On the period mod $m$ of polynomially-recursive sequences: a case study

Cyril Banderier\textsuperscript{1}\textsuperscript{*} \quad Florian Luca\textsuperscript{2,3,4}\textsuperscript{†}

March 5, 2019

\textsuperscript{1}: LIPN (UMR CNRS 7030), Université Paris Nord, France.
\textsuperscript{2}: School of Mathematics, University of the Witwatersrand, South Africa.
\textsuperscript{3}: King Abdulaziz University, Jeddah, Saudi Arabia.
\textsuperscript{4}: Department of Mathematics, University of Ostrava, Czech Republic.

Abstract

Polynomially-recursive sequences generally have a periodic behavior mod $m$. In this paper, we analyze the period mod $m$ of a second-order polynomially-recursive sequence. The problem originally comes from an enumeration of avoiding pattern permutations and appears to be linked with nice number theory notions (the Carmichael function, Wieferich primes, algebraic integers). We give the mod $a^k$ supercongruences, and generalize these results to a class of recurrences.

Keywords and phrases. D-finite function, Modular properties, P-recursive sequence, supercongruence, Carmichael function, Wieferich primes.

2010 Mathematics Subject Classification. 11B39, 11B50, 11B85, 05A15.

\textsuperscript{*}https://lipn.fr/~banderier \quad \textsuperscript{†}https://scholar.google.com/

https://orcid.org/0000-0003-0755-3022 \quad https://orcid.org/0000-0001-8581-449X
1 Introduction

In his analysis of sorting algorithms, Knuth introduced the notion of forbidden pattern in permutations, which later became a field of interest per se [10]. By studying the basis of such forbidden patterns for permutations reachable with \( k \) right-jumps from the identity permutation, the authors of [1] discovered that the permutations of size \( n \) in this basis were enumerated by the sequence of integers \( \{b_n\}_{n \geq 0} \) given by

\[
b_n+2 = 2nb_{n+1} + (1 + n - n^2)b_n \quad \text{for all} \quad n \geq 0.
\]

This is sequence \( \text{A265165} \) in the OEIS\(^1\), it starts like 0, 1, 2, 7, 32, 179, 1182, 8993, 77440, 744425, 7901410, 91774375... Such a sequence satisfying a recurrence with polynomial coefficients in \( n \) is called P-recursive (for polynomially recursive), D-finite, or holonomic, depending on the authors (see, e.g., [5, 7, 11, 14]). P-recursive sequences are ubiquitous in combinatorics, number theory, analysis of algorithms, computer algebra, etc. It is always the case that the corresponding generating function satisfies a linear differential equation, but it is not always the case that it has a closed form. In our case, the generating function of \( \{b_n\}_{n \geq 0} \) has in fact a nice closed form involving the golden ratio. Indeed, putting

\[
(\alpha, \beta) := \left(\frac{1 + \sqrt{5}}{2}, \frac{1 - \sqrt{5}}{2}\right)
\]

for the two roots of the quadratic equation \( x^2 - x - 1 = 0 \), it was shown in [1] that the exponential generating function of the \( \{b_n\}_{n \geq 0} \), namely

\[
B(x) = \sum_{n \geq 0} b_n \frac{x^n}{n!}, \quad \text{satisfies} \quad B(x) = \frac{\beta}{\beta - \alpha} (1 - x)^\alpha + \frac{\alpha}{\alpha - \beta} (1 - x)^\beta - 1. \tag{2}
\]

This is a noteworthy sequence in analytic combinatorics (see [5] for a nice presentation of this field), as it is one of the rare sequences exhibiting an irrational exponent in its asymptotics:

\[
\frac{b_n}{n!} \sim \frac{\alpha}{\sqrt{5}\Gamma(\alpha - 1)} n^{\alpha - 2}(1 + o(1)) \quad \text{as} \quad n \to \infty,
\]

where \( \Gamma(z) = \int_0^{\infty} t^{z-1} \exp(-t) \, dt \) is the Euler gamma function.

There is a vast literature in number theory analyzing the modular congruences of famous sequences (Pascal triangle, Fibonacci, Catalan, Motzkin, Apéry numbers, see [3, 6, 8, 12, 15]). The properties of \( b_n \mod m \) are sometimes called "supercongruences" when \( m \) is the power of a prime number: many articles consider \( m = 2^r \), or \( m = 3^r \). We now restate an important result which holds for any \( m \) (not necessarily the power of a prime number).

