A result on the digits of a^n

by

R. Blecksmith (DeKalb, Ill.), M. Filaseta (Columbia, S.C.) and C. Nicol (Columbia, S.C.)

Dedicated to the memory of David R. Richman

1. Introduction. Let $d_r d_{r-1} \dots d_1 d_0$ be the base b representation of a positive integer m. We refer to a block (of digits) of m base b as being a successive sequence of equal digits $d_i d_{i-1} \dots d_j$ of maximal length. For example, the base 10 number 8037776589 consists of 8 blocks: 8, 0, 3, 777, 6, 5, 8, and 9. We may view the number of blocks of m base b as one more than the number of $k \in \{0, 1, \dots, r-1\}$ for which $d_k \neq d_{k+1}$, and we denote the number of blocks by B(m, b). Thus, in the example above, B(8037776589, 10) = 8. If the base b is understood, we may omit any reference to it.

It is reasonable to suspect, from a probabilistic point of view, that whenever a is a positive integer and a is not a power of 10, then the number of blocks of a^n base 10 tends to infinity as n goes to infinity. For an arbitrary base b > 1, it is not difficult to show that $B(a^n, b)$ is bounded whenever $\log a/\log b$ is rational, and for other values of a, we would like to conclude that $B(a^n, b)$ tends to infinity with n. We show in fact that this is a consequence of a certain transcendence result.

Theorem 1. Let a and b be integers ≥ 2 . If $\log a/\log b$ is irrational, then

(1)
$$\lim_{n \to \infty} B(a^n, b) = \infty.$$

Theorem 1 can be improved whenever b is not a prime power and a is a prime divisor of the base b.

Research of the first author was supported in part by the NSF under grant number DMF-8902258.

Research of the second author was supported in part by the NSA under grant number MDA904-92-H-3011.

Theorem 2. Let b be a positive integer which is not a prime power and let p be a prime. Then p divides b if and only if

(2)
$$\lim_{n \to \infty} \min_{\substack{k \in \mathbb{Z}^+ \\ b \nmid p^n k}} B(p^n k, b) = \infty.$$

We will give an elementary proof of Theorem 2, so it is worth noting that Theorem 2 implies that (1) holds with b = 10 for $a = 2, 4, 5, 6, 8, 12, \dots$ and, in general, whenever the exponent of 2 in the largest power of 2 dividing a differs from the exponent of 5 in the largest power of 5 dividing a.

We make one further observation. Theorem 2 implies that there is a positive integer n such that every multiple of 2^n which is relatively prime to 5 contains two blocks formed from the same digit. We were able to establish computationally that n = 53 is the smallest such n. Similarly, any odd multiple of 5^{13} contains two blocks formed from the same digit, and the exponent 13 is best possible in this case. In particular, if \mathcal{B} is the set of all numbers not ending in the digit 0 base 10 and consisting of blocks formed from distinct digits, then there are exactly two numbers in \mathcal{B} divisible by 2^{52} . They are

$$\underbrace{3 \dots 3}_{9} \underbrace{7 \dots 7}_{16} 004999999 \underbrace{6 \dots 6}_{11} 88512$$

and

$$7\underbrace{6\dots 6}_{9}\underbrace{2\dots 2}_{16}995000000\underbrace{3\dots 3}_{11}11488.$$

On the other hand, there are infinitely many numbers in \mathcal{B} divisible by 5^{12} and these are given by the elements of \mathcal{B} ending in 336669921875 or 663330078125.

2. The proof of Theorem 1. We first show that Theorem 1 follows from

LEMMA 1. Let a and b be integers > 1 such that $\log a/\log b$ is irrational. Let a_1, a_2, \ldots, a_m be arbitrary integers. Then there are finitely many (m+1)tuples $(k_1, k_2, \ldots, k_m, n)$ of nonnegative integers satisfying

- (i) $k_1 < k_2 < \dots < k_m$, (ii) $\sum_{j=r}^m a_j b^{k_j} > 0 \text{ for } 1 \le r \le m$, and (iii) $\sum_{j=1}^m a_j b^{k_j} = (b-1)a^n$.

