ON THE LEAST SIGNIFICANT p–ADIC DIGITS OF CERTAIN LUCAS NUMBERS

Tamás Lengyel
Department of Mathematics, Occidental College, Los Angeles, California
lengyel@oxy.edu

Received: 6/13/13, Accepted: 2/4/14, Published: 3/7/14

Abstract

We calculate the least significant p-ary digits of certain Lucas numbers $V_n = V_n(P,Q)$ with $V_0 = 2$, $V_1 = P$ and $V_n = PV_{n-1} - QV_{n-2}$ for $n \geq 2$. We base our study on an observation regarding these numbers: as m increases, more and more p-adic digits match in V_{kp^m} with integer $k \geq 1$. We use multisection identities for generating functions and derive congruences for the underlying sequences.

1. Introduction

Let n and k be positive integers, and p be a prime, and let $\nu_p(k)$ denote the highest power of p dividing k, i.e., the p-adic order of k.

The sequences $U_n = U_n(P,Q)$ with $U_0 = 0$, $U_1 = 1$ and $U_n = PU_{n-1} - QU_{n-2}$ and $V_n = V_n(P,Q)$ with $V_0 = 2$, $V_1 = P$ and $V_n = PV_{n-1} - QV_{n-2}$ for $n \geq 2$ are called Lucas (or Lucas and companion Lucas, respectively) sequences associated with the pair (P,Q) (cf. [7]), with U_n and V_n considered the generalization of the original Fibonacci and Lucas sequences, i.e., $F_n = U(1,-1)$ and $L_n = V(1,-1)$, respectively. Usually, we use the short notations U_n and V_n except if explicitly specifying the parameters might be helpful. The corresponding generating functions are

$$U(x) = \sum_{n=0}^{\infty} U_n x^n = \frac{x}{1 - Px + Qx^2}$$

and

$$V(x) = \sum_{n=0}^{\infty} V_n x^n = \frac{2 - Px}{1 - Px + Qx^2}.$$

We define the characteristic polynomial $x^2 - Px + Q = 0$ associated with the Lucas sequences U_n and $V_n, n \geq 0$. Its discriminant is $D = D(P,Q) = P^2 - 4Q$. If $p \geq 3$ and $p \nmid PQD$ then we define the function $\psi(p) = \psi(p,P,Q) = p - \left(\frac{D}{p}\right)$ where

$\left(\frac{D}{p}\right)$ is the Legendre symbol (cf. [7]), i.e., it is 1 if D is a quadratic residue modulo p and -1 otherwise. We define the rank of apparition (or Fibonacci entry point or restricted or fundamental period modulo n) $\rho(n) = \rho(n, P, Q)$ of integer $n \geq 2$ for the Lucas sequence $U_k(P, Q), k \geq 0$: if there exists $m \geq 1$ such that n divides U_m then $\rho(n)$ is the smallest such m (cf. [7]). Since $Q = -1$, by observation (IV.19) in [7] we know that $\rho(p)$ exists for every odd prime p. The same applies to $p = 2$ by fact (IV.18) in [7] and all prime powers by fact (IV.20), i.e., $\rho(p^e)$ exists for any integer $e \geq 1$. The determination of the exact power of $\nu_p(F_{\rho(p^e)})$ is discussed in [3] and that of $\nu_p(U_{\rho(p^e)}(P, Q))$ in terms of $\nu_p(U_{\rho(p)}(P, Q))$ follows by (IV.20). By (IV.29) we also know that

$$n \mid U_m \text{ if and only if } \rho(n) \mid m. \tag{1.1}$$

We define the modulo p period (cf. [2]) or Pisano period modulo p, $\pi(p) = \pi(p, P, Q)$, as the smallest m so that $U_{n+m}(P, Q) \equiv U_n(P, Q) \pmod{p}$ for every $n \geq 0$. It is known that $\rho(p) \mid \pi(p)$.

We will use a basic relation among the members of a Lucas sequence

$$V_{2n} = V_n^2 - 2Q^n. \tag{1.2}$$

We also rely on fact (IV.10) in [7], which provides the identity

$$2^{n-1}V_n = P^n + \binom{n}{2}P^{n-2}D + \binom{n}{4}P^{n-4}D^2 + \dots \tag{1.3}$$

and its companion identity

$$2^{n-1}U_n = \binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \dots. \tag{1.4}$$

Our main goal is to prove that as m increases, more and more p-adic digits match in V_{kp^m} for different integers $k \geq 1$, and establish the rate at which these digits match. Similar investigations have been done for the Stirling numbers of the second kind in [4] and [5], and Motzkin numbers in [6]. In Section 2 we state the main Theorems 4, 5, 7, and 10. Their proofs are included in Section 3.

2. Main Results

In [8], an application of p-Honda sequences is mentioned in Section 3.4. It can be summarized as follows.

Proposition 1 (Beukers). *Let M be a $d \times d$ matrix with integer coefficients. Define $a_n = \mathrm{Tr}(M^n)$ and*

$$Z_{(p)} = \{a/b : \ a \in \mathbb{Z}, 0 \neq b \in \mathbb{N}, \text{ and } b \text{ prime to } p\}.$$

Then for any prime p, the sequence $a_n, n \geq 1$, is a p-Honda sequence with

$$a_m \equiv a_{m/p} \pmod{m\mathbb{Z}_{(p)}} \text{ if } p \mid m. \tag{2.1}$$

Corollary 2. *The Lucas sequence*

$$L_0 = 2, L_1 = 1, L_{n+1} = L_n + L_{n-1} \ (n \geq 1),$$

is a p-Honda sequence for any prime p.

We can easily extend this result and its proof (cf. [8]) for the general Lucas sequence $V_n(P, Q), n \geq 0$.

Corollary 3. *The Lucas sequence $V_n(P, Q)$ with*

$$V_0 = 2, V_1 = P, V_{n+1} = PV_n - QV_{n-1} \ (n \geq 1),$$

is a p-Honda sequence for any prime p.

The following theorem follows by Corollary 3 and congruence (2.1) after setting $m = kp^{n+1}$.

Theorem 4. *For integers $n \geq 0$ and $k \geq 1$, we have that*

$$\nu_p(V_{kp^{n+1}}(P, Q) - V_{kp^n}(P, Q)) \geq n + 1.$$

The main goal of this paper is to find cases with $Q = -1$ when Theorem 4 can be strengthened and the exact order $\nu_p(V_{kp^{n+1}}(P, -1) - V_{kp^n}(P, -1))$ and its congruential form can be determined. The results in this direction are summarized in Theorems 5 and 10, which deal with the p-adic orders and high power modulus congruences of the differences, in particular for $p = 2$. Theorem 10 extends Theorem 5 from $k = 1$ to other values and presents the cases in their congruential forms. We combine their proofs in Section 3.

