COMPLEX FIBONACCI AND LUCAS NUMBERS, CONTINUED FRACTIONS, AND THE SQUARE ROOT OF THE GOLDEN RATIO

I. J. Good
Virginia Polytechnic Institute & State University, Blacksburg, VA 24061

(Submitted February 1991)

1. INTRODUCTION

The golden ratio $\phi = (\sqrt{5}+1)/2$ is mathematically ancient (see [3] for example), while both ϕ and its square root are of historical architectural significance,[1] and are therefore points of contact between the "two cultures." (Compare the cultural and historical approach to the theory of numbers in [12].) It is pleasing that ϕ and $\sqrt{\phi}$ have a further relationship in terms of continued fractions. The formula

$$(1) \qquad \phi = 1 + \frac{1}{1+}\,\frac{1}{1+}\cdots$$

is very familiar and it will be proved below that

$$(2) \qquad \sqrt{1+2i} = \sqrt{\phi} + i/\sqrt{\phi} = 1 + i + \frac{1}{2+2i+}\;\frac{1}{2+2i+}\;\frac{1}{2+2i+}\cdots$$

where $i = \sqrt{-1}$. A similar result is

$$(3) \qquad \sqrt{1+i/2} = \frac{1}{2}(\sqrt{5}+2)^{1/2} + \frac{1}{2}i(\sqrt{5}-2)^{1/2} = \frac{1}{2}(1+i) + \frac{1}{1+i+}\;\frac{1}{1+i+}\cdots$$

[1] The golden ratio, or as Kepler, following Luca Pacioli [11], called it, the "divine proportion," and also its square root, are related to two of the most famous buildings of all time, the Parthenon at Athens and the Great Pyramid, respectively.

The golden rectangle is exemplified by the face of the Parthenon ([7, pp. 62 and 63]; [13, p. 139]). The Parthenon was built only about half a century after the death of Pythagoras so the choice of ϕ, if it was deliberate, might well have been influenced by the Pythagorean philosophy, for ϕ occurs conspicuously in the theory of the pentagram, which was the badge of the Pythagoreans [7, p. 28].

Reference [4, p. 162], refers to the "perfect phi pyramid" whose square base is 2 by 2 units, the length of the apothem (the segment from the apex to the midpoint of a side of the base) is ϕ, and the height is $\sqrt{\phi}$. Gardner says "Herodotus [the 'father of history'] was the first to suggest (c. 500 B.C.) that the area of the face of the Great Pyramid [of King Khufu (also called Cheops) at al-Jiza (Giza)] is equal to the square of the pyramid's height." This is another way of suggesting that the Great Pyramid is a perfect phi pyramid. But Gardner has now informed me that Fischler (1991), in a forthcoming article, has argued that the source of the alleged interpretation of Herodotus's wording goes back only to 1859. Herodotus's wording was seemingly incorrect. Nevertheless, according to [8] the measurements of the base are, in feet, 755.43, 756.08, 755.08, and 755.77, with an average of 755.59, while the height is 481.4 feet, so the ratio of the height to half the base is close to 1.274, whereas $\sqrt{\phi} =$ 1.2720. The deviation from the perfect phi pyramid is much too small to be discernible by eye and small enough to be due to erosion. The Egyptian architect, two thousand years before Herodotus was born, might well have aimed at a perfect phi pyramid. Maybe the architect's plans will eventually be found entombed with his mummy.

The left sides of (3) can also be expressed as

$$(3a)\qquad \frac{1}{2}\left\{(1+i)\sqrt{\phi}+(1-i)/\sqrt{\phi}\right\}.$$

We will see, in a corollary to Theorem 3, that there is another close relationship between (2) and (3).

Some related "complex Fibonacci and Lucas numbers" will be investigated.[2]

A condensed version of this work was published in [5].

2. PROOFS OF THE CONTINUED FRACTIONS

To prove (1)-(3), and similar results, we can make use of the following special case of a theorem given, for example, by [6, p. 146].

The numerator p_n and denominator q_n of the n^{th} convergent (n = 1, 2, 3, ...) of

$$(4)\qquad A+\frac{1}{A+}\;\frac{1}{A+}\cdots$$

are given by

$$(5)\qquad p_n=F_{n+2},\quad q_n=F_{n+1}$$

where

$$(6)\qquad F_n=(x^n-y^n)/(x-y)$$

and

$$(7)\qquad x=\frac{1}{2}\left(A+\sqrt{A^2+4}\right),\quad y=\frac{1}{2}\left(A-\sqrt{A^2+4}\right),$$

which are the roots of $x^2-Ax-1=0$. Of course $xy=-1$.

Reference [6] assumes that A is an integer. But everything in the (inductive) proof of the theorem in [6] is also applicable if A is any nonzero real or complex number and, in particular, when $A=a+ib$ where a and b are integers, that is, when A is a *Gaussian integer*.

It follows from the theorem that the infinite continued fraction (4) is equal to x if $|x|>|y|$ and to y if $|y|>|x|$. If A is a positive integer, as in (1), then $|x|>|y|$ and the continued fraction converges to x. The convergence is fast when $|y/x|$ is small.

