#A116 INTEGERS 21 (2021)

BINARY RECURRENCES WITH PRIME POWERS AS FIXED POINTS OF THEIR DISCRIMINATOR

Matteo Ferrari
Dipartimento di Scienze Matematiche "G.L. Lagrange", Politecnico di Torino, Turin, Italy
matteo.ferrari@polito.it

Received: 12/15/20, Accepted: 11/22/21, Published: 12/3/21

Abstract

The *discriminator sequence* $\{\mathcal{D}_{\mathbf{u}}(n)\}_{n\geq 0}$ of a sequence $\mathbf{u} = \{u_n\}_{n\geq 0}$ of distinct integers is defined for each n as the smallest positive integer m such that $u_0, \ldots, u_{n-1}$ are pairwise incongruent modulo m. Since in general, it is difficult to find an explicit characterization of the discriminator $\mathcal{D}_{\mathbf{u}}(n)$ of a given recurrence sequence $\mathbf{u} = \{u_n\}_{n\geq 0}$, we provide a bound for a specific type of binary recurrences. To do this, we investigate binary recurrences with prime powers as fixed points of their discriminator. We almost complete a characterization of the binary recurrences for which, for a given prime R, $\mathcal{D}_{\mathbf{u}}(R^k) = R^k$ for each $k \geq 0$. This paper is the continuation of a recent work by de Clercq et al., dealing with the case $R = 2$.

1. Introduction

The *discriminator sequence* of a sequence $\mathbf{u} = \{u_n\}_{n\geq 0}$ of distinct integers is defined as the sequence $\{\mathcal{D}_{\mathbf{u}}(n)\}_{n\geq 0}$ given by

$$\mathcal{D}_{\mathbf{u}}(n) := \min\{m \geq 1 : u_0, \ldots, u_{n-1} \text{ are pairwise distinct} \pmod{m}\}.$$

Trivially, we have

$$n \leq \mathcal{D}_{\mathbf{u}}(n) \leq \max\{u_0, \ldots, u_{n-1}\} - \min\{u_0, \ldots, u_{n-1}\} + 1.$$

The main problem is to give an easy description or characterization of $\{\mathcal{D}_{\mathbf{u}}(n)\}$. In general, this is a difficult task, but we observe that if we have, for some prime R,

$$\mathcal{D}_{\mathbf{u}}(R^k) = R^k \quad \text{for every } k \geq 1,$$

then $\mathcal{D}_{\mathbf{u}}(n) < Rn$ for each $n \geq 1$. This follows easily since given n, take k such that $R^k \leq n \leq R^{k+1}$; if $\mathcal{D}_{\mathbf{u}}(R^{k+1}) = R^{k+1}$, then we have $\mathcal{D}_{\mathbf{u}}(n) \leq R^{k+1} \leq Rn$.

For integers w_0, w_1, p and q, let $\mathbf{w} = \{w_n\}_{n\geq 0}$ be the sequence defined by

$$w_{n+2} = pw_{n+1} + qw_n \quad \text{for all } n \geq 0. \tag{1}$$

In [1] the following result is established.

Theorem 1. *Let $\mathbf{w} = \{w_n\}_{n\geq 0}$ be as in (1), if $(p,q) \equiv (2,3) \pmod 4$ and $w_0 + w_1$ is odd, then $\mathcal{D}_{\mathbf{w}}(2^k) = 2^k$ for every $k \geq 1$. If $(p,q) \not\equiv (2,3) \pmod 4$ and $k \geq 3$, then $\#\{w_n \pmod{2^k} : 0 \leq n \leq 2^k - 1\} < 2^k$.*

In this paper, we will prove a partial generalization, namely the following results.

Theorem 2. *Let $\mathbf{w} = \{w_n\}_{n\geq 0}$ be as in (1). If $(p,q) \equiv (2,2) \pmod 3$, $p + q \not\equiv 7 \pmod 9$ and $w_0 \not\equiv w_1 \pmod 9$, then $\mathcal{D}_{\mathbf{w}}(3^k) = 3^k$ for every $k \geq 1$.*

Theorem 3. *Let $\mathbf{w} = \{w_n\}_{n\geq 0}$ be as in (1) and $R \geq 5$ prime. If $(p,q) \equiv (2, R-1) \pmod R$ and $w_0 \not\equiv w_1 \pmod R$, then $\mathcal{D}_{\mathbf{w}}(R^k) = R^k$ for every $k \geq 1$.*

We will follow the line of reasoning of [1], focusing on the points where things change between $R = 2$ and all the other primes, with particular attention on the second exception: $R = 3$.

