ON THE DETERMINATION OF THE ZEROS OF THE FIBONACCI SEQUENCE

ROBERT P. BACKSTROM, Brighton High School, So. Australia

In his article [1], Brother U. Alfred has given a table of periods and zeros of the Fibonacci Sequence for primes in the range $2{,}000 < p < 3{,}000$. The range $p < 2{,}000$ has been investigated by D. D. Wall [2]. The present author has studied the extended range $p < 5{,}000$ by computer, and has found that approximately 68% of the primes have zeros which are maximal or half maximal, i.e., $Z(F,p) = p + 1,\ p - 1,\ (p + 1)/2$ or $(p - 1)/2$.

It would seem profitable, then, to seek a formula which gives the values of $Z(F,p)$ for some of these "time-consuming" primes. If these can be taken care of this way, the average time per prime would decrease since there are large primes with surprisingly small periods.

We have succeeded in producing a formula for two sets of primes. A table of zeros of the Fibonacci Sequence for primes in the range $3{,}000 < p <$ $< 10{,}000$ discovered by these formulas is included at the end of this paper. It is not known whether these formulae apply to more than a finite set of primes. See [3] for some discussion on this point.

To develop the ideas in a somewhat more general context, we introduce the Primary Numbers F_n defined by the recurrence relation:

$$F_{n+2} = aF_{n+1} + bF_n \ ; \ F_0 = 0, \ F_1 = 1 \ ,$$

where a and b are integral. F_n may be given explicitly in the Binet form;

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \ , \tag{1}$$

where α and β are the (assumed distinct) roots of the quadratic equation $x^2 - ax - b = 0$. In a like manner, we may define the Secondary Numbers which play the same role as the well known Lucas Numbers do to the Fibonacci Numbers. Thus the Secondary Numbers L_n are defined by the recurrence relation:

$$L_{n+2} = aL_{n+1} + bL_n \; ; \; L_0 = 2, \; L_1 = a \; .$$

L_n may also be given explicitly in the Binet form as:

$$L_n = \alpha^n + \beta^n \tag{2}$$

The following three properties of the Primary Sequences may easily be established by induction, or by using formula (1).

1) $F_r = -(-b)^r F_{-r}$
2) If $(a,b) = 1$, then $(F_n, b) = 1$
3) If $(a,b) = 1$, then $(F_n, F_{n+1}) = 1$.

Using formula (1), it is a simple algebraic exercise to prove the next result.

Lemma 1. $F_m = F_{i+1}F_{m-i} + bF_iF_{m-i-1}$

Proof: Since α and β are the roots of $x^2 - ax - b = 0$, we have $\alpha\beta = -b$.

$$\begin{aligned} \text{R. H. S.} &= ((\alpha^{i+1} - \beta^{i+1})(\alpha^{m-i} - \beta^{m-i}) - \alpha\beta\,(\alpha^i - \beta^i)(\alpha^{m-i-1} - \beta^{m-i-1}))/(\alpha - \beta)^2 \\ &= (\alpha^{m+1} - \alpha^{i+1}\cdot\beta^{m-i} - \alpha^{m-i}\cdot\beta^{i+1} + \beta^{m+1} - \beta\alpha^m + \alpha^{i+1}\cdot\beta^{m-i} + \alpha^{m-i} \\ &\qquad \cdot\,\beta^{i+1} - \alpha\beta^m)/(\alpha - \beta)^2 \\ &= (\alpha^{m+1} + \beta^{m+1} - \beta\alpha^m - \alpha\beta^m)/(\alpha - \beta)^2 \\ &= (\alpha - \beta)(\alpha^m - \beta^m)/(\alpha - \beta)^2 = (\alpha^m - \beta^m)/(\alpha - \beta) = \text{L. H. S.} \end{aligned}$$

Making use of properties 1) and 3) and Lemma 1, we may prove the following Theorem which tells us that the factors of Primary Sequences occur in similar patterns to those encountered in the Fibonacci Sequence itself.

