PERIODS AND ENTRY POINTS IN FIBONACCI SEQUENCE

A. ALLARD and P. LECOMTE
Université de Liège, Liège, Belgium

1. INTRODUCTION

Let the F 's be defined as follows:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n, \ \forall\, n \geq 0.$$

Let $k > 0$ be any integer. There is then a smallest positive m such that $k|F_m$ [if a, b denote integers, we sometimes write $a|b$ instead of $b \equiv 0 \pmod{a}$, $a||b$ instead of $b \equiv 0 \pmod{a}$, and $b \not\equiv 0 \pmod{a^2}$]. This unique m will be denoted by β_k; F_{β_k} is usually called the *entry point* of k. Moreover, the sequence $F_n \pmod{k}$ is well known to be periodical. We denote by 1_k the period and we let $\gamma_k = 1_k/\beta_k$.

Our purpose in this paper is to compute (at least in a theorical way) γ_p for each prime p. In [1], Vinson also computes γ_p, but our point of view and our methods are really different from those of Vinson, so that we obtain new results regarding γ_p and additional information about β_p.

This paper is based on a few results which are summarized in Section 2 and proved in Section 6. Some of these are well known and their proofs (elementary) are given for the benefit of the reader.

2. PROPOSITIONS

We now state those propositions that will be useful later.

Let p be a prime with $p > 5$. For simplicity, we let $\beta = \beta_p$, $1 = 1_p$, and $\gamma = \gamma_p$. Then

(1) $$p|F_m \Longleftrightarrow \beta|m, \ \forall\, m.$$

This shows that γ is an integer.

(2) $\gamma \in \{1, 2, 4\}$; *to be more precise*,

$$\gamma = 1 \Longleftrightarrow F_{\beta-1} \equiv 1 \pmod{p}$$
$$\gamma = 2 \Longleftrightarrow F_{\beta-1} \equiv -1 \pmod{p}$$
$$\gamma = 4 \Longleftrightarrow F^2_{\beta-1} \equiv -1 \pmod{p}$$

(3) $\gamma = 4 \Longleftrightarrow \beta$ *is odd*

$$4|\beta \Rightarrow \gamma = 2$$

(4) *The following holds for any* $j \in \{0, 1, \ldots, \beta - 1\}$ *and any* $k > 0$:

$$F_{k\beta-j} \equiv F^{k-1}_{\beta-1}F_{\beta-j} \pmod{p}.$$

In particular, letting $j = 1$, we obtain

$$F_{k\beta-1} \equiv F^k_{\beta-1} \pmod{p}.$$

(5) *For all* a, $b > 0$, *we have*

$$F_{ab} = \sum_{k=1}^{b} C^k_b F^k_a F^{b-k}_{a-1} F_k \quad \left(C^k_b = \frac{b!}{k!\,(b-k)!}\right).$$

[Note that if p is a prime, then $p|C_p^k$ for $k = 1, \ldots, p - 1$. Then the above formula with $a = q$ and $b = p$ together with Fermat's theorem implies that

$$F_{pq} \equiv F_p F_q \pmod{p}$$

for all prime p and all integers q.]

(6) *If* $p = 10m \pm 1$, *then* $F_p \equiv 1 \pmod{p}$ *and* $\beta|(p - 1)$.
If $p = 10m \pm 3$, *then* $F_p \equiv -1 \pmod{p}$ *and* $\beta|(p + 1)$.

(7) $$2\beta|(p \pm 1) \Longleftrightarrow p \equiv 1 \pmod{4}$$

[*according that* p *is* $(p - 1)$ *or is not* $(p + 1)$ *a quadratic residue* mod 5].

We are now in a position to state our main results. We will investigate separately the cases $p = 10m \pm 1$ and $p = 10m \pm 3$. The conclusions are of very different natures.

3. COMPUTATION OF γ WHEN $p = 10m \pm 3$

Theorem 1: Let p be of the form $10m \pm 3$. Then either $p = 4m' - 1$, $\gamma = 2$, and $4|\beta$, or $p = 4m' + 1$, $\gamma = 4$, and β is odd.

