THE ORDER OF THE FIBONACCI AND LUCAS NUMBERS

T. Lengyel

Occidental College, 1600 Campus Road, Los Angeles, CA 90041

(Submitted October 1993)

1. Introduction

In this paper $\nu_p(r)$ denotes the exponent of the highest power of a prime p which divides r and is referred to as the p-adic order of r. We characterize the p-adic orders $\nu_p(F_n)$ and $\nu_p(L_n)$, i.e., the exponents of a prime p in the prime power decomposition of F_n and L_n, respectively.

The characterization of the divisibility properties of combinatorial quantities has always been a popular area of research. In particular, finding the highest powers of primes which divide these numbers (e.g., factorials, binomial coefficients [14], Stirling numbers ([2], [1], [10], and [9]) has attracted considerable attention. The analysis of the periodicity *modulo* any integer ([3], [11], [14], and [8]) of these numbers helps exploring their divisibility properties (e.g., [9]). The periodic property of the Fibonacci and Lucas numbers has been extensively studied (e.g., [16], [13], [17], and [12]). Here we use some of these properties and methods to find $\nu_p(F_n)$ and $\nu_p(L_n)$. An application of the results to the Stirling numbers of the second kind is discussed at the end of the paper.

We note that Halton [5] obtained similar results on the p-adic order of the Fibonacci numbers, and additional references on earlier developments can be found in Robinson [13] and Vinson [15]. The approach presented here is based on a refined analysis of the periodic structure of the Fibonacci numbers by exploring its properties, in particular, around the points where $F_n \equiv 0 \pmod p$. (The smallest n such that $F_n \equiv 0 \pmod p$ is called the rank of apparition of prime p and is denoted by $n(p)$.) This technique is based on that of Wilcox [17] and provides a simple and self-contained analysis of properties related to divisibility. For instance, we obtain another characterization of the ratio of the period to the rank of apparition [15] in terms of $F_{n(p)-1} \pmod p$ for any prime p.

Knuth and Wilf [7] generalized Kummer's result on the highest power of a prime that divides the binomial coefficient. Kummer proved that the p-adic order of a binomial coefficient $\binom{n}{m}$ is the number of "carries" that occur when the integers m and $n-m$ are added in p-ary notation. Knuth and Wilf extended the use of counting "carries" to a broad class of generalized binomial coefficients which includes the Fibonacci numbers (Theorem 2 in [7]).

Their method is derived for *regularly divisible sequences* [7], however, it can be modified to include the Lucas numbers, too. We note that $L_{2n} = L_n^2 - 2(-1)^n$; therefore, (L_{2n}, L_n) is either 1 or 2 which illustrates that the Lucas numbers are not regularly divisible.

If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime-decomposition of m, then $\nu_m(N) = \min_{1\le i\le k} \lfloor \nu_{p_i}(N)/\alpha_i \rfloor$. Therefore, without loss of generality, we will focus on the characterization of $\nu_p(F_n)$ and $\nu_p(L_n)$ where p is a prime.

2. The 2- and 5-adic orders

It turns out that 5-adic order of the Fibonacci and Lucas numbers can be computed easily. For the Fibonacci numbers we use the well known identity [16]

$$2^{n-1} F_n = \sum_{k=0} \binom{n}{2k+1} 5^k, \quad n \ge 1, \tag{1}$$

and obtain

Lemma 1. For all $n \ge 0$ we have $\nu_5(F_n) = \nu_5(n)$. On the other hand, L_n is not divisible by 5 for any n.

Proof of Lemma 1. Observe that $\nu_5\left(\binom{n}{2k+1}5^k\right) = \nu_5(n) - \nu_5(2k+1) + \nu_5\left(\binom{n-1}{2k}5^k\right) \ge \nu_5(n) - \nu_5(2k+1) + k > \nu_5(n)$, except for $k = 0$ when $\nu_5\left(\binom{n}{2k+1}5^k\right) = \nu_5(n)$. Identity (1) implies $\nu_5(F_n) = \nu_5(n)$.

For the Lucas numbers the period of the sequence $\{L_n \bmod 5\}$ is 4 with the cycle $\{1,3,4,2\}$; therefore, 5 can never be a divisor of L_n. ∎

In order to derive the 2-adic orders of F_n and L_n, we use congruences proved by Jacobson [6].