Theorem 1. Let $(a,b) = 1$. Chose a prime p and an integer j such that p^j exactly divides F_d* $(d > 0)$, but no Primary Number with smaller subscript. Then p^j divides F_n (not necessarily exactly) if and only if $n = dt$ for some integer t. Or: $F_d | F_n$ iff $n = dt$ for some integer t.

Proof. Suppose that $n = dt$. We prove by induction on t that p^j divides F_n. $t = 1$. p^j divides F_d.

Assume true for $t = t$, $t \geq 1$.

---

*i. e., $p^j | F_d$ but $p^{j+1} \nmid F_d$.

Putting $m = d(t + 1)$ and $i = d$ in Lemma 1, we have the identity:

$$F_{d(t+1)} = F_{d+1}F_{dt} + bF_dF_{dt-1}$$

p^j divides F_d and F_{dt}, so by (1), divides $F_{d(t+1)}$.

Conversely, suppose that p^j divides F_n, where $n = dt + r$ for some r satisfying $0 < r < d$. We seek a contradiction, forcing r to equal 0.

Putting $m = dt$ and $i = -r$ in Lemma 1, we have the identity:

$$F_{dt} = F_{-r+1}F_{dt+r} + bF_{-r}F_{dt+r-1} \quad .$$

Multiplying through by $-(-b)^{r-1}$ and using the fact that $F_r = -(-b)^rF_{-r}$, we have:

$$-(-b)^{r-1}F_{dt} = F_{r-1}F_{dt+r} - F_rF_{dt+r-1} \quad .$$

Since p^j divides both F_{dt} and F_{dt+r} it divides F_rF_{dt+r-1}. However, if $(a, b) = 1$, consecutive Primary Numbers are co-prime, and so p does not divide F_{dt+r-1}. Thus p^j divides F_r which is a contradiction.

Another result which we will need is contained in the next Theorem. This result is a direct generalization of the well-known result applied to Fibonacci Numbers. The proof follows precisely the one given by Hardy and Wright in [4], and so need not be repeated here.

Theorem 2. Let $k = a^2 + 4b \neq 0$ and p be a prime such that $p \nmid 2b$, then p divides F_{p-1}, F_p or F_{p+1} according as the Legendre Symbol (k/p) is $+1$, 0 or -1.

Proof. Let the roots of the quadratic equation $x^2 - ax - b = 0$ be:

$$\alpha = (a + \sqrt{a^2 + 4b})/2 \qquad \text{and} \qquad \beta = (a - \sqrt{a^2 + 4b})/2 \quad .$$

Hence

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(a + \sqrt{k})^n - (a - \sqrt{k})^n}{2^n\sqrt{k}}$$

Case 1. $(k/p) = +1$

$$\begin{aligned}
2^{p-2}F_{p-1} &= ((a + \sqrt{k})^{p-1} - (a - \sqrt{k})^{p-1})/(2\sqrt{k}) \\
&= \left(\sum_{r=0}^{p-1} \binom{p-1}{r} a^{p-r-1}(\sqrt{k})^r - \sum_{r=0}^{p-1} \binom{p-1}{r} a^{p-r-1}(-\sqrt{k})^r\right)\Bigg/(2\sqrt{k}) \\
&= \left(\sum_{\substack{r \text{ odd} \\ 1 \le r \le p-2}} \binom{p-1}{r} a^{p-r-1}(\sqrt{k})^r\right)\Bigg/(\sqrt{k}) \\
&= \sum_{s=0}^{(p-3)/2} \binom{p-1}{2s+1} a^{p-2s-2}k^s
\end{aligned}$$

since $\binom{p-1}{2s+1} \equiv -1 \pmod p$ for $s = 0, 1, \cdots, (p-3)/2$, we find that

$$2^{p-2}F_{p-1} \equiv -\sum_{s=0}^{(p-3)/2} a^{p-2s-2}k^s \pmod p \quad .$$

Summing this geometric progression, we have:

