# Integer sequences that become periodic on reduction modulo k for all k

**Peter Bala, Dec 03 2017**

We find a family of sequences $\{a(n)\}$ with the property that for each positive integer $k$ the sequence $a(n) \pmod k$ is purely periodic.

Let $P(x)$ be a polynomial with integer coefficients. Using the binomial theorem we see that the sequence $a(n) := P(n)$ satisfies the congruence

$$a(n+k) - a(n) = P(n+k) - P(n) \equiv 0 \pmod k$$

for all $n$ and $k$. Therefore, for each positive integer $k$, the sequence $a(n) \pmod k$[1] is a purely periodic sequence whose exact period divides $k$. Our aim in this note is to find a larger class of sequences that share this property of becoming periodic modulo $k$ for every $k$.

A second source of such sequences comes from sequences satisfying a linear recurrence with polynomial coefficients. For example, consider an integer sequence $a(n)$ satisfying the second-order recurrence

$$a(n) = P_1(n)a(n-1) + P_2(n)a(n-2) + c, \tag{1}$$

where $P_1(n)$ and $P_2(n)$ are polynomials with integer coefficients and $c$ is an integer constant.

From (1)

$$\begin{aligned} a(n+k) &= P_1(n+k)a(n-1+k) + P_2(n+k)a(n-2+k) + c \\ &\equiv P_1(n)a(n-1+k) + P_2(n)a(n-2+k) + c \pmod k\,. \end{aligned} \tag{2}$$

Subtract (1) from (2) to find

$$\begin{aligned} a(n+k) - a(n) \equiv\ & P_1(n)(a(n-1+k) - a(n-1)) \\ & + P_2(n)\,(a(n-2+k) - a(n-2)) \pmod k\,. \end{aligned} \tag{3}$$

Suppose we can establish the pair of congruences $a(k) \equiv a(0) \pmod k$ and $a(k+1) \equiv a(1) \pmod k$ hold for all $k$ (perhaps using some known formula for $a(k)$). Then we can use (3) in an induction argument on $n$ to prove the congruence $a(n+k) \equiv a(n) \pmod k$ holds for all $n$ and $k$. Examples from the OEIS where this method works include A000522, A025168, A046662, A047974, A052143, A064570 and A229464. The OEIS gives exponential generating functions for each of these sequences. All the generating functions have the form $F(x)\exp(xG(x))$ with $F(x)$ and $G(x)$ integral power series. This observation lead us to Theorem 1 below. First we establish the following preliminary result.

[1] We take the set $\{0, 1, ..., k-1\}$ as our complete residue system modulo $k$.

**Lemma 1.** *Let $a(n)$ be an integer sequence such that $a(n+k) \equiv a(n)$ (mod $k$) for all $n$ and $k$. Let $F(x) = f_0 + f_1 x + f_2 x^2 + \cdots$ be an integral power series. Define an integer sequence $b(n)$ by*

$$\sum_{n=0}^{\infty} b(n) \frac{x^n}{n!} \quad := \quad F(x) \sum_{n=0}^{\infty} a(n) \frac{x^n}{n!} . \tag{4}$$

*Then*

$$b(n+k) \equiv b(n) \ (\textit{mod } k) \quad \textit{for all } n \textit{ and } \ k.$$

**Proof.** We use a strong induction argument on $n$.

(i) Case $n = 0$. Comparing the coefficients of $x^k$ on each side of (4) yields the formula

$$\begin{aligned} b(k) \quad &= \quad f_0 a(k) + f_1 k a(k-1) + f_2 k(k-1) a(k-2) \\ &\quad + \cdots + f_k k! a(0) . \end{aligned} \tag{5}$$

Taking $k = 0$ in (5) gives

$$b(0) \quad = \quad f_0 a(0) . \tag{6}$$

Subtract (6) from (5) to find

$$\begin{aligned} b(k) - b(0) \quad &= \quad f_0(a(k) - a(0)) + \text{terms divisible by } k \\ &\equiv \quad 0 \ (\text{mod } k) \end{aligned}$$

for all $k$, since by assumption $a(k) - a(0)$ is divisible by $k$ for all $k$.

(ii) Next we make the strong induction hypothesis that the congruence $b(n+k) \equiv b(n)$ (mod $k$) holds for all $k$ and for $0 \le n \le N$. We show the congruence also holds for all $k$ when $n = N+1$.