Lemma A. (Lemma 2 in [6]) Let $k \ge 5$ and $s \ge 1$. Then $F_{2^{k-3}3s} \equiv s2^{k-1} \pmod{2^k}$.

Lemma B. (Lemma 4 in [6]) Let $k \ge 5$ and $n \ge 0$ and assume $n \equiv 0 \pmod 6$. Then $F_{n+2^{k-3}3} \equiv F_n + 2^{k-1} \pmod{2^k}$.

Lemma C. (Lemma 5 in [6]) Let $n \ge 0$ and assume $n \equiv 3 \pmod 6$. Then $F_n \equiv 2 \pmod{32}$.

We assume that $n \ge 1$ from now on. If $n \equiv 1$ or $2 \pmod 3$, then we know that $F_n \equiv 1 \pmod 2$; thus $\nu_2(F_n) = 0$ for $n \equiv 1,2 \pmod 3$. Lemma A yields $\nu_2(F_{12n}) = \nu_2(n) + 4$. By Lemma C, we get $\nu_2(F_n) = 1$ if $n \equiv 3 \pmod 6$, and Lemma B (in the more convenient form $F_n \equiv F_{n+12} + 16 \pmod{32}$) implies that $F_6 = 8 \equiv F_{18} + 16 \equiv F_{30} \equiv F_{42} + 16 \equiv \cdots \pmod{32}$, and in general, $F_{12n+6} \equiv -8$ or $8 \pmod{32}$; therefore, $\nu_2(F_{12n+6}) = 3$.

Similarly, $L_n \equiv 1 \pmod 2$ for $n \not\equiv 0 \pmod 3$. By the duplication formula $F_{2n} = F_n L_n$, it follows that $\nu_2(L_n) = \nu_2(F_{2n}) - \nu_2(F_n)$. Therefore, $\nu_2(L_{6n+3}) = 2$ and $\nu_2(L_{6n}) = 1$, for it turns out that $\nu_2(L_{12n}) = \nu_2(L_{12n+6}) = 1$.

In summary,

Lemma 2.

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

and

$$\nu_2(L_n) = \begin{cases} 0, & \text{if } n \equiv 1,2 \mod 3, \\ 2, & \text{if } n \equiv 3 \quad \mod 6, \\ 1, & \text{if } n \equiv 0 \quad \mod 6. \end{cases}$$

3. p-adic orders

In this section we assume that p is a prime different from 2 and 5. It is well known that either F_{p-1} or F_{p+1} is divisible by p for every prime p.

Let $n = n(m)$ be the first positive index for which $F_n \equiv 0 \pmod m$. This index is often called the *rank of apparition (appearance)* or *Fibonacci entry-point* of m. The order of p in $F_{n(p)}$ will be denoted by $e = e(p)$, i.e., $e = e(p) = \nu_p(F_{n(p)}) \geq 1$, $F_{n(p)} \equiv 0 \pmod{p^e}$ and $F_{n(p)} \not\equiv 0 \pmod{p^{e+1}}$. In this paper $k(m)$ denotes the period *modulo* m of the Fibonacci series.

We shall need

Theorem A. (Theorem 3 in [16]) The terms for which $F_n \equiv 0 \pmod m$ have subscripts that form a simple arithmetic progression. That is, $n = x \cdot d$ for $x = 0, 1, 2, \ldots,$ and some positive integer $d = d(m)$, gives all n with $F_n \equiv 0 \pmod m$.

Note that $d(m)$ is exactly $n(m)$, and $d(p^i) = d(p) = n(p)$, for all $1 \leq i \leq e(p)$. It also follows that $F_m \not\equiv 0 \pmod p$ unless m is a multiple of $n(p)$. Clearly, $(p, n(p)) = 1$. From now on we will focus on indices of the form $cn(p)p^\alpha$ where $c \geq 1$ and $\alpha \geq 0$ integers, and $(c, p) = 1$.

