Integers With Digits 0 or 1

By D. H. Lehmer, K. Mahler and A. J. van der Poorten

Abstract. Let $g > 2$ be a given integer and $\mathcal{L}$ the set of nonnegative integers which may be expressed in base $g$ employing only the digits 0 or 1. Given an integer $k > 1$, we study congruences $l \equiv a \pmod{k}$, $l \in \mathcal{L}$ and show that such a congruence either has infinitely many solutions, or no solutions in $\mathcal{L}$. There is a simple criterion to distinguish the two cases. The casual reader will be intrigued by our subsequent discussion of techniques for obtaining the smallest nontrivial solution of the cited congruence.

1. Functional Equations. Let $g > 2$ be an integer, and let $\mathcal{L}$ be the language of all nonnegative integers which, in their base $g$ representation, employ only the digits 0 or 1. It is easy to see that a generating function $L(X)$ for $\mathcal{L}$ is given by

$$L(X) = \sum_{h \in \mathcal{L}} X^h = \prod_{n=0}^{\infty} (1 + X^g^n)$$

and it follows readily that $L$ has the functional equation

$$L(X) = (1 + X)L(X^g).$$

Indeed, denote by $\mathcal{P}_t$ the subset of words of $\mathcal{L}$ of at most $t$ digits. Then $\mathcal{P}_t$ has generating function

$$P_t(X) = (1 + X)(1 + X^g) \cdots (1 + X^g^{t-1}).$$

Iterating the original functional equation shows that $L(X)$ has the functional equations

$$L(X) = P_t(X)L(X^g^t), \quad t = 1, 2, \ldots.$$

We now show how to 'divide by $k$'. Let $k$ be a positive integer. In the sums below, $\zeta$ runs through the $k$ zeros of $X^k - 1$. Then,

$$k^{-1} \sum_{\zeta} (\zeta^{-a} \sum_{h \in \mathcal{L}} (\zeta X)^h) = X^a L_a(X^k), \quad a = 0, 1, \ldots, k - 1,$$

where

$$L_a(X) = \sum_{h \in \mathcal{L}_a} X^{(h-a)/k},$$

and

$$\mathcal{L}_a = \{ h \in \mathcal{L} : h \equiv a \pmod{k} \}.$$

Let $G$ be any positive integer and consider a sum

$$\sum_{\zeta} (\zeta^{-a} (\zeta X)^l \sum_{h \in \mathcal{L}} (\zeta X)^h G) = \sum_{\zeta} \sum_{h \in \mathcal{L}} \zeta^{hG-(a-l)} X^{hG+l}. $$

Received March 5, 1985.
1980 Mathematics Subject Classification. Primary 10A30.
The surviving terms are those with \( h \in \mathcal{L} \) and
\[
Gh \equiv a - l \pmod{k}.
\]

Set \((G, k) = D\). The congruence has no solution unless \( D \) divides \( a - l \) in \( \mathbb{Z} \). If \( D | (a - l) \), then the congruence has \( D \) distinct solutions \( \pmod{k} \). If \( c \) is one solution, then the \( D \) solutions are \( c + jk' \pmod{k} \), \( j = 0, 1, \ldots, D - 1 \), where we have set \( k' = k/D \). Further, set \( G' = G/D \). Denote by \( c \) the solution to the congruence so that \( 0 \leq Gc - (a - l) < G'k \) and set \( rk = Gc - (a - l) \). Then the sum we are considering becomes
\[
kX^a \sum_{j=0}^{D-1} X^{(r+jG)k}L_{c+jk}(X^{kG}),
\]
where the suffixes \( c + jk' \) are to be interpreted \( \pmod{k} \) so as to lie in \( \{0, 1, \ldots, k - 1\} \).

Fix \( t \) and set \( G = g' \). Then, we have shown that for each \( a = 0, 1, \ldots, k - 1 \),
\[
L_a(X) = \sum_{l \in \mathcal{P}_t} X^l \sum_{j=0}^{D-1} X^{jG}L_{c+jk'}(X^{G}).
\]
Here \( c_j \equiv (a - l)/G \pmod{A'} \) and \( 0 \leq kr_j = Gc_j - (a - l) < G'k \); and the suffixes \( c_j + jk' \) are to be interpreted \( \pmod{k} \).