$$2^p bF_{p-1} \equiv a^p - ak^{(p-1)/2} \pmod p \quad .$$

Making use of Euler's Criterion $k^{(p-1)/2} \equiv (k/p) \pmod p$ for the quadratic character of $k \pmod p$, assuming that $p \nmid 2b$, $(k/p) = +1$ and knowing that $a^p \equiv a \pmod p$, we have:

$$F_{p-1} \equiv 0 \pmod p \quad .$$

Case 2. $(k/p) = 0$

$$\begin{aligned}
2^{p-1}F_p &= ((a + \sqrt{k})^p - (a - \sqrt{k})^p)/(2\sqrt{k}) \\
&= \left(\sum_{r=0}^{p} \binom{p}{r} a^{p-r}(\sqrt{k})^r - \sum_{r=0}^{p} \binom{p}{r} a^{p-r}(-\sqrt{k})^r\right)\Bigg/(2\sqrt{k}) \\
&= \left(\sum_{\substack{r \text{ odd} \\ 1 \le r \le p}} \binom{p}{r} a^{p-r}(\sqrt{k})^r\right)\Bigg/(\sqrt{k}) = \sum_{s=0}^{(p-1)/2} \binom{p}{2s+1} a^{p-2s-1}k^s \quad .
\end{aligned}$$

p divides each Binomial Coefficient except the last and so:

$$2^{p-1}F_p \equiv k^{(p-1)/2} \pmod{p} \quad .$$

Since $p \nmid 2b$ and $(k/p) = 0$, we have

$$F_p \equiv 0 \pmod{p} \quad .$$

Case 3. $(k/p) = -1$

$$\begin{aligned}
2^pF_{p+1} &= ((a + \sqrt{k})^{p+1} - (a - \sqrt{k})^{p+1})/(2\sqrt{k}) \\
&= \left(\sum_{r=0}^{p+1} \binom{p+1}{r} a^{p-r+1}(\sqrt{k})^r - \sum_{r=0}^{p+1} \binom{p+1}{r} a^{p-r+1}(-\sqrt{k})^r \right) \bigg/ (2\sqrt{k}) \\
&= \left(\sum_{\substack{r \text{ odd} \\ 1 \le r \le p}} \binom{p+1}{r} a^{p-r+1}(\sqrt{k})^r \right) \bigg/ \sqrt{k} \\
&= \sum_{s=0}^{(p-1)/2} \binom{p+1}{2s+1} a^{p-2s}k^s \quad .
\end{aligned}$$

All the Binomial Coefficients except the first and last are divisible by p and so:

$$2^pF_{p+1} \equiv a^p + ak^{(p-1)/2} \pmod{p} \quad .$$

Since $p \nmid 2b$, $(k/p) = -1$ and $a^p \equiv a \pmod{p}$, we have:

$$F_{p+1} \equiv 0 \pmod{p} \quad .$$

Yet another well-known result which can be extended to the Primary Sequences is given in Lemma 2. A proof may be constructed on the model provided by Glenn Michael in [5], and is a simple exercise for the reader.

Lemma 2. If $(a,b) = 1$ and c,d are positive integers, then $(F_c, F_d) = |F_{(c,d)}|$.

Proof. Let $e = (c,d)$ and $D = (F_c, F_d)$. $e|c$ and $e|d$ hence by Theorem 1, $F_e|F_c$ and $F_e|F_d$. Thus $F_e|D$.

There exist integers x and y (given by the Euclidean Algorithm) such that $e = xc + yd$. Suppose without loss of generality that $x > 0$ and $y \leq 0$. Using Lemma 1 with $m = xc$ and $i = e$ we have:

$$F_{xc} = F_{e-1}F_{-yd} + bF_eF_{-yd-1} .$$

$D|F_c$ and F_d and so by Theorem 1, $D|F_{xc}$ and F_{-yd}. Thus $D|bF_eF_{-yd-1}$, but by property 2), $(D,b) = 1$, and by property 3), $(D, F_{-yd-1}) = 1$. Thus $D|F_e$. This, together with $F_e|D$ gives the result.