Theorem 5. *For the Lucas sequence $V_k = V_k(P, -1), k \geq 0$, we set $r_m(p) = \nu_p(V_{p^{m+1}} - V_{p^m})$, $e_m(p) = \nu_p(U_p(V_{p^{m+1}}, -1))$ and $e_m(2) = \nu_2(U_2(V_{2^{m+1}}, 1)$. Let $D = P^2 + 4$ be the discriminant of the sequence.*

For $p \geq 3$ odd and $m \geq 0$ we get

$$\frac{V_{kp^{m+1}} - V_{kp^m}}{V_{p^{m+1}} - V_{p^m}} \equiv kU_k(V_{p^{m+1}}(P, -1), -1) \bmod p^{r_m(p)}, \tag{2.2}$$

while for $p = 2$ and $m \geq 1$ we get

$$\frac{V_{k2^{m+1}} - V_{k2^m}}{V_{2^{m+1}} - V_{2^m}} \equiv kU_k(V_{2^{m+1}}(P, -1), 1) \bmod 2^{r_m(2)}. \tag{2.3}$$

For any prime $p \geq 2$, if $p \nmid D$ then $e_m(p) = 0$ for all integers $m \geq 0$. In this case, if $p \geq 3$ then

$$\nu_p(V_{p^{m+1}} - V_{p^n}) = m - 1 + \nu_p(V_{p^2} - V_p), \text{ for } m \geq 1, \tag{2.4}$$

and if $p \mid P$ holds too then

$$\nu_p(V_{p^{m+1}} - V_{p^m}) = m + \nu_p(P);$$

while if $p = 2$ then

$$\nu_2(V_{2^{m+1}} - V_{2^m}) = m - 1 + \nu_2(V_4 - V_2) = m + 1, \text{ for } m \geq 1. \tag{2.5}$$

If $p \geq 3$ is an odd prime and $p \mid D$ then $e_m(p) = 1$ for all $m \geq 0$. If $m \geq 1$ then

$$r_m(p) > 2 = 1 + e_m(p), \tag{2.6}$$

thus $2r_m(p) > r_m(p) + 1 + e_m(p) = r_m(p) + 2$, and

$$\nu_p(V_{p^{m+1}} - V_{p^m}) = 2(m-1) + \nu_p(V_{p^2} - V_p). \tag{2.7}$$

If $p = 2$ and $2 \mid D$, i.e., $2 \mid P$, then $e_m(2) = 1$ for all $m \geq 0$. If $m \geq 2$ then $r_m(2) > 2$, and

$$\nu_2(V_{2^{m+1}} - V_{2^m}) = 2(m-2) + \nu_2(V_8 - V_4) = 2(m - 1 + \nu_2(P)) + \chi_{4\nmid P}. \tag{2.8}$$

Remark 6. In Theorem 5 we need the smallest m that guarantees

$$r_m(p) > 1 + e_m(p) \tag{2.9}$$

and thus, the applicability of (2.2) and (2.3) with $k = p$. By Theorem 4, we immediately get that $r_2(p) \geq 3$, hence, $m \geq 2$ will be sufficiently large in Theorem 5, however, if $p \nmid D$ then $r_1(p) \geq 2 > 1 + e_1(p) = 1$ and $m = 1$ suffices. If $p \mid D$ then we have two cases. If $p = 2$ then it is easy to find examples when the smallest m is 2, e.g., if $P = 2$. However, we could not find any such case when $p \geq 3$, and in fact, $m = 1$ is sufficiently large. It turns out that if $p^2 \mid D = P^2 + 4$ then $r_0(p) \geq 2$, which makes $r_1(p) \geq 4 > 1 + e_1(p)$. It also appears that if we replace $p^2 \mid D$ with $p \mid D$ and even if $r_0(p) = \nu_p(V_p - V_1) = 1$, these assumptions already imply that $r_1(p) = \nu_p(V_{p^2} - V_p) \geq 3 > 1 + e_1(p)$. Thus, clearly $m = 1$ is sufficient in (2.7) of Theorem 5 as stated in Theorem 7.

Theorem 7. *With the notation of Theorem 5, if $p \geq 3$ and $p^2 \mid D$ then $r_0(p) \geq 2$ and $r_1(p) \geq 4 > 1 + e_1(p)$. If $p \mid D$ then $r_1(p) \geq 3 > 1 + e_1(p) = 2$. On the other hand, if $p \nmid D$ then $r_1(p) \geq 2 > 1 + e_1(p) = 1$. In each case, $m = 1$ is sufficiently large in Theorem 5. If $p = 2$ then $m = 2$ is required exactly if $\nu_2(P) = 1$.*

Remark 8. According to Theorem 5, if $p = 2$ or $p \geq 3$ with $p \mid P$ then the p-adic orders can be determined without calculating any value of the Lucas sequence.

Remark 9. There are two frequently occurring cases. If $r_0(p) = \nu_p(V_p - V_1) = 1$ and $e_0(p) = \nu_p(U_p(V_p, -1)) = 0$ then (2.4) implies that

$$\nu_p(V_{p^{n+1}} - V_{p^n}) = n + 1, \text{ for } n \geq 0 \tag{2.10}$$

with $r_0(p) = 1$ taking care of the case $n = 0$.

If $r_1(p) = \nu_p(V_{p^2} - V_p) = 3$ (cf. Theorem 7), and $e_1(p) = \nu_p(U_p(V_{p^2}, -1)) = 1$ then the inequality (2.6) is satisfied, and (2.7) implies that

$$\nu_p(V_{p^{n+1}} - V_{p^n}) = 2n + 1, \text{ for } n \geq 1. \tag{2.11}$$

Example 1. With $P = 1$ (and $Q = -1$) we work with the original Lucas and Fibonacci sequences. If $p = 5$ then $\rho(5) = 5$, and we get that $r_0(5) = 1$, $r_1(5) = 3$, $e_0(5) = e_1(5) = 1$, and $\nu_5(V_{5^{n+1}} - V_{5^n}) = 2n + 1$ for $n \geq 0$, in fact, it follows by (2.11) for $n \geq 1$ and by $r_0(5) = 1$ for $n = 0$.