What of all this? It is plain that if for some \( t \) there is no \( l \in \mathcal{P}_t \), so that \( a \equiv l \pmod{D} \), where \( D = (g, k) \), then \( L_a(X) = 0 \), so \( \mathcal{L}_a \) is empty. But little else seems obvious. In fact, however, we are essentially finished:

Evidently, either \((g, k) = 1\), in which case we set \( m = 1 \), or there is an \( m > 0 \) so that \((g^m - 1, k) < (g^m, k) = (g^{m+1}, k)\). In either case, we set \((g^m, k) = D\). We note that for all \( t \geq m \), we have \((g^t, k) = D\). Moreover, with \( k' = k/D \) we have \((g, k') = 1\). Hence, there are integers \( t \geq m \) so that \( g^t \equiv 1 \pmod{k'} \). Below, suppose for convenience that \( t \) has this property. Then \( G = g^t \equiv 1 \pmod{k'} \), so \( c_j \equiv a - l \pmod{mod k'} \) and \( kr_j = (G - 1)(a - l) + ig'k \), with the integer \( i \) so chosen that \( 0 \leq r_j < G' \). Our choice of \( t \) makes it easier to explicitly survey the functional equations.

**Theorem.** Let \( g \geq 2 \) and \( k \geq 1 \) be integers, and let \( \mathcal{L} \) be the set of nonnegative integers which in their base \( g \) representation employ only the digits \( 0 \) or \( 1 \). For each \( a = 0, 1, \ldots, k - 1 \), denote by \( \mathcal{L}_a \) the subset of those \( h \in \mathcal{L} \) satisfying the congruence \( h \equiv a \pmod{m} \). If \((g, k) = 1\), set \( m = 1 \) and \( D = 1 \). Otherwise, there is a unique positive integer \( m \), such that \((g^m - 1, k) < (g^m, k) = (g^{m+1}, k)\), and we write \((g^m, k) = D\). Let \( \mathcal{P}_m \) be the subset of elements of \( \mathcal{L} \) of at most \( m \) digits. Then, \( \mathcal{L}_a \) is infinite if and only if there is an \( l \in \mathcal{P}_m \) so that \( a \equiv l \pmod{D} \). Otherwise, \( \mathcal{L}_a \) is empty. In particular (since the condition is empty if \( D = 1 \)), each \( \mathcal{L}_a \) \((a = 0, 1, \ldots, k - 1) \) is infinite if \((g, k) = 1\).

**Proof.** Take \( l \in \mathcal{L} \). Since \( D \mid g^m \), there is no loss of generality, when studying \( l \pmod{D} \), in supposing that \( l \in \mathcal{P}_m \). But if \( l \equiv a \pmod{k} \), then, because \( D \mid k \), a fortiori \( l \equiv a \pmod{D} \). Hence, plainly, \( \mathcal{L}_a \) is indeed empty if there is no \( l \in \mathcal{P}_m \) such that \( a \equiv l \pmod{D} \).

Conversely, suppose that the criterion is satisfied for \( a \) but that \( \mathcal{L}_a \) is finite. We shall show that then all \( \mathcal{L}_a \) are finite, which is absurd because \( \mathcal{L} = \bigcup_{a=0}^{k-1} \mathcal{L}_a \) and \( \mathcal{L} \) is infinite. Firstly, suppose \((g, k) = 1\), and, as suggested, choose \( t \) such that \( g^t \equiv 1 \pmod{k} \). Recall that the series \( L_c \) have nonnegative coefficients (indeed only the coefficients \( 0 \) or \( 1 \)), so that \( L_a \) a polynomial implies that each \( L_c \), with \( c \equiv a - l \pmod{k} \) and \( l \in \mathcal{P}_t \), is a polynomial. Since \( 1 \in \mathcal{P}_t \), in particular \( L_{a-1} \) is a poly-
nominal. Iterating this remark (and, of course, interpreting the suffix mod \( k \)) implies that every \( L_a \) is a polynomial \((a = 0,1,\ldots, k - 1)\), which is a contradiction. We now return to the general case, noticing that we have already shown that \( \bigcup_{j=0}^{D-1} L_{a+jk'} \) is infinite, for this is a congruence subset mod \( k' \) of \( \mathcal{L} \) and \((g, k') = 1\). But \( L_a \) a polynomial implies that there is a \( c \) so that each of the \( L_{c+jk'} \) \((j = 0,1,\ldots, D - 1)\) is a polynomial and this already contradicts the remark just made.

Before mentioning some examples, we prove a simple auxiliary result.