For the sake of simplicity, let us consider the special case where $A=a+ia$ where a is a positive integer. Then

$$(8)\qquad x=\frac{1}{2}\left\{a+ia+\sqrt{4+2ia^2}\right\},\quad y=\frac{1}{2}\left\{a+ia-\sqrt{4+2ia^2}\right\},\quad xy=-1,$$

[2] Complex continued fractions can be used to solve problems in the theory of Gaussian integers similar to those solved for integers by using ordinary continued fractions. For example, one can solve a complex form of Pell's equation at least sometimes. This is shown, among other things, in my Technical Report 91-2 which, however, contains several incomplete proofs and conjectures.

where √ denotes the complex square root with positive real part. By means of de Moivre's theorem (anticipated by Roger Cotes), and some trigonometry, we infer that

$$(9)\qquad \begin{aligned} 2x &= a+ia+\left\{\left(\sqrt{4+a^4}+2\right)^{1/2}+i\left(\sqrt{4+a^4}-2\right)^{1/2}\right\} \\ 2y &= a+ia-\left\{\left(\sqrt{4+a^4}+2\right)^{1/2}+i\left(\sqrt{4+a^4}-2\right)^{1/2}\right\} \end{aligned}$$

(Note the checks that $xy=-1$ and $(x-y)^2=4+2ia^2$.) It is straightforward to show that $|x|>|y|$ by calculating $|2x|^2-|2y|^2$. Therefore,

$$(10)\qquad \frac{1}{2}\left(\sqrt{4+a^4}+2\right)^{1/2}+\frac{i}{2}\left(\sqrt{4+a^4}-2\right)^{1/2}\frac{1}{2}(a+ia)+\frac{1}{a+ia+}\ \frac{1}{a+ia+}\cdots .$$

Equations (2) and (3) are the special cases $a=2$ and $a=1$.

3. COMPLEX AND GAUSSIAN FIBONACCI AND LUCAS NUMBERS

Let us write

$$(11)\qquad F_{\xi,n}=\frac{\xi^n-\eta^n}{\xi-\eta},\quad L_{\xi,n}=\xi^n+\eta^n\quad (\xi\neq\eta,\ \xi\eta=-1)$$

where n is any integer (not necessarily positive) and ξ and η might be complex (in which case we can think of $F_{\xi,n}$ and $L_{\xi,n}$ as *complex Fibonacci and Lucas numbers*). Note that

$$F_{\xi,-n}=(-1)^{n-1}F_{\xi,n},\quad L_{\xi,-n}=(-1)^n L_{\xi,n}.$$

The ordinary Fibonacci and Lucas numbers are $F_n=F_{\phi,n}$, and $L_n=L_{\phi,n}$.

Theorem 1: The sequences $\{F_{\xi,n}\}$ and $\{L_{\xi,n}\}$ $(n=\cdots-2,-1,0,1,2,\ldots)$ satisfy the recurrence relations

$$(12)\qquad F_{\xi,n+1}=(\xi+\eta)F_{\xi,n}+F_{\xi,n-1}$$

and

$$(13)\qquad L_{\xi,n+1}=(\xi+\eta)L_{\xi,n}+L_{\xi,n-1}.$$

The proofs are left to the reader.

Vajda [13, pp. 176-84] lists 117 identities satisfied by the ordinary Fibonacci and Lucas numbers. Most of these identities apply equally to $F_{\xi,n}$ and $L_{\xi,n}$ and can be readily proved straight from the definitions (11).

Theorem 2: A necessary and sufficient condition for $F_{\xi,n}$ and $L_{\xi,n}$ to be Gaussian (or natural) integers for all n is that $\xi+\eta$ should be a Gaussian integer (or a natural integer, respectively).

Proof: That the condition is necessary is obvious because $\xi+\eta=L_{\xi,1}=F_{\xi,2}$. That the condition is also sufficient follows inductively, both for positive and negative n, from the recurrence relations (12) and (13) because $F_{\xi,0}$, $F_{\xi,1}$, $L_{\xi,0}$, and $L_{\xi,1}$ are Gaussian integers, namely, 0, 1, 2, and $\xi+\eta$, respectively, and because the recurrence relations (12) and (13) work backwards as well as forwards.

In this paper we will be mainly concerned with the case in which $\xi+\eta=a+ia$ where a is a positive integer, especially the cases a = 1 and a = 2 with which we began in the Introduction. Then $\xi=x$ and $\eta=y$ where x and y are defined by equations (8) or (9). We write $F_{x,n}=F_n^{(a)}$ and $L_{x,n}=L_n^{(a)}$, but when a is held fixed in some context *we usually abbreviate the notations* to F_n and L_n. We call $F_n^{(a)}$ and $L_n^{(a)}$ *Gaussian* Fibonacci and Lucas numbers. Also we write $F_n=f_n+if_n'$ and $L_n=\ell_n+i\ell'_n$ to show the real and imaginary parts Some numerical values are listed in Tables 1 and 2 for the cases a = 1 and a = 2. These tables can be generated from the recurrence relations

$$(14)\qquad F_0=0,\ F_1=1,\ F_{n+2}=(a+ia)F_{n+1}+F_n$$

and

$$(15)\qquad L_0=2,\ L_1=a+ia,\ L_{n+2}=(a+ia)L_{n+1}+L_n$$

where n is any integer, positive, negative, or zero.