2. Preliminaries

The Lucas sequence $\mathbf{u(p,q)} = \{u_n\}_{n\geq 0}$ for $p, q \in \mathbb{Z}$ is defined as

$$\begin{cases} u_0 = 0, \\ u_1 = 1, \\ u_{n+2} = pu_{n+1} + qu_n \quad n \geq 0. \end{cases}$$

The general idea is to prove something for a Lucas sequence, and then generalize to an arbitrary binary recurrence, seeing it as a shifted Lucas sequence. For this purpose, in [1], in order to prove Theorem 1, the following result is established first.

Lemma 1. *For a Lucas sequence $\mathbf{u(p,q)}$, $\mathcal{D}_{\mathbf{u(p,q)}}(2^k) = 2^k$ for all $k \geq 0$ if and only if $(p,q) \equiv (2,3) \pmod 4$.*

We will prove analogous results for the other primes.

Lemma 2. *For a Lucas sequence $\mathbf{u(p,q)}$, $\mathcal{D}_{\mathbf{u(p,q)}}(3^k) = 3^k$ for all $k \geq 0$ if and only if $(p,q) \equiv (2,2) \pmod 3$ and $p + q \not\equiv 7 \pmod 9$.*

Lemma 3. *For a Lucas sequence $\mathbf{u(p,q)}$, given $R > 3$ prime, if $(p,q) \equiv (2, R-1) \pmod R$, then $\mathcal{D}_{\mathbf{u(p,q)}}(R^k) = R^k$ for all $k \geq 0$.*

The converse is proved only numerically for $R = 5, 7, 11, 13$.

Conjecture. For a Lucas sequence $\mathbf{u(p,q)}$, given $R > 3$ prime, if $\mathcal{D}_{\mathbf{u(p,q)}}(R^k) = R^k$ for all $k \geq 0$, then $(p, q) \equiv (2, R-1) \pmod R$.

Let $\nu_q(n)$, for q prime, be the exponent of q in the prime factorization of the integer n.

Theorem 4 (Kummer, 1852, cf. [2], pp. 30-33.)**.** *Let p be a prime number. The exponent of p in $\binom{n}{m}$, i.e. $v_p\left(\binom{n}{m}\right)$, is the number of base p carries when summing m with $n-m$ in base p.*

Lemma 4. *Given an odd prime R, we have*

$$\nu_R\left(\binom{l}{k}R^k\right) \geq \nu_R(Rl) = \nu_R(l) + 1$$

for all $l \geq 1$ and for all $k \leq l$. Further, for all $k \geq 1$ and for all $l \leq R^k$

$$\nu_R\left(\binom{R^k}{l}R^l\right) \geq k+1;$$

for all $k \geq 1$ and for all $l \leq R^k/2$

$$\nu_R\left(\binom{R^k}{2l}R^l\right) \geq k+1;$$

finally, for all $k \geq 1$ and for all $l \leq (R^k-1)/2$, with the exception $l = 1$ and $R = 3$,

$$\nu_R\left(\binom{R^k}{2l+1}R^l\right) \geq k+1.$$

Proof. We use Theorem 4 with $p = R$. Since the first inequality is clear when $k = 1$, we may assume $k \geq 2$. If $\nu_R(l) \leq 1$, the inequality is obvious too. Since it is also clear if $k \geq \nu_R(l) + 1$, we may assume that $k < \nu_R(l) + 1$. Then, we have $\nu_R(k) < k < \nu_R(l) + 1$. By summing up k with $l-k$, we have at least $\nu_R(l) - \nu_R(k)$ carries in base R. Thus, we obtain

$$\nu_R\left(\binom{l}{k}R^k\right) \geq \nu_R(l) - \nu_R(k) + k \geq \nu_R(l) + 1.$$

