The p-adic Valuation of the Lucas Sequences

Aram Tangboonduangjit

MUIC

February 6, 2019

Outline

1. Abstract
2. p-adic Valuation of the Fibonacci Numbers
3. p-adic Valuation of the Lucas Sequences
4. Application

Outline

1. Abstract
2. p-adic Valuation of the Fibonacci Numbers
3. p-adic Valuation of the Lucas Sequences
4. Application

Abstract

For relatively prime integers P and Q, the Lucas sequence $(U_n)_{n\geq 0} = (U_n(P,Q))_{n\geq 0}$ is defined recursively by $U_0 = 0$, $U_1 = 1$, and $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}$ for $n \geq 2$. A recent work by Sanna has revealed an astounding formula for realizing the exponent of a prime in the prime factorization of the Lucas sequence. Sanna's work is a generalization of the work by Lengyel who gave such formula only for the Fibonacci numbers (and the Lucas numbers) which are the quintessential Lucas sequence with $P = 1$ and $Q = -1$. In this talk, I will discuss such formula and give an application which is joint work with Panraksa.

Outline

1. Abstract
2. p-adic Valuation of the Fibonacci Numbers
3. p-adic Valuation of the Lucas Sequences
4. Application

p-adic Valuation

- For a prime p, the p-adic valuation of a natural number n denoted by $\nu_p(n)$ is defined to be the exponent of p in the prime factorization of n, i.e., if $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is a prime factorization of n, then $\nu_{p_i}(n) = \alpha_i$ for $i = 1, \ldots, k$.

p-adic Valuation

- For a prime p, the p-adic valuation of a natural number n denoted by $\nu_p(n)$ is defined to be the exponent of p in the prime factorization of n, i.e., if $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is a prime factorization of n, then $\nu_{p_i}(n) = \alpha_i$ for $i = 1, \ldots, k$.
- For example, $\nu_2(1024) = 10$, $\nu_5(875) = 3$.

Fibonacci Numbers

- $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

Fibonacci Numbers

- $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.
- The first few Fibonacci numbers are:
  $0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \ldots$

5-adic Valuation of the Fibonacci Numbers

Theorem (Lengyel, 1995)

The 5-adic valuation of the Fibonacci numbers F_n is given by

$$\nu_5(F_n) = \nu_5(n).$$

5-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_5(F_{75}) = \nu_5(2111485077978050) =$
  $\nu_5(2 \times 5^2 \times 61 \times 3001 \times 230686501) = 2 = \nu_5(75)$

5-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_5(F_{75}) = \nu_5(2111485077978050) =$
  $\nu_5(2 \times 5^2 \times 61 \times 3001 \times 230686501) = 2 = \nu_5(75)$
- $\nu_5(F_{39}) = \nu_5(63245986) = \nu_5(2 \times 233 \times 135721) = 0 = \nu_5(39)$

Proof

Theorem (Wall, 1960)

For $n \geq 1$,

$$2^{n-1} F_n = \sum_{k \geq 0} \binom{n}{2k+1} 5^k.$$

Proof

Theorem (Wall, 1960)

For $n \geq 1$,

$$2^{n-1}F_n = \sum_{k\geq 0} \binom{n}{2k+1} 5^k.$$

Observe that

$$\begin{aligned}\nu_5\left[\binom{n}{2k+1}5^k\right] &= \nu_5(n) - \nu_5(2k+1) + \nu_5\left[\binom{n-1}{2k}5^k\right] \\ &\geq \nu_5(n) - \nu_5(2k+1) + k > \nu_5(n),\end{aligned}$$

except for $k = 0$ when

$$\nu_5\left[\binom{n}{2k+1}5^k\right] = \nu_5(n).$$

Proof

Theorem (Wall, 1960)

For $n \geq 1$,

$$2^{n-1} F_n = \sum_{k \geq 0} \binom{n}{2k+1} 5^k.$$

Observe that

$$\begin{aligned} \nu_5 \left[\binom{n}{2k+1} 5^k \right] &= \nu_5(n) - \nu_5(2k+1) + \nu_5 \left[\binom{n-1}{2k} 5^k \right] \\ &\geq \nu_5(n) - \nu_5(2k+1) + k > \nu_5(n), \end{aligned}$$

except for $k = 0$ when

$$\nu_5 \left[\binom{n}{2k+1} 5^k \right] = \nu_5(n).$$

Hence, by Wall's theorem, $\nu_5(F_n) = \nu_5(n)$.