This theorem allows us to calculate γ by a simple examination of the number p. Such a result does not hold in the case where $p = 10m \pm 1$.

Proof: By (6) above, we can write $p = \mu\beta - 1$ and $F_p \equiv -1 \pmod{p}$. Thus, by (4), we have

(3.1) $$F_{\beta-1}^{\mu} \equiv -1 \pmod{p}.$$

Since $\gamma = 1$ implies $F_{\beta-1} \equiv 1 \pmod{p}$ and since $F_{\beta-1}^4 \equiv 1 \pmod{p}$, we conclude from (3.1) that $\gamma > 1$ and $4\nmid\mu$.

Suppose β is even. Then $\gamma = 2$ and $F_{\beta-1} \equiv -1 \pmod{p}$. From (3.1), this implies that μ is odd. Suppose $2||\beta$. Then $p = \mu\beta - 1 \equiv 1 \pmod{4}$, so that by (7), $2\beta|(p + 1)$, which is a contradiction. Thus, $4|\beta$ and $p \equiv -1 \pmod{4}$.

Suppose β is odd. Then $\gamma = 4$ and $F_{\beta-1}^2 \equiv -1 \pmod{p}$. From (3.1), this implies that $2||\mu$. Hence, $p = \mu\beta - 1 \equiv 1 \pmod{4}$. The theorem is proved.

From the preceding proof, we obtain another statement.

Theorem 2: If $\gamma = 1$, then $p = 10m \pm 1$.

4. COMPUTATION OF γ WHEN $p = 10m \pm 1$

This case is more complicated and it is convenient to introduce the *characteristic exponent* α *of* p, well defined [recall (6)] by

$$= 2^{\alpha}\nu\beta + 1, \ \nu \text{ odd}.$$

The explicit computation of α will be made later, by means of the following lemma.

Lemma: If $p = 10m \pm 1 = 2^{\alpha}\nu\beta + 1$ with ν odd, then

(8) $$\gamma = 1 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha} \pmod{p}$$

(9) $$\gamma = 2 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv -2^{\alpha} \pmod{p}$$

(10) $$\gamma = 4 \Rightarrow \frac{F_{p-1}}{F_{\nu\beta}} \equiv -2^{\alpha} F^{\nu}_{\beta-1} \pmod{p}.$$

In fact, apply (5), with $a = \nu\beta$ and $b = 2^{\alpha}$. Then

$$F_{p-1} = \sum_{k=1}^{2^{\alpha}} C^{k}_{2^{\alpha}} F^{k}_{\nu\beta} F^{2^{\alpha}-k}_{\nu\beta} F_k .$$

This implies that

(4.1) $$\frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha} F^{\nu(2^{\alpha}-1)}_{\beta-1} \pmod{p}.$$

On the other hand, (6) and (4) imply

(4.2) $$F^{2^{\alpha}\nu}_{\beta-1} \equiv 1 \pmod{p}.$$

Then, from (4.1) and (4.2):

(4.3) $$F^{\nu}_{\beta-1} \cdot \frac{F_{p-1}}{F_{\nu\beta}} \equiv 2^{\alpha} \pmod{p}.$$

Suppose $\gamma = 1$, then $F_{\beta-1} \equiv 1 \pmod{p}$ and (8) follows from (4.3).

Suppose $\gamma = 2$, then $F_{\beta-1} \equiv -1 \pmod{p}$, and since ν is odd, (9) follows from (4.3).

Suppose $\gamma = 4$, then $F^2_{\beta-1} \equiv -1 \pmod{p}$. Since ν is odd, we have $F^2_{\beta-1} \equiv -1 \pmod{p}$, so that (10) follows from (4.3).

