 2 \quad \text{for all } i = 1, \ldots, k-1. \tag{3.1.2}$$

<u>Proof</u>: Suppose (3.1.1) fails for some m. Then each mx_i has leftmost digit ≥ 2. Choose j such that $2b^j \leq x_1 < b^{j+1}$, and let $n = j - k_1$. If (3.1.2) is true, an induction shows that $ma_i < b^{n+1}$ for each i ($ma_{i+1} \leq 2ma_i < 2b^{n+1}$ implies $ma_{i+1} < b^{n+1}$). This gives a contradiction since $2b^{n+1} \leq mba_1 \leq 2ma_k < b^{n+1}$.

Conversely, suppose (3.1.2) fails. If $a_{j+1} > 2a_j$ for some j, set $m_i = k_i$ for $i \leq j$ and $m_i = k_i+1$ for $i > j$. Then it is straightforward to verify that the inequalities $a_1 \leq \ldots \leq a_j < \frac{a_{j+1}}{2} \leq \ldots \leq \frac{a_k}{2}$ can be rewritten as:

$$\max \left\{ \frac{2b^{m_i}}{x_i} : 1 \leq i \leq k \right\} \quad < \quad \min \left\{ \frac{b^{m_i+1}}{x_i} : 1 \leq i \leq k \right\} \tag{3.1.3}$$

(3.1.3) is also true when $\frac{b}{2} > \frac{a_k}{a_1}$ provided $m_i = k_i$ for every i. Accordingly we can find rational numbers of the form $\frac{m}{b^q}$ strictly between the two bounds in (3.1.3). Then $2b^{m_i+q} < mx_i < b^{m_i+q+1}$ for all i and (3.1.1) fails. ■

Part i) of Result 1 is an immediate consequence of 3.1 since (3.1.1) can only be true if $\frac{b}{2} \leq \frac{a_k}{a_1} = (\frac{a_2}{a_1}) \cdot \ldots \cdot (\frac{a_k}{a_{k-1}}) \leq 2^{k-1}$, and this cannot occur if $2^k < b$.

A set Y is called a <u>multiple</u> of $\{x_1,\ldots,x_k\}$ if and only if Y = $\{mx_1,\ldots,mx_k\}$ for some positive integer m. Y is called a <u>quasimultiple</u> (in base b) of $\{x_1,\ldots,x_k\}$ if and only if Y = $\{m'\cdot x_1\cdot b^{n(1)},\ldots,m'\cdot x_k\cdot b^{n(k)}\}$ where m' is a positive integer and $n(1),\ldots,n(k)$ are nonnegative integers. For example, $\{6,9,15\}$ is a multiple of $\{2,3,5\}$, and $\{9,600,150\}$ is a quasimultiple (in base 10) of $\{2,3,5\}$.

Part ii) of Result 1 follows from the next proposition.

<u>Proposition 3.2</u>: Let $2^k \geq b$. Then every quasimultiple $\{x_1,\ldots,x_k\}$ of $\{1,2,\ldots,2^{k-1}\}$ has property (3.1.1). There are other sets with this property if and only if $2^k > b$.

<u>Proof</u>: The set $T = \{1,2,\ldots,2^{k-1}\}$ satisfies (3.1.2) if $2^k \geq b$. Hence it satisfies (3.1.1). Since (3.1.1) is preserved under quasimultiplication (multiplication by powers of b merely adjoins zeros on the right), quasimultiples of T also satisfy (3.1.1).

If $\{x_1,\ldots,x_k\}$ has property (3.1.1) and is indexed as in Proposition 3.1, then (3.1.2) can be rewritten as:

$$1 \leq \frac{a_{i+1}}{a_i} \leq 2 \quad , \frac{b}{2} \leq \left(\frac{a_2}{a_1}\right)\cdot\ldots\cdot\left(\frac{a_k}{a_{k-1}}\right) \leq 2^{k-1} . \qquad (3.2.1)$$