Greater generality would be possible by writing $(a+ib)F_{n+1}+(c+id)F_n$ on the right of (14) where a, b, c, and d are integers [and similarly for (15)], but simplicity is also a virtue, and there is plenty to say about the special case of $F_n^{(a)}$ and $L_n^{(a)}$.

Individual values of F_n and L_n. can be computed from the formulas

$$(16)\qquad F_n=\frac{r^ne^{in\theta-i\psi}-r^{-1}e^{-in(\theta+\pi)-i\psi}}{\sqrt{2}\left(4+a^4\right)^{1/4}},\text{ and } L_n=r^ne^{in\theta}+r^{-n}e^{-in(\theta+\pi)},$$

where

$$2r=\left[(a+\gamma)^2+(a+\delta)^2\right]^{1/2},$$

$$\theta=\arctan\left(\frac{a+\delta}{a+\gamma}\right),\quad \psi=\arctan(\delta/\gamma),$$

where

$$\gamma=(\beta+2)^{1/2},\ \delta=(\beta-2)^{1/2},\ \beta=(4+a^4)^{1/2}.$$

The notations r, θ, ψ, β, γ, δ are provisional and are introduced here only to simplify the printing of the formulas for F_n and L_n. and to make them easier to program. (I used a hand-held calculator, an HP15C.) In spite of the heirarchy of square roots, F_n and L_n. are, of course, Gaussian integers, a fact that acts as an excellent check on computer programs.

The tables can be used for checking and guessing various properties of the Gaussian Fibonacci and Lucas numbers. In this section I give a small selection of the most easily proved properties.

The first few properties resemble formulas (10.14.16)–(10.14.9) of [6] and are almost as easy to prove as in the real case if one holds in mind that xy = −1 and, for (19) and (21), that $(x-y)^2=4+2ia^2$. We have

(17) $2F_{m+n} = F_m L_n + F_n L_m,$

and in particular,

(18) $F_{2n} = F_n L_n;$

(19) $L_n^2 - (4+2ia^2)F_n^2 = (-1)^n 4,$

(20) $F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1},$

(20k) $F_n^2 - F_{n+k}F_{n-k} = (-1)^{n+k} F_k^2,$

(21) $L_n^2 - L_{n-1}L_{n+1} = (-1)^n (4+2ia^2).$

Two similar formulas (see [13, formulas (11) and (17c)]), convenient for "leaping ahead," are

(22) $F_{2n+1} = F_{n+1}^2 + F_n^2$

and

(23) $L_{2n} = L_n^2 + (-1)^{n-1}2.$

A couple of results, corresponding to Theorem 179 of [6], and which readily follow inductively from the recurrence relations (14) and (15), are

(24) $(F_n, F_{n+1}) = 1, \quad (L_n, L_{n-1}) = (2, a),$

meaning, for example, that F_n and F_{n+1} have no common factor other than the units ± 1 and $\pm i$; and, for all r and n,

(25) $F_n | F_{rn}$

(meaning that F_n "divides" F_{rn}). But the proof of (25) given by [6] for ordinary Fibonacci numbers does not extend so easily as for (17)–(24). Instead, the proof in [13, pp. 66 and 67] extends immediately, and has the merit of expressing F_{rn}/F_n explicitly in terms of Lucas numbers, in fact as a linear combination. For example,

(26) $F_{3n}/F_n = L_{2n} + (-1)^n, \quad F_{5n}/F_n = L_{4n} + (-1)^n L_{2n} + 1.$

Several surprising formulas can be obtained by the methods of [1]. For example,

(27) $$\frac{1}{F_1} + \frac{1}{F_2} + \frac{1}{F_4} + \frac{1}{F_8} + \cdots = y + 1 + \frac{2}{a+ia}$$

and

(28) $$\frac{L_1}{F_3} + \frac{L_3}{F_9} + \frac{L_9}{F_{27}} + \cdots = -y.$$

4. A RELATIONSHIP BETWEEN THE SEQUENCES $\{L_n^{(1)}\}$ AND $\{L_n^{(2)}\}$

Theorem 3:

(29) $L_n^{(2)} = i^n \overline{L_{2n}^{(1)}}$ for all n,

where the vinculum indicates complex conjugacy.