Theorem 10. *With the notations of Theorem 5, for $k \geq 1$ we get the following congruences and consequently, the appropriate p-adic orders.*

If $p \geq 3$ and $p \mid D$ then with $m \geq 1$, we have that

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} k^2 2^{1-k \pmod{p-1}} P^{k-1} p^{2m-2}(V_{p^2} - V_p) & \mod p^{2m-1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1, \\ p^{2m}(V_{p^2} - V_p) & \mod p^{2m+1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } k = p, \end{cases}$$

with the convention that $0 \leq a \pmod{b} < b$.

If $p \geq 3$, $p \nmid D$, and $p \nmid P$ then for $m \geq 1$, we get that

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} p^{m-1}(V_{p^2} - V_p) k U_k(V_{p^{m+1}}, -1) \left(\frac{D}{p}\right)^{m-1} & \mod p^{m+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1 \text{ and} \\ & \gcd(k, \psi(p, V_{p^{m+1}}, -1)) = 1, \\ p^m(V_{p^2} - V_p) \left(\frac{D}{p}\right)^m & \mod p^{m+1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } k = p. \end{cases}$$

If $p \geq 3$, $p \nmid D$, and $p \mid P$ then for $m \geq 1$, we have that

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} p^{m-1}(V_{p^2} - V_p) k U_k(V_{p^{m+1}}, -1) & \mod p^{m+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1 \text{ and } k \text{ odd}, \\ p^m(V_{p^2} - V_p) & \mod p^{m+1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } k = p. \end{cases}$$

If $p = 2$ and $p \mid D$, i.e., $p \mid P$, then with $k \geq 1$ odd and $m \geq s \geq 2$, we have that

$$V_{k2^{m+1}} - V_{k2^m} \equiv 2^{2(m-s)}(V_{2^{s+1}} - V_{2^s})kU_k(V_{2^{m+1}}, 1) \mod 2^{2(m-s-1+r_s(2))}.$$

If $p = 2$, $p \nmid D$, and $\gcd(k, 6) = 1$ then for $m \geq s \geq 1$, we get

$$V_{k2^{m+1}} - V_{k2^m} \equiv (-2)^{m-s}(V_{2^{s+1}} - V_{2^s})kU_k(V_{2^{m+1}}, 1) \mod 2^{m+s+1}.$$

Remark 11. In the congruences of Theorem 10, the difference between the p-adic order of the right-hand side quantity and that of the modulus is 1 for $p \geq 3$, $r_s(2) - 2 = 2s - 4 + 2\nu_2(P) + \chi_{4\nmid P} \geq 2s - 1 \geq 3$ if $p = 2 \mid P$ (by (3.21)), and $s \geq 1$ if $p = 2 \nmid P$.

3. Proofs

Proof of Corollary 3. We apply Proposition 1 to the matrix $M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$. The characteristic polynomial of M is $x^2 - Px + Q$, hence $M^2 - PM + Q = 0$ by the Hamilton–Cayley theorem. We deduce $M^{n+2} = PM^{n+1} - QM^n$ $(n \geq 0)$. Since $\mathrm{Tr}(M^0) = \mathrm{Tr}(I_2) = 2$ and $\mathrm{Tr}(M) = P$, this proves that $V_n = \mathrm{Tr}(M^n)$ is the mentioned Lucas sequence. □

In the proofs of the main theorems we need some auxiliary results. The first result is due to Lehmer, cf. Theorem 1.6 in [1]. We need only its version stated as part of the facts (IV.20) and (IV.7) in [7].

Theorem 12. *Let $e \geq 1$, and let p^e be the exact power of p dividing U_k. If $p \nmid r$ and $f \geq 0$ then p^{e+f} divides U_{krp^f}. Moreover, if $p \nmid Q$ and $p^e \neq 2$, then p^{e+f} is the exact power of p dividing U_{krp^f}.*

From now on we focus on the cases with $Q = -1$ only (although a subcase with $p = 2$ will require the use of U_k with $Q = 1$).

Theorem 13. *If P is odd and k is an odd multiple of 3 then we have that $\nu_2\left(U_k(V_{2^{m+1}}(P, -1), 1)\right) = m + 3$, for all $m \geq 0$.*

If P is odd then $U_2(V_{2^{m+1}}(P, -1), 1) = V_{2^{m+1}}(P, -1) \equiv -1 \pmod{2^{m+2}}$ for all $m \geq 0$, while if P is even then $\nu_2\left(U_2(V_{2^{m+1}}(P, -1), 1) - 2\right) = \nu_2\left(V_{2^{m+1}}(P, -1) - 2\right) = 2(m - 1 + \nu_2(P)) + \nu_2(V_2(P, -1) + 2) \geq 2(m + \nu_2(P))$ for all $m \geq 1$, and thus, $U_2(V_{2^{m+1}}(P, -1), 1) \equiv 2 \pmod{2^{2(m+\nu_2(P))}}$ for all $m \geq 0$.

For an odd prime p, if $p \mid P$, $k \geq 2$ even, and $\gcd(k, p) = 1$ then we have that $\nu_p\left(U_k(V_{p^{m+1}}(P, -1), -1)\right) = m + 1 + \nu_p(P)$, for all $m \geq 0$.

Proof of Theorem 13. For any odd P and with $V_k = V_k(P, -1)$, we get that $V_2^2 - 1 = (P^2 + 2)^2 - 1 \equiv 8 \mod 16$, and thus, $\nu_2(V_2^2 - 1) = 3$. By induction we can prove

that $\nu_2(V_{2^{m+1}}^2-1)=m+3$ for any $m\geq 0$. In fact, we just demonstrated the case with $m=0$. For the inductive step with $m\geq 0$, we use identity (1.2):

$$V_{2^{m+2}}^2-1=(V_{2^{m+1}}^2-2)^2-1=(V_{2^{m+1}}^2-1)(V_{2^{m+1}}^2-3),$$

hence, $\nu_2(V_{2^{m+2}}^2-1)=m+4$ by the inductive hypothesis.

We note that $U_3(P,1)=P^2-1$. Since $U_3(V_{2^{m+1}},1)=V_{2^{m+1}}^2-1$, it now follows that $\nu_2(U_3(V_{2^{m+1}},1))=\nu_2(V_{2^{m+1}}^2-1)=m+3>1$, and by Theorem 12 we derive that $\nu_2(U_{3r}(V_{2^{m+1}},1))=m+3$ for $p\nmid r$.