**Lemma.** Distinct elements of \( \mathcal{P}_m \) are incongruent modulo \( D \).

**Proof.** If \( l \neq l' \), then reading from the right, \( l - l' \) has a first nonzero digit, say its \( n \)th digit, the coefficient of \( g^{n-1} \). Set \( D_j = (g', k) \) and note that \( 1 = D_0 < D_1 < \ldots < D_m = D \). Evidently, \( l - l' = \pm g^{n-1} \) (mod \( D_n \)). Thus \( l \neq l' \) (mod \( D \)), seeing that \( D_n \) | \( D \), but \( D_{n-1} < D_n \), so \( g^{n-1} \neq 0 \) (mod \( D_n \)).

**Example 1.** Take \( g = 6, k = 15 \). Here, \( m = 1, D = 3 \). For \( L_a \) not to be empty, we require that there be an \( r \in \mathcal{P}_1 \) with \( a \equiv l \) (mod 3), which is \( a \equiv 0 \) or 1 (mod 3). Hence, the congruence subsets \( L_2(6; 15), L_5(6; 15), L_8(6; 15), L_{11}(6; 15) \) and \( L_{14}(6; 15) \) are empty; the other \( L_a(6; 15) \) are infinite.

**Example 2.** Take \( g = 6, k = 45 \). Here, \( m = 2, D = 9 \). We require that there be an \( r \in \mathcal{P}_2 \) with \( a \equiv l \) (mod 9). The elements of \( \mathcal{P}_2(6) \) are 0,1,6 and 7. Thus the 25 congruence subsets \( L_a(6; 45) \) with \( a \equiv 2,3,4,5 \) or 8 (mod 9) are empty.

**Example 3.** Take \( g = 6, k = 351 = 13 \times 27 \). Here, \( m = 3, D = 27 \), and noting that \( g^2 \equiv 9 \) (mod 27), the elements of \( \mathcal{P}_3 \) modulo 27 are 0,1,6,7,9,10,15 and 16. Hence there are 13(27 - 8) = 247 subsets \( L_a(6; 351) \) that are empty.

**Example 4.** On the other hand, take \( g, k \) so that \( D = 2^m \). There are \( 2^m \) elements in \( \mathcal{P}_m \), and, by the lemma, they are distinct modulo \( D \). In this case every subset \( L_a(g; k) \) is infinite, notwithstanding \( D > 1 \).

2. **The Smallest Nontrivial Element of a Congruence Subset of \( \mathcal{L} \).** In the previous section we expressed the generating functions \( L_a(X) \) as sums of series

\[ X^r L_{c_i}(X^G). \]

We chose \( 0 \leq r_i < G \) and interpreted \( c_i \mod k \). We might equivalently have chosen \( 0 \leq c_i < k \) and have interpreted \( r_i \mod G \). In either case, \( kr_i = Gc_i - (a - l) \). It is easy to see that \( L_a(X) \) has nonzero constant term if and only if \( c \in \mathcal{L} \), \( 0 \leq c < k \). Hence, the terms of degree less than \( G = g' \) in \( L_a(X) \) are given by \( X^r \) for those \( l \) so that \( c_i \in \mathcal{L} \) and \( 0 \leq c_i < k \).

**Example 5.** Take \( g = 10, k = 9 \) and \( a = 0 \). Here, \( m = 1, D = 1 \). Moreover, \( 10^t \equiv 1 \) (mod 9) for all \( t = 1,2,\ldots \). The only elements of \( \mathcal{L} \) less than \( k = 9 \) are 0 and 1. But \( c = 0 \) yields only \( r = 0 \), which is trivial. So, consider \( 1 = c_i \equiv 0 \) (mod 9). The smallest \( l \in \mathcal{L} \) satisfying this congruence is \( 11111111 = (10^8 - 1)/9 \), and it is an element of \( \mathcal{P}_8 \). In fact, \( 10^8 \equiv 1 \) (mod 9), so 8 is a 'convenient' value for \( t \). We have \( 9r_t = 10^8 \times 1 + (10^8 - 1)/9 \), so \( r_t = (10^9 - 1)/9^2 = 12345679 \). The smallest nontrivial element of \( \mathcal{L}_0(10; 9) \) thus is \( 9 \times 12345679 = 11111111 \). Note that only \( l = 0 \) and \( l = (10^8 - 1)/9 \) in \( \mathcal{P}_8 \) yield \( c_i \) with \( c_i \in \mathcal{L} \).