Proof: (29) is true when $n = 0$, and when $n = 1$, because

$$L_0^{(2)} = 2 \text{ while } \overline{L_0^{(1)}} = 2$$

$$L_1^{(2)} = 2+2i,\ L_2^{(1)} = (1+i)^2+2 = 2+2i,\ i\,\overline{L_2^{(1)}} = 2+2i = L_1^{(2)}.$$

So an inductive proof will follow if we can show that the sequences $\{L_n^{(2)}\}$ and $\{K_n\}$ satisfy the same recurrence relation, where $K_n = i^n\, \overline{L_{2n}^{(1)}}$ by definition

The recurrence relation satisfied by $L_n^{(2)}$ is, of course,

$$L_{n+1}^{(2)} = (2+2i)L_n^{(2)} + L_{n-1}^{(2)}.$$

To obtain the recurrence relation satisfied by $\{K_n\}$, note first that

$$L_{\xi,m+2} = L_{\xi,2}L_{\xi,m} - L_{\xi,m-2}$$

which follows readily from (11). It is stated in [13, formula (17a)] for ordinary Lucas numbers, but it is equally clear for complex Lucas numbers and, in particular, for Gaussian numbers. On putting $m = 2n$ we get, again in particular,

$$L_{2n+2}^{(1)} = L_2^{(1)}L_{2n}^{(1)} - L_{2n-2}^{(1)} = (2+2i)L_{2n}^{(1)} - L_{2n-2}^{(1)}.$$

Therefore,

$$\overline{L_{2n+2}^{(1)}} = (2-2i)\overline{L_{2n}^{(1)}} - \overline{L_{2n-2}^{(1)}}.$$

Multiply by i^{n+1} to get

$$\begin{aligned} K_{n+1} &= i(2-2i)K_n - i^2K_{n-1} \\ &= (2+2i)K_n + K_{n-1} \end{aligned}$$

so the sequence$\{K_n\}$ does satisfy the same recurrence relation as $\{L_n^{(2)}\}$ as required.

A more direct but slightly messy proof can be obtained from equation (8). Note that $L_n^{(2a)} \neq i^n\, L_{2n}^{(a)}$ unless $a = 1$.

Corollary to Theorem 3:

$$(30)\qquad i\left[1-i+\frac{1}{1-i+}\ \frac{1}{1-i+}\cdots\right]^2 = 2+2i+\frac{1}{2+2i+}\ \frac{1}{2+2i+}\cdots$$

Proof: From the theorem, we have

$$(31)\qquad i\,\overline{L_{2n+2}^{(1)}} \,/\, \overline{L_{2n}^{(1)}} = L_{n+1}^{(2)} \,/\, L_n^{(2)}.$$

Now, in the theorem at the start of Section 2, take $A = 2 + 2i$ [when x is given by (9) with $a = 2$]. Then the continued fraction (4) equals

$$\begin{aligned} \lim_{n\to\infty}(p_n/q_n) &= \lim(x^{n+2}-y^{n+2})/(x^{n+1}-y^{n+1}) = x \text{ (because } |x|>|y|) \\ &= \lim(x^{n+1}+y^{n+1})/(x^n+y^n) = \lim L_{n+1}^{(2)}/L_n^{(2)} \end{aligned}$$

so the right side of (31) tends to that of (30). Again, in (4), take $A = 1 + i$ to find that

$$1+i+\frac{1}{1+i+}\;\frac{1}{1+i+}\cdots=\lim(L_{n+1}^{(1)}/L_n^{(1)})=\lim(L_{n+2}^{(1)}/L_{n+1}^{(1)}).$$

Therefore,

$$\left(1+i+\frac{1}{1+i+}\;\frac{1}{1+i+}\cdots\right)^2=\lim\frac{L_{n+1}^{(1)}}{L_n^{(1)}}\cdot\frac{L_{n+2}^{(1)}}{L_{n+1}^{(1)}}=\lim\frac{L_{n+2}^{(1)}}{L_n^{(1)}}$$

and hence,

$$i\left(1-i+\frac{1}{1+i+}\;\frac{1}{1+i+}\cdots\right)^2=\lim i\,\overline{L_{n+2}^{(1)}}\,/\,\overline{L_n^{(1)}},$$

so the left side of (31) tends to that of (30) and this completes the proof.

Equation (30) was discovered by the method shown above. A less interesting proof can be obtained from (2) and (3) or (3a).

5. CONGRUENCE PROPERTIES

Hardy & Wright [6, p. 149] prove that every ordinary (rational) prime divides some ordinary Fibonacci number (and therefore an infinity of them). To prove similar results we need to recall that a prime Gaussian integer $\alpha+i\beta$ (with $\alpha\beta\neq 0$) can be defined by the property that $\alpha^2+\beta^2$ is either 2 or an ordinary prime congruent to 1 modulo 4. For any such ordinary prime p, the corresponding Gaussian prime is unique up to conjugacy or multiplication by a unit (a power of i). This beautiful and famous theorem is proved, for example, in [10, p. 128]. Denote one of the Gaussian primes that corresponds to p by p_G and its complex conjugate by $\overline{p}_G$. Then, of course,

(32) $\quad p_G\overline{p}_G=p.$

Using this notation we have the following divisibility result, the proof being an elaboration of that of Theorem 180 in [6].

Definition: We call a number *pure* if it is either purely real or purely imaginary.

