$\mathbb{Z}[\varphi]$ AND THE FIBONACCI SEQUENCE MODULO n

SAMIN RIASAT

Abstract. It has long been known that the Fibonacci sequence modulo n is periodic for any integer $n > 1$. In this paper we present an elementary approach of proving properties of this period by working on $\mathbb{Z}[\varphi]$ and also deduce some new results. In the last section a method of proving identities is shown using examples.

1. Periodicity Modulo n

We will use the following notations:

- n is a positive integer.
- F_i is the i-th Fibonacci number, with $F_0 = 0$, $F_1 = 1$ and $F_{i+1} = F_i + F_{i-1}$ for all $i \geq 1$.
- L_i is the i-th Lucas number, with $L_0 = 2$, $L_1 = 1$ and $L_{i+1} = L_i + L_{i-1}$ for all $i \geq 1$.
- $\varphi = \frac{1+\sqrt{5}}{2}$, the golden ratio.

And all congruences are taken modulo n unless otherwise stated.

Definition 1.1. *For $n > 1$, $k(n)$ is the smallest positive index such that $n \mid F_{k(n)}$. We will often denote $k(n)$ simply by k for brevity.*

Example: $k(2) = 3$, $k(10) = 15$ etc.

Definition 1.2. *For $n > 1$, $\ell(n)$ is the length of the period of the Fibonacci sequence modulo n.*

Example: $\ell(2) = 3$, $\ell(10) = 60$ etc.

We also define the integral domain

$$\mathbb{Z}[\varphi] = \{a + b\varphi \mid a, b \in \mathbb{Z}\}$$

and congruence in $\mathbb{Z}[\varphi]$ such that

(i) If 5 is a quadratic residue modulo n, then $a+b\varphi \equiv c+d\varphi \pmod{n} \Leftrightarrow (a-c) \equiv (d-b)\varphi \pmod{n}$.

(ii) If 5 is a quadratic non-residue modulo n, then $a+b\varphi \equiv c+d\varphi \pmod{n} \Leftrightarrow a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$.

The following theorem was stated by Wall in [5].

Theorem 1.3. *The Fibonacci sequence* $\bmod n$ *is periodic.*

Proof. The terms of the Fibonacci sequence $\bmod n$ can take only n possible values, namely $0, 1, \ldots, n-1$. Note that if a sub-sequence F_k, F_{k+1} repeats at some point, the whole sequence will repeat from that point, since $F_{k+2} = F_{k+1} + F_k$ and so on. There are at most n^2 possible choices for the sub-sequence F_k, F_{k+1}. So it must re-appear at some point and hence the sequence will become periodic. □

Corollary 1.4. *Every positive integer divides infinitely many Fibonacci numbers.*

Proof. Since the Fibonacci sequence $\bmod n$ is periodic for every positive integer n, there exists infinitely many positive integers k such that $F_{k+1} \equiv F_{k+2} \equiv 1$. Then $F_k \equiv 1 - 1 = 0$ for all such k and the conclusion follows immediately. □

Proposition 1.5. $\ell(n) = k \cdot \mathrm{ord}_n(F_{k+1})$.

Proof. Since $F_k \equiv 0$, we have $F_{k+1} \equiv F_{k-1} \equiv \lambda$ $(0 \leq \lambda \leq n-1)$ and from the Fibonacci recurrence it follows that $F_{k+i} \equiv \lambda F_i$ for all i. Let $g = \mathrm{ord}_n(\lambda)$. Then by the recursion we obtain

$$F_{gk+1} \equiv F_{gk+2} \equiv \lambda^g \equiv 1.$$

Also, since g is the order, there does not exist $g' < g$ such that $F_{g'k+1} \equiv F_{g'k+2} \equiv \lambda^{g'} \equiv 1$. Hence we conclude that $\ell(n) = gk = k \cdot \mathrm{ord}_n(\lambda)$. □

Corollary 1.6. $n \mid F_m \Leftrightarrow k(n) \mid m$.

Proposition 1.7. $\ell(n) \in \{k, 2k, 4k\}\, \forall n > 1$.