By (5)

$$\begin{aligned} b(N+1) \quad &= \quad f_0 a(N+1) + f_1 (N+1) a(N) + f_2 (N+1) N a(N-1) \\ &\quad + \cdots + f_{N+1} (N+1)! a(0) \end{aligned} \tag{7}$$

and also for all $k \ge 1$

$$\begin{aligned} b(N+1+k) \quad &= \quad f_0 a(N+1+k) + f_1 (N+1+k) a(N+k) + f_2 (N+1+k)(N+k) a(N+k-1) \\ &\quad + \cdots + f_{N+1} (N+1+k) ... (k+1) a(k) \\ &\quad + \text{terms divisible by } k, \end{aligned}$$

from which we obtain

$$\begin{aligned} b(N+1+k) \quad &\equiv \quad f_0 a(N+1+k) + f_1 (N+1) a(N+k) + f_2 (N+1) N a(N+k-1) \\ &\quad + \cdots + f_{N+1} (N+1)! a(k) \quad (\text{mod } k) . \end{aligned} \tag{8}$$

Subtracting (7) from (8) yields

$$\begin{aligned} b(N+1+k)-b(N+1) &\equiv f_0(a(N+1+k)-a(N+1))+f_1(N+1)(a(N+k)-a(N)) \\ &\quad +\cdots+f_{N+1}(N+1)!(a(k)-a(0)) \pmod{k}. \end{aligned}$$

All the summands on the right-hand side are divisible by $k$, since by assumption $a(n+k)=a(n) \pmod{k}$ for all $n$ and $k$. Hence we conclude that $b(N+1+k)-b(N+1)$ is divisible by $k$ for all $k$, completing the induction argument. □

**Theorem 1.** *Suppose the integer sequence $a(n)$ has an exponential generating function $A(x)$ of the form*

$$\begin{aligned} A(x) &:= \sum_{n=0}^{\infty} a(n)\frac{x^n}{n!} \\ &= F(x)\exp(xG(x)), \end{aligned}$$

*where $F(x), G(x) \in \mathbb{Z}[[x]]$ are formal power series with integer coefficients and $G(0)=1$. Then the conguence*

$$a(n+k) \equiv a(n) \pmod{k}$$

*holds for all $n$ and $k$.*

**Proof**. By Lemma 1, it is sufficient to prove the result in the case $F(x)=1$. We can therefore assume the e.g.f. of the sequence $a(n)$ is

$$A(x) = \exp(xG(x)), \quad G(x) \in \mathbb{Z}[[x]],\, G(0)=1. \tag{9}$$

Firstly, we find a recurrence equation satisfied by the sequence. Differentiating (9) gives

$$A'(x) = \sum_{n=0}^{\infty} a(n+1)\frac{x^n}{n!} = A(x)\left(G(x)+xG(x)'\right). \tag{10}$$

By the assumptions on $G(x)$, the power series $G(x)+xG'(x)$ has the form $1+g_1x+g_2x^2+\cdots$, where the coefficients $g_i$ are integers. Hence (10) becomes

$$\sum_{n=0}^{\infty} a(n+1)\frac{x^n}{n!} = \left(\sum_{n=0}^{\infty} a(n)\frac{x^n}{n!}\right)\left(1+g_1x+g_2x^2+\cdots\right).$$

Extracting the coefficient of $x^n$ on both sides of this equation leads to the recurrence equation

$$a(n+1) = a(n)+ng_1a(n-1)+n(n-1)g_2a(n-2)+\cdots+n!g_na(0). \tag{11}$$

We shall use this recurrence to prove the congruence $a(n+k) \equiv a(n) \pmod{k}$ holds for all $n$ and $k$ by a strong induction argument on $n$. The proof is similar to the proof of the Lemma.

(i) Case $n = 0$. We claim $a(k) \equiv a(0) \pmod{k}$ for all $k$.

It follows from $A(x) = \sum_{n=0}^{\infty} a(n) \frac{x^n}{n!} = \exp(xG(x))$ that $a(0) = 1$.