We prove

Theorem. For $p \neq 2$ and 5,

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + e(p), & \text{if } n \equiv 0 \pmod{n(p)}, \\ 0, & \text{if } n \not\equiv 0 \pmod{n(p)}, \end{cases} \tag{2}$$

and

$$\nu_p(L_n) = \begin{cases} \nu_p(n) + e(p), & \text{if } k(p) \neq 4n(p) \text{ and } n \equiv \frac{n(p)}{2} \pmod{n(p)}, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Proof of the Theorem. The basic idea of the proof is based on the identity [16]

$$F_{an} = 2^{1-a} F_n (K F_n^2 + a L_n^{a-1}), \tag{4}$$

where K is an integer. We set $a = p, \alpha \geq 1$, and $n = cn(p)p^{\alpha-1}$ such that $(c, p) = 1$. Identity (4) and Theorem A imply that

$$F_{cn(p)p^\alpha} = 2^{1-p} F_{cn(p)p^{\alpha-1}} (K' p^2 + p L_{cn(p)p^{\alpha-1}}^{p-1}),$$

with some integer K'; therefore,

$$\nu_p(F_{cn(p)p^\alpha}) = \nu_p(F_{cn(p)p^{\alpha-1}}) + 1,$$

for (F_n, L_n) is either 1 or 2, and inductively,

$$\nu_p(F_{cn(p)p^\alpha}) = \nu_p(F_{cn(p)}) + \alpha. \tag{5}$$

We now prove $\nu_p(F_{cn(p)}) = \nu_p(F_{n(p)})$. The multiplication identity [4]

$$F_{kn} \equiv k F_n F_{n+1}^{k-1} \pmod{F_n^2} \tag{6}$$

yields $F_{cn(p)} \equiv c F_{n(p)} F_{n(p)+1}^{c-1} \pmod{p^{2e}}$ by setting $n = n(p)$, $k = c$, and $e = e(p)$. We show that $(F_{n(p)+1}, p) = 1$ by deriving the congruences

$$F_{n(p)+1}^2 \equiv F_{n(p)-1}^2 \equiv \begin{cases} -1 \bmod p, & \text{if } k(p) = 4n(p), \\ +1 \bmod p, & \text{otherwise,} \end{cases} \tag{7}$$

which prove that $\nu_p(F_{cn(p)}) = \nu_p(F_{n(p)})$, for $(c, p) = 1$, and $\nu_p(F_{n(p)}) = e < 2e$. Identity (5) implies $\nu_p(F_{cn(p)p^\alpha}) = \nu_p(F_{n(p)}) + \alpha = e(p) + \alpha$ and identity (2).

In order to prove identity (7), we set

$$F_{n(p)-1} \equiv x \pmod{p}, \tag{8}$$

and observe that the Fibonacci series around the term $F_{n(p)} \equiv 0 \pmod{p}$ must have the form $\cdots, -8x, 5x, -3x, 2x, -x, x, 0, x, x, 2x, 3x, 5x, 8x, \cdots$. This sequence can be continued backward until we reach the term $F_1 = 1$, i.e., $(-1)^{n(p)} F_{n(p)-1} x \equiv 1 \pmod p$. The forward continuation yields $F_{2n(p)-1} \equiv F_{n(p)-1} x \pmod p$. If $n(p)$ is even then

$$F_{n(p)-1} x \equiv 1 \pmod p \tag{9}$$

and by identity (8), $x^2 \equiv 1 \pmod p$ follows, i.e., $F_{n(p)-1} \equiv x \equiv \pm 1 \pmod p$. On the other hand, $F_{n(p)-1} x \equiv 1 \pmod p$ implies that if $x \equiv 1 \pmod p$ then $k(p) = n(p)$, and $n(p)/2$ is odd (see [17], Theorem 1, case (iv)). It follows that $k(p)$ is not a multiple of 4 thus $p \equiv \pm 1 \pmod{10}$ (see [16], Corollary, p. 529). On the other hand, if $x \equiv -1 \pmod p$ then $F_{n(p)-1} \equiv -1, F_{2n(p)-1} \equiv F_{n(p)-1} x \equiv 1 \pmod p$, therefore, $k(p) = 2n(p)$.