2-adic Valuation of the Fibonacci Numbers

Theorem (Lengyel, 1995)

The 2-adic valuation of the Fibonacci numbers F_n is given by

$$\nu_2(F_n) = \begin{cases} 0, & \text{if } n \equiv 1, 2 \pmod 3, \\ 1, & \text{if } n \equiv 3 \pmod 6, \\ 3, & \text{if } n \equiv 6 \pmod{12}, \\ \nu_2(n) + 2, & \text{if } n \equiv 0 \pmod{12}. \end{cases}$$

2-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_2(F_{35}) = \nu_2(9227465) = 0$

2-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_2(F_{35}) = \nu_2(9227465) = 0$
- $\nu_2(F_{39}) = \nu_2(63245986) = \nu_2(2 \times 233 \times 135721) = 1$

2-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_2(F_{35}) = \nu_2(9227465) = 0$
- $\nu_2(F_{39}) = \nu_2(63245986) = \nu_2(2 \times 233 \times 135721) = 1$
- $\nu_2(F_{42}) = \nu_2(267914296) = \nu_2(2^3 \times 13 \times 29 \times 211 \times 421) = 3$

2-adic Valuation of the Fibonacci Numbers

For example,

- $\nu_2(F_{35}) = \nu_2(9227465) = 0$
- $\nu_2(F_{39}) = \nu_2(63245986) = \nu_2(2 \times 233 \times 135721) = 1$
- $\nu_2(F_{42}) = \nu_2(267914296) = \nu_2(2^3 \times 13 \times 29 \times 211 \times 421) = 3$
- $\nu_2(F_{48}) = \nu_2(4807526976) = \nu_2(2^6 \times 3^2 \times 7 \times 23 \times 47 \times 1103) = 6 = 4 + 2 = \nu_2(48) + 2$

Proof

Lemma (Jacobson, 1992)

(A) *Let* $k \geq 5$ *and* $s \geq 1$. *Then* $F_{2^{k-3}3s} \equiv s2^{k-1} \pmod{2^k}$.
(B) *Let* $k \geq 5$ *and* $n \geq 0$ *and assume that* $n \equiv 0 \pmod 6$. *Then* $F_{n+2^{k-3}3} \equiv F_n + 2^{k-1} \pmod{2^k}$.
(C) *Let* $n \geq 0$ *and assume that* $n \equiv 3 \pmod 6$. *Then* $F_n \equiv 2 \pmod{32}$.

- **Case 1** $n \equiv 1, 2 \pmod 3$. A well-known divisibility property states that F_m is divisible by F_n if and only if either m is divisible by n, or $n = 2$. Consequently, $F_n \equiv 1 \pmod 2$ or

$$\boxed{\nu_2(F_n) = 0.}$$

Proof

Lemma (Jacobson, 1992)

(A) *Let* $k \geq 5$ *and* $s \geq 1$. *Then* $F_{2^{k-3}3s} \equiv s2^{k-1} \pmod{2^k}$.
(B) *Let* $k \geq 5$ *and* $n \geq 0$ *and assume that* $n \equiv 0 \pmod 6$. *Then* $F_{n+2^{k-3}3} \equiv F_n + 2^{k-1} \pmod{2^k}$.
(C) *Let* $n \geq 0$ *and assume that* $n \equiv 3 \pmod 6$. *Then* $F_n \equiv 2 \pmod{32}$.