To prove Theorem 1, it suffices to show that for any positive integer M, there are only finitely many n for which $B(a^n, b) \leq M$. Given $M \in \mathbb{Z}^+$, consider any n such that $B(a^n, b) \leq M$. Let $m = B(a^n, b) + 1$, $k_1 = 0$, and define d_1 to be the first right-most digit of a^n base b. Let d_2 be the next right-most digit of a^n satisfying $d_2 \neq d_1$ and continue in this manner, Digits of a^n

defining d_{j+1} as the next digit of a^n such that $d_{j+1} \neq d_j$, until d_{m-1} has been defined. There exist positive integers k_2, \ldots, k_m with $k_2 < k_3 < \ldots < k_m$ such that

$$a^{n} = (d_{1} - d_{2}) \frac{b^{k_{2}} - 1}{b - 1} + \ldots + (d_{m-2} - d_{m-1}) \frac{b^{k_{m-1}} - 1}{b - 1} + d_{m-1} \frac{b^{k_{m}} - 1}{b - 1}.$$

Condition (iii) of Lemma 1 holds with $a_1 = -d_1$, $a_j = d_{j-1} - d_j$ for $j \in \{2, \ldots, m-1\}$, $a_m = d_{m-1}$. Note that regardless of the value of n, we have $|a_j| \leq b-1$ for every $j \in \{1, \ldots, m\}$. Thus, each n produces a solution to one of at most $(2b-1)^{M+1}$ equations of the form given in (iii). Moreover, with the k_j and a_j defined as above, (i) is clearly satisfied and (ii) holds since $a_m = d_{m-1} \geq 1$ and

$$\sum_{j=r}^{m} a_j b^{k_j} \ge b^{k_m} - \sum_{j=r}^{m-1} |a_j| b^{k_j} \ge b^{k_m} - \sum_{j=r}^{m-1} (b-1) b^{k_j} > 0.$$

We deduce from Lemma 1 that there are only finitely many n for which $B(a^n, b) \leq M$. Theorem 1 follows.

Instead of applying Lemma 1 above, we could have appealed to the following result of Revuz [2]: If $\lambda_1, \ldots, \lambda_M, \mu_1, \ldots, \mu_N$ are algebraic numbers, then the equation $\sum_{i=1}^M \lambda_i \theta^{m_i} = \sum_{j=1}^N \mu_j \phi^{n_j} \neq 0$ holds for only a finite number of rational integer (m+n)-tuples (m_i, n_j) , provided $\log |\theta|/\log |\phi|$ is irrational. It appears, however, that counterexamples exist to this statement, although perhaps the conditions of the theorem can be modified to make a correct verifiable result. For example, if θ is the positive real root of $x^2 - x - 1$, one can conclude from this statement that

$$\theta^{k_5} - \theta^{k_4} - \theta^{k_3} + \theta^{k_2} - \theta^{k_1} = 2^m$$

has finitely many solutions in integers m, k_1, \ldots, k_5 ; however, the equation is satisfied whenever $(m, k_1, \ldots, k_5) = (0, 1, 2, k, k+1, k+2)$ where k is an arbitrary integer. Note that we could replace 2^m on the right-hand side of this example with i^m and then take m = 4n, thereby introducing a second integer parameter.

We say that an algebraic number α has degree d and height A if α satisfies an irreducible polynomial $f(x) = \sum_{j=0}^d a_j x^j \in \mathbb{Z}[x]$ with $a_d \neq 0$, $\gcd(a_d,\ldots,a_1,a_0)=1$, and $\max_{0\leq j\leq d}|a_j|=A$. To prove Lemma 1, we make use of the following result which can be found in [1]. (See Theorem 3.1 and the comments following it. Note that a stronger result could have been stated.)

LEMMA 2. Let $\alpha_1, \ldots, \alpha_r$ be nonzero algebraic numbers with degrees at most d and heights at most A. Let $\beta_0, \beta_1, \ldots, \beta_r$ be algebraic numbers with degrees at most d and heights at most $B \geq 2$. Suppose that

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_r \log \alpha_r \neq 0.$$

Then there are numbers C = C(r, d) > 0 and $w = w(r) \ge 1$ such that $|A| > B^{-C(\log A)^w}$.