Theorem 4: Let a be fixed and let $p\equiv 1 \pmod 4$ be a rational prime, not a factor of $4+a^4$. Then,

(33) (i) $F_p^2\equiv 1 \pmod p$;

(This, of course, makes an assertion about both the real and imaginary parts of F_p^2.)

(34) (ii) F_p is pure, modulo p;

(35) (iii) $|F_p|^2\equiv\left(\dfrac{4+a^4}{p}\right)=\pm 1$

(the Legendre symbol is not 0 because p does not divide $4+a^4$);

(36) (iv) p divides $|F_{p-1}|^2$ or $|F_{p+1}|^2$ or both;

(37) (v) p_G (and $\overline{p}_G$) divides either F_{p-1} or F_{p+1} but not both apart from the uninteresting case in which p divides a.

Thus every Gaussian prime divides some Gaussian Fibonacci number [and therefore, by (25), an infinity of them].

(vi) For $n \geq 2$ we have $L_{2^n} \equiv 2 \pmod{2^n}$.

(vii) For $n \geq 2$ we have $F_{2^n} \equiv 2 \pmod{2^n}$

Before proving this theorem, let us look at some numerical examples deduced from Tables 1 and 2 combined with formulas (18), (22), and (23). These examples are shown in Table 3. Note, for example, that this table confirms Part (iii) of the theorem in that $4+1^4$ and $4+2^4$ are squares (quadratic residues) modulo 29 but not modulo 13, 17, or 37.

TABLE 1. Values of F_n andL_n when$a = 1$

$$F_n = f_n + if'_n \quad L_n = \ell_n + \ell'_n$$

n	f_n	f'_n	ℓ_n	ℓ'_n	n	f_n	f'_n	ℓ_n	ℓ'_n
−1	1	0	−1	−1	16	1728	1520	2818	3968
0	0	0	2	0	17	1513	3608	1361	8161
1	1	0	1	1	18	−367	6641	−3982	13,490
2	1	1	2	2	19	−5495	9882	−16,111	17,669
3	1	2	1	5	20	−15,744	11,028	−37,762	15,048
4	0	4	−2	8	21	−32,267	5166	−68,921	−5045
5	−3	6	−9	11	22	−53,177	−16,073	−101,638	−58,918
6	−9	7	−22	10	23	−69,371	−64,084	−111,641	−165,601
7	−19	4	−41	−1	24	−58,464	−149,528	−47,678	−336,160
8	−32	−8	−62	−32	25	21,693	−272,076	176,841	−549,439
9	−43	−36	−71	−95	26	235,305	−399,911	678,602	−708,758
10	−39	−87	−38	−198	27	656,909	−436,682	1,564,201	−579,595
11	5	−162	89	−331	28	1,328,896	−179,684	2,822,398	275,848
12	128	−244	382	−440	29	2,165,489	712,530	4,110,751	2,518,651
13	377	−278	911	−389	30	2,781,855	2,698,335	4,414,498	6,905,250
14	783	−145	1682	82	31	2,249,009	6,192,720	1,619,999	13,838,399
15	1305	360	2511	1375	32	−1,161,856	11,140,064	−7,803,902	22,363,648

TABLE 2. Values of F_n and L_n when $a = 2$

$$F_n = f_n + if'_n \quad L_n = \ell_n + i\ell'_n$$

n	f_n	f'_n	ℓ_n	ℓ'_n	n	f_n	f'_n	ℓ_n	ℓ'_n
−1	1	0	−2	−2	10	13,386	−2358	37,762	15,048
0	0	0	2	0	11	34,625	18,552	58,918	101,638
1	1	0	2	2	12	45,532	103,996	−47,678	336,160
2	2	2	2	8	13	−82,303	317,608	−708,758	678,602
3	1	8	−10	22	14	−754,290	574,606	−2,822,398	275,848
4	−12	20	−62	32	15	−2,740,095	−41,760	−6,905,250	−4,414,498
5	−63	24	−198	−38	16	−6,150,960	−4,989,104	−7,803,902	−22,363,648
6	−186	−58	−382	−440	17	−5,063,807	−22,321,888	22,214,242	−64,749,598
7	−319	−464	−82	−1682	18	28,365,202	−59,760,494		
8	104	−1624	2818	−3968					
9	3137	−3504	13,490	−3982	20	540,965,316	112,389,732		

TABLE 3(i), $a = 1$. Values modulo p

p	F_p	F_p^2	$\lvert F_p\rvert^2$	F_{p-1}	F_{p+1}
13	$-5i$	1	−1	$-2+3i$	$3-2i$
17	$4i$	1	−1	$(3+i)(4+i)$	$(3-i)(1+4i)$
29	1	1	1	0	$1+i$
37	$-6i$	1	−1	$(2i-3)(1+6i)$	$(4+3i)(1-6i)$