In the second inequality we have $l \in [1, R^k]$. In that case the number of carries from summing l with $R^k - l$ is at least, by the previous argument, $k - \nu_R(l)$, since $\nu_R(l) \leq \nu_R(R^k) = k$. Hence, by using Theorem 4 again, we obtain

$$\nu_R\left(\binom{R^k}{l}R^l\right) \geq k - \nu_R(l) + l \geq k+1.$$

In the third inequality we have $l \in [1, R^k/2]$. Then, similarly, the number of carries from summing $2l$ with $R^k - 2l$ is at least $k - \nu_R(2l)$. Therefore, using again Theorem 4, we conclude

$$\nu_R\left(\binom{R^k}{2l}R^l\right) \geq k - \nu_R(2l) + l = k - \nu_R(l) + l \geq k + 1$$

since R is odd. For the fourth inequality we have $l \in [1, (R^k - 1)/2]$. Then, again the number of carries from summing $2l+1$ with $R^k - 2l - 1$ is at least $k - \nu_R(2l+1)$. Hence, by using for the last time Theorem 4, we obtain

$$\nu_R\left(\binom{R^k}{2l+1}R^l\right) \geq k - \nu_R(2l+1) + l.$$

Now the only exception occurs when $l = 1$ and $R = 3$, in that case $\nu_R(2l + 1) = \nu_3(3) = 1 = l$, in all the other cases $-\nu_R(2l + 1) + l \geq 1$. □

3. Proofs of the Main Theorems

Lemma 5. *For a Lucas sequence* $\mathbf{u}(\mathbf{p}, \mathbf{q})$*, given a prime* $R > 3$*, if* $(p, q) \equiv (2, R-1) \pmod{R}$*, then* $\mathcal{D}_{\mathbf{u}(\mathbf{p},\mathbf{q})}(R^k) = R^k$ *for all* $k \geq 0$*.*

Proof. Suppose $(p, q) \equiv (2, R-1) \pmod{R}$. We consider the quadratic polynomial $x^2 - px - q$ having discriminant $\Delta = p^2 + 4q$. The equation $x^2 - px - q = 0$ is the characteristic equation for the Lucas sequence $\mathbf{u}(\mathbf{p}, \mathbf{q})$.

`The degenerate case.` In the case $\Delta = 0$, we have a generic solution

$$u_n = Ap_0^n + Bnp_0^n,$$

with $p_0 = p/2$. Imposing the starting condition, we obtain $u_n = np_0^{n-1}$. We notice that if $\Delta = p^2 + 4q = 0$, then p is even, and so $p_0 \in \mathbb{Z}$; moreover, since $p \equiv 2 \pmod{R}$ and $R > 2$, then $p_0 \equiv 1 \pmod{R}$. So we obtain

$$\{u_0, u_1, u_2, \ldots, u_{R-1}\} = \{0, 1, 2p_0, \ldots, (R-1)p_0^{R-2}\} \equiv \{0, 1, 2, \ldots, R-1\} \pmod{R}.$$

We claim that $\nu_R(u_m - u_n) = \nu_R(m - n)$ for all $m > n$. Indeed, if there exist $n < m \leq R^k$ such that $u_n \equiv u_m \pmod{R^k}$, then we would expect $\nu_R(m - n) = \nu_R(u_m - u_n) \geq k$. Since $u_m - u_n = mp_0^{m-1} - np_0^{n-1}$, we have $u_m - u_n \equiv m - n \pmod{R}$. So $\nu_R(u_m - u_n) = 0$ if and only if $\nu_R(m - n) = 0$. We assume that $m \equiv n \pmod{R}$ and write $m = n + Rl$. Then we obtain

$$u_m - u_n = (n + Rl)p_0^{n+Rl-1} - np_0^{n-1} = p_0^{n-1}\big((n + Rl)(p_0^{Rl} - 1) + Rl\big). \quad (2)$$

We write $p_0^R = 1 + Rp_1$, with $p_1 \in \mathbb{N}$ (this can be done since $p_0 \equiv 1 \pmod R$), and so $p_0 = 1 + Rt$ and $p_0^R = 1 + Rt\sum_{j=0}^{R-1}\binom{R}{j+1}(Rt)^j$). Thus, we obtain

$$p_0^{Rl} - 1 = (1 + Rp_1)^l - 1 = \sum_{s=1}^{l}\binom{l}{s}(Rp_1)^s.$$

From the latter equation and (2) we conclude

$$u_m - u_n = p_0^{n-1}\Big((n + Rl)\sum_{s=1}^{l}\binom{l}{s}(Rp_1)^s + Rl\Big).$$

Since by Lemma 4 for every $s \geq 1$ we have

$$\nu_R\left(\binom{l}{s}(Rp_1)^s\right) \geq \nu_R\left(\binom{l}{s}R^s\right) \geq \nu_R(Rl),$$

we conclude that

$$\nu_R(u_m - u_n) = \nu_R(Rl) = \nu_R(m - n),$$

thus establishing the claim.

