



# On Modular Representations of C-Recursive Integer Sequences

M. Prunescu

University of Bucharest

Research Center for Logic, Optimization and Security (LOS)

Faculty of Mathematics and Computer Science

Academiei 14

Bucharest (RO-010014)

Romania

and

Institute of Logic and Data Science

Bucharest

Romania

and

Simion Stoilow Institute of Mathematics of the Romanian Academy

Research Unit 5

P. O. Box 1-764

Bucharest (RO-014700)

Romania

[mihai.prunescu@imar.ro](mailto:mihai.prunescu@imar.ro)

[mihai.prunescu@gmail.com](mailto:mihai.prunescu@gmail.com)

J. M. Shunia

Independent Researcher

Ann Arbor, MI

USA

[jshunia@gmail.com](mailto:jshunia@gmail.com)

## Abstract

Prunescu and Sauras-Altuzarra showed that all C-recursive sequences of natural numbers have an arithmetic div-mod representation that can be derived from their

generating function. This representation consists of computing the quotient of two exponential polynomials and taking the remainder of the result modulo a third exponential polynomial, and works for all integers  $n \geq 1$ . Using a different approach, Prunescu proved the existence of two other representations, one of which is the mod-mod representation, consisting of two successive remainder computations. This result has two weaknesses: the representation works only ultimately, and a correction term must be added to the first exponential polynomial. We show that a mod-mod representation without inner correction term holds for all integers  $n \geq 1$ . This follows directly from the div-mod representation by an arithmetic short-cut from outside.

## 1 Introduction

The *C-recursive sequences of order  $d$*  are sequences  $t : \mathbb{N} \rightarrow \mathbb{C}$  satisfying a relation of recurrence with constant coefficients

$$t(n+d) + \alpha_1 t(n+d-1) + \cdots + \alpha_{d-1} t(n+1) + \alpha_d t(n) = 0$$

for all  $n \in \mathbb{N}$ , with  $\alpha_d \neq 0$ . With the recurrence rule, we associate the polynomial

$$B(X) := 1 + \alpha_1 X + \cdots + \alpha_d X^d.$$

Observe that  $\deg B = d$ . We let  $\tilde{B}(X)$  denote the *reciprocal polynomial*

$$\tilde{B}(X) = X^d B(X^{-1}) = X^d + \alpha_1 X^{d-1} + \cdots + \alpha_d.$$

According to [6, Theorem 4.1.1] and [3, Theorem 1], the C-recursive sequences are exactly the sequences  $(s(n))$  such that the generating function

$$f(X) = \sum_{n \geq 0} t(n) X^n$$

is a rational function  $A(X)/B(X)$  with  $\deg(A) := k < \deg(B) = d$ . We define  $\tilde{A}(X) = X^k A(X^{-1})$  to be the reciprocal polynomial of  $A(X)$ . We observe that

$$f(X^{-1}) = \frac{X^{d-k} X^k A(X^{-1})}{X^d B(X^{-1})} = X^{d-k} \cdot \frac{\tilde{A}(X)}{\tilde{B}(X)}.$$

Prunescu and Sauras-Altuzarra proved [5] that if  $f$  is the generating function of a sequence consisting of natural numbers only, then there exists  $c \in \mathbb{N}$  such that for all  $n \in \mathbb{Z}^+$ , we have

$$t(n) = \left\lfloor c^{n^2} f(c^{-n}) \right\rfloor \bmod c^n.$$

The exact statement will be given below (see Theorem 2). In brief, if the sequence is C-recurrent, its generating function  $f$  is a rational function  $A(X)/B(X)$  with  $A(X), B(X) \in$

$\mathbb{Z}[X]$ ,  $\deg(A(X)) = k < \deg(B(X)) = d$ , and such that both polynomials  $A(X)$  and  $B(X)$  take positive values for real positive  $X$  inside the disk of convergence around 0. Then we have a *div-mod representation*

$$t(n) = \left\lfloor \frac{c^{n^2+dn} A(c^{-n})}{c^{dn} B(c^{-n})} \right\rfloor \bmod c^n = \left\lfloor \frac{c^{n^2} c^{n(d-k)} \tilde{A}(c^n)}{\tilde{B}(c^n)} \right\rfloor \bmod c^n.$$

We note that “*div-mod*” refers to the successive application of an integer division and a modular reduction.

