**Example 5.24.** With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Now altering $a_0$ to $551$ the sequence produced is

$$551, 778, 95, 402, 599, 186, 463, 130, 487, 234.$$

Keeping everything fixed except $n = 8000$ we obtain

$$551, 7178, 5695, 4402, 599, 2586, 7663, 130, 1287, 3434.$$

With $n = 40$, $m = 22$, $c = 20$ and $a_0 = 13$ we obtain

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Of course such sequences are not random (by definition) and we have a formula for the terms.

**Theorem 5.25.** *The $kth$ term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)}\right) \pmod{n},$$

*with $0 \leq a_k < n$.*

Also note that there are at most $n$ values for the terms of the sequence, which must all lie between $0$ and $n-1$. Therefore, after at most $n$ terms have been generated there are two terms which are the same. Since the $k+1$ term depends only on the $k$ term this means that the sequence repeats itself from this point on: if $a_s = a_t$, with $s > t$, then $a_{s+1} = a_{t+1}$, $a_{s+2} = a_{t+2}$, and so on. The sequence then looks far from random. The **period** of the sequence is the smallest integer $d$ such that, for some $s, t$, we have $a_s = a_{s+d}$. The period is at most $n$; but some choices of $c, m$ and $n$ result in periods shorter than $n$. In fact it can be shown that the period is $n$ if and only if $\gcd(c, n) = 1$, $m \equiv 1 \pmod{p}$, for all primes $p$ dividing $n$, and $m \equiv 1 \pmod{4}$ if $4|n$.

Analysis of "how random" a pseudo-random sequence is involves applying statistical tests to the sequence. For instance the frequency of occurence of a particular integers in the sequence can be tested; as can the frequency of occurence of pairs of integers.

### 5.10 Objectives

After covering this chapter of the course you should be able to:

(i) recall the definition of congruence;

(ii) recall the statement of Lemma 5.8 and understand its proof;

(iii) do arithmetic modulo $n$;

(iv) understand how various divisibility tests work and be able to apply them;

(v) decide whether or not an integer has an inverse modulo $n$;

(vi) generate a sequence of pseudo-random numbers.