Proof. We will work on $\mathbb{Z}[\varphi]$. Since $F_k \equiv 0$, we have

$$\begin{aligned} & \varphi^k \equiv (1-\varphi)^k \\ \Leftrightarrow \quad & \varphi^{k+1} \equiv \varphi(1-\varphi)^k \\ \Leftrightarrow \quad & \varphi^{k+1} - (1-\varphi)^{k+1} \equiv (1-\varphi)^k(2\varphi - 1) \\ \Leftrightarrow \quad & \varphi^{k+1} - (1-\varphi)^{k+1} \equiv \sqrt{5}\varphi^k \\ \Leftrightarrow \quad & F_{k+1} \equiv \varphi^k \pmod{n}. \end{aligned}$$

On the other hand, using $1 - \varphi = -1/\varphi$ we get

$$\varphi^k \equiv \left(-\frac{1}{\varphi}\right)^k \Rightarrow \varphi^{2k} \equiv (-1)^k \Rightarrow \varphi^{4k} \equiv 1. \tag{1.1}$$

If $\varphi^k \equiv 1$ then $F_{k+1} \equiv 1$ and $\ell(n) = k$. Otherwise, (i) if k is even then $F_{2k+1} \equiv \varphi^{2k} \equiv 1$ which implies $\ell(n) = 2k$. (ii) if k is odd then $F_{4k+1} \equiv \varphi^{4k} \equiv 1$ implying $\ell(n) = 4k$. Hence the conclusion. □

Remark: It is not difficult to see that $\varphi^k = F_k\varphi + F_{k-1}$ holds for all k. Thus $F_{k+1} \equiv F_{k-1} \equiv \varphi^k$ follows from here as well.

From $F_{k+1} \equiv \varphi^k \pmod{n}$ we can propose a new definition for $\ell(n)$:

Definition 1.8. $\ell(n) = \mathrm{ord}_n(\varphi) \quad \forall n > 1$.

Now we present a very short proof of another theorem of Wall in [5].

Theorem 1.9. $\ell(n)$ *is even for* $n > 2$.

Proof. Assume that $\ell(n) \notin \{2k, 4k\}$. Then $\ell(n) = k$ implies $\varphi^k \equiv 1$. Hence $\varphi^{2k} \equiv 1$ and by (1.1), $(-1)^k \equiv 1$. Therefore k is even (since $n > 2$) and the conclusion follows. $\square$

Proposition 1.10. *If $n > 2$ and $k(n)$ is odd, then $\ell(n) = 4k(n)$.*

Proof. From the last theorem it follows that $\ell(n) \neq k$. Suppose that $\ell(n) = 2k$. Then (1.1) implies, $1 \equiv \varphi^{2k} \equiv (-1)^k \equiv -1$, a contradiction. Therefore $\ell(n) = 4k$. $\square$

Now we shall prove the central theorems of this section. From here onwards p will represent a prime.

Theorem 1.11. *If $p > 3, n > 1$ and $n \mid F_p$, then $k(n) = p$ and $\ell(n) = 4p$.*

Proof. It is well known that $\gcd(F_i, F_j) = F_{\gcd(i,j)}$. Hence $\forall i \not\equiv 0 \pmod p$ we have $\gcd(F_p, F_i) = 1$, which implies $\gcd(n, F_i) = 1$. Thus we conclude that p is the smallest positive integer such that $n \mid F_p$, i.e. $k(n) = p$. Since $3 \nmid p$, F_p is odd, implying n is odd, and so $n > 2$. Since $k(n)$ is odd, by **Proposition 1.10** we conclude that $\ell(n) = 4p$. $\square$

Theorem 1.12. *If n is prime and $p > 3$, then $\ell(n) = 4p \Leftrightarrow n \mid F_p$.*

Proof. Using **Theorem 1.11**, we need only prove that $\ell(n) = 4p \Rightarrow n \mid F_p$. From **Proposition 1.7** we have $4p \in \{k(n), 2k(n), 4k(n)\}$. Hence $k(n) \in \{p, 2p, 4p\}$. If $k(n) = p$ we are done. So assume that $k(n) = 2p$. Since $n \mid F_{2p} = F_p L_p$ and $n \nmid F_p$ we must have $n \mid L_p = \varphi^p + (-1/\varphi)^p$. Therefore $\varphi^{2p} \equiv 1$, which implies $\ell(n) = 2p$, contradiction.