Prunescu proved in [4] the following *mod-mod representation*. Let  $\alpha_d \neq 0$  be the constant term of the recurrence rule for a C-recursive sequence, i.e., the constant term of  $\tilde{B}(X)$ . Then there are  $c, n_0 \in \mathbb{N}$  such that for  $n \geq n_0$  we have

$$t(n) = \frac{\left( \left( c^{n(d-1)+\lceil n/2 \rceil} - \operatorname{sgn}(\alpha_d) \cdot c^{n^2} c^{n(d-k)} \tilde{A}(c^n) \right) \bmod \tilde{B}(c^n) \right) \bmod c^n}{|\alpha_d|}.$$

This representation has the advantage that

$$(c^{n(d-1)+\lceil n/2 \rceil} - \operatorname{sgn}(\alpha_d) \cdot c^{n^2} c^{n(d-k)} \tilde{A}(c^n)) \bmod \tilde{B}(c^n)$$

can be computed faster by modular arithmetic, but it has two disadvantages:

- (i) It needs in general a correction term  $c^{n(d-1)+\lceil n/2 \rceil}$  in the innermost exponential polynomial.
- (ii) It holds only ultimately, for  $n$  greater than or equal to some a priori undetermined  $n_0 \in \mathbb{N}$ . In fact, such an  $n_0$  can be determined by conditions used in the proof, but it is not clear that one can always take  $n_0 = 1$ .

In the following we show that this result can be improved. *If the constant term of  $\tilde{B}(X)$  is  $\alpha_d \neq 0$ , there exists an integer  $r \geq c$  such that the following holds for all  $n \geq 1$ :*

$$t(n) = \frac{-1 - \operatorname{sgn}(\alpha_d)}{2} + \frac{1}{|\alpha_d|} \left( \left( (-\operatorname{sgn}(\alpha_d) \cdot r^{n^2} r^{n(d-k)} \tilde{A}(r^n)) \bmod \tilde{B}(r^n) \right) \bmod r^n \right).$$

Observe that this representation does not contain any correction term and works for  $n \geq 1$ . The proof, done by a short-cut of modular arithmetic, uses only the div-mod representation given above.

Other possibilities and methods to represent C-recursive sequences can be found in the monograph of Kauers and Paule [2].

## 2 Technical preparations

We define  $\mathbb{N}$  as the set of natural numbers with 0 included.

The first three useful results refer to C-recursive sequences. The next lemma can also be found in Everest et al. [1].

**Lemma 1.** [Prunescu & Sauras-Altuzarra, [5, Lemma 4]] *If  $t : \mathbb{N} \rightarrow \mathbb{C}$  is C-recursive, then there is an integer  $g \geq 1$  such that  $|t(n)| < g^{n+1}$  for every integer  $n \geq 0$ .*

**Theorem 2.** [Prunescu & Sauras-Altuzarra, [5, Theorems 1 and 2]] *If  $t : \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(X)$  is its generating function,  $R$  is the radius of convergence of  $f(X)$  at zero, and  $c$ ,  $m$ , and  $n$  are three integers such that  $c \geq 2$ ,  $n \geq m \geq 2$ ,  $c^{-m} < R$ , and  $t(n) < c^{n-2}$  for every integer  $n \geq m$ , then*

$$t(n) = \left\lfloor c^{n^2} f(c^{-n}) \right\rfloor \bmod c^n.$$

*Also, if  $c \geq 8$ ,  $c^{-1} < R$ , and  $t(n) < c^{n/3}$  for every  $n \geq 1$ , then the representation works for every  $n \geq 1$ .*

The following corollary follows easily from Theorem 2.