If $n(p)$ is odd then $F_{n(p)-1} x \equiv -1 \pmod p$, and similarly to identity (8) we set

$$F_{2n(p)-1} \equiv y \pmod p$$

and repeat the previous argument by substituting the even $2n(p)$ for $n(p)$ and y for x. Here we have $F_{2n(p)-1} y \equiv 1$ and $y^2 \equiv 1 \pmod p$ with $y \equiv F_{2n(p)-1} \equiv F_{n(p)-1} x \equiv -1 \pmod p$. By identity (8), we obtain that $x^2 \equiv -1 \pmod p$. We know from [16] that $k(p)$ must be even and a multiply of $n(p)$, therefore $k(p) = 4n(p)$ must hold. This case occurs, for example, if p is 13, 17, or 61.

To prove identity (3), we apply the duplication formula $L_n = \frac{F_{2n}}{F_n}$ from which we can easily deduce $\nu_p(L_n)$. We have three cases: either $n \not\equiv 0 \pmod{n(p)}$ and $2n \not\equiv 0 \pmod{n(p)}$, or $n \not\equiv 0 \pmod{n(p)}$ but $2n \equiv 0 \pmod{n(p)}$, or $n \equiv 0 \pmod{n(p)}$.

In the first case, $\nu_p(F_{2n}) = \nu_p(F_n) = 0$ implies that $\nu_p(L_n) = 0$. Similarly, the third case yields $\nu_p(F_{2n}) = \nu_p(F_n) = \nu_p(n) + e(p)$ and $\nu_p(L_n) = 0$. The second case can never happen if $n(p)$ is odd, that is, $k(p) = 4n(p)$. Otherwise, $n = d \cdot \frac{n(p)}{2}$ must hold with some odd integer d; therefore, $\nu_p(F_{2n}) = \nu_p(F_{dn(p)}) = \nu_p(d) + e(p)$ while $\nu_p(F_n) = 0$ for n is not a multiple of $n(p)$. The p-adic order of L_n is now $\nu_p(n) + e(p)$. ∎

In passing, we note that we fully characterized $\frac{k(p)}{n(p)}$ in terms of $x \equiv F_{n(p)-1} \pmod p$ and we found

Lemma 3.

$$\begin{aligned} k(p) &= n(p), \text{ iff } & x &\equiv 1 \bmod p, \\ k(p) &= 2n(p), \text{ iff } & x &\equiv -1 \bmod p, \\ k(p) &= 4n(p), \text{ iff } & x^2 &\equiv -1 \bmod p. \end{aligned}$$

In the first case, p must have the form $10l \pm 1$ while the third case requires that $p = 4l + 1$.

We note that identities (6) and (7) actually imply

Lemma 4. For every even c and p such that $(c,p)=1$,

$$F_{cn(p)} \equiv \begin{cases} (-1)^{\frac{c-2}{2}} cF_{n(p)}F_{n(p)+1} \pmod{p^2}, & \text{if } k(p)=4n(p), \\ cF_{n(p)}F_{n(p)+1} \pmod{p^2}, & \text{otherwise.} \end{cases}$$

For every odd c and p such that $(c,p)=1$,

$$F_{cn(p)} \equiv \begin{cases} (-1)^{\frac{c-1}{2}} cF_{n(p)} \pmod{p^2}, & \text{if } k(p)=4n(p), \\ cF_{n(p)} \pmod{p^2}, & \text{otherwise.} \end{cases}$$

The theorem yields $\nu_p\big(F_{cn(p)p^\alpha}\big) = \alpha+1$ if $e(p)=\nu_p\big(F_{n(p)}\big)=1$. We note that a prime p is called a *primitive prime factor* of F_n if $p|F_n$, but p does not divide any preceding number in the sequence. According to our notation p is a primitive prime factor of $F_{n(p)}$. We can consider the *primitive part* F'_n of F_n for which $F_n = F'_n \cdot F''_n$ such that $(F'_n, F''_n)=1$, and p divides F'_n if and only if p is a primitive prime factor of F_n. If we set $m=n(p)$ then F'_m is square-free exactly if $e(p')=1$ for every primitive prime factor p' of F_m, e.g., for $p'=p$. (Clearly, $m=n(p')$ for all these prime factors.) It appears, however, that saying anything about F'_n being square-free is a difficult problem ([12], p. 49). The interested reader will find a lively discussion on the primitive prime factors of the generalized Lucas sequences in [12].