Similarly to the above steps, we can also prove that $\nu_2(V_{2^{m+1}}+1)=m+2$ with $V_k=V_k(P,-1)$ for any $m\geq 0$ and odd P by induction. We have $\nu_2(V_2+1)=2$ for $m=0$ since with $V_1=P=4k\pm 1$ we get that $V_2+1=P^2+3\equiv 4 \pmod 8$. For the inductive step with $m\geq 0$, we use identity (1.2) again: $V_{2^{m+2}}+1=(V_{2^{m+1}}^2-2)+1=V_{2^{m+1}}^2-1$, and since $\nu_2(V_{2^{m+1}}^2-1)=m+3$ as we have just seen it, we obtain that $\nu_2(V_{2^{m+2}}+1)=m+3$; hence, $V_{2^{m+2}}\equiv -1 \pmod{2^{m+3}}$. On the other hand, if P is even then we prove that $\nu_2\left(U_2(V_{2^{m+1}}(P,-1),1)-2\right)=\nu_2\left(V_{2^{m+1}}(P,-1)-2\right)=2(m-1+\nu_2(P))+\nu_2(V_2(P,-1)+2)\geq 2(m+\nu_2(P))$ for $m\geq 1$, and thus, $U_2(V_{2^{m+1}}(P,-1),1)\equiv 2 \pmod{2^{2(m+\nu_2(P))}}$ by induction on $m\geq 0$. Indeed, $\nu_2(P)\geq 1$ and $V_2=P^2+2\equiv 2 \pmod{2^{2\nu_2(P)}}$ when $m=0$, and by identity (1.2) we have for $m\geq 0$ that

$$V_{2^{m+2}}-2=(V_{2^{m+1}}^2-2)-2=(V_{2^{m+1}}-2)(V_{2^{m+1}}+2),$$

hence, by the case $m=0$ and the inductive hypothesis, $\nu_2(V_{2^{m+2}}-2)=2(m+\nu_2(P))+\nu_2(V_2(P,-1)+2)\geq 2(m+1+\nu_2(P))$.

For an odd prime p with $p\mid P$, $\gcd(k,p)=1$, and $k\geq 2$ even, we first observe that (1.3) implies that $\nu_p(V_{p^{m+1}})=m+1+\nu_p(P)$ for all $m\geq 0$. By (IV.19) in [7] we know that $p\mid U_k(V_{p^{m+1}},-1)$ exactly if k is even. Moreover, by Theorem 12, we also know that $\nu_p(U_k(V_{p^{m+1}},-1))=\nu_p(U_2(V_{p^{m+1}},-1))=m+1+\nu_p(P)$ as long as $\gcd(k,p)=1$, since $U_2(V_{p^{m+1}},-1)=V_{p^{m+1}}$. □

Now we present the combined proof of Theorems 5 and 10.

Proof of Theorems 5 and 10. We will prove the congruences (2.2) and (2.3) that in turn, will imply the identities (2.4), (2.5), (2.7), (2.8), and the congruences in Theorem 10.

We need some preparation. First we observe that with $U_k=U_k(P,-1)$

$$\sum_{n=1}^{\infty}nU_nx^n=xU'(x)=x\frac{(1-Px-x^2)-x(-P-2x)}{(1-Px-x^2)^2}=\frac{x(1+x^2)}{(1-Px-x^2)^2}. \quad (3.1)$$

By a multisection identity [2], we get that with $V_k=V_k(P,-1)$

$$\sum_{k=0}^{\infty}V_{kn}x^k=\frac{2-V_nx}{1-V_nx+(-1)^nx^2}. \quad (3.2)$$

Now we assume that $p \geq 3$ and n is odd. By (3.2), we get that

$$\sum_{k=0}^{\infty} V_{kn} x^k = \frac{2 - V_n x}{1 - V_n x - x^2}.$$

We apply this with $n = p^{m+1}$ and $n = p^m$ and, after normalizing by the factor $V_{p^{m+1}} - V_{p^m}$, we derive for the normalized difference that

$$\begin{aligned} W_m(x) = \sum_{k=0}^{\infty} \frac{V_{kp^{m+1}} - V_{kp^m}}{V_{p^{m+1}} - V_{p^m}} x^k &= \frac{1}{V_{p^{m+1}} - V_{p^m}} \left(\frac{2 - V_{p^{m+1}} x}{1 - V_{p^{m+1}} x - x^2} - \frac{2 - V_{p^m} x}{1 - V_{p^m} x - x^2} \right) \\ &= \frac{x + x^3}{(1 - V_{p^{m+1}} x - x^2)(1 - V_{p^m} x - x^2)}. \end{aligned}$$

It implies that

$$W_m(x) = \frac{x(1+x^2)}{(1 - V_{p^{m+1}} x - x^2)^2} \tag{3.3}$$

$$- \left(\frac{x(1+x^2)}{(1 - V_{p^{m+1}} x - x^2)^2} - \frac{x(1+x^2)}{(1 - V_{p^{m+1}} x - x^2)(1 - V_{p^m} x - x^2)} \right). \tag{3.4}$$

The term on the right-hand side of (3.3) corresponds to the generating function $\sum_{k=0}^{\infty} k U_k(V_{p^{m+1}}, -1) x^k$ by identity (3.1), while the other terms, i.e., those in (3.4), contribute

$$\begin{aligned} &- x(1+x^2) \frac{(1 - V_{p^m} x - x^2) - (1 - V_{p^{m+1}} x - x^2)}{(1 - V_{p^{m+1}} x - x^2)^2 (1 - V_{p^m} x - x^2)} \\ &= -x^2(1+x^2)(V_{p^{m+1}} - V_{p^m}) \frac{1}{(1 - V_{p^{m+1}} x - x^2)^2 (1 - V_{p^m} x - x^2)} \end{aligned}$$

with terms that are multiples of $V_{p^{m+1}} - V_{p^m}$ with p-adic order of at least $\nu_p(V_{p^{m+1}} - V_{p^m})$. Thus, by (3.3) and (3.4) we obtain (2.2).