**Corollary 3.** *If the representation stated in Theorem 2 holds for some  $c \in \mathbb{N}$  for all  $n \geq m$ , then it holds also if we replace  $c$  with any integer  $r \geq c$  for all  $n \geq m$ .*

The next three lemmas are easy remarks of modular arithmetic.

**Lemma 4.** *If  $B \geq 2$ ,  $A \geq 1$ ,  $B \nmid A$ , then  $- \lfloor -A/B \rfloor = \lfloor A/B \rfloor + 1$ .*

**Lemma 5.** *If  $a, y, C \in \mathbb{N}$  and  $0 \leq (ay) < C$ , then  $((ay) \bmod C) = a(y \bmod C)$ .*

**Lemma 6.** *If  $x, C \in \mathbb{N}$ ,  $C \geq 2$ ,  $x \not\equiv (C-1) \pmod{C}$ , then  $(x+1) \bmod C = (x \bmod C) + 1$ .*

The next lemma is the principal tool of this note.

**Lemma 7.** *Let  $a, A, B, C \in \mathbb{Z}$  such that  $A, B > 0$ ,  $C \geq 2$ ,  $C \mid A$ ,  $B \nmid A$ ,  $B \bmod C \equiv a \bmod C$ ,  $a \neq 0$ , and  $|a|(\lfloor A/B \rfloor \bmod C) < C$  if  $a < 0$  (respectively,  $a + a(\lfloor A/B \rfloor \bmod C) < C$  if  $a > 0$ ).*

(i) *If  $a < 0$ , then*

$$(A \bmod B) \bmod C = |a|(\lfloor A/B \rfloor \bmod C).$$

(ii) *If  $a > 0$ , then*

$$((-A) \bmod B) \bmod C = a(1 + \lfloor A/B \rfloor \bmod C).$$

*Proof.* For both cases below we apply Lemmas 4 and 5. For the second case we apply also Lemma 6. We proceed with the cases.

(i)  $a < 0$ :

$$\begin{aligned}
(A \bmod B) \bmod C &= (A \bmod C - (B \bmod C)(\lfloor A/B \rfloor \bmod C)) \bmod C \\
&= (0 - (-|a|)(\lfloor A/B \rfloor \bmod C)) \bmod C \\
&= (|a|(\lfloor A/B \rfloor \bmod C)) \bmod C \\
&= |a|(\lfloor A/B \rfloor \bmod C).
\end{aligned}$$

(ii)  $a > 0$ :

$$\begin{aligned}
((-A) \bmod B) \bmod C &= ((-A) \bmod C - (B \bmod C)(\lfloor A/B \rfloor \bmod C)) \bmod C \\
&= (0 - a(\lfloor (-A)/B \rfloor \bmod C)) \bmod C \\
&= (a \cdot (-\lfloor (-A)/B \rfloor \bmod C)) \bmod C \\
&= (a \cdot (1 + \lfloor A/B \rfloor \bmod C)) \bmod C \\
&= (a + a \lfloor A/B \rfloor \bmod C) \bmod C \\
&= a(1 + \lfloor A/B \rfloor \bmod C).
\end{aligned}$$

□

### 3 Applications to C-recursive sequences

**Theorem 8.** *Suppose that for all natural numbers  $n \geq 1$ , a sequence  $t : \mathbb{N} \rightarrow \mathbb{N}$  has the div-mod representation*

$$t(n) = \left\lfloor \frac{c^{n^2} c^{n(d-k)} \tilde{A}(c^n)}{\tilde{B}(c^n)} \right\rfloor \bmod c^n.$$

*If the constant term of  $\tilde{B}(X)$  is  $\alpha_d < 0$ , then there is some natural number  $r$  such that for all  $n \geq 1$  we have*

$$t(n) = \frac{1}{|\alpha_d|} \left( \left( (r^{n^2} r^{n(d-k)} \tilde{A}(r^n)) \bmod \tilde{B}(r^n) \right) \bmod r^n \right).$$