**Theorem 1** (Supercongruences for D-finite functions [1, Theorem 7]).

Consider any \( P \)-recurrence of order \( r \):

\[
P_0(n)u_n = \sum_{i=1}^{r} P_i(n)u_{n-i},
\]

where the polynomials \( P_0(n), \ldots, P_r(n) \) belong to \( \mathbb{Z}[n] \), and where the polynomial \( P_0(n) \) is invertible mod \( m \). Then the sequence \( (u_n \mod m)_{n \geq 0} \) is eventually periodic\(^2\). In particular, sequences such that \( P_0(n) = 1 \) are periodic mod \( m \). Additionally, the preperiod and period are bounded by \( m^{2r+1} \), therefore one can use the Knuth–Floyd cycle-finding algorithm (the tortoise and hare algorithm) to compute them.

N.B.: It is not always the case that \( P \)-recursive sequences are periodic mod \( p \). E.g., it was proven in [9] that Motzkin numbers are not periodic mod \( m \), and it seems that

\[(n + 3)(n + 2)u_n = 8(n - 1)(n - 2)u(n - 2) + (7n^2 + 7n - 2)u(n - 1), \quad u_0 = 0, u_1 = 1,
\]

is also not periodic mod \( m \), for any \( m > 2 \) (this \( P \)-recursive sequence counts a famous class of permutations, namely, the Baxter permutations). This is coherent with Theorem 1, as the leading term in the recurrence (the factor \((n + 3)(n + 2)\)) is not invertible mod \( m \), for infinitely many \( n \).

For our sequence \( \{b_n\}_{n \geq 1} \) (defined by recurrence (1)), this theorem explains the periodic behavior of \( b_n \mod m \). By brute-force computation, we can get \( b_n \mod m \), for any given \( m \). For example \( b_n \mod 15 \) is periodic of period 12 (after a preperiod \( n_{12} = 9 \)):

\[
\{b_n \mod 15\}_{n \geq 9} = (10, 5, 10, 0, 10, 5, 10, 5, 0, 5)^\infty.
\]

The period can be quite large, for example \( b_n \mod 3617 \) has period 26158144. More generally, for every positive integer \( m \), the sequence \( \{b_n \mod m\}_{n \geq 1} \) is eventually periodic: there exist \( T_m > 0 \) and \( n_m \) such that, for all \( n \geq n_m \), one has \( b_{n + T_m} \equiv b_n \pmod{m} \). We write \( T_m \) for the smallest such period. In this paper, we study some of the properties of \( \{T_m\}_{m \geq 1} \).

This is sequence A306699 in the OEIS. Here are its first few values \( T_2, \ldots, T_{100} \):

\[
2, 12, 8, 1, 12, 8, 36, 2, 1, 24, 104, 84, 12, 16, 544, 36, 1, 8, 84, 2, 1012, 24, 1, 104, 108, 168, 1, 12, 1, 32, 12, 544, 84, 72, 2664, 2, 312, 8, 1, 84, 3612, 8, 36, 1012, 4324, 48, 588, 2, 1632, 104, 5512, 108, 1, 168, 12, 2, 1, 24, 1, 2, 252, 64, 104, 12, 2948, 544, 3036, 84, 1, 72, 10512, 2664, 12, 8, 84, 312, 1, 16, 324, 2, 13612, 168, 544, 3612, 12, 8, 1, 36, 2184, 2024, 12, 4324, 1, 96, 18624, 588, 36, 8.
\]

Do you detect some hidden patterns in this sequence? This is what we tackle in the next section.

\(^2\)An eventually periodic sequence of period \( p \) is a sequence for which \( u_{n+p} = u_n \) for all \( n \geq n_p \) (\( n_p \) is called the preperiod). Some authors use the terminology “ultimately periodic” instead. In the sequel, as the context is clear, we will often omit the word “eventually”.

Cyril Banderier & Florian Luca

Period mod \( m \) of \( P \)-recursive sequences: a case study
2 Periodicity mod $m$, supercongruences and links with number theory

Our main result is the following.