Lemma 3.

$$F_{2n-1} - F_{n-1}L_n = (-b)^{n-1}$$

Proof.

$$\begin{aligned}
\text{L.H.S.} &= (\alpha^{2n-1} - \beta^{2n-1} - (\alpha^{n-1} - \beta^{n-1})(\alpha^n + \beta^n))/(\alpha - \beta) \\
&= (\alpha^{2n-1} - \beta^{2n-1} - \alpha^{2n-1} - \alpha^{n-1}\beta^n + \beta^{n-1}\alpha^n + \beta^{2n-1})/(\alpha - \beta) \\
&= (-\alpha^{n-1}\beta^n + \beta^{n-1}\alpha^n)/(\alpha - \beta) \\
&= (\alpha - \beta)(\alpha\beta)^{n-1}/(\alpha - \beta) = (\alpha\beta)^{n-1} = (-b)^{n-1} = \text{R.H.S.}
\end{aligned}$$

MAIN RESULTS

We shall divide the main results of this paper into 6 parts — four Lemmas in which the essential ideas are proven, a Theorem utilizing these ideas and a Corollary applying them in particular to the Fibonacci Numbers. It will be implicitly understood that from now on, $(a,b) = 1$ and $p \nmid 2abk$.

Lemma 4. If $(-b/p) = (k/p) = +1$ (Legendre Symbols), then $p|F_{(p-1)/2}$.

Proof. Using Lemma 3 with $n = (p+1)/2$ gives

$$F_p - F_{\frac{p-1}{2}} L_{\frac{p+1}{2}} = (-b)^{(p-1)/2} .$$

In the proof of Theorem 2 we find that

$$2^{p-1}F_p \equiv F_p \equiv (k/p) \pmod{p} \quad .$$

Thus:

$$(k/p) - F_{\frac{p-1}{2}} L_{\frac{p+1}{2}} \equiv (-b/p) \pmod{p} \tag{3}$$

Putting $(-b/p) = (k/p) = +1$ we have:

$$F_{\frac{p-1}{2}} L_{\frac{p+1}{2}} \equiv 0 \pmod{p} \quad .$$

Suppose, now, that p divides $L_{(p+1)/2}$. Since $L_{(p+1)/2} = F_{p+1}/F_{(p+1)/2}$, p divides F_{p+1}. Theorem 2 tells us that p divides F_{p-1} since $(k/p) = +1$. Applying Lemma 2, we see that p divides $F_{(p-1,\,p+1)}$ which is F_2.

But $F_2 = a$ and so we have a contradiction.

Lemma 5. If $(-b/p) = (k/p) = -1$, then $p \nmid F_{(p+1)/2}$.

Proof. Using (3) with $(-b/p) = (k/p) = -1$ we have:

$$F_{\frac{p-1}{2}} L_{\frac{p+1}{2}} \equiv 0 \pmod{p} \quad .$$

Suppose that $p | F_{(p-1)/2}$. Therefore $p | F_{p-1}$. By Theorem 2, $p | F_{p+1}$, and so as before, we find that $p | F_2 = a$ a contradiction. Hence $p | L_{(p+1)/2}$.

Since $L_n = aF_n + 2bF_{n-1}$, any prime divisor common to F_n and L_n must divide $2b$ by property 3). These primes are excluded, and so $p \nmid F_{(p+1)/2}$ as asserted.

Lemma 6. If $(-b/p) = +1$, $(k/p) = -1$, then $p | F_{(p+1)/2}$.