The case with $p = 2$ is slightly different. We need the corresponding generating function for $U_k = U_k(P, 1)$ (rather than for $U_k(P, -1)$)

$$U(x) = \sum_{n=0}^{\infty} U_n x^n = \frac{x}{1 - Px + x^2}$$

and thus,

$$\sum_{n=1}^{\infty} n U_n x^n = x U'(x) = x \frac{(1 - Px + x^2) - x(-P + 2x)}{(1 - Px + x^2)^2} = \frac{x(1 - x^2)}{(1 - Px + x^2)^2}. \tag{3.5}$$

Also, the multisection identity (3.2) yields that

$$\sum_{k=0}^{\infty} V_{kn} x^k = \frac{2 - V_n x}{1 - V_n x + x^2}$$

with $V_k = V_k(P,-1)$ and n even. We apply this with $n = 2^{m+1}$ and $n = 2^m, m \geq 1$, and, after normalizing by the factor $V_{2^{m+1}} - V_{2^m}$, we derive for the normalized difference that

$$W_m(x) = \sum_{k=0}^{\infty} \frac{V_{k2^{m+1}} - V_{k2^m}}{V_{2^{m+1}} - V_{2^m}} x^k = \frac{1}{V_{2^{m+1}} - V_{2^m}} \left(\frac{2 - V_{2^{m+1}} x}{1 - V_{2^{m+1}} x + x^2} - \frac{2 - V_{2^m} x}{1 - V_{2^m} x + x^2} \right) \tag{3.6}$$

$$= \frac{x - x^3}{(1 - V_{2^{m+1}} x + x^2)(1 - V_{2^m} x + x^2)}.$$

Note that this is the reason for requiring $m \geq 1$ in Theorems 5 and 10 if $p = 2$. Identity (3.6) implies that

$$W_m(x) = \frac{x(1-x^2)}{(1 - V_{2^{m+1}} x + x^2)^2} \tag{3.7}$$

$$- \left(\frac{x(1-x^2)}{(1 - V_{2^{m+1}} x + x^2)^2} - \frac{x(1-x^2)}{(1 - V_{2^{m+1}} x + x^2)(1 - V_{2^m} x + x^2)} \right). \tag{3.8}$$

The term on the right-hand side of (3.7) corresponds to the generating function $\sum_{k=0}^{\infty} k U_k(V_{2^{m+1}}, 1) x^k$ by identity (3.5), while the other terms, i.e., those in (3.8), contribute

$$- x(1-x^2) \frac{(1 - V_{2^m} x + x^2) - (1 - V_{2^{m+1}} x + x^2)}{(1 - V_{2^{m+1}} x + x^2)^2 (1 - V_{2^m} x + x^2)}$$

$$= -x^2(1-x^2)(V_{2^{m+1}} - V_{2^m}) \frac{1}{(1 - V_{2^{m+1}} x + x^2)^2 (1 - V_{2^m} x + x^2)}$$

with terms that are multiples of $V_{2^{m+1}} - V_{2^m}$ with 2-adic order of at least $\nu_2(V_{2^{m+1}} - V_{2^m})$. Thus, by (3.7) and (3.8), we obtain (2.3).

We are ready for the actual proof and start with the case when p is an odd prime. Recall that we use the notation $V_k = V_k(P,-1)$. The basic idea is to prove that

$$V_{p^m} \equiv P \bmod p \quad \text{for } m \geq 0. \tag{3.9}$$

To see this, we apply identity (1.3) modulo p with the setting $n = p^m$ and observe that $\binom{p^m}{i} \equiv 0 \pmod{p}$ for $m \geq 1$ and $1 \leq i \leq p^m - 1$. It follows that

$$D' = D(V_{p^{m+1}}, -1) = V_{p^{m+1}}^2 + 4 \equiv P^2 + 4 = D(P,-1) \mod p, \tag{3.10}$$

and therefore,

$$p \mid D \text{ if and only if } p \mid D'. \tag{3.11}$$

Note that the companion identity (1.4) taken modulo p implies (cf. fact (IV.13) in [7]) that for an odd prime p

$$U_p \equiv \left(\frac{D}{p} \right) \bmod p. \tag{3.12}$$

After these preparatory steps, we proceed with the proofs in three cases.

Case 1: ($p \mid D$, p odd prime). First we assume that $p \mid D = D(P,-1)$. Note that in this case $p \geq 5$ since clearly, $D = P^2 + 4 \not\equiv 0 \pmod 3$. The proof is by induction on $m \geq 1$. We set $k = p$ in (2.2). If $m = 1$ then the statement follows by inequality (2.6), which holds by Theorem 7. Here we also use identity (1.4), now for $U_n(P', -1)$

$$2^{n-1}U_n = \binom{n}{1}(P')^{n-1} + \binom{n}{3}(P')^{n-3}D' + \binom{n}{5}(P')^{n-5}(D')^2 + \dots \tag{3.13}$$

taken modulo p^2, with $n = p$, $P' = V_{p^{m+1}} \equiv P \pmod p$ (by (3.9)), and $p \mid D'$. Indeed, we obtain that

$$2^{p-1}U_p = \binom{p}{1}(P')^{p-1} + \binom{p}{3}(P')^{p-3}D' + \binom{p}{5}(P')^{p-5}(D')^2 + \dots + \binom{p}{p}(D')^{\frac{p-1}{2}}$$

and

$$U_p(V_{p^{m+1}}, -1) \equiv pP^{p-1} \equiv p \mod p^2$$

since $\binom{p}{3}D', \binom{p}{5}(D')^2, \dots, \binom{p}{p}(D')^{\frac{p-1}{2}}$ is divisible by p^2 for every prime $p \geq 5$ and $m \geq 0$; thus, $e_m(p) = \nu_p(U_p(V_{p^{m+1}}, -1)) = 1$ for $p \mid D$ implies $p \nmid P$. Theorem 7 yields (2.6) with $m = 1$. Since $r_{m+1}(p) > r_m(p)$, the inequality (2.6) remains true for all $m \geq 2$. If (2.7) holds with $m \geq 1$ then the above argument also guarantees that it holds for $m + 1$, too. Note that we get that

$$pU_p(V_{p^{m+1}}, -1) \equiv p^2 \mod p^3 \tag{3.14}$$

and similarly, for $\gcd(k, p) = 1$ and with $n = k$ in (3.13), we also obtain on the right-hand side of (2.2) that for $m \geq 0$

$$kU_k(V_{p^{m+1}}, -1) \equiv k^2 2^{1-k \pmod{p-1}} P^{k-1} \mod p.$$

Hence, for $m \geq 1$,

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} k^2 2^{1-k \pmod{p-1}} P^{k-1} p^{2m-2}(V_{p^2} - V_p) & \mod p^{2m-1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1, \\ p^{2m}(V_{p^2} - V_p) & \mod p^{2m+1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } k = p, \end{cases}$$

and $\nu_p\left(V_{kp^{m+1}} - V_{kp^m}\right) = 2m - 2 + \nu_p(V_{p^2} - V_p)$ if $\gcd(k, p) = 1$.