Theorem 2. Let $b_n$ be the sequence defined by the recurrence of Formula 1. The period $T_m$ of this sequence $b_n$ mod $m$ satisfies:

a) If $m = p_1^{e_1} \cdots p_k^{e_k}$ (where $p_1, \ldots, p_k$ are distinct primes), then

$$T_m = \text{lcm}(T_{p_1^{e_1}}, \ldots, T_{p_k^{e_k}}).$$

b) We have $T_m = 1$ if and only if $m$ is the product of primes $p \equiv 0, 1, 4 \pmod{5}$.

c) For every prime $p$, we have $T_p \mid 2\nu(p)$.

d) If $T_m > 1$ then $2 \mid T_m$ if $m$ is even, and $4 \mid T_m$ if $m$ is odd.

e) For $m \geq 3$, we have $T_m = 2$ if and only if $m$ is even and $\frac{m}{2}$ is the product of primes $p \equiv 0, 1, 4 \pmod{5}$.

f) For every prime $p$, we have $T_{p^k} \mid 2^{p^k}(p - 1)$.

The function $T_m$ thus shares some similarities with the Carmichael function introduced in [2, p. 39], and it is expected that its asymptotic behavior is also similar (following, e.g., the lines of [4]). In this article, we focus on the rich arithmetic properties of this function. Note that Theorem 2 allows computing $T_m$ in a much faster way than the brute-force algorithm mentioned in Section 1: the complexity goes from $m^{2r+1}$ via brute-force to $\ln(m)^3$ via Shor’s factorization algorithm [13] (or to sub-exponential complexity in $\ln(m)$ with other efficient algorithms, if one does not want to rely on the use of quantum computers).

Proof of Part a). The proof will use a little preliminary result and the following definition.

We call $T_m$ the “eventual period of the sequence mod $m$”, or for short with a slight abuse of terminology, the “period of the sequence mod $m$” (even if the sequence starts with some terms which does not satisfy the periodic pattern). The following lemma holds for all eventually periodic sequences of integers.

Lemma 1. $T_m$ divides all other periods of $\{u_n\}_{n \geq 0}$ modulo $m$.

Proof. Let $T_m = a$ and assume there is $b$ (not a multiple of $a$) which is also a period modulo $m$. Thus, there are $n_a, n_b$ such that $u_{n_a+a} \equiv u_n \pmod{m}$ for all $n > n_a$ and $u_{n+b} \equiv u_n \pmod{m}$ for all $n > n_b$. Let $d = \gcd(a, b)$. By Bézout’s identity, one has then $d = Aa + Bb$ for some integers $A, B$. Let $n_{a,b} = \max\{n_a, n_b\} + |A|a + |B|b$ and assume that $n > n_{a,b}$. Then $u_{n+a} = u_{n+a+Aa+Bb} \equiv u_{n+a} \pmod{m}$ so $d < a$ is a period of $\{u_n\}_{n \geq 0}$ modulo $m$, contradicting the minimality of $a$. \qed

\(^3\)As usual, lcm stands for the least common multiple.
An immediate consequence is the following\(^4\):

**Corollary 1.** We have \(T_{[m_1, \ldots, m_r]} = [T_{m_1}, \ldots, T_{m_r}]\).

**Proof.** First consider \(r = 2\), and let \(a := m_1, b := m_2\). Since \([T_a, T_b]\) is a multiple of both \(T_a\) and \(T_b\), it follows that it is a period of \(\{u_n\}_{n \geq 0}\) modulo both \(a\) and \(b\), so modulo \([a, b]\). It remains to prove that it is the minimal one. To this aim, suppose that \(T_{[a, b]} < [T_a, T_b]\). Then either \(T_a \not\mid T_{[a, b]}\) or \(T_b \not\mid T_{[a, b]}\). Since the two cases are similar, we only deal with the first one. In this case we would have that both \(T_a\) and \(T_{[a, b]}\) would be periods modulo \(a\). By the previous lemma, this would force \(\gcd(T_a, T_{[a, b]} < T_a\), which would obviously be a contradiction. Now, a trivial induction on the number \(r \geq 2\) gives that

\[
T_{[m_1, \ldots, m_r]} = [T_{m_1}, \ldots, T_{m_r}]
\]

holds for all positive integers \(m_1, \ldots, m_r\). \(\square\)

In particular Part a) of Theorem 2 holds: \(T_m = \text{lcm}(T_{p_{e_1}}, \ldots, T_{p_{e_k}})\). Let us now tackle the proofs of Parts b)–f).