- **Case 1** $n \equiv 1, 2 \pmod 3$. A well-known divisibility property states that F_m is divisible by F_n if and only if either m is divisible by n, or $n = 2$. Consequently, $F_n \equiv 1 \pmod 2$ or

$$\boxed{\nu_2(F_n) = 0.}$$

- **Case 2** $n \equiv 0 \pmod 3$. Then $F_n \equiv 0 \pmod 2$ or $\nu_2(F_n) \geq 1$.

Proof

Lemma (Jacobson, 1992)

(A) *Let* $k \geq 5$ *and* $s \geq 1$. *Then* $F_{2^{k-3}3s} \equiv s2^{k-1} \pmod{2^k}$.
(B) *Let* $k \geq 5$ *and* $n \geq 0$ *and assume that* $n \equiv 0 \pmod 6$. *Then* $F_{n+2^{k-3}3} \equiv F_n + 2^{k-1} \pmod{2^k}$.
(C) *Let* $n \geq 0$ *and assume that* $n \equiv 3 \pmod 6$. *Then* $F_n \equiv 2 \pmod{32}$.

- **Case 1** $n \equiv 1, 2 \pmod 3$. A well-known divisibility property states that F_m is divisible by F_n if and only if either m is divisible by n, or $n = 2$. Consequently, $F_n \equiv 1 \pmod 2$ or

$$\boxed{\nu_2(F_n) = 0.}$$

- **Case 2** $n \equiv 0 \pmod 3$. Then $F_n \equiv 0 \pmod 2$ or $\nu_2(F_n) \geq 1$.
- **Case 2.1** $n \equiv 1 \pmod 2$. Then $n \equiv 3 \pmod 6$. By Lemma C, we have $F_n \equiv 2 \pmod{32}$ so that $F_n = 2(2^4k + 1)$ for some integer k. Hence

$$\boxed{\nu_2(F_n) = 1.}$$

Proof

- **Case 2.2** $n \equiv 0 \pmod 2$. Then $n \equiv 0 \pmod{12}$ or $n \equiv 6 \pmod{12}$.

Proof

- **Case 2.2** $n \equiv 0 \pmod 2$. Then $n \equiv 0 \pmod{12}$ or $n \equiv 6 \pmod{12}$.
- **Case 2.2.1** $n \equiv 0 \pmod{12}$. Write $n = 12s$ for some integer s. We claim that

$$\boxed{\nu_2(F_{12s}) = \nu_2(s) + 4.}$$

Indeed, write $s = 2^\ell t$ for some $\ell \geq 0$ and t odd. By Lemma A, we have

$$F_{12s} = F_{2^{\ell+2}3t} \equiv t2^{\ell+4} \pmod{2^{\ell+5}},$$

or

$$F_{12s} = 2^{\ell+4}(t + 2r) \quad \text{for some integer } r.$$

Since t is odd, $t + 2r$ is odd, and so $\nu_2(F_{12s}) = \ell + 4 = \nu_2(s) + 4$. Now since $n = 12s$, we have $\nu_2(n) = \nu_2(s) + 2$ and

$$\nu_2(F_n) = \nu_2(s) + 4 = \nu_2(n) - 2 + 4 = \boxed{\nu_2(n) + 2.}$$

Proof

- **Case 2.2.2** $n \equiv 6 \pmod{12}$. By Lemma B (with $k = 5$), we have $F_m = F_{m+12} + 16 \pmod{32}$ for all $m \geq 0$, so that

$$F_6 = 8 \equiv F_{18} + 16 \equiv F_{30} \equiv F_{42} + 16 \equiv \cdots \pmod{32}.$$

That is, $F_{12k+6} \equiv -8, 8 \pmod{32}$ for all $k \geq 0$. Thus, $F_n \equiv -8, 8 \pmod{32}$ or $F_n = 32\ell \pm 8 = 8(4\ell \pm 1)$ for some integer ℓ. Hence

$$\boxed{\nu_2(F_n) = 3.}$$

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Definition

Let $\ell = \ell(m)$ be the first positive index for which $F_\ell \equiv 0 \pmod{m}$.