Proof of Lemma 1. Throughout the proof, we will make use of the notation $f \ll g$ which will mean that $|f| \leq cg$ for some constant $c = c(m, a, b, a_1, \ldots, a_m)$ and for all k_1, \ldots, k_m , and n being considered. We also will add to the conditions (i), (ii), and (iii) of the lemma, a fourth condition:

(iv)
$$\sum_{j=1}^{r} a_j b^{k_j} \neq 0$$
 for $1 \leq r \leq m$.

We justify being able to do so by showing that if Lemma 1 is true with the additional condition (iv), then it is true without it. Suppose that Lemma 1 with (iv) holds. If $(k_1, k_2, \ldots, k_m, n)$ satisfies conditions (i), (ii), and (iii) of Lemma 1, but not (iv), then let $r \in \{1, 2, \ldots, m\}$ be as large as possible such that $\sum_{j=1}^r a_j b^{k_j} = 0$. Note by (ii) that r < m. Observe now that $(k_{r+1}, k_2, \ldots, k_m, n)$ satisfies $k_{r+1} < \ldots < k_m, \sum_{j=t}^m a_j b^{k_j} > 0$ for $r+1 \le t \le m$. One can then appeal to Lemma 1 with (iv) to conclude that there are only finitely many such $(k_{r+1}, k_2, \ldots, k_m, n)$. But for each such solution $(k_{r+1}, \ldots, k_m, n)$, there is only a finite number of choices for (k_1, \ldots, k_r) satisfying $0 \le k_1 < \ldots < k_r < k_{r+1}$. Since there are at most m-1 possible values of r, we see that if Lemma 1 holds under condition (iv), then it must hold in general.

Assume that $(k_1, k_2, ..., k_m, n)$ satisfies conditions (i)–(iv). If m = 1, then (iii) becomes

$$a_1b^{k_1}=(b-1)a^n$$
.

Observe that if k_1 and n satisfy the above equation and k_1' and n' are integers for which $a_1b^{k_1'}=(b-1)a^{n'}$, then $b^{k_1-k_1'}=a^{n-n'}$. Since $\log a/\log b$ is irrational, we could then deduce that n'=n and $k_1'=k_1$. In other words, the above equation has at most one solution in integers k_1 and n. Lemma 1 follows immediately, in this case.

Suppose now that m > 1. We make some preliminary estimates. Since $a^n \leq Mb^{k_m}$, where

$$M = \sum_{j=1}^{m} |a_j| \ge 1,$$

we have

$$n \ll k_m$$
.

We improve this estimate to

$$n \ll k_m - k_1$$
.

This is just the previous bound on n if $k_1 = 0$. Suppose now that $k_1 > 0$. Then conditions (i) and (iii) of the lemma imply that every prime divisor of

Digits of a^n

335

b divides a. Let p_1, \ldots, p_t be the distinct prime divisors of a. Write

$$a = \prod_{j=1}^t p_j^{e_j}$$
 and $b = \prod_{j=1}^t p_j^{f_j}$,

where $e_j \ge 1$ and $f_j \ge 0$ for each $j \in \{1, ..., t\}$. We show that for some u and v in $\{1, ..., t\}$,

$$(3) e_u f_v < e_v f_u.$$

If some $f_v = 0$, then (3) holds upon taking p_u to be any prime divisor of b. On the other hand, if each $f_j > 0$, then the values of e_j/f_j for $j \in \{1, \ldots, t\}$ cannot all be the same, since otherwise $\log a/\log b$ would equal this common value and, hence, would be rational. Thus, there are u and v in $\{1, \ldots, t\}$ for which $e_u/f_u < e_v/f_v$, so (3) holds in this case. Fix u and v as in (3) and consider equation (iii). Note that $f_u > 0$. The largest power of p_u dividing the right-hand side of (iii) is $p_u^{e_u n}$. Since $p_u^{f_u}$ divides b and b^{k_1} divides the left-hand side of (iii), we obtain $k_1 f_u \leq e_u n$. Now divide both sides of (iii) by b^{k_1} . Then the left-hand side becomes

$$\sum_{j=1}^{m} a_j b^{k_j - k_1} \le M b^{k_m - k_1} \ll b^{k_m - k_1} ,$$

while the right-hand side $(b-1)a^n/b^{k_1}$ will be a positive integer divisible by p_v^w , where

$$w = e_v n - k_1 f_v \ge (e_v f_u - e_u f_v) n / f_u \ge \frac{n}{f_u}.$$

It follows that

$$p_v^{n/f_u} \ll b^{k_m-k_1}.$$

Since p_v and f_u depend only on a and b, we deduce the inequality $n \ll k_m - k_1$, as desired.