**Proof of Part b).** We use the generating function (2), which tells us that

\[
[x^n]B(x) = \frac{b_n}{n!} = \frac{(-1)^n}{\sqrt{5}} \left( \left\langle \frac{\beta}{n} \right\rangle - \left\langle \frac{\alpha}{n} \right\rangle \right), \tag{3}
\]

Thus,

\[
b_n = \frac{(-1)^{n-1}}{\sqrt{5}} \left( \beta \alpha (\alpha - 1) \cdots (\alpha - (n - 1)) - \alpha \beta (\beta - 1) \cdots (\beta - n + 1) \right). \tag{4}
\]

By Fermat’s little theorem,

\[
\prod_{k=0}^{p-1} (X - k) = X^p - X \pmod p. \tag{5}
\]

Assume now that \(p \equiv 1, 4 \pmod 5\). Then

\[
\prod_{k=0}^{p-1} (\alpha - k) \equiv \alpha^p - \alpha \pmod p \equiv 0 \pmod p,
\]

where for the last congruence we used the law of quadratic reciprocity: since \(p \equiv 1, 4 \pmod 5\), we have

\[
\left( \frac{5}{p} \right) = \left( \frac{p}{5} \right) = 1,
\]

where \(\left( \frac{\ast}{p} \right)\) is the Legendre symbol. Thus,

\[
\alpha^p = \left( \frac{1 + \sqrt{5}}{2} \right)^p \equiv \frac{1 + \sqrt{5} \cdot 5^{(p-1)/2}}{2^p} \pmod p \equiv \alpha \pmod p, \tag{6}
\]

because \(5^{(p-1)/2} \equiv \left( \frac{5}{p} \right) \equiv 1 \pmod p\) by Euler’s criterion.

\(^4\)We use the notation \([m_1, \ldots, m_r] = \text{lcm}(m_1, \ldots, m_r)\) for the least common multiple of integers \(m_1, \ldots, m_r\).
In the above and in what follows, for two algebraic integers \( \delta, \gamma \) and an integer \( m \) we write 
\[
\delta \equiv \gamma \pmod{m}
\]
if the number \((\delta - \gamma)/m\) is an algebraic integer. This shows that 
\[
\frac{1}{p} \prod_{k=0}^{p-1}(\alpha - k)
\]
is an algebraic integer. The same is true with \( \alpha \) replaced by \( \beta \). Now take \( r \geq 1 \) be any integer and take \( n \geq pr \). Then, for each \( \ell = 0, 1, \ldots, r-1 \), we have that both 
\[
\frac{1}{p} \prod_{k=0}^{p-1}(\alpha - (p\ell + k)) \quad \text{and} \quad \frac{1}{p} \prod_{k=0}^{p-1}(\beta - (p\ell + k))
\]
are algebraic integers. Thus, if \( n \geq pr \), then 
\[
\frac{\sqrt{5}b_n}{p^r} = (-1)^{n-1} \left( \beta \prod_{\ell=0}^{p-1} \prod_{k=0}^{r-1} (\alpha - (p\ell + k)) \prod_{k=pr}^{n-1} (\alpha - k) - \alpha \prod_{\ell=0}^{p-1} \prod_{k=pr}^{r-1} (\beta - (p\ell + k)) \prod_{k=pr}^{n-1} (\beta - k) \right)
\]
is an algebraic integer. Thus, \( 5b_n^2/p^{2r} \) is an algebraic integer and a rational number, so an integer. Since \( p \neq 5 \), it follows that \( p^{2r} \mid b_n^2 \), so \( p^r \mid b_n \) for \( n \geq pr \). This shows that \( T_{pr} = 1 \) for all such primes \( p \) and positive integers \( r \). The same is true for \( p = 5 \). There we use that \( \alpha - 3 = \sqrt{5} \beta \), so \( \sqrt{5} \mid \alpha - 3 \). Thus, if \( n \geq 10r \), we have that 
\[
\prod_{k=1}^{n} (\alpha - k) \quad \text{is a multiple of} \quad \prod_{\ell=0}^{2r-1} (\alpha - (3 + 5\ell)) \quad \text{in} \quad \mathbb{Z}[(1 + \sqrt{5})/2],
\]
which in turn is a multiple of \( 5^r = \sqrt{5}^{2r} \) in \( \mathbb{Z}[(1 + \sqrt{5})/2] \). Thus, if \( n \geq 10r \), then \( 5^r \mid b_n \). This shows that also \( T_{5r} = 1 \) and in fact, \( m \mid b_n \) for all \( n > n_m \) if \( m \) is made up only of primes \( 0, 1, 4 \) (mod \( 5 \)). This finishes the proof of (b).