4. An application

It turns out that the 5-adic analysis of the series F_n and L_n plays a major role in determining $\nu_5(k!S(n,k))$ where $S(n,k)$ denotes the Stirling numbers of the second kind and $n=a\cdot 5^q, k=2b\cdot 5^z, a, b,$ and q are positive integers such that $(a,5)=(b,5)=1$, and $4|a$, while z is a nonnegative integer. For instance, if q is sufficiently large and $z>0$ then we can derive the identities

$$k!\,S(n,k) \equiv -2\cdot 5^{\frac{b}{2}5^z-1} L_{b\cdot 5^z} \pmod{5^{q+1}}, \quad \text{if } b \text{ is even},$$

and

$$k!\,S(n,k) \equiv 2\cdot 5^{\frac{b\cdot 5^z-1}{2}} F_{b\cdot 5^z} \pmod{5^{q+1}}, \quad \text{if } b \text{ is odd}.$$

In general, for even k, we obtain

$$\nu_5(k!\,S(n,k)) = \begin{cases} \frac{k}{4}-1, & \text{if } k\equiv 0,4,8,12,16 \pmod{20}, \\ \frac{k-2}{4}, & \text{if } k\equiv 2,6,14 \pmod{20}, \\ \frac{k-2}{4}+\nu_5(k), & \text{if } k\equiv 10 \pmod{20}, \\ \frac{k-2}{4}+\nu_5(k+2), & \text{if } k\equiv 18 \pmod{20}. \end{cases}$$

Notice that for $n = a \cdot 5^q, 4|a, (a, 5) = 1$, and q sufficiently large, $\nu_5(k!\, S(n,k))$ can depend on n only if k is odd. Actually, it does depend on n if and only if $k/5$ is an odd integer. The proof will appear in a forthcoming paper. We note that the above identities are generalizations of the identity

$$\nu_2(k!S(n,k)) = k - 1,$$

where $n = a \cdot 2^q$, a is odd, and q is sufficiently large (see [9]).

Acknowledgment

The author would like to thank the referee for helpful comments and drawing his attention to a significant reference.

References

1. Clarke, F., *Hensel's lemma and the divisibility by primes of Stirling-like numbers*, preprint, 1993
2. Davis, D. M., *Divisibility by 2 of Stirling-like numbers*, Proceedings of the American Mathematical Society 110(1990), 597-600.
3. Gessel, I., *Congruences for Bell and tangent numbers,* Fibonacci Quarterly 19(1981), 137-144.
4. Graham, R. L., Knuth, D. E., and Patashnik, O., *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1989.
5. Halton, J. H., *On the divisibility properties of Fibonacci numbers*, Fibonacci Quarterly 4(1966), 217-240.
6. Jacobson, E., *Distribution of the Fibonacci numbers* mod 2^k, Fibonacci Quarterly 30(1992), 211-215.
7. Knuth, D. E. and Wilf, H. S., *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. 396(1989), 212-219.
8. Kwong, Y. H. Harris, *Periodicities of a class of infinite integer sequences modulo M*, J. Number Theory 31(1989), 64-79.

9. Lengyel, T., *On the divisibility by 2 of the Stirling numbers of the second kind.* Fibonacci Quarterly 32(1994), 194-201.

10. Lundell, A., *A divisibility property for Stirling numbers*, J. Number Theory 10(1978), 35-54.

11. Nijenhuis, A. and Wilf, H. S., *Periodicities of partition functions and Stirling numbers modulo p*, J. Number Theory 25(1987), 308-312.

12. Ribenboim, P., *The Little Book of Big Primes*, Springer-Verlag, New York–Berlin, 1990.

13. Robinson, D. W., *The Fibonacci matrix modulo m*, Fibonacci Quarterly 1(1963), 29-36.

14. Sved, M., *Divisibility–with visibility*, Math. Intelligencer 10(1988), 56-64.

15. Vinson, J., *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence,* Fibonacci Quarterly 1(1963), 37-45.

16. Wall, D. D., *Fibonacci series modulo m*, Amer. Math. Monthly 67(1960), 525-532.

17. Wilcox, H., *Fibonacci sequences of period n in groups*, Fibonacci Quarterly 24(1986), 356-361.

AMS Classification Numbers: 11B39, 11B50, 11B73