`The non-degenerate case.` Here we suppose $\Delta \neq 0$. Since by assumption $p \equiv 2 \pmod R$ and $q \equiv R - 1 \pmod R$, it follows that $\Delta = p^2 + 4q \equiv 4 + 4(R - 1) \equiv 0 \pmod R$. Let $\alpha := p/2 + \sqrt{\Delta}/2$ and $\beta := p/2 - \sqrt{\Delta}/2$ be the roots of $x^2 - px - q = 0$. The generic solution is $u_n = A\alpha^n + B\beta^n$. On imposing the initial condition we obtain

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{3}$$

We introduce the companion sequence $\mathbf{v} = \{v_n\}_{n\geq 0}$ given by

$$\begin{cases} v_0 = 2, \\ v_1 = p, \\ v_{n+2} = pv_{n+1} + qv_n \quad n \geq 0. \end{cases}$$

By induction $v_n \equiv 2 \pmod R$, for all $n \geq 0$. Further, we obtain

$$v_n = \alpha^n + \beta^n \quad \text{for all } n \geq 0. \tag{4}$$

Next we will show that

$$u_{n+R^k} \equiv u_n + R^k \pmod{R^{k+1}}$$

for all $k \geq 1$ and for all $n \geq 0$. We have

$$(2\alpha)^{R^k} = \left(p + \sqrt{\Delta}\right)^{R^k} = \sum_{l=0}^{R^k}\binom{R^k}{l}p^{R^k - l}\Delta^{l/2},$$

and similarly

$$(2\beta)^{R^k} = \left(p - \sqrt{\Delta}\right)^{R^k} = \sum_{l=0}^{R^k} \binom{R^k}{l} p^{R^k - l} \left(-\Delta^{1/2}\right)^l = \sum_{l=0}^{R^k} (-1)^l \binom{R^k}{l} p^{R^k - l} \Delta^{l/2}.$$

So we have

$$\begin{aligned}(2\alpha)^{R^k+n} - (2\beta)^{R^k+n} &= (2\alpha)^n \sum_{l=0}^{R^k} \binom{R^k}{l} p^{R^k-l} \Delta^{l/2} \\ &\quad - (2\beta)^n \sum_{l=0}^{R^k} (-1)^l \binom{R^k}{l} p^{R^k-l} \Delta^{l/2}.\end{aligned}$$

We have $\alpha - \beta = \sqrt{\Delta}$ and, since $\Delta \neq 0$, we obtain

$$\begin{aligned}\frac{(2\alpha)^{R^k+n} - (2\beta)^{R^k+n}}{\alpha - \beta} &= 2^n \frac{\alpha^n - \beta^n}{\alpha - \beta} \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l} \Delta^l \\ &\quad + 2^n(\alpha^n + \beta^n) \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1} \Delta^l.\end{aligned}$$

Recalling (3) and (4) we obtain

$$\begin{aligned}\frac{(2\alpha)^{R^k+n} - (2\beta)^{R^k+n}}{\alpha - \beta} &= 2^n u_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l} \Delta^l \\ &\quad + 2^n v_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1} \Delta^l.\end{aligned}$$

We want to show now that

$$u_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l} \Delta^l \equiv 2^{R^k} u_n \pmod{R^{k+1}}$$

and

$$v_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1} \Delta^l \equiv 2^{R^k} R^k \pmod{R^{k+1}}.$$

For the first one, observe that

$$\sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l} \Delta^l = p^{R^k} + \sum_{l=1}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l} \Delta^l,$$

since $p \equiv 2 \pmod{R}$ we have $p = 2 + hR$ and

$$p^{R^k} = (2+hR)^{R^k} = 2^{R^k} + \sum_{j=1}^{R^k} \binom{R^k}{j} 2^{R^k-j}(hR)^j.$$

For each $j \geq 1$, recalling Lemma 4

$$\binom{R^k}{j} 2^{R^k-j}(hR)^j \equiv 0 \pmod{R^{k+1}},$$

so $p^{R^k} \equiv 2^{R^k} \pmod{R^{k+1}}$. It remains to show that

$$\sum_{l=1}^{(R^k-1)/2} \binom{R^k}{2l} p^{R^k-2l}\Delta^l \equiv 0 \pmod{R^{k+1}},$$

but this is true again for each $l \geq 1$ from Lemma 4 since $\Delta \equiv 0 \pmod{R}$.