**Proof of Part c.** The claim is satisfied for \( p = 2 \), as \( \{b_n \mod 2 \}_{n \geq 0} = (1, 0)^\infty \), thus \( T_2 = 2 \mid 4 \). Consider now \( p > 2 \). Evaluating Formula (5) at \( \alpha = \frac{1 + \sqrt{5}}{2} \), one has 
\[
\prod_{k=0}^{p-1} (\alpha - k) \equiv \alpha^p - \alpha \quad \pmod{p}.
\]
Since \( 5(p^2 - 1)/2 \equiv -1 \pmod{p} \), the argument from (6) shows that \( \alpha^p \equiv \beta \pmod{p} \). Thus 
\[
\prod_{k=1}^{2p} (\alpha - k) = \prod_{k=1}^{p} (\alpha - k) \prod_{k=p+1}^{2p} (\alpha - k) \equiv (\beta - \alpha)^2 \quad \pmod{p} \equiv 5 \quad \pmod{p}.
\]
The same is true for \( \alpha \) replaced by \( \beta \). Thus, it follows that for \( n > 2p \), we have 
\[
b_{n+2p} = \frac{(-1)^{n+2}p-1}{\sqrt{5}} \left( \beta \prod_{k=0}^{p-1} (\alpha - k) - \alpha \prod_{k=0}^{n+2p-1} (\beta - k) \right)
\]
\[
\equiv \frac{(-1)^{n-1}}{\sqrt{5}} \left( \beta \prod_{k=0}^{n-1} (\alpha - k) - \alpha \prod_{k=0}^{n-1} (\beta - k) \right) \quad \pmod{p}
\]
\[
\equiv 5b_n \quad \pmod{p}.
\]
Applying this \( k \) times, we get

\[
b_{n+2pk} \equiv 5^k b_n \pmod{p}.
\]

Taking \( k = p - 1 \) and applying Fermat's little theorem \( 5^{p-1} \equiv 1 \pmod{p} \), we get \( T_p \mid 2p(p-1) \).

We can optimize this idea by taking \( k = \text{ord}_p(5) \), where \( \text{ord}_p(5) \) is the order of 5 modulo \( p \) (the smallest \( k > 0 \) such that \( 5^k \equiv 1 \pmod{p} \)), this gives the stronger wanted claim: \( T_p \mid 2p \text{ord}_p(5) \).

**Proof of Part d).** By a), we know that \( T_p \mid T_{pm} \). Taking \( p = 2 \), one gets \( 2 \mid T_m \). Now, if \( T_m > 1 \), by b), there is at least a prime \( p = 2, 3 \pmod{5} \) such that \( p \mid m \). We then have \( T_p \mid T_m \) by a). We now prove by contradiction that \( T_p \) is a multiple of 4.

Take a prime \( p \geq 3 \) and assume \( \nu_2(T_p) < 2 \), where \( \nu_2(a) \) is the exponent of 2 in the factorization of \( a \). That is, \( T_p \) would either be odd or 2 times an odd number. Since \( T_p \mid 2p(p-1) \), it would follow that if we write \( p-1 = 2^a k \), where \( k \) is odd, then \( T_p \mid 2pk \). Thus, one would have

\[
b_n \equiv b_{n+2pk} \equiv 5^k b_n \pmod{p} \quad (7)
\]

for all \( n > n_p \). Since \( p = 2, 3 \pmod{5} \), 5 is not a quadratic residue, and thus \( 5^k \not\equiv 1 \pmod{p} \) (since \( -1 \equiv 5^{(p-1)/2} \equiv (5^2)^{(p-1)/4} \equiv \pmod{p} \)). So, the above congruence (7) would imply that \( p \mid (5^k - 1)b_n \) but \( p \nmid 5^k - 1 \), so \( b_n \equiv 0 \pmod{p} \) for all large \( n \). Take \( n \) and \( n + 1 \) and rewrite what we got, i.e., \( b_n \equiv b_{n+1} \equiv 0 \pmod{p} \) in \( \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \) as

\[
b_n = \beta \prod_{k=0}^{n-1} (\alpha - k) - \alpha \prod_{k=0}^{n-1} (\beta - k) \equiv 0 \pmod{p},
\]

\[
b_{n+1} = \beta \left( \prod_{k=0}^{n-1} (\alpha - k) \right) (\alpha - n) - \beta \left( \prod_{k=0}^{n-1} (\beta - k) \right) (\beta - n) \equiv 0 \pmod{p}.
\]