*If the constant term of  $\tilde{B}(X)$  is  $\alpha_d > 0$ , then there is some natural number  $r$  such that for all  $n \geq 1$  we have*

$$t(n) = -1 + \frac{1}{\alpha_d} \left( \left( (-r^{n^2} r^{n(d-k)} \tilde{A}(r^n)) \bmod \tilde{B}(r^n) \right) \bmod r^n \right).$$

*Proof.* In order to apply Lemma 7, we recall that according to Corollary 3 there is a  $c_0 \in \mathbb{N}$  such that for all  $r \geq c_0$  and for all  $n \geq 1$  we have

$$t(n) = \left\lfloor \frac{r^{n^2} r^{n(d-k)} \tilde{A}(r^n)}{\tilde{B}(r^n)} \right\rfloor \bmod r^n.$$

Let  $r \geq c_0$  be a natural number to fulfill also other conditions, which will be stated below. We introduce the notations  $A = r^{n^2} r^{n(d-k)} \tilde{A}(r^n)$ ,  $B = \tilde{B}(r^n)$ , and  $C = r^n$  and we prove that for a good choice of  $r$ , which has to be sufficiently large, these numbers fulfill the conditions of Lemma 7.

The conditions  $C \mid A$  and  $B \nmid A$  are always fulfilled. The conditions  $A, B > 0$  and  $C \geq 2$  are fulfilled for all  $n \geq 1$  if  $r$  is sufficiently large, as the main coefficients of  $\tilde{A}(X)$  and  $\tilde{B}(X)$  are positive. Let  $\alpha_d$  be the constant term of the polynomial  $\tilde{B}(X) = X^d B(\frac{1}{X})$ , meaning that  $a = \alpha_d$ . For  $r$  sufficiently large, we have  $B \equiv \alpha_d \pmod{C}$ . By definition, we have  $\alpha_d \neq 0$  because  $\deg(B) = \deg(\tilde{B}) = d$ . We have to show that for  $r$  sufficiently large,  $|\alpha_d|(\lfloor A/B \rfloor \bmod C) < C$  if  $\alpha_d < 0$  respectively  $\alpha_d + \alpha_d(\lfloor A/B \rfloor \bmod C) < C$  if  $\alpha_d > 0$ , for all  $n \geq 1$ . We recall that  $\lfloor A/B \rfloor \bmod C = t(n)$ .

If  $\alpha_d < 0$ , the inequality  $|\alpha_d|(\lfloor A/B \rfloor \bmod C) < C$  means that  $|\alpha_d|t(n) < r^n$  and must be true for  $n \geq 1$ .

If  $\alpha_d > 0$ , the inequality  $\alpha_d + \alpha_d(\lfloor A/B \rfloor \bmod C) < C$  means that  $\alpha_d(t(n) + 1) < r^n$  and must be true for  $n \geq 1$ .

But we know from 1 that if  $s : \mathbb{N} \rightarrow \mathbb{C}$  is a C-recursive sequence, then there exists a  $g \in \mathbb{N}$  such that for all  $n \in \mathbb{N}$  we have  $|s(n)| < g^{n+1}$ . As  $s(n) = 2|\alpha_d|t(n)$  is itself a C-recursive sequence and its values are natural numbers, there is some positive  $g \in \mathbb{N}$  such that  $2|\alpha_d|t(n) < g^{n+1}$  for all  $n \geq 1$ . We can always find an  $r \in \mathbb{N}$  such that  $g^{n+1} < r^n$  for all  $n \geq 1$ .

If  $t(n) \geq 1$ , as  $2|\alpha_d|t(n) > |\alpha_d|t(n)$  in the first case, respectively  $2|\alpha_d|t(n) \geq |\alpha_d|(1+t(n))$  in the second case, the conditions of Lemma 7 are fulfilled. If  $t(n) = 0$ , the conditions are fulfilled for every  $r \geq 1$  in the first case and for every  $r > \alpha_d$  in the second case.