TABLE 3(ii), $a = 2$. Values modulo p

p	F_p	F_p^2	$\lvert F_p\rvert^2$	F_{p-1}	F_{p+1}
13	$5i$	1	−1	$3(2+3i)$	$-2(2-3i)$
17	$-4i$	1	−1	$-3(1+4i)$	$(1+i)(1-4i)$
29	1	1	1	0	$2(1+i)$
37	$6i$	1	−1	$3(-13+14i)(1+6i)$	$1-6i$

Proof of Theorem 4: From (7), where $A = a + ia$, we have (by the binomial theorem)

$$2^{p-1}F_p = 2^{p-1}(x^p - y^p)/(A^2+4)^{1/2}$$

$$= pA^{p-1} + \binom{p}{3}A^{p-3}(A^2+4) + \binom{p}{5}A^{p-5}(A^2+4)^2 + \cdots + (A^2+4)^{(p-1)/2}$$

$$\equiv (A^2+4)^{(p-1)/2} \pmod{p} \text{ since } p \text{ is prime.}$$

Therefore,

$$F_p \equiv (A^2+4)^{(p-1)/2} \pmod{p} \text{ (by Fermat's theorem, not the "last" but not least)}$$
$$= (4+2ia^2)^{(p-1)/2} = 2^{(p-1)/2}(2+ia^2)^{(p-1)/2}.$$

Therefore,

$$(38) \qquad F_p^2 \equiv 2^{p-1}(2+ia^2)^{p-1} \equiv (2+ia^2)^{p-1} \pmod{p}\cdot$$

and

$$(39) \qquad |F_p|^2 \equiv 2^{p-1}(4+a^4)^{(p-1)/2} \equiv (4+a^4)^{(p-1)/2} \pmod{p},$$

again by Fermat's theorem. Part (iii) of the theorem now follows from (39) combined with Theorem 83 of [6].

From (38) we obtain

$$\begin{aligned}(2+ia^2)F_p^2 &\equiv (2+ia^2)^p \\ &\equiv 2^p + i^p a^{2p} \quad \text{(again by the binomial theorem)} \\ &\equiv 2+ia^2 \quad [\text{because } p \equiv 1 \pmod 4 \text{ and is prime}].\end{aligned}$$

But $(4+a^4,\, p)=1$ and therefore $(2+ia^2,\, p)=1$. Hence, $F_p^2 \equiv 1 \pmod{p}$, which is Part (i) of the theorem.

To prove Part (ii), assume that $F_p \equiv \alpha + i\beta \pmod{p}$. Thus $F_p^2 \equiv \alpha^2 - \beta^2 + 2i\alpha\beta$. But $F_p^2 \equiv 1$ and is therefore real, so $\alpha\beta = 0$. Thus $\alpha = 0$ or $\beta = 0$ so F_p is pure $(\operatorname{mod} p)$.

Part (i) combined with (20) shows that $F_{p-1}F_{p+1} \equiv 0 \pmod{p}$. Since p is not a *Gaussian* prime, it does not follow that p divides either F_{p-1} or F_{p+1}, but Part (v) *does* follow because we must have $F_{p-1}F_{p+1} \equiv 0$ (mod p_G and also mod $\bar{p}_G$). [The recurrence relation (14), together with Part (i), shows that p_G cannot divide both F_{p-1} and F_{p+1} when p does not divide a. But sometimes both p_G and $\bar{p}_G$ divide F_{p-1}, or perhaps both divide F_{p+1}, and then p divides either F_{p-1} or F_{p+1} but not both.] Then Part (iv) follows from Part (v).

To prove Part (vi), note that

$$L_4 = 4(1-a^4+2ia^2) - 2 \equiv -2 \pmod 4 \equiv 2 \pmod 4,$$

and the result then follows by induction from formula (23).

To prove Part (vii), we have

$$F_4 = 2a[(1-a^2)+(1+a^2)] \equiv 0 \pmod 4$$

whether a is even or odd. Then the result follows by induction from (18) combined with Part (vi).

Lemma: For any integer n, L_{2n} is of the form $2s+2ti$ and L_{2n+1} is of the form $a \pm ai + 2au + 2avi$ where s, t, u, and v are integers.

Proof: Note first that it is irrelevant whether we take the plus sign or the minus sign. Now $L_0 = 2$ and $L_1 = a + ai$, so we can "start" an inductive proof, and we can readily complete the induction by means of the recurrence relation (15).

Theorem 5: Let p be an odd (ordinary) prime. Then

$$(40)\qquad \begin{aligned} L_p &\equiv a+ia \pmod{p} \text{ if } p \equiv 1 \pmod{4} \\ L_p &\equiv a-ia \pmod{p} \text{ if } p \equiv 3 \pmod{4}. \end{aligned}$$

More informatively,

$$(41)\qquad \begin{aligned} L_p &\equiv a+ia \pmod{2ap} \text{ if } p \equiv 1 \pmod{4} \\ L_p &\equiv a-ia \pmod{2ap} \text{ if } p \equiv 3 \pmod{4}. \end{aligned}$$