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Definition

Let $\ell = \ell(m)$ be the first positive index for which $F_\ell \equiv 0 \pmod{m}$.

- Such index $\ell(m)$ is called the rank of apparition (appearance) or Fibonacci entry-point of m.

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Definition

Let $\ell = \ell(m)$ be the first positive index for which $F_\ell \equiv 0 \pmod{m}$.

- Such index $\ell(m)$ is called the rank of apparition (appearance) or Fibonacci entry-point of m.
- Since, from a well-known fact, F_{p-1} or F_p or F_{p+1} is divisible by p for every prime p, it follows that $\ell(p)$ exists for every prime p.

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Theorem (Lengyel, 1995)

For prime $p \neq 2$ and 5, the p-adic valuation of the Fibonacci numbers F_n is given by

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + \nu_p(F_{\ell(p)}), & \text{if } n \equiv 0 \pmod{\ell(p)}, \\ 0, & \text{if } n \not\equiv 0 \pmod{\ell(p)}. \end{cases}$$

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Example

Prove that $11 \mid F_n$ if and only if $10 \mid n$.

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Example

Prove that $11 \mid F_n$ if and only if $10 \mid n$.

- one can check that $F_{10} = 55$ and $\ell(11) = 10$ and so, by the theorem, $\nu_{11}(F_n) = \nu_{11}(n) + \nu_{11}(F_{10}) = \nu_{11}(n) + 1 \geq 1$ if $n \equiv 0 \pmod{10}$ and $\nu_{11}(F_n) = 0$ if $n \not\equiv 0 \pmod{10}$.

p-adic Valuation of the Fibonacci Numbers ($p \neq 2, 5$)

Example

Prove that $11 \mid F_n$ if and only if $10 \mid n$.

- one can check that $F_{10} = 55$ and $\ell(11) = 10$ and so, by the theorem, $\nu_{11}(F_n) = \nu_{11}(n) + \nu_{11}(F_{10}) = \nu_{11}(n) + 1 \geq 1$ if $n \equiv 0 \pmod{10}$ and $\nu_{11}(F_n) = 0$ if $n \not\equiv 0 \pmod{10}$.
- For example, we find $F_{20} = 6765 = 3 \times 5 \times \boxed{11} \times 41$ and $F_{40} = 102334155 = 3 \times 5 \times 7 \times \boxed{11} \times 41 \times 2161$ while $F_{44} = 701408733 = 3 \times 43 \times 89 \times 199 \times 307$ and $F_{59} = 956722026041 = 353 \times 2710260697$.

Outline

1. Abstract
2. p-adic Valuation of the Fibonacci Numbers
3. p-adic Valuation of the Lucas Sequences
4. Application

Lucas Sequences

- For relatively prime integers P and Q, we define the Lucas sequence $(U_n)_{n\geq 0} = (U_n(P,Q))_{n\geq 0}$ by $U_0 = 0$, $U_1 = 1$, and

$$U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}, \quad \text{for } n \geq 2.$$

Lucas Sequences

- For relatively prime integers P and Q, we define the Lucas sequence $(U_n)_{n\geq 0} = (U_n(P,Q))_{n\geq 0}$ by $U_0 = 0$, $U_1 = 1$, and

$$U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}, \quad \text{for } n \geq 2.$$

- Characteristic polynomial of the Lucas sequence $(U_n(P,Q))$ is defined to be $x^2 - Px + Q$ with discriminant Δ.