Case 2: ($p \nmid D$, p odd prime). On the other hand, $p \nmid D = D(P,-1)$ implies that $p \nmid U_p(V_{p^{m+1}}, -1)$. By (3.11) it follows that $p \nmid D' = D(V_{p^{m+1}}, -1)$.

Case 2.1: $(p \nmid P)$. If $p \nmid P$ and thus, $p \nmid P' = V_{p^{m+1}}$ by (3.9), then by $p \nmid P'QD'$ and $\rho(p, V_{p^{m+1}}, -1) \mid \psi(p, V_{p^{m+1}}, -1) = p - \left(\frac{D'}{p}\right)$, we get that $\gcd(p, \rho(p, V_{p^{m+1}}, -1)) = 1$, which yields that $p \nmid U_p(V_{p^{m+1}}, -1)$ by (1.1). In fact,

$$U_p(V_{p^{m+1}}, -1) \equiv \left(\frac{D'}{p}\right) \mod p \tag{3.15}$$

by (3.12), hence $e_m(p) = 0$ for $m \geq 0$ and $r_m(p) \geq 2 > 1 + e_m(p)$, i.e., inequality (2.9) holds for all $m \geq 1$. We note that for $m \geq 0$ we get that $\left(\frac{D'}{p}\right) = \left(\frac{D}{p}\right)$ by (3.10), too. In general, the congruences become more complicated if $p \nmid D$. For instance, we get that for $m \geq 1$

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} p^{m-1}(V_{p^2} - V_p) k U_k(V_{p^{m+1}}, -1) \left(\frac{D}{p}\right)^{m-1} & \mod p^{m+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1 \text{ and} \\ & \gcd(k, \psi(p, V_{p^{m+1}}, -1)) = 1, \\ p^m (V_{p^2} - V_p) \left(\frac{D}{p}\right)^m & \mod p^{m+1+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } k = p. \end{cases}$$

In fact, a little more can be said. If besides $\gcd(k,p) = 1$ we have $\rho(p, V_{p^{m+1}}, -1) \nmid k$ then the first congruence applies. On the other hand, if $\rho(p, V_{p^{m+1}}, -1) \mid k$ then $\nu_p(U_k(V_{p^{m+1}}, -1))$ seems to be increasing as m grows (and the fact that it is non-decreasing for any even k follows by (1.4) and the first congruence with $k = 1$). Now we derive only the lower bound $\nu_p(V_{kp^{m+1}} - V_{kp^m}) \geq m - 1 + \nu_p(V_{p^2} - V_p)$, although it can be improved to $\nu_p(V_{kp^{m+1}} - V_{kp^m}) \geq 2m + a$ with some constant a if $\nu_p(U_k(V_{p^{m+1}}, -1))$ increases as m increases. Note, however, that checking a condition that involves the rank of apparition is more difficult than establishing $\gcd(k, \psi(p, V_{p^{m+1}}, -1)) = 1$.

Case 2.2: $(p \mid P)$. If $p \mid P$ and therefore, $p \mid V_{p^{m+1}} = P'$ by (3.9) and $D' \equiv 4 \pmod p$, which implies that $\left(\frac{D'}{p}\right) = 1$ for $m \geq 0$. Then, by fact (IV.19) in [7], we get that $p \mid U_k(V_{p^{m+1}}, -1)$ exactly if k is even, hence $p \nmid U_p(V_{p^{m+1}}, -1)$. Note that $U_p(V_{p^{m+1}}, -1) \equiv \left(\frac{D'}{p}\right) \equiv 1 \pmod p$ by (3.12). In both cases, we have $e_m(p) = 0$ for all $m \geq 0$, and the result follows by the congruence (2.2) with $k = p$. In this case, for $m \geq 1$ we obtain

$$V_{kp^{m+1}} - V_{kp^m} \equiv \begin{cases} p^{m-1}(V_{p^2} - V_p) k U_k(V_{p^{m+1}}, -1) & \mod p^{m+\nu_p(V_{p^2}-V_p)}, \\ & \text{if } \gcd(k,p) = 1 \text{ and } k \text{ odd}, \\ p^m (V_{p^2} - V_p) & \mod p^{m+1+\nu_k(V_{p^2}-V_p)}, \\ & \text{if } k = p. \end{cases}$$

If $\gcd(k,p) = 1$ and k even, we get the lower bound $\nu_p(V_{kp^{m+1}} - V_{kp^m}) \geq 2(m - 1 + \nu_p(V_{p^2} - V_p)) = 2(m + \nu_p(P))$ by Remark 16.

Case 3: $(p = 2)$. If $p = 2$ then, with a little extra work and Theorem 13, we can improve the congruences by increasing the exponent of the powers in the modulus. We have two cases.

Case 3.1: $(2 \mid P)$. If $2 \mid P$ then $V_{2^{m+1}} \equiv V_{2^m} \equiv \cdots \equiv V_2 = P^2 - 2Q \equiv 2 \mod 4$ by repeated applications of the recurrence (1.2). It follows that $U_2(V_{2^{m+1}}, 1) = V_{2^{m+1}} \equiv 2 \mod 4$ which yields that $e_m(2) = \nu_2(U_2(V_{2^{m+1}}, 1)) = 1$ for all $m \geq 0$. Note that (2.9) is satisfied for $m \geq 2$ since $r_m(2) \geq 3$. Let $k \geq 1$ be an odd integer, then for $m \geq 2$ we also get by (2.3) and $U_k \equiv k \pmod 2$ (cf. fact (IV.18) in [7]) that

$$\nu_2(V_{k2^{m+1}} - V_{k2^m}) = 2m - 4 + \nu_2(V_8 - V_4) = 2(m - 1 + \nu_2(P)) + \chi_{4\nmid P}.$$

In the last equation we use $r_2(2) = \nu_2(V_8 - V_4)$ as it is given in (3.21). In order to obtain useful 2-adic congruences, we increase the exponent in the power of 2 in the modulus of (2.3). With $m \geq s \geq 2$ and by repeated applications of (2.3) with $k = 2$ and Theorem 13, we obtain that

$$V_{k2^{m+1}} - V_{k2^m} \equiv 2^{2(m-s)}(V_{2^{s+1}} - V_{2^s})kU_k(V_{2^{m+1}}, 1) \mod 2^{2(m-s-1+r_s(2))}.$$

This guarantees a difference of $r_s(2) - 2 = 2s - 4 + 2\nu_2(P) + \chi_{4\nmid P} \geq 2s - 1 \geq 3$ by (3.21) in the exponents of the powers of 2 in the modulus and the right-hand side quantity.