We will also want

$$(4) k_m \ll n+1,$$

so we show next that this is a consequence of (i)–(iii). For $r \in \{2, 3, ..., m\}$, we obtain

$$(b-1)a^{n} = \sum_{j=1}^{m} a_{j}b^{k_{j}} = \left(\sum_{j=r}^{m} a_{j}b^{k_{j}-k_{r}}\right)b^{k_{r}} + \sum_{j=1}^{r-1} a_{j}b^{k_{j}}$$

$$\geq b^{k_{r}} - \left(\sum_{j=1}^{r-1} |a_{j}|\right)b^{k_{r-1}} \geq b^{k_{r}-k_{r-1}} - \sum_{j=1}^{r-1} |a_{j}|,$$

provided that this last expression is positive. Since $b^{k_r-k_{r-1}} \ll 1$ if this last

expression is nonpositive, it follows that in either case

$$k_r - k_{r-1} \ll n + 1$$
 for $r \in \{2, 3, \dots, m\}$.

Therefore,

$$k_m - k_1 = (k_m - k_{m-1}) + (k_{m-1} - k_{m-2}) + \ldots + (k_2 - k_1) \ll n + 1.$$

From (iii), we obtain $b^{k_1} \mid a^n$ so that $k_1 \ll n+1$. Hence, (4) follows.

The basic idea now is to use Lemma 2 to strengthen these estimates. More precisely, we consider n > 2 and show that

(5)
$$k_{m-i+1} - k_{m-i} \ll (\log n)^{w^{i-1}i} \quad \text{for } 1 \le i \le m-1,$$

where w = w(4) is as in Lemma 2. This will imply that

(6)
$$n \ll k_m - k_1 = (k_m - k_{m-1}) + (k_{m-1} - k_{m-2}) + \dots + (k_2 - k_1)$$

 $\ll (\log n)^{w^{m-1}m}$.

Since m and w are fixed, we can conclude that n is bounded. By (4) and (i), we conclude that all the k_i are bounded, thereby completing the proof.

It remains to establish (5), which we now prove by induction on i. Assume n > 2 and consider first the case when i = 1. Using (ii) with r = m, we see that $a_m > 0$. From (iii) we get

(7)
$$a_m b^{k_m} (1+D) = (b-1)a^n,$$

where from (i),

$$|D| = \left| \sum_{j=1}^{m-1} \frac{a_j}{a_m} b^{k_j - k_m} \right| \le M b^{k_{m-1} - k_m}.$$

If $k_m - k_{m-1} \leq \log(2M)/\log b$, then since $n \geq 3$, we have immediately $k_m - k_{m-1} \ll \log n$, which is (5) for the case i = 1. So suppose $k_m - k_{m-1} > \log(2M)/\log b$. It follows that |D| < 1/2 and hence

$$|\log(1+D)| \le \sum_{j=1}^{\infty} \frac{|D|^j}{j} \le |D| + \frac{|D|^2}{2(1-|D|)}$$

 $< (1+|D|)|D| < \frac{3}{2}|D| \ll b^{k_{m-1}-k_m}.$

Taking the logarithm of both sides of (7) gives

(8)
$$\log a_m + k_m \log b - \log(b-1) - n \log a \ll b^{k_{m-1}-k_m}.$$

We use Lemma 2 with d=1, r=4, $A=\max\{b,a,a_m\}\ll 1$, and $B=\max\{k_m,n\}\ll n$, where the last inequality follows from (4). Observe that the left-hand side of (8) is zero if and only if D=0. But D=0 implies that $\sum_{j=1}^{m-1}a_jb^{k_j}=0$, contradicting (iv) since $m\geq 2$. So $D\neq 0$ and, therefore,

the left-hand side of (8) is nonzero. It follows from Lemma 2 that

$$b^{k_{m-1}-k_m} \gg B^{-C(\log A)^w}$$
.