**Example 6.** Take \( g = 10, k = 36 \) and \( a = 0 \). Here, \( m = 2, D = 4 \); so \( k' = 9 \). As above, all \( t = 2,3,\ldots \) are convenient. The only elements of \( \mathcal{L} \) less than \( k = 36 \) are 0,1, 10 and 11. Consider \( 11 = c_i \equiv 0 \) (mod 9) and \( l \equiv 0 \) (mod 4). The smallest \( l \in \mathcal{L} \) satisfying these congruences is \( 11111100 = 10^2(10^7 - 1)/9 \) (obviously
Example 7. Take \( g = 7, k = 66 \) and \( a = 0 \). Here, \( m = 1, D = 1 \) and \( 7^{10} = 1 \) (mod 66) with only multiples of 10 being convenient values of \( t \). The only elements of \( \mathcal{L} \) less than 66 are 0, 1, 2, 3, 5, 6, 7, 8, 9. One might notice that 7 = 120450 = 66 \times 1825 thus chancing upon the smallest nontrivial element of \( \mathcal{L}_0(7; 66) \). But this is unsatisfying. We accordingly forget about ‘convenient’ \( t \) and, using the hint just provided, we look at the functional equation for \( L_0(X) \) with \( t = 6 \). Of the \( 2^6 = 64 \) elements of \( \mathcal{P}_6(7) \), there happened to be 6, so that with \( 7c_i = -l \) (mod 66), we obtain \( c_i \in \mathcal{L} \). The relevant pairs \( l, c_i \) are \( \{0, 1; 101011, \ldots; 111111, \ldots\} \). In each case, we have \( 66r_i = 7c_i + l \) yielding, as smallest nontrivial element of \( \mathcal{L}_0(7; 66) \), the element \( 6 \times 7^6 + 7^5 - 1 \) = 66 \times 1825, as we had already guessed. In fact, the final case shows us that \( t = 4 \) would have sufficed, yielding with \( l \in \mathcal{P}_4 \), the two pairs 0, 50 and 50, 50. The latter provides \( 66r_i = 7^4 \times 50 + 400 = 66 \times 1825 \) as expected.

We conclude that convenient \( t \) may be inconveniently large.

Example 8. Take \( g = 11, k = 40 \) and \( a = 0 \). Here, \( m = 1, D = 1 \) and \( 11^2 = 1 \) (mod 40) so any even \( t \) is convenient. The elements of \( \mathcal{L} \) less than 40 are 0, 1, 11, 12. In \( \mathcal{P}_{11} \), one first finds \( l \) so that \( c_i \in \mathcal{L} \). The pair providing the smallest positive \( r_i \) is \( l = 1 01011 11111(1), c_i = 11 \), yielding \( r_i = 7 91145 52723 \). Thus, the smallest nontrivial element of \( \mathcal{L}_0(11; 40) \) is \( 40r_i = 101 01011 11111(1) \). In this case, it is as if the smallest convenient \( t \) is inconveniently small. In fact, the only arithmetic required is \( 11^{2n} = 1, 11^{2n+1} = 11 \) (mod 40), and a look at \( \mathcal{P}_{13} \) allows one to chance directly upon the sought for element of \( \mathcal{L}_0 \).

In concluding this section, we remark that our functional equations do not play an essential role in determining the smallest nontrivial element of a subset \( \mathcal{L}_a(g; k) \). Indeed, for \( h = 0, 1, \ldots \) set \( b_h = g^h \) (mod \( k \)), with \( 0 \leq b_h < k \) uniquely determining the \( b_h \). The sequence \( \mathcal{B} = (b_h) \) is, of course, periodic and one readily verifies that the sequence has preperiod of length \( m \) and period of length \( t \), where \( t > 0 \) is minimal so that \( g^t = 1 \) (mod \( k' \)). In particular, if \( (g, k) = 1 \) then \( \mathcal{B} \) is pure-periodic. In general, we may write:

\[
\mathcal{B}(g; k) = \{b_0, \ldots, b_{m-1}, b_m, \ldots, b_{m+t-1}\}.
\]

To find elements of, say, \( \mathcal{L}_0 \) we need only notice that \( l \in \mathcal{L}_0 \) implies \( g^m | l \) so

\[
l \equiv x_0b_0 + \cdots + x_{t-1}b_{t-1} \equiv 0 \pmod{k'},
\]

with nonnegative integers \( x_0, \ldots, x_{t-1} \). Indeed, there is an evident correspondence between elements of \( \mathcal{L}_0 \) and such \( t \)-tuples \( x_0, \ldots, x_{t-1} \). At the small cost of some extra notation, we may give a similar description of the elements of any \( \mathcal{L}_a \), thereby obtaining an elementary proof of our Theorem.