Finally we choose  $r$  sufficiently large such that  $r \geq c_0$  and all the conditions above are fulfilled.  $\square$

Below we put both cases in only one formula.

**Corollary 9.** *Suppose that for all natural numbers  $n \geq 1$ , a sequence  $t : \mathbb{N} \rightarrow \mathbb{N}$  has the representation*

$$t(n) = \left\lfloor \frac{c^{n^2} c^{n(d-k)} \tilde{A}(c^n)}{\tilde{B}(c^n)} \right\rfloor \bmod c^n.$$

*If the constant term of  $\tilde{B}(X)$  is  $\alpha_d \neq 0$ , there exists an integer  $r \geq c$  such that, for all  $n \geq 1$ , one has*

$$t(n) = \frac{-1 - \text{sgn}(\alpha_d)}{2} + \frac{1}{|\alpha_d|} \left( \left( (-\text{sgn}(\alpha_d) \cdot r^{n^2} r^{n(d-k)} \tilde{A}(r^n)) \bmod \tilde{B}(r^n) \right) \bmod r^n \right).$$

*Remark 10.* In [4] there is also an application to C-recursive sequences  $t : \mathbb{N} \rightarrow \mathbb{Z}$ . According to Lemma 1, for such a sequence there is an  $h \in \mathbb{N}$  such that for all  $n \geq 0$  we have

$|t(n)| < h^{n+1}$ . The sequence  $s(n) = t(n) + h^{n+1}$  has values in  $\mathbb{N}$  and is also C-recursive. Indeed, the generating function of  $s$  is a rational function and can be computed by

$$f(X) + \frac{h}{1 - hX},$$

where  $f(X)$  is the generating function of the sequence  $t$ . Consequently, the sequence  $s$  has a representation according to Corollary 9, while the sequence  $t$  has the representation  $t(n) = s(n) - h^{n+1}$ .

In [4], also the following *mod-div representation* is proved: *There exist  $c, n_0 \in \mathbb{N}$  such that for all  $n \geq n_0$  we have*

$$t(n) = \left\lfloor \frac{\left( c^{n(d-2)+\lceil n/2 \rceil} + c^{n^2} c^{n(d-k)} \tilde{A}(c^n) \right) \bmod \tilde{B}(c^n)}{c^{n(d-1)}} \right\rfloor.$$

**Open Problem 11.** Is it possible to find a purely arithmetic trick which shows that the mod-div representation (or even an improved version) is only a corollary of the div-mod representation, in a similar way as the short-cut shown here?

## 4 Examples

In this section, all representations are derived from the respective representations in [5]. In some cases a larger exponentiation base  $e > c$  is needed in order to keep the representation true for all natural numbers  $n \geq 1$ .

### 4.1 Degree 2, natural numbers, negative constant term

The first group of examples consists of sequences of order 2 with  $a < 0$ . As in [4] it was shown that this kind of sequence does not need any inner correction term, these representations are not different from the representations displayed there. In what follows, OEIS refers to the *On-Line Encyclopedia of Integer Sequences*.

**Example 12.** [*Fibonacci numbers*, OEIS [A000045](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$s(n) = \left( 3^{n^2+n} \bmod (3^{2n} - 3^n - 1) \right) \bmod 3^n.$$

**Example 13.** [*Lucas numbers*, OEIS [A000032](#)] The div-mod representation works for  $c = 3$  (see Prunescu and Sauras-Altuzarra [5]). The mod-mod representation works for  $r = 5$ : For all  $n \in \mathbb{Z}^+$ , we have

$$s(n) = \left( (2 \cdot 5^{n^2+2n} - 5^{n^2+n}) \bmod (5^{2n} - 5^n - 1) \right) \bmod 5^n.$$