Proof: We have $L_p = x^p + y^p$, so

$$2^{p-1}L_p = A^p + \binom{p}{2}A^{p-2}(A^2+4) + \cdots + pA(A^2+4)^{(p-1)/2}$$

Now $2^{p-1} \equiv 1 \pmod{p}$, by Fermat's theorem, so

$$\begin{aligned} L_p &\equiv A^p \pmod{p} = (a+ia)(2ia^2)^{(p-1)/2} \\ &= (a+ia)\left(\frac{2}{p}\right)i^{(p-1)/2}a^{p-1} \equiv (a+ia)\left(\frac{2}{p}\right)i^{(p-1)/2} \end{aligned}$$

again by Fermat's theorem. Formulas (40) are therefore proved if p divides a, so we shall now assume that it does not. Now, by [6, p. 75], we have

$$\left(\frac{2}{p}\right) = 1 \;\text{ if } p \equiv \pm 1 \pmod{8}$$

and equations (40) follow readily. But by the Lemma we have $L_p - a \mp ia = M(2a)$ and (41) follows at once because $(2a, p) = 1$. [$\lambda = M(\mu)$ means $\lambda \equiv 0 \pmod{\mu}$.]

Corollary: ***(i)*** If p is an odd prime, then

$$(42)\qquad |L_p|^2 \equiv 2a^2 \pmod{p}.$$

(ii) If p is an odd prime and a is not a multiple of p, then $|L_p|^2/(2a^2)$ is an integer and is congruent to 1 modulo p.

Proof: From (41), L_p is of the form $a + ai + 2ap(s+it)$ where s and t are integers. Hence

$$\begin{aligned} |L_p|^2 &= (a+2aps)^2 + (a+2apt)^2 \\ &= 2a^2(1+2ps+2pt+2p^2s^2+2p^2t^2) \end{aligned}$$

and the Corollary follows at once.

Comment: If p is an odd number and fails to satisfy any of the conclusions in Theorems 4 and 5, then p is composite, and if it does satisfy the theorems it can perhaps be described as "probably" prime or at least as a new kind of "pseudoprime." For example, $L_n \not\equiv a \pm ia \pmod{n}$ for any composite n shown in Table 1 or 2.

Theorem 5 and its corollary are analogous to the theorem that the ordinary Lucas number $L_{\phi,p} \equiv 1 \pmod{p}$; see, for example, [13, p. 80], where it is mentioned, with a reference, that $L_{\phi,705} \equiv 1 \pmod{705}$ although 705 is composite. So the converse of our Theorem 5 is probably false. Anyway, the converse would be too good to be true. It would be interesting to know whether any parts of Theorems 4 and 5 have "modified converses."

Theorem 6: Every Gaussian number $G = g + ig'$ (not just the Gaussian primes) divides some Gaussian Fibonacci number (apart from F_0). (We are still regarding a as fixed.)

Proof: The sequence of Gaussian Fibonacci numbers (mod G) must be periodic with period no more than $(gg')^2 - 1$. This follows by the argument given, for example, in [13, p. 88] with a minor modification to allow for the complexity of G. But 0 is one of the Fibonacci numbers, and is divisible by G, and the result follows.

We next prove two congruence relations needed in Section 6. The first part sharpens Part (vi) of Theorem 4.

Theorem 7: (i) $L_{2^n} \equiv 2 \pmod{2^{n+2}}$ when $n \geq 3$, for all a.

(ii) $L_{2^n} \equiv 2 \pmod{2^{n+2}}$ when $n \geq 3$, while $1 \leq a \leq 5$.

[Part (i) can probably be sharpened, for example, $xL_{32}^{(1)} \equiv 2 \pmod{512}$, while Part (ii) might be true for all values of a.]

Proof: We have

$$L_2 = (a + ia)L_1 + L_0 = 2 + 2ia^2$$

so, by (23),

$$L_4 = L_2^2 - 2 = 2 - 4a^4 + 8ia^2 \equiv (-1)^a 2 \pmod 8.$$

Therefore, again by (23),

$$L_8 = L_4^2 - 1 = [M(8) + (-1)^a 2]^2 - 2 \equiv 2 \pmod{32}.$$

Therefore,

$$L_{16} = L_8^2 - 2 = [M(32) + 2]^2 - 2 \equiv 2 \pmod{64},$$

and so on, inductively, giving Part (i).

To prove Part (ii), note first that it is true for $n = 3$ and for $n = 4$ as we can see for $a = 1$ or 2 from Tables 1 and 2 and by calculations, not shown here, for $a = 3$, 4, and 5. We complete the proof inductively by noting first that

$$L_{\xi,2m+1} = L_{\xi,m} L_{\xi,m+1} - (-1)^m (\xi + \eta) \quad (m = 0, 1, 2, \ldots)$$

as follows easily from (11). On putting $\xi = x$ and $m = 2^{n-1}$, we infer that

$$\begin{aligned} L_{2^n+1} &= L_{2^{n-1}} L_{2^{n-1}+1} - (a + ia) \quad (n \geq 2) \\ &\equiv 2L_{2^{n-1}+1} - (a + ia) \pmod{2^{n+1}, n \geq 4} \text{ [by Part (i)]} \\ &\equiv 2[M(2^{n-1}) + a + ia] - (a + ia) \pmod{2^{n+1}, n \geq 4} \\ &\quad \text{(by the inductive hypothesis)} \\ &\equiv a + ia \pmod{2^n, n \geq 4} \end{aligned}$$

and this completes the inductive proof.