We want to show now that

$$v_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1}\Delta^l \equiv 2^{R^k}R^k \pmod{R^{k+1}}.$$

As before we split

$$v_n \sum_{l=0}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1}\Delta^l = v_n R^k p^{R^k-1} + v_n \sum_{l=1}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1}\Delta^l.$$

Since $v_n \equiv 2 \pmod{R}$ for all n, we have $v_n p^{R^k-1} \equiv 2^{R^k} \pmod{R}$. Multiplication of both sides by R^k, then yields the congruence $v_n R^k p^{R^k-1} \equiv 2^{R^k}R^k \pmod{R^{k+1}}$.

We notice that all the work done for now doesn't exclude the case $R = 3$, the only difference is in evaluating the next sum. We want to show that for $R > 3$ prime

$$\sum_{l=1}^{(R^k-1)/2} \binom{R^k}{2l+1} p^{R^k-2l-1}\Delta^l \equiv 0 \pmod{R^{k+1}}.$$

This is an easy consequence of the fourth part of Lemma 4 and $\Delta \equiv 0 \pmod{R}$.

Then, for $R > 3$, we infer

$$u_{n+R^k} \equiv u_n + R^k \pmod{R^{k+1}}, \tag{5}$$

which by induction leads to $\mathcal{D}_{\mathbf{u(p,q)}}(R^k) = R^k$ for all $k \geq 1$. Since $\mathcal{D}_{\mathbf{u(p,q)}}(n) \geq n$, we have to show only that $u_m \not\equiv u_n \pmod{R^{k+1}}$ for every pair (n,m) with $0 \leq n < m < R^{k+1}$. This is true using repeatedly $u_{n+R^h} \equiv u_n + R^h \pmod{R^{h+1}}$ for $h \leq k$ and induction on k. $\square$

Theorem 5. *For a Lucas sequence* $\mathbf{u(p,q)}$*, it holds* $\mathcal{D}_{\mathbf{u(p,q)}}(3^k) = 3^k$ *for all* $k \geq 1$ *if and only if* $(p,q) \equiv (2,2) \pmod 3$ *and* $p+q \not\equiv 7 \pmod 9$*.*

Proof. The proof is similar to the general one. We have only to deal more accurately with the sum

$$\sum_{l=1}^{(3^k-1)/2} \binom{3^k}{2l+1} p^{3^k-2l-1}\Delta^l \equiv 0 \pmod{3^{k+1}}.$$

In particular, from Lemma 4 for $l \geq 2$ each term is zero but, in general, the term with $l = 1$

$$\binom{3^k}{3} p^{3^k-3}\Delta = \frac{3^{k-1}(3^k-1)(3^k-2)}{2} p^{3^k-3}\Delta$$

is not zero. It depends on the class of $\Delta \pmod 9$. If $(p,q) \equiv (2,2) \pmod 3$, then we have $(p,q) \equiv (2,2)$, $(2,5)$, $(5,2)$, $(5,5)$, $(2,8)$, $(8,2)$, $(5,8)$, $(8,5)$ or $(8,8) \pmod 9$. We have three cases:

- when $p+q \equiv 4 \pmod 9$, i.e. when $(p,q) \in \{(2,2),(5,8),(8,5)\} \pmod 9$, in which case $\Delta \equiv 3 \pmod 9$;
- when $p+q \equiv 1 \pmod 9$, i.e. when $(p,q) \in \{(5,5),(2,8),(8,2)\} \pmod 9$, in which case $\Delta \equiv 0 \pmod 9$;
- when $p+q \equiv 7 \pmod 9$, i.e. when $(p,q) \in \{(8,8),(2,5),(5,2)\} \pmod 9$, in which case $\Delta \equiv 6 \pmod 9$.