Proof. Putting $(-b/p) = +1$ and $(k/p) = -1$ in (3) we have:

$$F_{\frac{p-1}{2}} L_{\frac{p+1}{2}} \equiv -2 \pmod{p} \quad .$$

Thus $p \nmid L_{(p+1)/2}$ since $p \neq 2$. Suppose, to the contrary, that $p \nmid F_{(p+1)/2}$. By Theorem 2, $p \mid F_{p+1}$, and so $p \mid F_{p+1}/F_{(p+1)/2} = L_{(p+1)/2}$ a contradiction.

Lemma 7. If $(-b/p) = -1$ and $(k/p) = +1$, then $p \nmid F_{(p-1)/2}$.

Proof. Similarly we have:

$$F_{\frac{p-1}{2}} \; L_{\frac{p+1}{2}} \equiv +2 \pmod{p} \quad .$$

Clearly

$$p \nmid F_{(p-1)/2} \quad .$$

To distinguish from the Fibonacci case, we shall employ the terminology $Z(F;a,b;p)$ for the first non-trivial zero (mod p) of the Primary Sequence with parameters a and b. Thus $Z(F;1,1;p) = Z(F,p)$ following the notation used by Brother U. Alfred in [1]. Similar remarks apply to $Z(L;a,b;p)$.

Main Theorem.

1) If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = (k/p) = +1$, then $Z(F;a,b;p) = r$.

2) If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = (k/p) = -1$, then $Z(F;a,b;p) = p + 1$.

3) If s is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = +1$, and $(k/p) = -1$, then $Z(F;a,b;p) = s$.

4) If r is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = -1$, and $(k/p) = +1$, then $Z(F;a,b;p) = p - 1$.

Proof of the Main Theorem.

1) Since $(k/p) = +1$, we see from Theorems 1 and 2 that $p \mid F_d$, where d is a divisor of $p - 1 = 2r$. The only divisors of 2r are 1, 2, r and 2r since r is prime. Clearly $p \nmid F_1 = 1$ and by assumption $p \nmid F_2 = a$. Lemma 4 tells us that $p \mid F_r$ and so $Z(F;a,b;p) = r$.

2) Since $(k/p) = -1$, $p \mid F_d$, where $d \mid p + 1 = 2s$. The divisors of 2s are 1, 2, s and 2s. $p \nmid F_1$ and $p \nmid F_2$. Lemma 5 then tells us that $p \nmid F_s$ and so p must divide $F_{2s} = F_{p+1}$, i.e., $Z(F;a,b;p) = p + 1$.

3) Since $(k/p) = -1$, $p \mid F_d$, where $d \mid p + 1 = 2s$. Thus d must be 1, 2, s or 2s because of the primality of s. $p \nmid F_1$ and $p \nmid F_2$. Lemma 6 tells us that $p \mid F_s$ and so $Z(F;a,b;p) = s$.

4) Since $(k/p) = +1$, $p \mid F_d$ where $d \mid p - 1 = 2r$. Again d must be one of: $1, 2, r$ or $2r$ since r is prime. $p \nmid F_1$ and $p \nmid F_2$. Lemma 7 tells us that $p \nmid F_r$ and so p must divide $F_{2r} = F_{p-1}$. Hence $Z(F;a,b;p) = p - 1$.

Specializing the above results to the case of the Fibonacci Sequence ($F_{n+2} = F_{n+1} + F_n$; $F_0 = 0$, $F_1 = 1$) by choosing $a = b = 1$ and hence $k = 5$, we find that parts 1) and 2) of the Main Theorem are now vacuous. Indeed, 1) requires p to be of the form $20k + 1$ or 9, and thus r to be of the form $10k + 0$ or 4 which cannot be prime; 2) requires p to be of the form $20k + 3$ or 7, and thus s to be of the form $10k + 2$ or 4 giving only the prime 2; 3) requires p to be of the form $20k + 13$ or 17 requiring s to be of the form $10k + 7$ or 9 which may now be prime and 4) requires p to be of the form $20k + 11$ or 19 and thus r to be of the form $10k + 5$ or 9 giving primes 5 and $10k + 9$. Thus we have established the following result:

Corollary. Employing the symbol $Z(F, p)$ to denote the first non-trivial zero (mod p) among the Fibonacci Sequence ($F_{n+2} = F_{n+1} + F_n$; $F_0 = 0$, $F_1 = 1$) we have:

1) $s = 2$ and $p = 2s - 1 = 3$ are both prime, and so $Z(F, 3) = 4$.