where C = C(4,1) and w = w(4). Thus,

$$k_m - k_{m-1} \ll C(\log A)^w \log B \ll \log n$$
,

proving that (5) holds for i = 1. Now fix i in the range $2 \le i \le m - 1$ and suppose that (5) holds for each positive integer j < i. Then from (iii), we obtain

$$D_1 b^{k_{m-i+1}} (1 + D_2) = (b-1)a^n$$
,

where from (ii) with r = m - i + 1,

$$0 < D_1 = a_m b^{k_m - k_{m-i+1}} + a_{m-1} b^{k_{m-1} - k_{m-i+1}} + \dots + a_{m-i+1} \ll b^{k_m - k_{m-i+1}}$$

and

$$|D_2| = \left| \sum_{j=1}^{m-i} \frac{a_j}{D_1} b^{k_j - k_{m-i+1}} \right| \le M b^{k_{m-i} - k_{m-i+1}} \ll b^{k_{m-i} - k_{m-i+1}}.$$

The induction hypothesis implies that

$$k_m - k_{m-i+1} = (k_m - k_{m-1}) + \dots + (k_{m-i+2} - k_{m-i+1}) \ll (\log n)^{w^{i-2}(i-1)}$$

so that

(9)
$$\log D_1 \ll (\log n)^{w^{i-2}(i-1)}.$$

If $k_{m-i+1} - k_{m-i} \le \log(2M)/\log b$, then $k_{m-i+1} - k_{m-i} \ll (\log n)^{w^{i-1}i}$, as desired. So suppose $k_{m-i+1} - k_{m-i} > \log(2M)/\log b$. As in the above case for i = 1 we have $|D_2| < 1/2$ and hence $|\log(1 + D_2)| < 3|D_2|/2$. Thus,

(10)
$$\log D_1 + k_{m-i+1} \log b - \log(b-1) - n \log a \ll b^{k_{m-i}-k_{m-i+1}}.$$

We use Lemma 2 with $d=1, r=4, A=\max\{b,a,D_1\}$, and $B=\max\{k_{m-i+1},n\}\ll n$. Observe that the left-hand side of (10) is zero if and only if $D_2=0$. But $D_2=0$ implies $\sum_{j=1}^{m-i}a_jb^{k_j}=0$, which contradicts (iv) since $m\geq m-i\geq 1$. Hence the left-hand side of (10) is nonzero. Therefore, from Lemma 2,

$$b^{k_{m-i}-k_{m-i+1}} \gg B^{-C(\log A)^w}$$

where C = C(4,1) and w = w(4). Note that (9) implies that

$$\log A \ll (\log n)^{w^{i-2}(i-1)}.$$

Thus, we easily deduce that

$$k_{m-i+1} - k_{m-i} \ll C(\log A)^w \log B \ll (\log n)^{w^{i-1}i}$$

which completes the induction and the proof.

3. The proof of Theorem 2. Fix b not a prime power, and let pbe a prime. If p does not divide b, then for each positive integer m, p^n divides $b^{m\phi(p^n)} - 1$, a number having exactly one block, and so (2) does not hold. Conversely, suppose p divides b. To prove (2), it suffices to show that for each positive integer k, there is a positive integer n such that every multiple of p^n not ending in the digit 0 base b has > k blocks base b. Assume to the contrary that there exists a positive integer k such that for each positive integer n there is a multiple m_n of p^n which does not end in 0 and which has $\leq k$ blocks. Since $\{m_n\}_{n=1}^{\infty}$ is an infinite sequence, some infinite subsequence S_1 satisfies the condition that every $m \in S_1$ ends in the same nonzero digit d_1 base b. There must now exist an infinite subsequence S_2 of S_1 such that every $m \in S_2$ ends in the same two digits d_2d_1 base b. Continue in this manner so that for $j \geq 2$, S_i is a subsequence of S_{i-1} such that every $m \in S_j$ ends in the same j digits $d_j d_{j-1} \dots d_1$ base b. We now have an infinite sequence $\{d_j\}_{j=1}^{\infty}$, where $d_1 \neq 0$, such that for each positive integer n, there is a multiple m of p^n such that the last n digits of m are $d_n d_{n-1} \dots d_1$ and $B(m,b) \leq k$. Since each such m has $\leq k$ blocks, there are at most k-1 integers $j \geq 2$ such that $d_j \neq d_{j-1}$. Hence, there exists an integer $J \ge 2$ and a $d \in \{0, 1, 2, \dots, b-1\}$ such that $d_j = d$ for every $j \ge J$. Write

$$(d_{J-1}d_{J-2}\dots d_1)_b = p^{n_1}u$$
 and $b^{J-1}d = p^{n_2}v$,

where the integers u and v are relatively prime to p. We consider two cases, arriving at a contradiction in each case.

