SOME SEQUENCES OF LARGE INTEGERS

Henry Ibstedt
ö. Förstadsgatan 10 b, 21131 Malmö, Sweden
(Submitted June 1988)

1. Introduction

One of the many interesting problems posed in the book *Unsolved Problems in Number Theory* [1] concerns the sequence

$$nx_n = x_{n-1}^m(x_{n-1} + n - 1),\ x_1 \in N.$$

It was introduced by Fritz Göbel and has been studied by Lenstra [1] for $m = 1$ and $x_1 = 2$. Lenstra states that x_n is an integer for all $n \le 42$, but x_{43} is not. For $m = 2$ and $x_1 = 2$, David Boyd and Alf van der Poorten state that for $n \le 88$ the only possible denominators in x_n are products of powers of 2, 3, 5, and 7. Why do these denominators cause a problem? Is it possible to find even longer sequences of integers by choosing different values of x_1 and m? These questions were posed by M. Mudge [2].

The terms in these sequences grow fast. For $m = 1$, $x_1 = 2$, the first ten terms are:

3, 5, 10, 28, 154, 3520, 15518880, 267593772160, 160642690122633501504.

If the number of digits in x_n is denoted $N(n)$, then $N(11) = 43$, $N(12) = 85$, $N(13) = 168$, $N(14) = 334$, $N(15) = 667$, $N(16) = 1332$, and $N(17) = 2661$. The last integer in this sequence, x_{42}, has approximately 89288343500 digits.

The purpose of this study is to find a method of determining the number of integers in the sequence and apply the method for the parameters $1 \le m \le 10$ and $2 \le x_1 \le 11$. In particular, the problem of Boyd and van der Poorten will be solved. Some explanations will be given to why some of these sequences are so long. It will be observed and explained why the integer sequences are in general longer for even than for odd values of m.

2. Method

For given values of x_1 and m consider the equation

(1) $$kx_k = x_{k-1}(x_{k-1}^m + k - 1)$$

where the prime factorization of k is given by

(2) $$k = \prod_{i=1}^{\ell} p_i^{n_i}.$$

Let us assume that x_{k-1} is an integer and expand x_{k-1} and $x_{k-1}^m + k - 1$ in a number system with $G_i = p_i^{t_i}$, $(t_i > n_i)$ as base.

(3a) $$x_{k-1} = \sum_j a_j G_i^j \quad (0 \le a_j < G_i)$$

and

(3b) $$x_{k-1}^m + k - 1 = \sum_j b_j G_i^j \quad (0 \le b_j < G_i).$$

Since $x_{k-1} \ne 0$, it is always possible to choose t_i so that $a_0 \ne 0$ and $b_0 \ne 0$. With this t_i we have

(4) $$x_{k-1}(x_{k-1}^m + k - 1) = \sum_{j,\ell} a_j b_\ell G_i^{j+\ell} \equiv a_0 b_0 \pmod{G_i}.$$

The congruence

(5) $kx_k \equiv a_0 b_0 \pmod{G_i}$

is soluble iff $(k, G_i) | a_0 b_0$, or, in this case, iff $p_i^{n_i} | a_0 b_0$. But, if $p_i^{n_i} | a_0 b_0$, then by (4) we also have

$$p_i^{n_i} | x_{k-1}(x_{k-1}^m + k - 1).$$

Furthermore, if (5) is soluble for all expansions originating from (2), then it follows that

$$k | x_{k-1}(x_{k-1}^m + k - 1)$$

and, consequently, that x_k is an integer. The solution $x_k \pmod{G_i}$ to $kx_k \equiv a_0 b_0 \pmod{G_i}$ is equal to the first term in the expansion of x_k using the equivalent of (3a). The previous procedure is repeated using (3b), (4), and (5) to examine if $x_{k+1} \pmod{G_i}$ is an integer.

From the computational point of view, the testing is done up to a certain pre-set limit $k = k_{\max}$ for consecutive primes $p = 2, 3, 5, 7, \ldots$ to $p \le k_{\max}$. One of three things will happen:

1. All congruences are soluble modulus G_i for $k \le k_{\max}$ for all $p_i \le k_{\max}$.
2. $a_0 b_0 = 0$ for a certain set of values $k \le k_{\max}$, $p_i \le k_{\max}$.
3. The congruence $kx_k \equiv a_0 b_0 \pmod{G_i}$ is soluble for all $k < n \le k_{\max}$, but not soluble for $k = n$ and $p = p_i$.