We treat this as a linear system in the two unknowns

\[(X, Y) = \left( \beta \prod_{k=0}^{n-1} (\alpha - k), \alpha \prod_{k=0}^{n-1} (\beta - k) \right) \]

in the field with \( p^2 \) elements \( \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \). This is homogeneous. None of \( X \) or \( Y \) is 0 since \( p \) cannot divide \( \beta \prod_{k=0}^{n-1} (\alpha - k) \). Thus, it must be that the determinant of the above matrix is 0 modulo \( p \), but this is

\[
\begin{vmatrix}
1 & -1 \\
\alpha - n & -(\beta - n)
\end{vmatrix} = \sqrt{5},
\]

which is invertible modulo \( p \). Thus, indeed, it is not possible that \( b_n \) and \( b_{n+1} \) is a multiple of \( p \) for all large \( n \), getting a contradiction. This shows that \( T_p \) is a multiple of 4.
Proof of Part e). Let \( m \) be of shape different from the one required in Part b), i.e., \( m \) has now at least one prime \( p \equiv 2, 3 \mod 5 \) such that \( p \mid m \). Then \( 4 \mid T_p \) by what we have done above, and so \( 4 \mid T_m \) by a). Thus, such \( m \) cannot participate in the situations described either at d) or e). Further, one has \( T_4 = 8 \) as \( \{ b_n \mod 4 \}_{n \geq 0} = (1, 0, 1, 2, 3, 0, 3, 2)^\infty \). Thus, if \( 4 \mid m \), then \( 8 \mid T_m \). Hence, if \( T_m = 2 \), then the only possibility is that \( 2 \mid m \) and \( m/2 \) is a product of primes congruent to \( 0, 1, 4 \) modulo 5. Conversely, if \( m \) has such structure then \( T_m = 2 \) by a) and the fact that \( T_2 = 2 \) and \( T_{p^r} = 1 \) for all odd prime power factors \( p^r \) of \( m \). This ends the proof of e).

Proof of Part f). Finally, f) is based on a preliminary result: a slight generalization of (5), namely
\[
\prod_{k=0}^{p^r-1} (X - k) \equiv (X^p - X)^{p^r-1} \mod p^r \tag{8}
\]
valid for all odd primes \( p \) and \( r \geq 1 \). Let us prove (8) by induction on \( r \). We first prove it for \( r = 2 \). We return to (5) and write
\[
\prod_{k=0}^{p-1} (X - k) = X^p - X + pH_1(X),
\]
where \( H_1(X) \in \mathbb{Z}[X] \). Changing \( X \) to \( X - p\ell \) for \( \ell = 0, 1, \ldots, p - 1 \), we get that
\[
\prod_{k=0}^{p-1} (X - (p\ell + k)) = (X - p\ell)^p - (X - p\ell) + pH(X - p\ell) \equiv (X^p - X - pH(X)) - p\ell \mod p^2.
\]
In the above, we used the fact that \( H(X - p\ell) \equiv H(X) \mod p \). Thus,
\[
\prod_{k=0}^{p^2-1} (X - k) = \prod_{\ell=0}^{p-1} \prod_{k=0}^{p-1} (X - (p\ell + k))
\]
\[
\equiv \prod_{\ell=0}^{p-1} ((X^p - X - pH(X)) - p\ell) \mod p^2
\]
\[
\equiv (X^p - X - pH(X))^p - (X^p - X - pH(X))^{p-1}p\left(\sum_{\ell=0}^{p-1} \ell\right) \mod p^2
\]
\[
\equiv (X^p - X)^p - (X^p - X - pH(X))^{p-1}p\left(\frac{p(p-1)}{2}\right) \mod p^2
\]
\[
\equiv (X^p - X)^p \mod p^2.
\]
In the above, we used the fact that \( p \) is odd so \( p(p-1)/2 \) is a multiple of \( p \). This proves (8) for \( r = 2 \). Now, assuming that (8) holds for \( p^r \), for some \( r \geq 2 \), we get that for all \( \ell \geq 0 \), we have
\[
\prod_{k=0}^{p^{r+1}-1} (X - (p^r\ell + k)) \equiv ((X - p^r\ell)^p - (X - p^r\ell))^{p^{r+1}-1} + p^rH_r(X - p^r\ell) \mod p^{r+1}
\]
\[
\equiv (X^p - X)^{p^{r+1}} + p^rH_r(X) \mod p^{r+1},
\]
\[
8
\]
where \( H_r(X) \in \mathbb{Z}[X] \). This allows concluding the induction step, and thus the generalization (8) that we wanted:

\[
\prod_{k=0}^{p^{r+1}-1} (X - k) = \prod_{\ell=0}^{p^r-1} \prod_{k=0}^{p^r-1} (X - (p^r \ell + k)) \\
= ((X^p - X)^{p^r-1} + p^r H_r(X))^p \quad \text{(mod } p^{r+1}) \\
= (X^p - X)^{p^r} \quad \text{(mod } p^{r+1}).
\]

Equipped with this preliminary result, letting \( p > 2 \) be congruent to 2, 3 (mod 5), evaluating the above identity in \( \alpha \), and using that \( \alpha^p \equiv \beta \) (mod \( p \)), we get that

\[
\prod_{k=0}^{p^r-1} (\alpha - k) \equiv (X^p - X)^{p^r-1} \quad \text{(mod } p^r) \equiv (\alpha^p - \alpha)^{p^r-1} \quad \text{(mod } p^r) \equiv (\beta - \alpha)^{p^r-1} \quad \text{(mod } p^r).
\]

This shows that

\[
\prod_{k=0}^{2p^r-1} (\alpha - k) \equiv (\beta - \alpha)^{2p^r-1} \quad \text{(mod } p^r) \equiv 5^{p^r-1} \quad \text{(mod } p^r).
\]

The same is true for \( \beta \); this leads to

\[
b_{n+2p^r} = \frac{(-1)^{n+2p^r-1}}{\sqrt{5}} 5^{p^r-1} \left( \beta \prod_{k=0}^{n-1} (\alpha - k) - \alpha \prod_{k=0}^{n-1} (\beta - k) \right) \quad \text{(mod } p^r) \equiv 5^{p^r-1} b_n \quad \text{(mod } p^r).
\]

Thus, applying this \( k \) times, we get

\[
b_{n+2p^r} = 5^{p^r-1} b_n \quad \text{(mod } p^r). \tag{9}
\]

By Euler’s theorem \( \alpha^{\phi(n)} \equiv 1 \) (mod \( n \)), one has \( 5^{p^r-1} (p-1) \equiv 1 \) (mod \( p^r \)). Thus, taking \( k = p - 1 \) in (9), we get \( b_{n+2p^r} \equiv b_n \) (mod \( p^r \)). Therefore, \( \ell_{p^r} | 2p^r(p-1) \).

N.B.: As in the proof of c), we can optimize this idea; indeed \( \text{ord}_5(p^r) = p^r - 1 \text{ord}_5(p) \) and thus taking \( k = \text{ord}_5(p) \), one gets \( \ell_{p^r} | 2p^r \text{ord}_5(p) \).

Finally, it remains to prove f) for \( p = 2 \). Here, by inspection, we have

\[
\prod_{k=0}^{7} (X - k) \equiv (X^2 - X)^4 \quad \text{(mod } 4).
\]

By induction on \( r \geq 2 \), one shows that

\[
\prod_{k=0}^{2^{r+1}-1} (X - k) \equiv (X^2 - X)^{2^r} \quad \text{(mod } 2^r).
\]

Evaluating this in \( \alpha \), we get

\[
\prod_{k=0}^{2^{r+1}-1} (\alpha - k) \equiv (\alpha^2 - \beta)^{2^r} \equiv 5^{2^r-1} \quad \text{(mod } 2^r).
\]

The same holds for \( \beta \), so

\[
b_{n+2^{r+1}} = \frac{(-1)^{n+2^{r+1}-1}}{\sqrt{5}} 5^{2^r-1} \left( \beta \prod_{k=0}^{n-1} (\alpha - k) - \alpha \prod_{k=0}^{n-1} (\beta - k) \right) \quad \text{(mod } 2^r) \approx 5^{2^r-1} b_n \quad \text{(mod } 2^r) \equiv b_n \quad \text{(mod } 2^r)
\]

showing that \( \ell_{2^r} | 2^{r+1} \) for all \( r \geq 2 \).
3 Comments and generalizations

Along the proof of our main result we showed that if \( p \equiv 2, 3 \pmod{5} \), then

\[
b_{n+2p} \equiv 5b_n \pmod{p}.
\]