Theorem 4: Let $p = 10m \pm 1$. Then, p can be written uniquely as $p = 2^r s + 1$ with s odd, and we have

$$\gamma = 4 \Longleftrightarrow \frac{F_{p-1}}{F_s} \not\equiv 0 \pmod{p}$$

$$\gamma = 1 \Longleftrightarrow \frac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}$$

$$\gamma = 2 \Longleftrightarrow \frac{F_{p-1}}{F_s} \equiv 0 \quad \text{and} \quad \frac{F_{p-1}}{F_{2s}} \not\equiv 2^{r-1} \pmod{p}.$$

(The statement concerning $\gamma = 2$ will be made more precise later.)

Proof: Suppose $\gamma = 4$. Then, β is odd and, thus, $\alpha = r$, $\nu\beta = s$, so that, by the lemma, we have

$$\frac{F_{p-1}}{F_s} \quad -2^r F^{\nu}_{\beta-1} \not\equiv 0 \pmod{p}.$$

Suppose $\gamma = 1$. Then, β is even, but $2 \| \beta$, since $4 | \beta$ implies $\gamma = 2$. So $\alpha = r - 1$ and $\nu\beta = 2s$; thus, by the lemma, we have

$$\frac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}.$$

Conversely, suppose $\dfrac{F_{p-1}}{F_s} \not\equiv 0 \pmod{p}$. Then $p|F_s$, since $p|F_{p-1}$. Thus, $\beta|s$, and so β is odd, proving that $\gamma = 4$. Suppose that $\dfrac{F_{p-1}}{F_{2s}} \equiv 2^{r-1} \pmod{p}$. We want to prove that $\gamma = 1$ in this case. We now have $\beta|2s$. If β is odd, then $\gamma = 4$ and, as seen above, $\dfrac{F_{p-1}}{F_s} \equiv -2^r F^{\nu}_{\beta-1} \pmod{p}$. But, since $\beta|s$,

$$F_{s-1} + F_{s+1} \equiv F_{\nu\beta-1} + F_{\nu\beta+1} \equiv 2F^{\nu}_{\beta-1} \pmod{p},$$

so that

$$2^{r-1} \equiv \frac{F_{p-1}}{F_2} \equiv \frac{F_{p-1}}{F_s(F_{s-1} + F_{s+1})} \equiv \frac{-2^r F^{\nu}_{\beta-1}}{2F^{\nu}_{\beta-1}} \equiv -2^{r-1} \pmod{p}.$$

This is clearly a contradiction, since p is odd. If $2||\beta$ and $\gamma = 2$, we have $\alpha = r - 1$ and $\nu\beta = 2s$. So, by the lemma, $\dfrac{F_{p-1}}{F_{2s}} \equiv -2^{r-1} \pmod{p}$. But, we assume that $\dfrac{F_{p-1}}{F_2} \equiv 2^{r-1} \pmod{p}$. Hence, a contradiction. Thus $\gamma = 1$, and the lemma follows.

Corollary: If $p = 10m \pm 1 = 4m' - 1$, then $\gamma = 1$.

In fact, one has $4m' - 1 = 2s + 1$, s odd, if and only if $r = 1$. In this case, $F_{p-1} = F_{2s}$ and, by Theorem 4, $\gamma = 1$.

We are now in a position to compute the characteristic exponent α of p. It is clear that if $\gamma = 4$, then $\alpha = r$; if $\gamma = 1$, then $\alpha = r - 1$. We have only to look at the case $\gamma = 2$.

Theorem 5: Let $1 < k \le r$. Then $\alpha = r - k$ and $\gamma = 2$ if and only if

$$(4.4) \qquad \frac{F_{p-1}}{F_s} \equiv \cdots \equiv \frac{F_{p-1}}{F_{2^{k-1}s}} \equiv 0 \quad \text{and} \quad \frac{F_{p-1}}{F_{2^k s}} \equiv -2^{r-k} \pmod{p}.$$

We see that α is determined by the rank of the first nonvanishing $\dfrac{F_{p-1}}{F_{2^j s}} \pmod{p}$.