**Example 14.** [*Pell numbers*, OEIS [A000129](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$s(n) = \left( 3^{n^2+n} \bmod (3^{2n} - 2 \cdot 3^n - 1) \right) \bmod 3^n.$$

**Example 15.** [*Pell-Lucas numbers*, OEIS [A002203](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$s(n) = \left( (2 \cdot 9^{n^2+2n} - 2 \cdot 9^{n^2+n}) \bmod (9^{2n} - 2 \cdot 9^n - 1) \right) \bmod 9^n.$$

## 4.2 Degree 2, natural numbers, positive constant term

**Example 16.** [*Natural numbers*, OEIS [A001477](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$\left( \left( (-4^{n^2+n}) \bmod (4^{2n} - 2 \cdot 4^n + 1) \right) \bmod 4^n \right) - 1 = n.$$

**Example 17.** [*All-twos*, OEIS [A007395](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$\left( \left( (-2 \cdot 4^{n^2+2n} + 2 \cdot 4^{n^2+n}) \bmod (4^{2n} - 2 \cdot 4^n + 1) \right) \bmod 4^n \right) - 1 = 2.$$

**Example 18.** [*Mersenne numbers*, OEIS [A000225](#)] For all  $n \in \mathbb{Z}^+$ , we have

$$\frac{1}{2} \cdot \left( \left( (-6^{n^2+n}) \bmod (6^{2n} - 3 \cdot 6^n + 2) \right) \bmod 6^n \right) - 1 = 2^n - 1.$$

**Example 19.** [ $2^n + 1$ , OEIS [A000051](#)] The div-mod representation works for  $c = 6$  (see Prunescu and Sauras-Altuzarra [5]). The mod-mod representation works for  $r = 9$ : For all  $n \in \mathbb{Z}^+$ , we have

$$\frac{1}{2} \cdot \left( (-2 \cdot 9^{n^2+2n} + 3 \cdot 9^{n^2+n}) \bmod (9^{2n} - 3 \cdot 9^n + 2) \bmod 9^n \right) - 1 = 2^n + 1.$$

**Example 20.** [OEIS [A001081](#), OEIS [A001080](#)] Consider Pell's equation

$$X^2 - kY^2 = 1. \tag{1}$$

The sequence of solutions  $(x(n), y(n))$  with  $(x(0), y(0)) = (1, 0)$  are known to be C-recursive sequences (see [5]). It is proved there that the sequences  $(x(n))$  and  $(y(n))$  are C-recursive and can be represented as

$$x(n) = \left\lfloor \frac{b^{n^2+2n} - x(1)b^{n^2+n}}{b^{2n} - 2x(1)b^n + 1} \right\rfloor \bmod b^n,$$

$$y(n) = \left\lfloor \frac{y(1)b^{n^2+n}}{b^{2n} - 2x(1)b^n + 1} \right\rfloor \bmod b^n.$$

For  $k = 7$ , the fundamental solution is  $(x(1), y(1)) = (8, 3)$ . If  $n \in \mathbb{Z}^+$ , then

$$x(n) = \left( \left( (-143^{n^2+2n} + 8 \cdot 143^{n^2+n}) \bmod (143^{2n} - 16 \cdot 143^n + 1) \right) \bmod 143^n \right) - 1,$$

$$y(n) = \left( \left( (-3 \cdot 64^{n^2+n}) \bmod (64^{2n} - 16 \cdot 64^n + 1) \right) \bmod 64^n \right) - 1.$$



### 4.3 Degree 2, integers, negative constant term

In this subsection, we obtain formulas for two Lucas sequences that take positive and negative values. They are computed according to Remark 10.