2) If $s \equiv 7$ or $9 \pmod{10}$ and $p = 2s - 1$ are both prime, then $Z(F, p) = s$.

3) $r = 5$ and $p = 2r + 1 = 11$ are both prime, and so $Z(F, 11) = 10$.

4) If $r \equiv 9 \pmod{10}$ and $p = 2r + 1$ are both prime, then $Z(F, p) = p - 1$.

It would be interesting to discover other sets of primes which have determinable periods and zeros. One such set is the set of Mersenne primes $M_p = 2^p - 1$, where p is a prime of the form $4t + 3$. Since $(-1/M_p) = (5/M_p) = -1$, Lemma 5 tells us that $M_p \nmid F_{2^{4t+2}}$ and so $M_p \nmid F_{2^g}$ for $0 \le g < 4t + 2$, otherwise we could obtain a contradiction from Theorem 1. However, Theorem 2 tells us that $M_p \mid F_{2^p}$, and so $Z(F, M_p) = 2^p$.

A definite formula for $Z(F, p)$ is not to be expected for the same reason that one would not expect to find a formula for the exponent to which a given integer c belongs modulo p. However, some problems, such as that of classifying the set of primes for which $Z(F, p)$ is even (the set of divisors of the Lucas Numbers ($p \neq 2$)) may have partial or complete solutions, and so we leave the reader to investigate them.

TABLE OF ZEROS

p	Z(F,p)	p	Z(F,p)	p	Z(F,p)
3119	3118	5399	5398	7393	3697
3217	1609	5413	2707	7417	3709
3253	1627	5437	2719	7477	3739
3313	1657	5639	5638	7537	3769
3517	1759	5879	5878	7559	7558
3733	1867	5939	5938	7753	3877
3779	3778	6037	3019	7933	3967
4057	2029	6073	3037	8039	8038
4079	4078	6133	3067	8053	4027
4139	4138	6217	3109	8317	4159
4177	2089	6337	3169	8353	4177
4259	4258	6373	3187	8677	4339
4273	2137	6599	6598	8699	8698
4357	2179	6637	3319	8713	4357
4679	4678	6659	6658	8819	8818
4799	4798	6719	6718	8893	4447
4919	4918	6779	6778	9013	4507
4933	2467	6899	6898	9133	4567
5077	2539	6997	3499	9277	4639
5099	5098	7057	3529	9817	4909
5113	2557	7079	7078	9839	9838
5233	2617	7213	3607	9973	4987

REFERENCES

1. Brother U. Alfred, "Additional Factors of the Fibonacci and Lucas Series," Fibonacci Quarterly, Vol. 1, No. 1, Feb. 1963, pp. 34-42.
2. D. D. Wall, "Fibonacci Series Modulo m," The American Mathematical Monthly, Vol. 67, No. 6, June-July 1960, pp. 525-532.
3. Daniel Shanks, Solved and Unsolved Problems in Number Theory.
4. Hardy and Wright, An Introduction to the Theory of Numbers.
5. Glenn Michael, "A New Proof for an Old Property," The Fibonacci Quarterly, Vol. 2, No. 1, February 1964, pp. 57-58.

★ ★ ★ ★ ★

Continued from p. 306

12. P. Lafer and C. T. Long, "A Combinatorial Problem," The American Mathematical Monthly, Nov. 1962, pp. 876-883.
13. C. G. Lekkerkerker, Voorstelling van natuurlyke getallen door een som van Fibonacci, Simon Stevin, 29 (1951-52) pp. 190-195.

★ ★ ★ ★ ★