If $2^k = b$, $\frac{a_{i+1}}{a_i}$ must equal 2 for each i. Then $x_i = 2^{i-1}a_1 b^{k_i}$ for each i where $a_1 = \frac{x_1}{b^{k_1}}$ is a fraction of the form $\frac{m}{2^q}$ with m odd. It follows easily that $x_i = m\cdot 2^{m_i}$ where each m_i is a distinct integer mod k. Hence $\{x_1,\ldots,x_k\}$ is a quasimultiple of T. On the other hand, if $2^k > b$, we can choose fractions $r_i = \frac{a_{i+1}}{a_i}$ satisfying (3.2.1) with each inequality satisfied strictly and the product less than min $\{b, 2^{k-1}\}$. We also choose a fraction $a_1 \geq 1$ such that $a_1 \cdot r_2 \cdot \ldots \cdot r_k < b$. All of these fractions can be taken to have the form $\frac{m}{b^q}$ with m odd. Multiplying each $a_i = a_1 \cdot r_2 \cdot \ldots \cdot r_i$ by the smallest power of b that makes the product an integer, we get x_i's satisfying (3.1.2) and hence (3.1.1). Since each x_i is odd, $\{x_1, \ldots, x_k\}$ cannot be a quasimultiple of T. ∎

4. THE RIGHTMOST DIGIT CASE

Proposition 4.1: Let b be neither a prime nor a prime power. Then for any set of positive integers $x_1, \ldots, x_k$ there is an integer $m \geq 1$ such that none of $mx_1, \ldots, mx_k$ has rightmost nonzero digit 1.

Proof: Express b as the product of two relatively prime integers r and s greater than 1. Let t be the highest power of r that occurs in any of $x_1, \ldots, x_k$, and let $m = s^{t+1}$.

If for some i the rightmost nonzero digit of mx_i is 1, then $mx_i = s^{t+1}x_i \equiv b^{n-1} \pmod{b^n}$ for some positive integer n. So r^{n-1} divides x_i and $n - 1 \leq t$. Removing the common factor s^{n-1} from the equation above, we conclude that s divides a power of r. Since this is impossible, all of the integers mx_i have rightmost nonzero digit distinct from 1. ∎

Proposition 4.2: Let $b = p^n$ where p is a prime. Then the following are equivalent:

for each integer $m \geq 1$ at least one of
$mx_1, \ldots, mx_k$ has rightmost nonzero digit 1; (4.2.1)

and

for each positive integer c in $\{1, \ldots, b-1\}$ that is relatively prime to p and each integer i in $\{0, \ldots, n-1\}$, there is an x in $\{x_1, \ldots, x_k\}$ such that $y \equiv cp^i \pmod{p^{n+i}}$ where y is the quotient obtained by dividing x by the highest power of b in x. (4.2.2)

<u>Proof</u>: Suppose that (4.2.2) holds. To establish (4.2.1), we assume without loss of generality that m is a positive integer not divisible by b. Then $m = ap^s$ where a is a positive integer not divisible by p and $0 \leq s \leq n-1$. Because a and b are relatively prime, there are integers c and d such that $ac + bd = 1$ with $1 \leq c \leq b-1$. If $s = 0$, let $i = 0$ and choose x,y as in (4.2.2) so that $y \equiv c \pmod b$. Then $my \equiv mc \equiv 1 \pmod b$. So my has rightmost digit 1, and (4.2.1) holds for mx. If $s \geq 1$, let $i = n - s$ and choose x,y as in (4.2.2) so that $y \equiv cp^{n-s} \pmod{p^{2n-s}}$. Then $my \equiv acp^n \pmod{p^{2n}} \equiv p^n \pmod{p^{2n}} \equiv b \pmod{b^2}$. Thus my has its two rightmost digits equal to 10, mx has rightmost nonzero digit 1, and (4.2.1) holds.