We have made some brief suggestions as to how one might find, or, more usefully, verify that one has found the least nontrivial element of sets \( \mathcal{L}_a(g; k) \). We recall that for \( a = 0 \) such sets are always infinite, and we denote by \( \mathcal{M} = \mathcal{M}(g; k) \) the least...
positive multiple of \( k \) whose base \( g \) digits are 0 or 1. The arithmetic functions

\[ k \mapsto \mathcal{M}(g; k) \]

seem quite complicated and it would be interesting to understand them more fully. To this end, we include a brief table listing \( \mathcal{M} \) for \( 3 \leq g \leq 12 \) and \( 1 \leq k \leq 100 \). For compactness, elements of \( \mathcal{M} \) are given in octal; thus the symbols in the body of the table are to be read as:

\[
\begin{align*}
0:000 &\quad 1:001 &\quad 2:010 &\quad 3:011 &\quad 4:010 &\quad 5:011 &\quad 6:100 &\quad 7:101 &\quad 8:110 &\quad 9:111 \\
10 &\quad 11 &\quad 12 &\quad 13 &\quad 14 &\quad 15 &\quad 16 &\quad 17 &\quad 18 &\quad 19 \\
20 &\quad 21 &\quad 22 &\quad 23 &\quad 24 &\quad 25 &\quad 26 &\quad 27 &\quad 28 &\quad 29 \\
30 &\quad 31 &\quad 32 &\quad 33 &\quad 34 &\quad 35 &\quad 36 &\quad 37 &\quad 38 &\quad 39 \\
40 &\quad 41 &\quad 42 &\quad 43 &\quad 44 &\quad 45 &\quad 46 &\quad 47 &\quad 48 &\quad 49 \\
50 &\quad 51 &\quad 52 &\quad 53 &\quad 54 &\quad 55 &\quad 56 &\quad 57 &\quad 58 &\quad 59 \\
60 &\quad 61 &\quad 62 &\quad 63 &\quad 64 &\quad 65 &\quad 66 &\quad 67 &\quad 68 &\quad 69 \\
70 &\quad 71 &\quad 72 &\quad 73 &\quad 74 &\quad 75 &\quad 76 &\quad 77 &\quad 78 &\quad 79 \\
80 &\quad 81 &\quad 82 &\quad 83 &\quad 84 &\quad 85 &\quad 86 &\quad 87 &\quad 88 &\quad 89 \\
90 &\quad 91 &\quad 92 &\quad 93 &\quad 94 &\quad 95 &\quad 96 &\quad 97 &\quad 98 &\quad 99 \\
100 &\quad 101 &\quad 102 &\quad 103 &\quad 104 &\quad 105 &\quad 106 &\quad 107 &\quad 108 &\quad 109 \\
\end{align*}
\]

thereby transforming the entries to their base \( g \) representation which, of course, employs only the digits 0 and 1.

\[
\mathcal{M}(g; k)
\]
3. Remarks. The power series $L(X)$ and the nontrivial $L_a(X)$ that appear in the present note are transcendental functions with the unit circle as their natural boundary. Indeed, their only coefficients are 0 and 1, and each series has arbitrarily long sequences of zero coefficients (cf. Pólya and Szegő [3], Mahler [2]). Arithmetic properties of functions satisfying functional equations as in the present case were studied by the second author and have recently become the subject of further extensive investigation. In particular, if $a$ is algebraic and $0 < |a| < 1$, then $L_a(a)$ is transcendental whenever $S^a$ is nonempty; and $L(a)$ is transcendental. Moreover, interest in these matters has been heightened by the realization that the class of
functions, of which the present ones are examples, is the class of generating functions of sequences recognized by finite automata. For an informal introduction see FOLDS! [1], especially pp. 178ff.

Department of Mathematics
University of California
Berkeley, California 94720

Department of Mathematics
Institute of Advanced Studies
The Australian National University
P. O. Box 4
Canberra, Australia

School of Mathematics and Physics
Macquarie University
North Ryde, N. S. W. 2113, Australia