Journal of Integer Sequences, Vol. 19 (2016),
Article 16.2.3

Generalized Multiple Counting Jacobsthal Sequences of Fermat Pseudoprimes

M. Hüsrev Cılasun
Emerging Circuits and Computation Group
Electrical and Electronics Faculty
Istanbul Technical University
Maslak, Istanbul
Turkey
cilasun@itu.edu.tr

Abstract

This study involves definitions of regular and representational multiple-counting Jacobsthal sequences of Carmichael numbers. We introduce recurrence relations for multiple-counting Jacobsthal sequences and show their association with Fermat's little theorem. We also provide matrix representations and generalized Binet formulas for defined sequences. This leads to a better understanding of how certain composite numbers are distributed among consecutive powers.

1 Introduction

The Jacobsthal sequence [2] is defined as follows:

$$j_{n+2} = j_{n+1} + 2j_n, j_1 = 1, j_0 = 0, n \geq 0 \tag{1}$$

Horadam and Hoggatt have written many papers [2, 4, 8] about the Jacobsthal sequence, which has many remarkable properties, such as counting microcontroller skip instructions [10] and counting the number of ways to tile a $3 \times (n-1)$ rectangle with 2×2 and 1×1 tiles [9]. The Jacobsthal sequence can be expressed in floor function notation [1]. It is given in the description of sequence A001045 that the elements of the Jacobsthal sequence count the multiples of 3 in between successive powers of 2, as illustrated in Table 1.

Interval boundaries of powers of 2	2^0		2^1		2^2		2^3		2^4		2^5
Number of multiples of 3 in each interval.		0		1		1		3		5	

Table 1: Number of multiples of 3 in between powers of 2. The sequence is identical to the original Jacobsthal sequence.

As the initial motivation of this paper, it is notable that there are other Jacobsthal-like recurrence relations that hold between some other exponents and bases. For instance, as it can be understood from a superficial glance at the sequence A007910, when double of any term is added to three consecutive terms, the very next term is obtained. This study investigates various aspects of those recurrence sequences.

Another concept that will be discussed in this paper is Fermat's little theorem [3], which can be summarized as $x^{\rho-1} \equiv 1 \pmod{\rho}$. The theorem states that the given condition is satisfied when ρ and x are coprime and ρ is prime. However, vice versa is not always true. The condition is still valid for some composite ρs called *Fermat pseudoprimes* [11], *Carmichael numbers* [6] or K_1 *Knödel numbers* [12]. In particular for the $x = 2$ case, the ρs are called *Poulet numbers* [13] or *Fermatians* [6] if they satisfy Fermat's given condition [3].

2 Generalized multiple-counting Jacobsthal sequences

Definition 1. Let x and ρ be elements of $\{2, 3, 4, 5, \dots\}$ and n be an element of $\{0, 1, 2, 3, \dots\}$. The *multiple-counting Jacobsthal sequence* $J(x, \rho)$ is defined by setting J_n equal to the number of multiples of ρ which are greater than x^n and less than x^{n+1}.

In floor function notation, the number of multiples of ρ less than x^{n+1} is $\left\lfloor \frac{x^{n+1}}{\rho} \right\rfloor$. Therefore, the number of multiples of ρ greater than x^n and less than x^{n+1} is found as follows:

$$J_n = \left\lfloor \frac{x^{n+1}}{\rho} \right\rfloor - \left\lfloor \frac{x^n}{\rho} \right\rfloor \tag{2}$$

Theorem 2. *Let x and ρ be elements of $\{1, 2, 3, \dots\}$. Let x and ρ be relatively prime and satisfy Fermat's $x^{\rho-1} \equiv 1$ (mod ρ) condition. For any number n from the set $\{0, 1, 2, \dots\}$, the sequence with starting terms $J_0, J_1, \dots J_{\rho-1}$ which counts the multiples of ρ between x^n and x^{n+1} also satisfies the following recurrence relation for $\rho \geq 3$:*

$$J_{n+\rho-1} = (x-1)\sum_{i=1}^{\rho-2} J_{n-i+\rho-1} + xJ_n \tag{3}$$

Proof. The expression in (3) can be transformed to

$$J_{n+\rho-1} = (x-1)\sum_{i=1}^{\rho-1} J_{n-i+\rho-1} + J_n \tag{4}$$

Replace J_n with its floor function notation (2). The following expression is obtained when intermediate elements of the sigma notation are eliminated.