Now suppose that $k(n) = 4p$. This implies $n \mid F_{4p} = F_{2p} L_{2p}$ and since $n \nmid F_{2p}$, $n \mid L_{2p} = \varphi^{2p} + (-1/\varphi)^{2p}$. But then $\varphi^{4p} \equiv -1$, contradiction. Therefore $k(n) = p$. $\square$

Theorem 1.13. *If q is a prime and $p > 3$, then $\ell(q^n) = 4p \Leftrightarrow q^n \mid F_p$.*

Proof. $q \neq 2$; otherwise $3 = \ell(2) \mid \ell(2^n) = 4p$, which contradicts $p > 3$. Thus q is odd. Now $L_i = F_{i+1} + F_{i-1}$ implies $\gcd(F_i, L_i) \in \{1, 2\}\, \forall i$. The rest of the proof is similar to that of **Theorem 1.12**. $\square$

Theorem 1.14. *If $p > 3$ and $\ell(n) = 4p$, then n has a prime factor q with multiplicity $r \geq 1$ such that $q^r \mid F_p$.*

Proof. Let $n = p_1^{a_1} \cdots p_j^{a_j}$ be the prime factorization of n. Then

$$\ell(n) = \operatorname{lcm}(\ell(p_1^{a_1}), \ldots, \ell(p_j^{a_j})) = 4p. \tag{1.2}$$

Therefore $\ell(p_i^{a_i}) \in \{2, 4, p, 2p, 4p\}\, \forall i$. But there is no x such that $\ell(x) \in \{2, 4, p\}$. Hence $\ell(p_i^{a_i}) \in \{2p, 4p\}\, \forall i$. If $\ell(p_i^{a_i}) = 4p$ for some i, we are done by **Theorem 1.13**. Otherwise, $\ell(p_i^{a_i}) = 2p\, \forall i$, which implies from (1.2) $\ell(n) = 2p$, a contradiction. Hence the result. $\square$

As a consequence of these results we arrive at the following conclusion.

Proposition 1.15. *If q is an odd prime and $r \geq 2$, then the following statements are equivalent, and they imply that q is a Wall-Sun-Sun prime.*

(i) $q^r \mid F_p$.

(ii) $k(q^r) = k(q^{r-1}) = \cdots = k(q^2) = k(q) = p$.

(iii) $\ell(q^r) = \ell(q^{r-1}) = \cdots = \ell(q^2) = \ell(q) = 4p$.

Proof. The above theorems imply that (i), (ii) and (iii) are equivalent. On the other hand, it is well known that $q \mid F_{q-\left(\frac{q}{5}\right)}$ for all odd primes q, where $\left(\frac{a}{b}\right)$ is the *Legendre symbol*. Since p is the smallest index such that $q \mid F_p$, we must have $p \mid q - \left(\frac{q}{5}\right)$ i.e. $F_p \mid F_{q-\left(\frac{q}{5}\right)}$. Therefore $q^2 \mid q^r \mid F_p \mid F_{q-\left(\frac{q}{5}\right)}$, implying q must be a Wall-Sun-Sun prime, as desired. □

It should, however, be noted that no prime p has yet been found such that $q^2 \mid F_p$, and the results obtained above may suggest a possible approach for investigating the existence of such primes.

2. The Range of ℓ

In 1913, R. D. Carmichael proved the following theorem:

Theorem 2.1. *Every Fibonacci number except F_1, F_2, F_6 and F_{12} has a prime divisor which does not divide any smaller Fibonacci number. Such prime divisors are called characteristic divisors.*

Based on this result let us attempt to find X, the range of ℓ.

Proposition 2.2. $\ell(2) = 3$ *is the only odd element of X.*

Proof. This follows directly from **Theorem 1.9**. □

Proposition 2.3. $8n + 4 \in X \, \forall n$.

Proof. For $n = 1$ we have $\ell(8) = 12$. Otherwise, let p be a characteristic divisor of F_{2n+1}. Then $k(p) = 2n+1$ and from **Proposition 1.10**, $\ell(p) = 4(2n+1) = 8n+4$, as desired. □

Proposition 2.4. $4n + 2 \in X \, \forall n$.

Proof. For $n = 1$ we have $\ell(4) = 6$. Otherwise, let p be a characteristic divisor of $F_{4n+2} = F_{2n+1}L_{2n+1}$. Then $p \mid L_{2n+1} = \varphi^{2n+1} + (-1/\varphi)^{2n+1}$ which implies $\varphi^{4n+2} \equiv 1 \pmod{p}$. Thus $\ell(p) = 4n + 2$. □

Proposition 2.5. $8n \in X \, \forall n$.

Proof. For $n = 3$ we have $\ell(6) = 24$. Otherwise, let p be a characteristic divisor of $F_{4n} = F_{2n}L_{2n}$. Then $p \mid L_{2n} = \varphi^{2n} + (-1/\varphi)^{2n}$ which implies $\varphi^{4n} \equiv -1 \pmod{p}$. Thus $\varphi^{8n} \equiv 1 \pmod{p}$ and we conclude that $\ell(p) = 8n$. □

The above results may be summarized into the following theorem:

Theorem 2.6. *The elements of X are precisely* 3 *and all even numbers* > 4.