Conversely, suppose (4.2.1) holds. Remove all powers of b from each x_i, and the resulting set $\{y_1, \ldots, y_k\}$ still satisfies (4.2.1) with none of the y_i's divisible by b. Let c be any integer from 1 to b-1 relatively prime to p. Choose integers a and d such that $ac + bd = 1$ and $1 \leq a \leq b-1$. Let $m = ap^{n-i}$ with $0 \leq i \leq n-1$, and by (4.2.1) choose y in $\{y_1, \ldots, y_k\}$ such that my has rightmost nonzero digit 1. Then $my \equiv ap^{n-i}y \equiv b^s \pmod{b^{s+1}}$ for some $s \geq 0$. Since p does not divide a and b does not divide y, $s = 1$ and p^i divides y. Then $ay \equiv p^i \pmod{p^{n+i}}$, and $y = (ac + bd)y \equiv cp^i \pmod{p^{n+i}}$, as required in (4.2.2). ■

<u>Corollary 4.3</u>: Let $b = p^n$. Then there exist sets $\{x_1, \ldots, x_k\}$ such satisfying (4.2.1) if and only if $k \geq n(p^n - p^{n-1})$.

<u>Proof</u>: The number of positive integers c in $\{1, \ldots, b-1\}$ relatively prime to p is $p^n - p^{n-1}$, and the number of equations of the form $y \equiv cp^j \pmod{p^{n+j}}$, with c as above and $0 \leq j \leq n-1$, is $n(p^n - p^{n-1})$. It is easy to see that no integer y satisfies two different equations of this form. Thus (4.2.2), and hence (4.2.1), can be satisfied precisely when $k \geq n(p^n - p^{n-1})$. ■

Parts i) and ii) of Result 2 follow at once from Proposition 4.1 and Corollary 4.3.

<u>5. STRINGS OF RIGHTMOST DIGITS</u>

<u>Lemma 5.1</u>: Let $(z_1, \ldots, z_k)$ be an ordered k-tuple of positive integers satisfying

$$\sum_{i=1}^{k} \gcd(b, z_i) \leq b - 2. \tag{5.1.1}$$

Then for every ordered k-tuple $(y_1, \ldots, y_k)$ of integers, there is an integer m in $\{1, \ldots, b-1\}$ such that none of the equations

$$mz_i \equiv y_i \pmod b \qquad i = 1,\ldots,k \quad (5.1.2)$$

is true.

If it is assumed that

$$\sum_{i=1}^{k} \gcd(b,z_i) \leq b - 1, \qquad (5.1.3)$$

the conclusion above holds for some integer m in $\{0,\ldots,b-1\}$.

Proof: By elementary number theory ([4], p. 102) the equation $mz_i \equiv y_i \pmod b$ has a solution m in the integers mod b if and only if y_i is divisible by $\gcd(b,z_i)$. When such a solution exists, there are exactly $\gcd(b,z_i)$ of them. If we assume the worst, then equations (5.1.2) all have distinct solutions. This leaves $[b - 1 - \sum_{i=1}^{k} \gcd(b,z_i)]$ (> 0) integers m among the integers $1,2,\ldots,b-1$ to satisfy the conditions of the lemma.

The last statement is proved similarly. ∎

The n rightmost nonzero digits of x refers to the string of n successive digits in x whose rightmost member is the rightmost nonzero digit of x. Thus, for example, in base 10 the three rightmost nonzero digits of 740,500 are 405.

Proposition 5.2: Let $\{x_1,\ldots,x_k\}$ be a set of positive integers whose rightmost nonzero digits satisfy (5.1.1), and let n be a positive integer. Then there exists an integer m in $\{1,\ldots,b^n-1\}$ such that none of $mx_1,\ldots mx_k$ has the digit 1 among its n rightmost nonzero digits.

Proof: Let $z_1,\ldots,z_k$ be the rightmost digits of $x_1,\ldots,x_k$, none of them zero without loss of generality. By Lemma 5.1 choose m_0, the rightmost digit of m, in $\{1,\ldots,b-1\}$ so that the equations

$$\begin{aligned} m_0 z_i &\equiv 1 \pmod b \quad \text{for } i \text{ such that } \gcd(b,z_i) = 1 \\ m_0 z_i &\equiv 0 \pmod b \quad \text{for } i \text{ such that } \gcd(b,z_i) > 1 \end{aligned} \tag{5.2.1}$$

$(i = 1,\ldots,k)$ are all false. Then $m_0 z_i \pmod b$, the rightmost digit of mx_i, is in the set $\{2,\ldots,b-1\}$ for each i.