**Example 21.** [*Generalized Gaussian Fibonacci integers*, OEIS [A088137](#)] If  $n \in \mathbb{Z}^+$ , then

$$t(n) = \frac{1}{9} \left( \left( 3 \cdot 91^{n^2+3n} - 5 \cdot 91^{n^2+2n} + 6 \cdot 91^{n^2+n} \right) \bmod (91^{3n} - 5 \cdot 91^{2n} + 9 \cdot 91^n - 9) \right) \bmod 91^n \\ - 3^{n+1}.$$

The div-mod representation works for  $c = 32$  (see Prunescu and Sauras-Altuzarra [5]). The mod-mod representation works for  $r = 91$ , which is a spectacular difference.

**Example 22.** [OEIS [A002249](#)] If  $n \in \mathbb{Z}^+$ , then

$$s(n) = \frac{1}{4} \left( \left( 4 \cdot 21^{n^2+3n} - 7 \cdot 21^{n^2+2n} + 6 \cdot 21^{n^2+n} \right) \bmod (21^{3n} - 3 \cdot 21^{2n} + 4 \cdot 21^n - 4) \right) \bmod 21^n \\ - 2^{n+1}.$$

The div-mod representation works for  $c = 8$  (see Prunescu and Sauras-Altuzarra [5]). The mod-mod representation works for  $r = 21$ , so we remark again a big difference.

### 4.4 Degree 3, natural numbers, negative constant term

We finally apply the theory to some C-recursive natural sequences of degree three, whose recursions do not contain positive coefficients. Consequently, these representations do not need correction terms.

**Example 23.** [*Tribonacci numbers*, OEIS [A000073](#)] If  $n \in \mathbb{Z}^+$ , then

$$s(n) = \left( 2^{n^2+n} \bmod (2^{3n} - 2^{2n} - 2^n - 1) \right) \bmod 2^n.$$

**Example 24.** [*Padovan numbers*, OEIS [A000931](#)] If  $n \in \mathbb{Z}^+$ , then

$$s(n) = \left( (2^{n^2+3n} - 2^{n^2+n}) \bmod (2^{3n} - 2^n - 1) \right) \bmod 2^n.$$

**Example 25.** [*Narayana's cows sequence*, OEIS [A000930](#)] If  $n \in \mathbb{Z}^+$ , then

$$s(n) = \left( 2^{n^2+3n} \bmod (2^{3n} - 2^{2n} - 1) \right) \bmod 2^n.$$

## 5 Acknowledgments

We thank the anonymous referee for their careful reading and helpful suggestions.

## References

- [1] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, Vol. 104, American Mathematical Society, 2003.
- [2] M. Kauers and P. Paule, *The Concrete Tetrahedron*, Texts and Monographs in Symbolic Computation, Springer, 2011.
- [3] M. Petkovšek and H. Zakrajšek, Solving linear recurrence equations with polynomial coefficients, in J. Blümlein and C. Schneider, eds., *Computer Algebra in Quantum Field Theory. Integration, Summation and Special Functions*, Springer, 2013, pp. 259–284.
- [4] M. Prunescu, On other two representations of the C-recursive integer sequences by terms in modular arithmetic, *J. Symbolic Comput.* **130** (2025).
- [5] M. Prunescu and L. Sauras-Altuzarra, On the representation of C-recursive integer sequences by arithmetic terms, *J. Difference Equ. Appl.* **31** (2025), 1263–1285.
- [6] R. P. Stanley, *Enumerative Combinatorics*, 2nd edition, Cambridge University Press, 2011.

---

2020 *Mathematics Subject Classification*: Primary 11B37; Secondary 39A06.

*Keywords*: C-recursive sequence, modular arithmetic, term representation.

---

(Concerned with sequences [A000032](#), [A000045](#), [A000051](#), [A000073](#), [A000129](#), [A000225](#), [A000930](#), [A000931](#), [A001080](#), [A001081](#), [A001477](#), [A002203](#), [A002249](#), [A007395](#), and [A088137](#).)

---

Received March 11 2025; revised versions received March 12 2025; September 16 2025.  
Published in *Journal of Integer Sequences*, September 16 2025.

---

Return to [Journal of Integer Sequences home page](#).