Proof: Suppose that $\gamma = 2$ and $\alpha = r - 1$. By the lemma, we can conclude that $\dfrac{F_{p-1}}{F_{2^k s}} \equiv -2^{r-k} \pmod{p}$. On the other hand, since $2^j s \not\equiv 0 \pmod{p}$ for $j = 0, \ldots, k - 1$, we see that (4.4) holds.

Conversely, suppose (4.4) holds. Then, by Theorem 4, since $k > 1$, $\gamma < 4$, and $\gamma \ne 1$, that is $\gamma = 2$. Moreover, $\beta|2^k s$, but $\beta\nmid 2^{k-1}s$. Thus $\nu\beta = 2^k s$ and $\alpha = r - k$. Hence the result.

5. FURTHER PROPERTIES OF γ AND SOME INTERESTING RESULTS

Proposition 1: For any prime p, $\gamma = 2$ implies $4|\beta$.

In fact, when $p = 10m \pm 3$, this follows from Theorem 1. When $p = 10m \pm 1$, we prove that $2||\beta$ implies $\gamma = 1$. As $2||\beta$, $\gamma < 4$, and $p|F_{2s}$, but $p\nmid F_s$ and so

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

But $F_{2s-1} \equiv F_{s-1}^2 + F_s^2$ and, as s is odd, $F_{s-1}F_{s+1} = F_s^2 - 1$. Thus, since $2s = \nu\beta$, we can write

$$F_{\beta-1} \equiv F_{\beta-1} \equiv F_{2s-1} \equiv -F_{s-1}F_{s+1} + F_s^2 \equiv 1 \pmod{p}.$$

Hence $\gamma = 1$, and the result is proved.

Proposition 2: If $p = 10m \pm 1$, then $\gamma = 2$ if and only if $\frac{F_{p-1}}{F_s} \equiv \frac{F_{p-1}}{F_{2s}} \equiv 0 \pmod{p}$.

This is obvious from what precedes. Practically, however, this can be of some interest: to compute γ, compute $F_s \pmod{p}$. If $F_s \not\equiv 0 \pmod{p}$, then $\frac{F_{p-1}}{F_s} \equiv 0 \pmod{p}$ and, thus, $\gamma \neq 4$. Compute then $F_{s-1} + F_{s+1} \pmod{p}$. If it does not vanish, then $F_{2s} \not\equiv 0 \pmod{p}$ so that $\gamma \neq 1$ and, thus, $\gamma = 2$.

Proposition 3: Let p be any given prime number. Then the greatest t such that $p^t | F_{\beta_p}$ is the greatest t such that $p^t | F_{p\pm1}$.

In fact, either $p = 10m \pm 1$, $p = \lambda\beta + 1$, or $p = 10m \pm 3$, $p = \mu\beta - 1$. By (5), this implies

$$\frac{F_{p-1}}{F_\beta} \equiv \lambda F_{\beta-1}^{\lambda-1} \not\equiv 0 \pmod{p} \quad \text{or} \quad \frac{F_{p-1}}{F_\beta} \equiv \mu F_{\beta-1}^{\mu-1} \not\equiv 0 \pmod{p},$$

respectively. Hence, Proposition 3.

6. PROOFS OF PROPOSITIONS

This section is devoted to the proofs of the propositions stated in Section 2, except for (7), for which the reader is referred to *The Fibonacci Quarterly* 8, No. 1 (1970):23-30.

Proof of (4): Since the sequence $F_n \pmod{p}$ starts with

$$F_1 \equiv 1, \quad F_2 \equiv 1, \quad F_3 \equiv 2, \ \ldots, \ F_{\beta-1}, 0,$$

it follows from $F_{n+2} = F_{n+1} + F_n$ that the following β members of this sequence are obtained by multiplying the first β one by $F_{\beta-1}$ so that, for any $j = 0, \ldots, \beta - 1$, $F_{2\beta-j} \equiv F_{\beta-1}F_{\beta-j} \pmod{p}$. The argument can be applied again to prove that $F_{3\beta-j} \equiv F_{\beta-1}F_{\beta-j}$ and, more generally, that $F_{k\beta-1} \equiv F_{\beta-1}F_{(k-1)\beta-1} \pmod{p}$. Proposition (4) then holds in an obvious way.