3. Proving Identities

In this section we will extensively use the following facts, which are very easy to prove, to prove some identities.

If a, b, c, d are integers then

- $a + b\varphi = c + d\varphi \Leftrightarrow a = b,\ c = d$.
- $(a + b\varphi) + (c + d\varphi) = e + f\varphi$ for integers e, f such that $e = a + c, f = b + d$.
- $(a+b\varphi)(c+d\varphi) = k+l\varphi$ for integers k, l such that $k = ac+bd, l = ad+bc+bd$.
- $\varphi^n = F_n\varphi + F_{n-1}$.

Identity 3.1.

$$\sum_{i=1}^{n} F_n = F_{n+2} - 1. \tag{3.1}$$

Proof. Let $S_n = \sum_{i=1}^{n} F_n$. We have

$$\begin{aligned} \frac{\varphi^{n+1} - 1}{\varphi - 1} - 1 &= \sum_{k=1}^{n} \varphi^k \\ &= \sum_{k=1}^{n} (F_k\varphi + F_{k-1}) \\ &= S_n\varphi + S_{n-1}. \end{aligned}$$

On the other hand, $\varphi^{n+1} - 1 = F_{n+1}\varphi + F_n - 1$. Hence

$$\begin{aligned} & \frac{F_{n+1}\varphi + F_n - 1}{\varphi - 1} = S_n\varphi + S_{n-1} + 1 \\ \Leftrightarrow\quad & F_{n+1}\varphi + F_n = S_n(\varphi^2 - \varphi) + (S_{n-1} + 1)\varphi - S_{n-1} \\ \Leftrightarrow\quad & F_{n+1}\varphi + F_n = (S_{n-1} + 1)\varphi + S_n - S_{n-1}. \end{aligned}$$

Therefore we conclude that $S_{n-1} + 1 = F_{n+1}$, as desired. □

Identity 3.2.

$$F_{m+n-1} = F_mF_n + F_{m-1}F_{n-1}, \quad \textit{or}, \quad F_{m+n} = F_mF_{n+1} + F_{m-1}F_n. \tag{3.2}$$

Proof. Since $\varphi^{m+n} = \varphi^m \cdot \varphi^n$, we get

$$\begin{aligned} & F_{m+n}\varphi + F_{m+n-1} \\ =& (F_m\varphi + F_{m-1})(F_n\varphi + F_{n-1}) \\ =& (F_mF_n + F_{m-1}F_n + F_mF_{n-1})\varphi + F_mF_n + F_{m-1}F_{n-1} \\ =& (F_mF_{n+1} + F_{m-1}F_n)\varphi + F_mF_n + F_{m-1}F_{n-1}. \end{aligned}$$

Hence (3.2) follows. □

Identity 3.3.

$$F_{kn+c} = \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} F_{c+i}. \tag{3.3}$$

Proof. From $\varphi^{kn+c} = (\varphi^k)^n \cdot \varphi^c$, we can write

$$\begin{aligned}
F_{kn+c}\varphi + F_{kn+c-1} &= (F_k\varphi + F_{k-1})^n \cdot \varphi^c \\
&= \left(\sum_{i=0}^{n} \binom{n}{i} F_k^i \varphi^i F_{k-1}^{n-i}\right) \varphi^c \\
&= \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} \varphi^{c+i} \\
&= \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} (F_{c+i}\varphi + F_{c+i-1}) \\
&= \varphi \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} F_{c+i} + \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} F_{c+i-1}
\end{aligned}$$

Thus

$$F_{kn+c} = \sum_{i=0}^{n} \binom{n}{i} F_k^i F_{k-1}^{n-i} F_{c+i}.$$

□

It is clear that many other identities, if not all, can be proven in similar ways, and new identities may as well be deduced. Finally, the methods discussed here can easily be generalized to other Fibonacci-like sequences.

References

[1] Wikipedia, *Fibonacci number*, http://en.wikipedia.org/wiki/Fibonacci_number
[2] Wikipedia, *Pisano period*, http://en.wikipedia.org/wiki/Pisano_period
[3] Mathworld, *Pisano period*, http://mathworld.wolfram.com/PisanoPeriod.html
[4] Wikipedia, *Carmichael's theorem*, http://en.wikipedia.org/wiki/Carmichael's_theorem
[5] D. D. Wall, *Fibonacci Series Modulo m*, American Mathematical Monthly **67** (1960), 525–532.

Samin Riasat, University of Dhaka, Bangladesh
E-mail address: `nayel71@gmail.com`