Case 1: $n_1 \neq n_2$. Since the *b*-ary number $111 \dots 11_b$ is congruent to $1 \pmod{b}$, we get $111 \dots 11_b \equiv 1 \pmod{p}$. Thus, $(dd \dots dd_{J-1} \dots d_1)_b = b^{J-1}d(11\dots 1)_b + (d_{J-1}\dots d_1)_b$ is a sum of two numbers, the first exactly divisible by p^{n_2} and the second exactly divisible by p^{n_1} . Let $t = \min\{n_1, n_2\}$. Since $n_1 \neq n_2$, we have

$$(11) p^t \parallel (dd \dots dd_{J-1} \dots d_1)_b,$$

for any positive number of d's. By the definition of S_{J+t} , there is an $m \in S_{J+t}$ such that p^{t+1} divides m. Also, we may write m in the form $b^{J+t}m' + (dd \dots dd_{J-1} \dots d_1)_b$, where m' is a positive integer and t+1 d's occur to the left of d_{J-1} . The fact that p^{t+1} divides both m and $b^{J+t}m'$ implies p^{t+1} divides $(dd \dots dd_{J-1} \dots d_1)_b$, contradicting (11).

Case 2: $n_1 = n_2$. Let w = v - u(b-1). First, we show that $w \neq 0$. For suppose w = 0. Since $d_1 \neq 0$, we deduce that $b^{J-1}d = p^{n_2}v = p^{n_1}v = p^{n_1}u(b-1) = (d_{J-1}\ldots d_1)_b(b-1)$ is not divisible by b. This contradicts the fact that b divides $b^{J-1}d$, since J was chosen ≥ 2 . Thus $w \neq 0$. Let t be the nonnegative integer for which p^t exactly divides w. Pick $m \in S_{J+t+n_1+1}$ such that p^{J+t+n_1+1} divides m and write m in the form $b^{J+t+n_1+1}m' + b$

Digits of a^n 339

 $(dd \dots dd_{J-1} \dots d_1)_b$, where m' is an integer and $t+n_1+2$ digits d occur to the left of d_{J-1} . We obtain

$$p^{J+t+n_1+1} \mid (dd \dots dd_{J-1} \dots d_1)_b = b^{J-1} d \left(\frac{b^{t+n_1+2}-1}{b-1} \right) + (d_{J-1} \dots d_1)_b.$$

Hence,

$$p^{n_1}v(b^{t+n_1+2}-1) \equiv -p^{n_1}u(b-1) \pmod{p^{J+t+n_1+1}}$$
.

Since p^{t+1} divides b^{t+n_1+2} , we get $v \equiv u(b-1) \pmod{p^{t+1}}$. This contradicts the fact that p^t exactly divides w = v - u(b-1).

In conclusion, the authors thank (blame) J. L. Selfridge for mentioning related questions which led to this work. The authors are also grateful to Titu Andrescue and Andrzej Schinzel for simplifying separate parts of the proof of Lemma 1.

References

- [1] A. Baker, Transcendental Number Theory, Cambridge Univ. Press, Cambridge 1979.
- [2] G. Revuz, Equations diophantiennes exponentielles, C. R. Acad. Sci. Paris Sér. A-B 275 (1972), 1143–1145.

DEPARTMENT OF MATHEMATICAL SCIENCES NORTHERN ILLINOIS UNIVERSITY DEKALB, ILLINOIS 60115 U.S.A.

E-mail: RICHARD@MATH.NIU.EDU

DEPARTMENT OF MATHEMATICS UNIVERSITY OF SOUTH CAROLINA COLUMBIA, SOUTH CAROLINA 29208 U.S.A.

E-mail: FILASETA@MATH.SCAROLINA.EDU NICOL@MATH.SCAROLINA.EDU