Proof of (5): Recall that

$$F_n = \frac{\varphi}{\varphi^2+1}\left[\varphi^n - \left(-\frac{1}{\varphi}\right)^n\right]$$

where φ and $-\frac{1}{\varphi}$ satisfy $y^2 = y + 1$. From this, it is clear that

$$\varphi^n = \varphi F_n + F_{n-1} \quad \text{and} \quad \left(-\frac{1}{\varphi}\right)^n = \left(-\frac{1}{\varphi}\right)F_n + F_{n-1}.$$

Then

$$F_{ab} = \frac{\varphi}{\varphi^2+1}\left[\varphi^{ab} - \left(-\frac{1}{\varphi}\right)^{ab}\right] = \frac{\varphi}{\varphi^2+1}\left[(\varphi F_a + F_{a-1})^b - \left(-\frac{1}{\varphi}F_a + F_{a-1}\right)^b\right]$$

$$= \sum_{k=1}^{b} C^k F^k F_{a-1}^{b-k} F_k, \text{ using binomial expansion and } F_0 = 0.$$

Proof of (1) and (2): Recall that for any integer m we have

$$F_{m-1}F_{m+1} = F_m^2 + (-1)^m.$$

Let $m = \beta$ in this formula. Thus,

$$F_{\beta-1}^2 \equiv (-1)^\beta \pmod{p}, \tag{6.1}$$

taking account of $F_{\beta+1} \equiv F_{\beta-1} \pmod{p}$. On the other hand, 1 is the smaller m such that $F_{\beta-1}^m \equiv F_{m\beta-1} \equiv 1 \pmod{p}$. Recall also that $1 = \gamma\beta$, by the very definition of γ. Then,

(a) suppose β odd. Thus, by (6.1),

$F_{\beta-1}^2 \equiv -1$ so that $F_{\beta-1} \not\equiv 1$ and $F_{\beta-1}^4 \equiv 1$.

Thus $\gamma = 4$.

(b) suppose β even. Then (6.1) implies that

$F_{\beta-1}^2 \equiv 1$.

Since p is a prime, either

$F_{\beta-1} \equiv 1$ and $\gamma = 1$, or $F_{\beta-1} \equiv -1$ and $\gamma = 2$.

Hence (2) is proved.

Proof of (3): To prove (3), we have only to show that $4|\beta$ implies $\gamma = 2$. For this, we show that

$$\left.\begin{array}{r} F_{4\lambda} \equiv 0 \pmod{p} \\ F_{4\lambda+1} \equiv 1 \pmod{p} \end{array}\right\} \Rightarrow F_{2\lambda} \equiv 0 \pmod{p}. \tag{6.2}$$

Suppose that the left member of this implication holds. Then from well-known formulas:

$$\begin{aligned} F_{4\lambda+1} &= F_{2\lambda}^2 + F_{2\lambda+1}^2 = F_{2\lambda}^2 + F_{2\lambda}F_{2\lambda+2} - (-1)^{2\lambda+1} \\ &= F_{2\lambda}(F_{2\lambda} + F_{2\lambda+2}) + 1 \equiv 1 \pmod{p}. \end{aligned}$$