From here we deduced that \( T_p \mid 2p(p - 1) \) via the fact that \( 5^{p-1} \equiv 1 \pmod{p} \). One may ask whether it can be the case that \( T_{p^2} \mid 2p(p - 1) \) for some prime \( p \). Well, first of all, we will need that \( 5^{p^2-1} \equiv 1 \pmod{p^2} \). This makes \( p \) a base-5 Wieferich prime. There is a conjecture that there are infinitely many such primes. The smallest known which is also congruent to

\[
2, 3 \pmod{5}
\]

is 40487. However, the condition of condition of \( p \) being base-5 Wieferich is not sufficient. A close analysis of our arguments show that in addition to this condition, it should also hold that

\[
\prod_{k=0}^{2p-1} (\alpha - k) - 5 \equiv 0 \pmod{p^2},
\]

and if this is the case then indeed \( T_{p^2} \mid 2p(p - 1) \). Since the integer

\[
\frac{1}{p} \left( \prod_{k=0}^{2p-1} (\alpha - k) - 5 \right) \in \mathbb{Z}[\alpha]
\]

should be the zero element in the finite field \( \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \), with \( p^2 \) elements, it could be that the “probability” that this condition happens is \( 1/p^2 \). By the same logic, the “probability” that \( p \) is base-5 Wieferich should be \( 1/p \). Assuming these events to be independent, we could infer that the probability that both these conditions hold is \( 1/p^3 \). Then, as the series

\[
\sum_{p=2,3 \pmod{5}} \frac{1}{p^3}
\]

is convergent, this heuristically suggests that there should be only finitely many primes \( p \equiv 2, 3 \pmod{5} \) such that \( T_{p^2} \mid 2p(p - 1) \).

Finally, our results apply to other sequences as well. More precisely, let \( a, b \) be integers and let \( \alpha, \beta \) be the roots of \( x^2 - ax - b \). Let

\[
B(x) = \frac{\beta}{\beta - \alpha} (1 - x)^\alpha + \frac{\alpha}{\alpha - \beta} (1 - x)^\beta - 1 = \sum_{n \geq 0} b_n \frac{x^n}{n!}.
\]

Accordingly, the sequence \( \{b_n\}_{n \geq 0} \) satisfies \( b_0 = 1, b_1 = 0 \), and, for \( n \geq 0 \)

\[
b_{n+2} = (2n - a + 1) b_{n+1} + (b + an - n^2) b_n.
\]

What are the periods \( \pmod{m} \) of such sequences?

- In case \( \alpha \) and \( \beta \) are rational (hence, integers), \( B(x) \) is a rational function, so \( b_n = n!u_n \), where \( \{u_n\}_{n \geq 0} \) is binary recurrent with constant coefficients. It then follows that \( b_n \equiv 0 \pmod{m} \) for all \( m \) provided \( n > n_m \) is sufficiently large. Thus, \( T_m = 1 \).
In case $\alpha, \beta$ are irrational, then we get a result similar to Theorem 2 (where we had $(a, b) = (1, 1)$). Namely, $b_n \equiv 0 \pmod{m}$ for all $n$ sufficiently large whenever $m$ is the product of odd primes $p$ for which the Legendre symbol $\left( \frac{\Delta}{p} \right) = 0, 1$, where $\Delta = a^2 + 4b$ is the discriminant of the quadratic $x^2 - ax - b$. In case $p$ is odd and $\left( \frac{\Delta}{p} \right) = -1$, we have that $T_p \mid 2p(p-1)$ and $T_p$ is a multiple of 4. Also, $T_{pr} \mid 2^{pr}(p-1)$ for all $r \geq 1$ in this case. The proofs are similar. In the case of the prime 2, one needs to distinguish cases according to the parities of $a, b$. For example, if $a$ and $b$ are odd, then $\Delta \equiv 5 \pmod{8}$, so 2 is not a quadratic residue modulo $\Delta$, so $T_2r \mid 2^{r+1}$ for all $r \geq 1$, whereas if $a$ is odd and $b$ is even then $T_2 = 1$.

This concludes our analysis of the periodicity of such $P$-recursive sequences $\pmod{m}$.

Acknowledgments: This work was initiated when the second author was invited professor at the Paris Nord University, in April 2018. In addition, Florian Luca was supported in part by grant CPRR160325161141 and an A-rated scientist award both from the NRF of South Africa and by grant no. 17-02804S of the Czech Granting Agency.

References