6. A PERIODICITY PROPERTY

Periodicity properties, modulo a given integer, of ordinary Fibonacci and Lucas sequences, are surveyed by Vajda [13, Chapter VII]. Our final theorem reveals a very simple periodicity of the Gaussian Lucas sequences at least when $a < 6$.

Theorem 8: For $1 \le a \le 5$, the period of the sequence $\dots L_{-2}, L_{-1}, L_0, L_1, L_2, \dots \pmod{2^n, n \ge 3}$ is a power of 2 not exceeding 2^n.

In view of the recurrence relation, in order to prove that 2^n is *a* period it is sufficient to prove that $L_m \equiv L_{m+2^n}$ for two consecutive values of m. By Theorem 7 this is achieved by taking $m = 0$ and $m = 1$.

The period (that is, the shortest period) must divide any known period and must therefore be a power of 2. There seems to be a 'tendency' for the period to be 2^n, for example, when $a = 1$ or 3 the periods modulo 8, 16, and 32 are, respectively, also 8, 16, and 32. But, when $a = 2$, the period modulo 32 is only 8.

7. LOOSE ENDS

There are many loose ends in this work. For example, we wondered whether Part (ii) of Theorem 7 is true for all values of a, in which case the same is true for Theorem 8. As another example, if $p \equiv 1 \pmod 4$ and $p > 5$, is $|F^{(a)}_{(p-1)/2}|^2$ always congruent to 0 or ±1 modulo p? I have verified this for $a = 1$ and 2 and $p < 113$, and for $a = 3$, $p < 61$. Note that $|L_p^{(1)}|^2/2$, where p is an odd prime, has a tendency to avoid having small factors, where the meaning of *small* increases when p increases. The values for $p = 3, 5, 7, 11, 13, 17$, and 19 are, respectively, 13, 101, 29^2, 58741 (prime), 53×9257, 34227121, and 185878941. Neither of the last two numbers has a factor less than 100. (Both are beyond the scope of [9].) It seems reasonable to conjecture that when the prime $p \to \infty$ and $a \ne M(p)$, then the smallest factor of $|L_p^{(1)}|^2/(2a^2)$ (which is an integer by the corollary of Theorem 5) also tends to infinity. The analogous property might be true also for the ordinary Lucas numbers $L_{\phi,p}$. It is possibly significant that 29^2 divides $|L_7^{(1)}|^2$, 29^3 divides $|F_7^{(2)}|^2$, and 89^2 divides $|L_{11}^{(2)}|^2$.

How much of the theory goes through if $a + ia$ is replaced by $a + ib$ throughout?

But the most interesting question is: Under what conditions is a "pseudoprime" a prime?

REFERENCES

1. P. S. Bruckman & I. J. Good. "A Generalization of a Series of de Morgan, with Applications of Fibonacci Type." *Fibonacci Quarterly* **14.2** (1976):193-96.
2. R. Fischler. "What Did Herodotus Really Say? or How To Build (a Theory of) the Great Pyramid." In *Environment and Planning B* (in press, 1991).
3. J. S. Frame. "Geometry, Euclidean." In *McGraw-Hill Encyclopedia of Science and Technology* **6** (1960):152-55.
4. M. Gardner. *The Magic Numbers of Dr. Matrix.* New York: Dorset, 1985.

5. I. J. Good. "Complex Fibonacci and Lucas Numbers, Continued Fractions and the Square Root of the Golden Ratio (Condensed Version)." *J. Operl. Res. Soc.* **43.8** (1992):837-42. Part of a Festschrift for Steven Vajda.
6. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford: Clarendon, 1938.
7. H. E. Huntley. *The Divine Proportion: A Study in Mathematical Beauty.* New York: Dover, 1970.
8. T. G. H. James. "Egyptian Art and Architecture, Ancient." *Encyclopaedia Britannica* **18** (1988):186-96.
9. D. N. Lehmer. *List of Prime Numbers from* 1 *to* 10,006,721. Carnegie Institution of Washington, Publication No. 165, Washington, D.C., 1914.
10. W. J. LeVeque. *Topics in Number Theory,* Vol. 1. Reading, Mass.: Addison-Wesley, 1956.
11. L. Pacioli. *De Divina Proportione.* 1509. (Pacioli wrote the first printed book on mathematics: see *Enc. Brit.*, 11th ed., Vol. 1, p. 618.)
12. D. Shanks. *Solved and Unsolved Problems in Number Theory.* New York: Chelsea, 1962-1978.
13. S. Vajda. *Fibonacci & Lucas Numbers, and the Golden Section.* Chichester, Sussex: Ellis Horwood, 1989.

AMS Classification Number: 11B39