$$\left\lfloor \frac{x^{n+\rho}}{\rho} \right\rfloor - \left\lfloor \frac{x^{n+\rho-1}}{\rho} \right\rfloor = (x-1)\left(\left\lfloor \frac{x^{n+\rho-1}}{\rho} \right\rfloor - \left\lfloor \frac{x^{n}}{\rho} \right\rfloor \right) + \left\lfloor \frac{x^{n+1}}{\rho} \right\rfloor - \left\lfloor \frac{x^{n}}{\rho} \right\rfloor \tag{5}$$

Let a be an arbitrary constant. Assume $x^{\rho-1}$ is equal to $a\rho+1$ as a result of the $x^{\rho-1} \equiv 1 \pmod{\rho}$ condition. When $a\rho+1$ is substituted into (5), the floor function takes the a-terms out due to its integer exclusion property. Both sides of the equation turn into aJ_n. The right and left hand sides then simplify, and the proof is complete. □

Example 3. Table 2 contains several examples of multiple-counting sequences for different ρs and xs

ρ	x	**Notes on sequences**
3	2	Identical to Jacobsthal sequence: $J_n = J_{n-1} + 2J_{n-2}, n \geq 2, J_0 = 0, J_1 = 1$
5	3	$J_n = 2J_{n-1} + 2J_{n-2} + 2J_{n-3} + 3J_{n-4}, n \geq 4, J_0 = 0, J_1 = 1, J_2 = 4, J_3 = 11$
3	10	$J_n = 9J_{n-1} + 10J_{n-2}, n \geq 2, J_0 = 3, J_1 = 30$ J_n counts $(n+1)$-digit numbers which are divisible by 3

Table 2: Some multiple-counting sequences

In their paper, Cook and Bacon [7] defines various sequences J_n for various ρs, called *higher order Jacobsthal sequences*, when $x = 2$.

Theorem 4. *For any element of J_n, the Binet expression*

$$J_n = \sum_{i=1}^{n} \lambda_i^{n-i+2} v_{1,i} (\sum_{j=1}^{n} v_{i,j}^{-1} u_j^{\rho-2}) \tag{6}$$

is always satisfied when the key matrix

$$K_{(\rho-1)\times(\rho-1)} = \begin{pmatrix} x-1 & x-1 & \dots & x-1 & x-1 & x \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ \end{pmatrix}$$

satisfies $Ku^n = u^{n+1}$ for the vector

$$u^n = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{p-1} \end{pmatrix} = \begin{pmatrix} J_n \\ J_{n-1} \\ \vdots \\ J_{n-p+2} \end{pmatrix}$$

if K is diagonalizable and K's eigenvector matrix V is non-singular. Note that elements u_i,v_{ij} belong to u,V.

Proof. The Binet form for J_n can be obtained using Kalman's method [5]. After decomposing $K = V\Lambda V^{-1}$, the equation $Ku^n = u^{n+1}$ is transformed to $V\Lambda V^{-1}u^n = u^{n+1}$ where Λ is the diagonal eigenvalue matrix of K. We only need the top elements of vectors, thus multiply the expression by

$$\begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$$

a $(\rho - 1) \times 1$ matrix from the left. Any particular term of the sequence J_n satisfies the equation

$$J_n = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} (V\Lambda^{n-\rho+2}(V^{-1}u^{\rho-2})) \tag{7}$$

Since

$$(V^{-1}u^{\rho-2}) = \begin{pmatrix} v_{1,1}^{-1} & v_{1,2}^{-1} & \dots & v_{1,\rho-1}^{-1} \\ v_{2,1}^{-1} & v_{2,2}^{-1} & \dots & v_{2,\rho-1}^{-1} \\ \dots & \dots & \ddots & \dots \\ v_{\rho-1,1}^{-1} & v_{\rho-1,2}^{-1} & \dots & v_{\rho-1,\rho-1}^{-1} \end{pmatrix} \begin{pmatrix} J_{\rho-2} \\ J_{\rho-3} \\ \vdots \\ J_0 \end{pmatrix}$$

and

$$V = \begin{pmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,\rho-1} \\ v_{2,1} & v_{2,2} & \dots & v_{2,\rho-1} \\ \dots & \dots & \ddots & \dots \\ v_{\rho-1,1} & v_{\rho-1,2} & \dots & v_{\rho-1,\rho-1} \end{pmatrix}$$

and

$$\Lambda^{n-\rho+2} = \begin{pmatrix} \lambda_1^{n-\rho+2} & 0 & \dots & 0 \\ 0 & \lambda_2^{n-\rho+2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_{\rho-1}^{n-\rho+2} \end{pmatrix}$$

are known, we can compute (7) after the required substitution. Recall that $\lambda_1, \lambda_2, \dots, \lambda_n$ denote the eigenvalues of K. After the outcome of the computation is simplified, we obtain the initial expression (6). □