If the first j digits of m from right to left - $m_0,\ldots,m_{j-1}$- have already been chosen, then the $(j+1)^{th}$ digit of mx_i will equal $m_j z_i + u_{ij} \pmod b$, where u_{ij} is an integer depending on the first j digits of m and x_i and the $(j+1)^{th}$ digit of x_i. By Lemma 5.1 choose m_j in $\{1,\ldots,b-1\}$ so that none of the equations $m_j z_i \equiv 1 - u_{ij} \pmod b$, $i = 1,\ldots,k$, holds. For $j \geq n$, set $m_j = 0$. Then m is as required. ∎

Proof of Result 3: Let q be the smallest prime factor of b. The rightmost nonzero digits z_i of x_i satisfy $\gcd(b,z_i) \leq \frac{b}{q}$. If

$$k\cdot\left(\frac{b}{q}\right) \leq b - 2, \tag{5.3.1}$$

then (5.1.1) is true and Proposition (5.2) yields Result 3.

When b is prime or $k \leq q - 1$, the hypotheses in Result 3 ensure that (5.3.1) holds. Thus we need only consider the case when b is composite and $k = q$.

Suppose until further notice that $\gcd(b,z_i)$ is smaller than b/q for at least one i. Then the left side of (5.1.1) is bounded above by $(q - 1)(b/q) + r'$ where r' is the second largest factor of b, the largest being $r = b/q$. If $r' \leq r - 2$, (5.1.1) applies again. If not, $b = 6$ or 4.

If $b = 6$, then $q = 2$ and $\{z_1, z_2\}$ is a pair. Either $m_0 = 1$ fails to satisfy each of the two equations (5.2.1) or else one of z_1 and z_2 is 1. In the latter case, $\gcd(b,z_1) + \gcd(b,z_2) \leq 3 + 1 \leq 6 - 2$, and (5.1.1) is fulfilled. In the former case, the induction in Proposition 5.2 can proceed using (5.1.3) since $\gcd(b,z_1) + \gcd(b,z_2) \leq 3 + 2 \leq 6 - 1$ and m_j can be chosen equal to zero if necessary (for $j \geq 1$).

If $b = 4$, then $q = 2$ again. An argument similar to the last one applies except when $\{z_1, z_2\} = \{1,2\}$. Then $m_0 = 3$ can be used to falsify equations (5.2.1), and $2 + 1 \leq 4 - 1$ insures that (5.1.3) applies to the later digits of m.

Finally, suppose $\gcd(b,z_i) = r$ for each $i = 1,\ldots,q$. Then each $x_i = y_i r^s$ with $s \geq 1$, where r^s is the largest power of r dividing all x_i. Then $\{y_1,\ldots,y_q\}$ is covered by the earlier arguments since not all y_i's are divisible by r. If none of $my_1,\ldots,my_q$ has 1's among the n rightmost digits, the same is true for $(q^s m)x_1,\ldots,(q^s m)x_q = my_1b^s,\ldots,my_qb^s$. ∎

6. FURTHER QUESTIONS

1. To what extent do these results apply to other digits (or strings of digits) and other positions? For example, under what conditions can we ensure that the two rightmost nonzero digits

differ from 1?

2. Can the hypotheses of Result 3 be weakened, or are they necessary as well as sufficient?

3. What are the smallest multipliers needed in Results 1, 2, and 3? The proofs provide upper bounds, but calculations suggest that much smaller multipliers will often suffice.

4. Under what conditions can 1's be eliminated in every position? Result 1 shows that $2k < b$ is a necessary condition. However, even the following elementary question remains unanswered for bases > 4: are there numbers x and y such that for every m at least one of mx or my contains the digit 1?

Reference

[1] L. E. Dickson, *History of the Theory of Numbers, Vol. 1, Divisibility and Primality*. Washington, D. C.: Carnegie Institute of Washington, 1919.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Fifth Edition. Oxford: Oxford University Press, 1979.

[3] D. E. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*. Reading, Mass.: Addison-Wesley, 1969.

[4] K. H. Rosen, *Elementary Number Theory and Its Applications*. Reading, Mass.: Addison-Wesley, 1984.