Hence

$$F_{2\lambda}(F_{2\lambda} + F_{2\lambda+2}) \equiv 0 \pmod{p}.$$

To prove (6.2), it suffices to show that $\mathrm{GCD}(F_{2\lambda} + F_{2\lambda+2}, p) = 1$. To do this, since $p|F_{4\lambda}$, it suffices to prove that $\mathrm{GCD}(F_{4\lambda}, F_{2\lambda} + F_{2\lambda+2}) = 1$. But

$$\delta = \mathrm{GCD}(F_{4\lambda}, F_{2\lambda} + F_{2\lambda+2}) = \mathrm{GCD}\big(F_{2\lambda}(F_{2\lambda+1} + F_{2\lambda-1}), F_{2\lambda} + F_{2\lambda+2}\big)$$

and, as $\mathrm{GCD}(F_{2\lambda}, F_{2\lambda+2}) = 1$,

$$\delta = \mathrm{GCD}(F_{2\lambda+1} + F_{2\lambda-1}, F_{2\lambda+2} + F_{2\lambda}).$$

It is then easily seen that

$$\delta|(F_{2\lambda+1} + F_{2\lambda-1}),\ \delta|(F_{2\lambda-1} + F_{2\lambda-3}),\ \ldots,\ \delta|F_2 = 1.$$

Hence (3).

Proof of (6): Recall first that $\left(\frac{p}{5}\right) = 1$ or -1, according that p is or is not a quadratic residue mod 5, that is, $p = 10m \pm 1$ or $p = 10m \pm 3$, respectively. Thus, we have to show that

$$\left(\frac{p}{5}\right) = \pm 1 \Rightarrow F_p \equiv \pm 1 \pmod{p} \quad \text{and} \quad \beta|(p \mp 1).$$

Recall also that $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) \equiv 5^{\frac{p-1}{2}}$ (mod p). Now we prove that $F_p \equiv \pm 1$ (mod p). We have

$$F_p = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p\right] = \frac{1}{2^{p-1}\sqrt{5}} \sum_{k \text{ odd}}^{p} C_p^k(\sqrt{5})$$

$$= \frac{1}{2^{p-1}}\left(\sum_{k=0}^{\frac{p-3}{2}} C_p^{2k+1}5^k + 5^{\frac{p-1}{2}}\right) = \frac{1}{2^{p-1}}\left(pK + 5^{\frac{p-1}{2}}\right)$$

since $p|C_p^{2k+1}$ for each $k \in \left\{0, 1, \ldots, \frac{p-3}{2}\right\}$. As $2^{p-1} \equiv 1$ (mod p), we have

$$F_p \equiv 5^{\frac{p-1}{2}} \pmod{p},$$

so that $\left(\frac{p}{5}\right) \equiv F_p$ (mod p). When $\left(\frac{5}{p}\right) = 1$, we can give another proof. There exists a ρ such that $\rho^2 \equiv 5$ (mod p). Then, for such a ρ, $\theta = \frac{1}{2}(\rho + 1)$ and $\theta' = \frac{1}{2}(\rho - 1)$ are roots of $x^2 - x - 1 \equiv 0$ (mod p) and thus,

$$\theta^n \equiv \theta^{n-1} + \theta^{n-2}, \quad \theta'^n \equiv \theta'^{n-1} + \theta'^{n-2} \pmod{p}.$$

It is then easily seen that

$$(6.3) \qquad F_n \equiv \frac{1}{\rho}[\theta^n - \theta'^n] \pmod{p}.$$

But, as p is a prime, $\theta^{p-1} \equiv \theta'^{p-1} \equiv 1$ (mod p) by Fermat's theorem. Now from (6.3) it is obvious that

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

Now, to prove that $\beta|(p + 1)$ according that $\left(\frac{5}{p}\right) = -1$, it will suffice to develop F_{p+1} in a way similar to the method used above for F_p.

ACKNOWLEDGMENT

We are grateful to Dr. E. Zeckendorf for his encouragement and fruitful discussions.

REFERENCES

1. J. Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m," *The Fibonacci Quarterly* 1, No. 2 (1963).
2. D. E. Daykin & L. A. G. Dresel, "Factorization of Fibonacci Numbers," *The Fibonacci Quarterly* 8, No. 1 (1970).
3. A. Andreassian, "Fibonacci Sequence Modulo m," *The Fibonacci Quarterly* 12, No. 1 (1974).

*****