Example 5. Table 3 contains several Binet formulas of multiple-counting sequences for different ρs and xs

ρ	x	**Sequence**	**Binet form**
3	2	$J_n = J_{n-1} + 2J_{n-2}$ $n \geq 2, J_0 = 0, J_1 = 1$	$\frac{2^n}{3} - \frac{(-1)^n}{3}$
3	4	$J_n = 3J_{n-1} + 4J_{n-2}$ $n \geq 2, J_0 = 1, J_1 = 4$	4^n
3	10	$J_n = 9J_{n-1} + 10J_{n-2}$ $n \geq 2, J_0 = 3, J_1 = 30$	$3\frac{10^n}{10}$

Table 3: Some Binet forms of multiple-counting sequences when ρ is 3.

3 Generalized multiple-counting representational Jacobsthal sequences

Definition 6. Let x and ρ be elements of $\{2, 3, 4, 5, \dots\}$ and n be an element of $\{0, 1, 2, 3, \dots\}$. Then $S(x, \rho)$ will be called a *multiple-counting representational Jacobsthal sequence* when S_n is equal to the number of integer multiples of ρ, that are greater than 0 and less than x^{n+1}. Representational sequences can be compactly expressed as

$$S_n = \left\lfloor \frac{x^{n+1}}{\rho} \right\rfloor \tag{8}$$

The strong interrelation between regular multiple-counting sequences and multiple-counting representational Jacobsthal sequences is expressed by

$$S_n = \sum_{i=0}^{n} J_i \tag{9}$$

The summation idea of a multiple-counting Jacobsthal sequence is very similar to the *Jacobsthal representation sequence* which Horadam [4] explores in detail. The representation sequence satisfies a similar recurrence relation. However, the constant term is different.

Theorem 7. *Let x and ρ be elements of $\{1, 2, 3, \dots\}$ and suppose they satisfy Fermat's $x^{\rho-1} \equiv 1 \pmod{\rho}$ condition. For any element n of $\{0, 1, 2, \dots\}$, the sequence with starting terms $S_0, S_1, \dots, S_{p-1}$, which counts multiples of ρ between 0 and x^{n+1}, satisfies the following recurrence relation:*

$$S_{n+\rho-1} = (x-1) \sum_{i=1}^{\rho-2} S_{n-i+\rho-1} + xS_n + \phi \tag{10}$$

or

$$S_{n+\rho-1} = (x-1) \sum_{i=1}^{\rho-1} S_{n-i+\rho-1} + S_n + \phi, \tag{11}$$

where ϕ is a unique constant derived from the particular combination of ρ, x and the initial conditions $J_0, J_1, \ldots, J_{p-2}$. Note that the formula for ϕ is

$$\phi = \sum_{i=0}^{\rho-1} J_i - (x-1)\sum_{i=1}^{\rho-1}\sum_{j=0}^{i-2} J_j \tag{12}$$

Proof. Rewrite (11) using property (9):

$$\sum_{i=0}^{n+\rho-1} J_i = (x-1)\sum_{i=1}^{\rho-1}\sum_{j=0}^{n-i+\rho-1} J_j + \sum_{i=0}^{n} J_i + \phi \tag{13}$$

Separate (13) into n-dependent and n-independent parts:

$$\sum_{i=0}^{\rho-2} J_i + \sum_{i=\rho-1}^{n+\rho-1} J_i = (x-1)\sum_{i=1}^{\rho-1}(\sum_{j=0}^{i-2} J_j + \sum_{j=i-1}^{n-i+\rho-1} J_j) + \sum_{i=0}^{n} J_i + \phi \tag{14}$$

$$\sum_{i=0}^{\rho-2} J_i + \underbrace{\sum_{i=\rho-1}^{n+\rho-1} J_i}_{} = (x-1)\sum_{i=1}^{\rho-1}\sum_{j=0}^{i-2} J_j + \underbrace{(x-1)\sum_{i=1}^{\rho-1}\sum_{j=i-1}^{n-i+\rho-1} J_j + \sum_{i=0}^{n} J_i}_{} + \phi \tag{15}$$

The n-dependent underbraced parts of Eq. (15) are eliminated by induction on (4). Since the n-independent parts of the expression above are constant for the whole sequence, ϕ also depends on a constant value and the required proof is provided. □

Theorem 8. *To obtain a matrix-based Binet representation for the sequence S, we use a similar approach as for the sequence J. Since the only difference between the definitions of the two sequences J and S is a constant ϕ, we can easily modify the key matrix to insert the ϕ dependency with notational changes to get a simple formula.*

$$S_n = \sum_{i=1}^{n} \mu_i^{n-i+2} w_{1,i}(\sum_{j=1}^{n} w_{i,j}^{-1}\tau_j^{\rho-1}) \tag{16}$$