In cases 1 and 2 increase $k_{\max}$, respectively, t_i in $G_i = p_i^{t_i}$ (if computer facilities permit) and recalculate. In case 3, x_n is not an integer, viz. n has been found so that x_k is an integer for $k < n$ but not for $k = n$.

3. Results

The results from using this method in the 100 cases $1 \le m \le 10$, $2 \le x_1 \le 11$ are shown in Table 1. In particular, it shows that the integer sequence holds up to $n = 88$ for $m = 2$, $x_1 = 2$ which corresponds to the problem of Boyd and van der Poorten. The longest sequence of integers was found for $x_1 = 11$, $m = 2$. For these parameters, the 600 first terms are integers, but x_{601} is not. In the 100 cases studied, only 32 different primes occur in the terminating values n. In 7 cases, the integer sequences are broken by values of n which are not primes. In 6 of these, the value of n is 2 times a prime which had terminated other sequences. For $x_1 = 3$, $m = 10$, the sequence is terminated by $n = 2 * 13^2$. The prime 239 is involved in terminating 10 of the 100 sequences studied. It occurs 3 times for $m = 6$ and 7 times for $m = 10$. It is seen from the table that integer sequences are in general longer for even than for odd values of m.

TABLE 1. x_n is the first noninteger term in the sequence defined by $nx_n = x_{n-1}(x_{n-1}^m + n - 1)$. The table gives n for parameters x_1 and m.

m	$x_1 = 2$	$x_1 = 3$	$x_1 = 4$	$x_1 = 5$	$x_1 = 6$	$x_1 = 7$	$x_1 = 8$	$x_1 = 9$	$x_1 = 10$	$x_1 = 11$
1	43	7	17	34	17	17	51	17	7	34
2	89	89	89	89	31	151	79	89	79	601
3	97	17	23	97	149	13	13	83	23	13
4	214	43	139	107	269	107	214	139	251	107
5	19	83	13	19	13	37	13	37	347	19
6	239	191	359	419	127	127	239	191	239	461
7	37	7	23	37	23	37	17	23	7	37
8	79	127	158	79	103	103	163	103	163	79
9	83	31	41	83	71	83	71	23	41	31
10	239	338	139	137	239	239	239	239	239	389

4. A Model To Explain Some Features of the Sequence

The congruence

$$x(k) \equiv \alpha(k) \pmod{p},\ \alpha(k) \in \{-1, 0, 1, \ldots, p - 2\}$$

studied in a number system with a sufficiently large base p^t, is of particular interest when looking at the integer properties of the sequence. Five cases will be studied. These are:

1. $\alpha(k)$ does not belong to cases 2, 3, 4, or 5 below
2. $\alpha(k) = -1,\ p \neq 2$
3. $\alpha(k) = 0$
4. $\alpha(k) = 1$
5. $\alpha(k) = \alpha(k + 1)$ and/or $\alpha(k) = \alpha(k - 1),\ \alpha(k) \neq -1, 0, 1$

These cases are mutually exclusive; however, in case 5 there may be more than one sequence of the described type for a given p, for example, for $m = 10$, $x_1 = 7$, and $p = 11$, we have $\alpha(k) = 7$ for $k = 1, 2, \ldots, 10$ and $\alpha(k) = 4$ for $k = 11, 12, \ldots, 15$. Therefore, when running through the values of k for a given p, it is possible to classify $\alpha(k)$ into states corresponding to cases 1, 2, 3, 4 or into one of several possible states corresponding to case 5. In this model, $\alpha(1)$ appears as a result of creation rather than transition from one state to another but, formally, it will be considered as resulting from transition from a state 0 ($k = 0$) to the state corresponding to $\alpha(1)$.

The study of transitions from one state to another in the above model is useful in explaining why there are such long sequences of integers and why they are in general longer for even than for odd m. Table 2 shows the number of transitions of each kind in the 100 cases studied. Let a_r be the number of transitions from state r to state s:

$$A_r = \sum_r a_{rs},\ B_s = \sum_s a_{rs},\ Q_s = 100A_s/B_s.$$

(Note that r and s refer to states not rows and columns in Table 2.) The transitions for odd and even values of m are treated separately. It is seen that transitions from states 4, 5, and 2 (for even m) are rare. Only between 5% and 14% of all such states "created" are "destroyed," while the corresponding percentage for other transitions range between 85% and 99%. It is the fact that transitions from certain states are rare, which makes some of these integer sequences so long. That transitions from state 2 are rare for even m (11%) and frequent for odd m (99%) make the integer sequences in general longer for even than for odd m. In all the many transitions observed, it was noted that certain types (underscored in Table 2) only occurred for values of k divisible by p, while other types never occurred for k divisible by p. Transitions from state 3 all occur for k divisible by p but, unlike the other transitions which occur for k divisible by p, they have a high frequency. Some of the observations made on the model are explained in the remainder of this paper.