We precisely will show that if $(p,q) \equiv (2,2) \pmod 3$ and $\Delta \neq 0$, then

$$\text{if } p+q \equiv 4 \pmod 9,\ \text{then } u_{n+3^k} \equiv u_n + 2\cdot 3^k \pmod{3^{k+1}}; \tag{6}$$
$$\text{if } p+q \equiv 1 \pmod 9,\ \text{then } u_{n+3^k} \equiv u_n + 3^k \pmod{3^{k+1}}; \tag{7}$$
$$\text{if } p+q \equiv 7 \pmod 9,\ \text{then } u_{n+3^k} \equiv u_n \pmod{3^{k+1}}. \tag{8}$$

From this we can conclude that $\mathcal{D}_{\mathbf{u(p,q)}}(3^k) = 3^k$ if and only if $(p,q) \equiv (2,2) \pmod 3$ and $p+q \not\equiv 7 \pmod 9$. We notice that if $\Delta = 0$, then $p^2 = -4q^2$, and so $\pmod 9$ the only possibilities with $(p,q) \equiv (2,2) \pmod 3$ are $(p,q) \equiv (5,5) \pmod 9$, $(p,q) \equiv (2,8) \pmod 9$ or $(p,q) \equiv (8,2) \pmod 9$. Since $p+q \not\equiv 7 \pmod 9$ for these pairs (p,q), the claim it's true also for $\Delta = 0$.

We have to deal with

$$v_n \frac{3^{k-1}(3^k-1)(3^k-2)}{2} p^{3^k-3}\Delta$$

and we will prove that in the first case it is equal to $2^{3^k}3^k \pmod{3^{k+1}}$, in the second case equal to $0 \pmod{3^{k+1}}$ and in the third case equal to $2^{3^k+1}3^k \pmod{3^{k+1}}$, this will complete the proof. In general, we have

$$v_n \frac{3^{k-1}(3^k-1)(3^k-2)}{2} p^{3^k-3}\Delta \equiv v_n 3^{k-1} p^{3^k-3}\Delta \pmod{3^{k+1}}.$$

In the first case, since $\Delta \equiv 3 \pmod 9$, then $\Delta = 3 + 9d$ for some d, thus we claim that

$$v_n 3^k p^{3^k-3}(1+3d) \equiv 2^{3^k} 3^k \pmod{3^{k+1}}.$$

This is true since $v_n p^{3^k-3}(1+3d) \equiv 2^{3^k} \pmod 3$ and we can multiply both sides by 3^k. In the second case, since $\Delta \equiv 0 \pmod 9$, we can write $\Delta = 9d$ and see that

$$v_n 3^{k+1} p^{3^k-3} d \equiv 0 \pmod{3^{k+1}}.$$

For the third case, since $\Delta \equiv 6 \pmod 9$, we have $\Delta = 6 + 9d$ and therefore we claim that

$$v_n 3^k p^{3^k-3}(2+3d) \equiv -2^{3^k} 3^k \pmod{3^{k+1}}.$$

This is true since $v_n p^{3^k-3}(2+3d) \equiv -2^{3^k} \pmod 3$ and we can multiply both sides by 3^k. The converse can be shown numerically. $\square$

Now we are in the position to prove Theorems 2 and 3.

Proof of Theorem 2 and of Theorem 3. Suppose $R > 5$ or $R = 3$ with $p + q \not\equiv 7 \pmod 9$. Write w_n as a shifted Lucas sequence, $w_n = au_n + bu_{n+1}$, where u_n is the Lucas sequence $\mathbf{u}(\mathbf{p}, \mathbf{q})$. We find $b = w_0$, $a = w_1 - pw_0$. Then, if $R > 5$ or $R = 3$ with $p + q \equiv 1 \pmod 9$, by (5) and (7) we obtain

$$\begin{aligned} w_{n+R^k} &\equiv au_{n+R^k} + bu_{n+1+R^k} \equiv a(u_n + R^k) + b(u_{n+1} + R^k) \\ &\equiv (au_n + bu_{n+1}) + (a+b)R^k \equiv w_n + (a+b)R^k \pmod{R^{k+1}} \end{aligned}$$

for $k \geq 1$. We can conclude since $a + b \equiv w_1 - w_0 \not\equiv 0 \pmod R$. If $R = 3$ and $p + q \equiv 4 \pmod 9$ it is similar. $\square$

Acknowledgement. The author is grateful to Pieter Moree for his revision and his suggestions. Moreover, the author thanks the reviewers for their valuable comments

References

[1] A. De Clercq, F. Luca, L. Martirosyan, M. Matthis, P. Moree, M. A. Stoumen, and M. Weiß, Binary recurrences for which powers of two are discriminating moduli, *J. Integer Seq.* **23** (11) (2020).

[2] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.