Assuming L is the key matrix

$$L_{\rho\times\rho} = \begin{pmatrix} x-1 & x-1 & \ldots & x-1 & x-1 & x & 1 \\ 1 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \\ 0 & 0 & \ddots & 1 & 0 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 & 0 & 1 \\ \end{pmatrix}$$

of $L\tau^n = \tau^{n+1}$ where τ satisfies

$$\tau^n = \begin{pmatrix} \tau_1 \\ \tau_2 \\ \vdots \\ \tau_{p-1} \\ \phi \end{pmatrix} = \begin{pmatrix} S_n \\ S_{n-1} \\ \vdots \\ S_{n-p+2} \\ \phi \end{pmatrix}$$

if L is diagonalizable and L's eigenvector matrix W is non-singular. Note that the elements w_{ij} belong to W and $\mu_1, \mu_2, \ldots, \mu_n$ denote the eigenvalues of L.

Proof. Proof is similar to the proof of Theorem 4 and therefore omitted. □

4 Concluding remarks

Several sequences in OEIS [1] are identical to some multiple-counting Jacobsthal sequences. A007910 is a multiple-counting Jacobsthal sequence when ($x = 2$, $\rho = 5$) and A077947 when ($x = 2$, $\rho = 7$), which are also called fourth and sixth order Jacobsthal sequences [7]. Additionally, A000302 and A093138 are multiple-counting Jacobsthal sequences for ($x = 4$, $\rho = 3$) and ($x = 10$, $\rho = 3$).

Unlike the prime-counting function $\pi(x)$ (which is A006880 of OEIS [1]), the sequences J_n and S_n count the composites of a given prime ρ. There is only one exception for both sequences: their initial terms. If ρ is prime, J_n and S_n count all composites of the prime ρ.

The outcomes of this research can be used in various fields, such as electronics and computer science. The strong connection between the described sequences and Fermat's little theorem might lead to a better understanding of number fields. The distribution of prime and composite numbers is a significant field in present day number theory. Considering this, the future of multiple-counting Jacobsthal sequences is promising.

5 Acknowledgement

I would like to thank Mustafa Sefa Yörüker, Mustafa Zengin, Adem Şahin, and Ayhan Yenilmez for helpful advice.

References

[1] N. Sloane, The On-Line Encyclopedia of Integer Sequences, 2015, http://oeis.org.

[2] A. F. Horadam, Jacobsthal and Pell curves, *Fibonacci Quart.* **26** (1988), 77–83.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 1979.

[4] A. F. Horadam, Jacobsthal representation numbers, *Fibonacci Quart.* **34** (1996), 40–54.

[5] D. Kalman, Generalized Fibonacci numbers by matrix methods, *Fibonacci Quart.* **20** (1982), 73–76.

[6] D. Shanks, *Solved and Unsolved Problems in Number Theory*, AMS Chelsea, 2001.

[7] C. K. Cook and M. R. Bacon, Some identities for Jacobsthal and Jacobsthal-Lucas numbers satisfying higher order recurrence relations, *Ann. Math. Inform.* **41** (2013), 27–39.

[8] G. E. Bergum, L. Bennett, A. F. Horadam, and S. D. Moore, Jacobsthal polynomials and a conjecture concerning Fibonacci-like matrices, *Fibonacci Quart.* **23** (1985), 240–248.

[9] S. Heubach, Tiling an m-by-n area with squares of size up to k-by-k ($m \leq 5$), *Congr. Numer.* **140** (1999), 43–64.

[10] A. Daşdemir, On the Jacobsthal numbers by matrix method, *Fen Derg.* **7** (2012), 69–76.

[11] R. Crandall and C. B. Pomerance, *Prime Numbers: a Computational Perspective*, Springer Science Business Media, 2006.

[12] A. Makowski, Generalization of Morrow's D numbers, *Bull. Belg. Math. Soc. Simon Stevin* **36** (1962), 71.

[13] D. H. Lehmer, Errata for Poulet's table, *Math. Comp.* **25** (1971), 944–945.

2010 *Mathematics Subject Classification*: Primary 11Bxx; Secondary 11Y55, 11A15.
Keywords: Carmichael number, Fermat's little theorem, Binet formula, floor function, multiple-counting sequence, Fermat pseudoprime, Jacobsthal sequence.

(Concerned with sequences A000302, A001045, A006880, A007910, A077947, and A093138.)

Received September 26 2015; revised versions received October 23 2015; December 1 2015; December 19 2015. Published in *Journal of Integer Sequences*, January 10 2016.

Return to Journal of Integer Sequences home page.