Case 3.2: $(2 \nmid P)$. If $2 \nmid P$ then $2 \nmid D$ and $V_{2^{m+1}} \equiv V_{2^m} \equiv \cdots \equiv V_1 = P \equiv 1 \pmod 2$ by (1.2) as above. We get that $U_2(V_{2^{m+1}}, 1) = V_{2^{m+1}} \equiv 1 \pmod 2$ and $e_m(2) = \nu_2(U_2(V_{2^{m+1}}, 1)) = 0$ for all $m \geq 0$. By setting $k = 2$, the repeated application of the congruence (2.3) yields the result (2.5). As in the case with $p \geq 3$, the inequality (2.9) is true for $m \geq 1$. Note that $r_1(2) = 2$ by (3.20). In addition, by the congruence (2.3) it also follows that for any odd k which is not a multiple of 3 and $m \geq 1$ that $\nu_2(V_{k2^{m+1}} - V_{k2^m}) = m - 1 + \nu_2(V_4 - V_2)$ and therefore, $\nu_2(V_{k2^{m+1}} - V_{k2^m}) = m + 1$ by (3.20) (cf. proof of Theorem 7) since if $P = 4k \pm 1$ then $\nu_2(3 + P^2) = 2$. Yet again, we increase the exponent in the power of 2 in the modulus and get useful 2-adic congruences by setting $m \geq s \geq 1$ and applying congruence (2.3) with $k = 2$ and Theorem 13. For any k such that $\gcd(k, 6) = 1$, we get that

$$V_{k2^{m+1}} - V_{k2^m} \equiv (-2)^{m-s}(V_{2^{s+1}} - V_{2^s})kU_k(V_{2^{m+1}}, 1) \mod 2^{m+s+1},$$

which guarantees a difference of $s \geq 1$ in the exponents of the powers of 2 in the modulus and the right-hand side quantity.

In fact, U_k is even exactly if k is a multiple of 3 by fact (IV.18) in [7]. However, in this case $\nu_2(U_k(V_{2^{m+1}}, 1)) = m + 3$ by Theorem 13, while $r_m(2) = m + 1$, and thus, we get only the lower bound $\nu_2(V_{k2^{m+1}} - V_{k2^m}) \geq 2(m + 1)$ for $m \geq 1$ by (2.3) and similarly to the above derivations. Although, numerical evidence seems to support the conjecture that equality holds. □

Remark 14. In some cases, the above calculations contain a factor U_k modulo a high prime power with a large index k. The periodicity of the sequence might make it easier to determine these factors.

We note that an alternative derivation of some part of the Case 3 of Theorem 5 follows by the following lemma which is of independent interest.

Lemma 15. *If $a > b \geq 1$ are integers and $V_k = V_k(P, -1)$, then $V_{4a} - V_{4b}$ is divisible by $V_{2a} - V_{2b}$. In fact,*

$$\frac{V_{4a} - V_{4b}}{V_{2a} - V_{2b}} = V_{2a} + V_{2b},$$

and in the special case using $a = k2^m$ and $b = k2^{m-1}$ with $m \geq 1$ and $k \geq 1$ integers, we have that

$$\frac{V_{k2^{m+2}} - V_{k2^{m+1}}}{V_{k2^{m+1}} - V_{k2^m}} = (V_{k2^m} - 1)(V_{k2^m} + 2). \tag{3.16}$$

Proof of Lemma 15. We use identity (1.2) and derive that $V_{4a} - V_{4b} = (V_{2a}^2 - 2) - (V_{2b}^2 - 2) = (V_{2a} - V_{2b})(V_{2a} + V_{2b})$. Furthermore, in the mentioned special case, we have that $V_{k2^{m+1}} + V_{k2^m} = (V_{k2^m}^2 - 2) + V_{k2^m} = (V_{k2^m} - 1)(V_{k2^m} + 2)$. □

We use (3.16) in its equivalent form

$$V_{k2^{m+2}} - V_{k2^{m+1}} = (V_{k2^{m+1}} - V_{k2^m})(V_{k2^m} - 1)(V_{k2^m} + 2), \tag{3.17}$$

which suggests a recurrence for the 2-adic order of $V_{k2^{m+2}} - V_{k2^{m+1}}$ after the 2-adic orders of the last two factors on the right-hand side are determined. For instance, the Case 3.1 can be treated as follows. If $p = 2$, P even, and $k \geq 1$ odd, then we set $g_{4k} = \nu_2(V_{4k} - 2)$ and get that $g_{4k} = \nu_2(V_{2k}^2 - 4) = \nu_2((V_{2k} - 2)(V_{2k} + 2)) \geq 3$. Identity (1.2) implies that

$$\begin{aligned} V_{k2^{m+2}} - 2 = V_{k2^{m+1}}^2 - 4 &= (V_{k2^{m+1}} - 2)(V_{k2^{m+1}} + 2) \\ &= (V_{k2^m} - 2)(V_{k2^m} + 2)(V_{k2^{m+1}} + 2) = \dots \\ &= (V_{4k} - 2) \prod_{i=2}^{m+1} (V_{k2^i} + 2), \end{aligned}$$

and thus, $\nu_2(V_{k2^{m+2}} - 2) \geq g_{4k} \geq 3$ for $m \geq 0$. It follows that $\nu_2(V_{k2^{m+2}} + 2) = 2$ and $\nu_2(V_{k2^{m+2}} - 1) = 0$. By repeated applications of (3.17), we get that $\nu_2(V_{k2^{m+2}} - V_{k2^{m+1}}) = 2(m-1) + \nu_2(V_{8k} - V_{4k})$ which completes the proof of (2.8) with $k = 1$. (We note that for any odd $k \geq 1$, $\nu_2(V_{8k} - V_{4k}) = \nu_2(V_8 - V_4)$ is guaranteed by Theorem 5.)

We conclude with the proof of Theorem 7.