TABLE 2. The number of transitions of each type for odd and even m

From state	To state 1 $2\nmid m$	To state 1 $2\mid m$	To state 2 $2\nmid m$	To state 2 $2\mid m$	To state 3 $2\nmid m$	To state 3 $2\mid m$	To state 4 $2\nmid m$	To state 4 $2\mid m$	To state 5 $2\nmid m$	To state 5 $2\mid m$	A_r $2\nmid m$	A_r $2\mid m$
0	467	1847	38	40	60	60	55	55	32	69	652	2071
1			220	701	252	791	247	642	75	307	794	2241
2	181	$\underline{55}$			71	$\underline{21}$	39	$\underline{7}$	2	0	293	83
3	$\underline{202}$	$\underline{634}$	$\underline{36}$	$\underline{30}$			$\underline{111}$	$\underline{80}$	$\underline{9}$	$\underline{16}$	358	760
4	$\underline{20}$	$\underline{35}$	$\underline{2}$	$\underline{6}$	$\underline{39}$	$\underline{12}$				$\underline{3}$	61	56
5	$\underline{2}$	$\underline{2}$	$\underline{1}$	$\underline{2}$	0	$\underline{3}$	0	$\underline{2}$	$\underline{2}$	$\underline{11}$	5	20
B_s	872	2573	297	779	422	887	452	786	120	406	2163	5431
Q_s %	92	95	99	11	85	86	14	8	5	5		

Transitions from state 4 and, for even m *only, from state 2*

It is evident from $kx_k = x_{k-1}(x_{k-1}^m + k - 1)$ that, if $x_{k-1} \equiv \pm 1 \pmod{p}$ and $(k, p) = 1$, then $x_k = \pm 1 \pmod{p}$. Assume that we arrive at $x_{k-1} \equiv \pm 1 \pmod{p}$ for $k < p - m$ and $m < p$. We can then write

(6) $\quad x_{p-m-1} \equiv \pm 1 + \alpha p \pmod{p^2},\ 0 \le \alpha < p$

and

(7) $\quad x_{p-m-1}^m \equiv (\pm 1 + \alpha p)^m \equiv 1 \pm m\alpha p \pmod{p^2}$ (m even).

Equations (6) and (7) give

$$(p - m)x_{p-m} \equiv \pm(p - m) \pmod{p^2}$$

or, since $(p - m, p) = 1$,

$$x_{p-m} \equiv \pm 1 \pmod{p^2} \quad \text{or} \quad x_k \equiv \pm 1 \pmod{p^2} \text{ for } p - m \le k \le p - 1.$$

For $k = p$, we have

$$px_p \equiv \pm 1(1 + p - 1) \pmod{p^2}$$

or, after division by p throughout

$$x_p \equiv \pm 1 \pmod{p}.$$

It is now easy to see that $x_k \equiv 1 \pmod{p}$ continues to hold also for $k > p$. The integer sequence may, however, be broken for $k = p^2$.

Transitions from state 3

Let us assume that $x_j \equiv 0 \pmod{p}$ for some $j < p$. If $(j + 1, p) = 1$, it follows that $x_{j+1} \equiv 0 \pmod{p}$ or, generally, $x_k \equiv 0 \pmod{p}$ for $j \le k \le p - 1$. For $k = p - 1$, we can write $x_{p-1} \equiv pa \pmod{p^2}$, $0 \le a < p - 1$. We then have

$$px_p \equiv pa(p^m a^m + p - 1) \pmod{p^2},$$

from which follows $x_p \equiv -a \pmod{p}$, viz. x_p is an integer; however, if $a \not\equiv 0$, the state is changed.

Transitions from states of type 5

When, for some $j < p - 1$, it happens that $x_j^m \equiv 1 \pmod{p}$, it is easily seen that $x_k \equiv x_j \pmod{p}$ for $j \le k < p$. This implies

$$px_p \equiv x_j(1 + p - 1) \pmod{p},$$

from which it is seen that x_p may not be congruent to $x_j \pmod{p}$ but also that x_p is an integer.

References

1. R. K. Guy. *Unsolved Problems in Number Theory*. New York: Springer-Verlag, 1981, p. 120.
2. *Personal Computer World*, December 1987, p. 213.

*****