Let [ ] denote the coefficient extractor operator. Then

$$
\begin{aligned}
a(k) &= k![x^k]\exp(xG(x)) \\
&= k!\left[x^k\right]\left(\sum_{i=0}^{\infty} x^i \frac{G(x)^i}{i!}\right) \\
&= k!\left(\sum_{i=0}^{k} [x^{k-i}] \frac{G(x)^i}{i!}\right) \\
&= 1 + \sum_{i=0}^{k-1} \frac{k!}{i!}\left[x^{k-i}\right] G(x)^i \\
&\equiv 1 \pmod{k},
\end{aligned}
$$

since $G(x)$ is an integral power series. Hence $a(k) \equiv 1 \pmod{k}$, that is, $a(k) \equiv a(0) \pmod{k}$.

(ii) We now make the strong induction hypothesis that the congruence $a(n+k) \equiv a(n) \pmod{k}$ holds for all $k$ and for $0 \leq n \leq N$. We show the congruence also holds for all $k$ when $n = N + 1$.

From the recurrence (11) we obtain

$$
\begin{aligned}
a(N+1) &= a(N) + Ng_1 a(N-1) + N(N-1)g_2 a(N-2) \\
&\quad + \cdots + N!g_N a(0)
\end{aligned} \tag{12}
$$

as well as for all $k \geq 1$

$$
\begin{aligned}
a(N+1+k) &= a(N+k) + (N+k)g_1 a(N-1+k) + (N+k)(N+k-1)g_2 a(N-2+k) \\
&\quad + \cdots + (N+k)...(k+1)g_N a(k) \\
&\quad + \text{terms divisible by } k,
\end{aligned}
$$

from which

$$
\begin{aligned}
a(N+1+k) &\equiv a(N+k) + Ng_1 a(N-1+k) + N(N-1)g_2 a(N-2+k) \\
&\quad + \cdots + N!g_N a(k) \pmod{k}.
\end{aligned} \tag{13}
$$

Subtract (12) from (13) to find

$$
\begin{aligned}
a(N+1+k) - a(N+1) &\equiv (a(N+k) - a(N)) + Ng_1(a(N-1+k) - a(N-1)) \\
&\quad + \cdots + N!g_N(a(k) - a(0)) \pmod{k}.
\end{aligned}
$$

By the strong induction hypothesis, each of the summands on the right-hand side is divisible by $k$. We conclude that $a(N+1+k) - a(N+1)$ is divisible by $k$ for all $k$, thus completing the induction argument. $\square$

**Corollary.** *Suppose the integer sequence $a(n)$ has an exponential generating function $A(x)$ of the form*

$$\begin{aligned} A(x) &:= \sum_{n=0}^{\infty} a(n)\frac{x^n}{n!} \\ &= F(x)\exp(-xG(x)), \end{aligned}$$

*where $F(x), G(x) \in \mathbb{Z}[[x]]$ are formal power series with integer coefficients and $G(0) = 1$. Then the conguence*

$$a(n+k) \equiv (-1)^k a(n) \pmod{k}$$

*holds for all $n$ and $k$.*

**Proof.** Change $x$ to $-x$ in Theorem 1. $\square$

For sequences $a(n)$ satisfying the conditions of the Corollary it follows that for even $k$ the sequence $a(n) \pmod{k}$ is purely periodic with exact period a divisor of $k$, while for odd $k$ the sequence $a(n) \pmod{k}$ is purely periodic with exact period a divisor of $2k$.

**Example.** The sequence of derangement numbers $d(n) =$ A000166(n) begins

$[1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570, 176214841, 2290792932, ...]$.

The sequence has the e.g.f. $\frac{1}{1-x}\exp(-x)$ and so satisfies the conditions of the Corollary. Calculation gives

$d(n) \pmod{10} = [\overline{1, 0, 1, 2, 9, 4, 5, 4, 3, 6}, 1, 0, 1, 2, 9, 4, 5, 4, 3, 6, ...]$ is purely periodic with period 10

and

$d(n) \pmod{7} = [\overline{1, 0, 1, 2, 2, 2, 6, 6, 0, 6, 5, 5, 5, 1}, 1, 0, 1, 2, 2, 2, 6, 6, 0, 6, 5, 5, 5, 1, ...]$ is purely periodic with period 14.

**Question.** Are there integer sequences $a(n)$ satisfying the congruence properties $a(n+k) \equiv a(n) \pmod{k}$ for all $n$ and $k$ but whose exponential generating function is not of the form $F(x)\exp(xG(x))$?