Lucas Sequences

- For relatively prime integers P and Q, we define the Lucas sequence $(U_n)_{n\geq 0} = (U_n(P,Q))_{n\geq 0}$ by $U_0 = 0$, $U_1 = 1$, and

$$U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}, \quad \text{for } n \geq 2.$$

- Characteristic polynomial of the Lucas sequence $(U_n(P,Q))$ is defined to be $x^2 - Px + Q$ with discriminant Δ.
- If the Lucas sequence is nondegenerate, that is, the ratio of the two roots α and β of the characteristic polynomial is not a root of unity, then

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{\Delta}}.$$

Lucas Sequences

- For relatively prime integers P and Q, we define the Lucas sequence $(U_n)_{n\geq 0} = (U_n(P,Q))_{n\geq 0}$ by $U_0 = 0$, $U_1 = 1$, and

$$U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}, \quad \text{for } n \geq 2.$$

- Characteristic polynomial of the Lucas sequence $(U_n(P,Q))$ is defined to be $x^2 - Px + Q$ with discriminant Δ.
- If the Lucas sequence is nondegenerate, that is, the ratio of the two roots α and β of the characteristic polynomial is not a root of unity, then

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{\Delta}}.$$

- If p is prime such that $p \nmid Q$, then the **rank of apparition** of p in the sequence (U_n), denoted $\tau(p)$, is defined to be the least positive integer such that $p \mid U_{\tau(p)}$.

Examples

- Fibonacci sequence F_n: $U_n(1, -1)$.

Examples

- Fibonacci sequence F_n: $U_n(1, -1)$.
- Mersenne numbers $2^n - 1$: $U_n(3, 2)$.

Examples

- Fibonacci sequence F_n: $U_n(1, -1)$.
- Mersenne numbers $2^n - 1$: $U_n(3, 2)$.
- Fibonacci polynomials: $U_n(x, -1)$.

p-adic Valuation of the Lucas Sequences

Theorem (Sanna, 2016)

If p is a prime number such that $p \nmid Q$, then

$$\nu_p(U_n) = \begin{cases} \nu_p(n) + \nu_p(U_p) - 1, & \text{if } p \mid \Delta,\ p \mid n, \\ 0, & \text{if } p \mid \Delta,\ p \nmid n, \\ \nu_p(n) + \nu_p(U_{p\tau(p)}) - 1, & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \mid n, \\ \nu_p(U_{\tau(p)}), & \text{if } p \nmid \Delta,\ \tau(p) \mid n,\ p \nmid n, \\ 0, & \text{if } p \nmid \Delta,\ \tau(p) \nmid n. \end{cases}$$

Outline

1. Abstract
2. p-adic Valuation of the Fibonacci Numbers
3. p-adic Valuation of the Lucas Sequences
4. Application

Application

- For a Lucas sequence $(U_n(P,Q))_{n\geq 0}$, and for $n \geq 0$, we define the **Lucas iteration sequence** $(G_k(n))_{k\geq 1}$ by $G_1(n) = U_n$ and $G_k(n) = U_{nG_{k-1}(n)}$ for $k \geq 2$.

Application

- For a Lucas sequence $(U_n(P,Q))_{n\geq 0}$, and for $n \geq 0$, we define the **Lucas iteration sequence** $(G_k(n))_{k\geq 1}$ by $G_1(n) = U_n$ and $G_k(n) = U_{nG_{k-1}(n)}$ for $k \geq 2$.

Theorem (Panraksa and T, 2018)

Let $n \geq 1$ and p a prime factor of U_n. Then, for $k \geq 1$,

1. *if (i) p is odd, or (ii) $p = 2$ and $2 \mid \Delta$, or (iii) $p = 2$ and $\nu_2(U_n) \geq 2$, we have*

$$\nu_p(G_k(n)) = k \cdot \nu_p(U_n);$$

2. *if $2 \nmid \Delta$ and $\nu_2(U_n) = 1$, we have*

$$\nu_2(G_k(n)) = (\gamma - 1)k + 2 - \gamma,$$

where $\gamma = \nu_2(U_{2\tau(2)}) = \nu_2(U_6)$.

The End