Proof of Theorem 7. We start with the case of odd primes. By the application of (1.3), it follows that $V_p - V_1 \equiv P\left((2^{p-1}P)^{p-1} - 1\right) \bmod p^2$. Since $p^2 \mid D = P^2 + 4$ implies that $P^2 \equiv -4 \mod p^2$, we derive

$$(2^{2(p-1)}P^2)^{\frac{p-1}{2}} - 1 \equiv (-1)^{\frac{p-1}{2}} 2^{p(p-1)} - 1 \equiv 0 \bmod p^2.$$

Note that $P^2 \equiv -4 \mod p^2$ (or for that matter, already $P^2 \equiv -4 \mod p$) yields that -4 is a quadratic residue modulo p, however, $\left(\frac{-4}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{-1}{p}\right) = 1$ only if $p \equiv 1 \bmod 4$. Hence, $r_0(p) = \nu_p(V_p - V_1) \geq 2$ and by the congruences (2.2) and (3.14), we have that $r_1(p) \geq \min\{1 + e_0(p) + r_0(p), 2r_0(p)\} \geq 4 > 1 + e_1(p)$.

Now we are ready to do the harder problem when we have only $p \mid D$. We use (1.3) modulo p^3 with $n = p$ and $n = p^2$, and get that

$$2^{p-1}V_p \equiv P^p + \binom{p}{2} P^{p-2} D \bmod p^3 \quad \text{and} \quad 2^{p^2-1}V_{p^2} \equiv P^{p^2} \bmod p^3. \tag{3.18}$$

After some manipulations (in fact, after moving the powers of 2 to the right-hand sides, then subtracting the former congruence from the latter one, and factoring out $2^{p^3-2p^2+1}P^{p-2}$), we get that in order to prove that $r_1(p) = \nu_p(V_{p^2} - V_p) \geq 3$ we need that

$$P^2\left(P^{p(p-1)} - 2^{p(p-1)}\right) - 2^{p(p-1)} p \frac{p-1}{2} D \equiv 0 \mod p^3. \tag{3.19}$$

Now we write $P^{p-1} = 2^{p-1} + \left(P^{p-1} - 2^{p-1}\right)$, and thus,

$$\begin{aligned} P^{p(p-1)} - 2^{p(p-1)} &= \left(2^{p-1} + \left(P^{p-1} - 2^{p-1}\right)\right)^p - 2^{p(p-1)} \\ &\equiv 2^{(p-1)^2} p \left(P^{p-1} - 2^{p-1}\right) \mod p^3. \end{aligned}$$

We will use the congruences $2^{p(p-1)} \equiv 1 \mod p^2$ and $2^{(p-1)^2} \equiv 1 \mod p$, and derive that, since $p \mid D$ and $p \equiv 1 \mod 4$,

$$P^{p-1} = P^{2\frac{p-1}{2}} = (-4 + D)^{\frac{p-1}{2}} \equiv (-4)^{\frac{p-1}{2}} + (-4)^{\frac{p-3}{2}} \frac{p-1}{2} D \mod p^2,$$

hence, since $p \mid D$,

$$2^{(p-1)^2}\left(P^{p-1} - 2^{p-1}\right) \equiv -2^{p-3} \frac{p-1}{2} D \equiv -\frac{p-1}{8} D \mod p^2.$$

On the left-hand side of congruence (3.19) it follows that

$$-P^2 p \frac{p-1}{8} D - p \frac{p-1}{2} D = -p \frac{p-1}{8} D(P^2 + 4) = -p \frac{p-1}{8} D^2 \equiv 0 \mod p^3.$$

If $p \nmid D$ then by Theorem 5, for all $m \geq 1$, we have $r_m(p) \geq 2 > 1 + e_m(p)$ since $e_m(p) = 0$ by (3.15).

If $p = 2$ then easy calculation shows that

$$V_4 - V_2 = P^2(3 + P^2). \tag{3.20}$$

If $2 \nmid P$ then since $e_m(2) = 0$ for $m \geq 0$ by Theorem 5, we derive that $r_1(2) = \nu_2(V_4 - V_2) = 2 > 1 + e_1(2)$ and $m = 1$ suffices.

If $2 \mid P$ then $e_m(2) = 1$ for $m \geq 0$, and $m = 2$ is necessary exactly if $r_1(2) = 2$, which happens exactly if $\nu_2(P) = 1$ by (3.20). In fact, we can determine that

$$r_2(2) = 2\nu_2(P) + 2 + \chi_{4\nmid P} \geq 5 \tag{3.21}$$

since $V_8 - V_4 = P^2(1 + P^2)(3 + P^2)(4 + P^2)$. □

Remark 16. We note that if for some odd prime p we have $p \nmid D$ and $p \mid P$, then $\left(\frac{D'}{p}\right) = 1$ by the arguments in the proof of Theorem 5, and in a similar fashion to the derivation of (3.18) from (1.3), we obtain that $V_{p^2} - V_p \equiv -2^{p^3-p^2-p+1}pP \pmod{p^3}$. Therefore, $r_1(p) = \nu_p(V_{p^2} - V_p) = 2$ if $\nu_p(P) = 1$ and $r_1(p) = \nu_p(V_{p^2} - V_p) \geq 3$, otherwise, and it gives the minimum $m = 1$ or 0 so that $r_m(p) > 1+e_m(p)$. Similarly, if $\nu_p(P) = 2$ then $r_1(p) = 3$ also follows. In fact, in general, Theorem 13 yields that $r_1(p) = \nu_p(P) + 1$ by setting $k = 2$ with $m = 0$ and 1. Note that in order to have a unified approach in Theorems 5 and 10, we didn't separate the cases with $m = 0$ and 1.

Acknowledgment. The author wishes to thank Gregory P. Tollisen for his helpful comments.

References

[1] D. H. Lehmer, An extended theory of Lucas functions, Ann. of Math. **31** (1930), 419–448.

[2] T. Lengyel, Divisibility properties by multisection, Fibonacci Quart. **41** (2003), 72–79.

[3] T. Lengyel, The order of the Fibonacci and Lucas numbers, Fibonacci Quart. **33** (1995), 234–239.

[4] T. Lengyel, On the 2-adic order of Stirling numbers of the second kind and their differences, 21st International Conference on Power Series and Algebraic Combinatorics (FPSAC 2009), Hagenberg, Austria, Discrete Math. Theor. Comput. Sci. Proceedings **AK**, 561–572, 2009. Downloadable from: `http://www.dmtcs.org/dmtcs-ojs/index.php/proceedings/article/view/dmAK0147/`.

[5] T. Lengyel, On the least significant 2-adic and ternary digits of certain Stirling numbers, INTEGERS **13** (2013), A13:47, 1–10.

[6] T. Lengyel, Exact p-adic orders for differences of Motzkin numbers, Int. J. Number Theory, accepted.

[7] P. Ribenboim, The new book of prime number records, Springer, 3rd edition, 1996.

[8] A. M. Robert, A course in p-adic analysis, Graduate texts in mathematics 198, Springer, 2010.