# 4 Linear Recurrence Relations & the Fibonacci Sequence

Recall the classic example of the Fibonacci sequence $(F_n)_{n=1}^{\infty} = (1, 1, 2, 3, 5, 8, 13, 21, \dots)$, defined by

$$\begin{cases} F_{n+2} = F_{n+1} + F_n \\ F_1 = F_2 = 1 \end{cases}$$

This sequence has well-known relations to population growth (famously breeding rabbits), spirals in the center of sunflowers, etc. From a number theory perspective, we have two main questions:

1. How do we find a formula for the $n^{\text{th}}$ Fibonacci number? More generally, how do we solve linear recurrence relations?
2. Does the Fibonacci sequence satisfy any interesting patterns when we consider its remainders modulo an integer?

## 4.1 Linear Recurrence Relations

The general theory of linear recurrences is analogous to that of linear differential equations.

**Definition 4.1.** A sequence $(x_n)_{n=1}^{\infty}$ satisfies a *linear recurrence relation of order* $r \in \mathbb{N}$ if there exist $a_0, \dots, a_r, f$ with $a_0, a_r \not\equiv 0$ such that

$$\forall n \in \mathbb{N}, \quad a_r x_{n+r} + a_{r-1} x_{n+r-1} + \cdots + a_0 x_n = f$$

The definition is malleable: in particular

- The sequence could start with $x_0$, or anywhere else;
- The coefficients $a_k$ are generally functions, though for us they will usually be *constant*;
- If $f \equiv 0$, the recurrence is *homogeneous*; this is usually be the case for us.

**Example 4.2.** Consider the linear recurrence $x_{n+1} = 2x_n - 1$ with initial condition $x_1 = 2$. A simple approach might be to list the values of $x_n$ and try to spot a pattern:

$$(x_n) = (2, 3, 5, 9, 17, 33, 65, 129, \dots)$$

Since the ratio $\frac{x_{n+1}}{x_n}$ appears to be approaching 2, we might guess that $x_n = \alpha \cdot 2^n + \beta$ for some constants $\alpha, \beta$. Substituting this into the original recurrence, we see that

$$\alpha \cdot 2^{n+1} + \beta = \alpha \cdot 2^{n+1} + 2\beta - 1 \iff \beta = 2\beta - 1 \iff \beta = 1$$

But then $x_1 = 2\alpha + 1 = 2 \iff \alpha = \frac{1}{2}$. The solution is therefore

$$x_n = \frac{1}{2} \cdot 2^n + 1 = 2^{n-1} + 1$$

If this ad hoc approach makes you uncomfortable, prove by induction that this really is the solution.

We will give some of the discussion in the language of second-degree equations. The proofs are simple exercises, and it should be obvious how the theory extends to recurrences of other orders.

**Theorem 4.3.** *Consider the second-order recurrence $ax_{n+2} + bx_{n+1} + cx_n = f$.*

1. *Given initial conditions $x_1, x_2$, there exists a unique solution $x_n$.*

2. *If $x_n^{(p)}$ is a fixed solution to the recurrence, then all solutions have the form $x_n = x_n^{(c)} + x_n^{(p)}$ where $x_n^{(c)}$ satisfies the associated homogeneous equation*[a]

$$ax_{n+2} + bx_{n+1} + cx_n = 0 \tag{$*$}$$

3. *The solutions to $(*)$ form a two-dimensional vector space: given linearly independent solutions $y_n$ and $z_n$, there exist unique constants $\alpha, \beta$ such that*

$$x_n = \alpha y_n + \beta z_n$$

4. *If $a, b, c$ are constant, the* characteristic equation *of $(*)$ is the quadratic $a\lambda^2 + b\lambda + c = 0$. There are two cases, dependent on the roots $\lambda_1, \lambda_2$:*

   (a) *If $\lambda_1 \neq \lambda_2$, then the general solution is $x_n = \alpha\lambda_1^n + \beta\lambda_2^n$*

   (b) *If $\lambda_1 = \lambda_2$, then the general solution is $x_n = (\alpha + \beta n)\lambda_1^n$*

[a] $x^{(p)}$ and $x^{(c)}$ should recall the *particular solution* and *complementary function* from differential equations.

**Example (4.2, mk. II).** In the context of the Theorem:

- $x_n^{(c)} = \alpha \cdot 2^n$ is the general solution to the homogeneous relation $x_{n+1} - 2x_n = 0$ with characteristic equation $\lambda - 2 = 0$.

- $x_n^{(p)} = 1$ is a single solution to the full recurrence $x_{n+1} = 2x_n - 1$.

- The general solution is $x_n = \alpha \cdot 2^n + 1$; applying the initial condition $x_1 = 2$ yields $\alpha = 1$.

For us, the important case is the Fibonacci sequence: the characteristic equation is

$$\lambda^2 - \lambda - 1 = 0 \implies \lambda = \frac{1 \pm \sqrt{5}}{2} = \phi, \hat{\phi}$$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio and $\hat{\phi} = \frac{1-\sqrt{5}}{2} = -\frac{1}{\phi}$. Choosing the constants such that $F_1 = F_2 = 1$, we conclude,

**Theorem 4.4 (Binet's Formula).** *Fhe Fibonacci sequence has $n^{th}$ term*

$$F_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}} = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

**Exercises** 1. Solve the homogeneous recurrence relation

$$\begin{cases} x_{n+2} - 4x_{n+1} + 4x_n = 0 \\ x_1 = 1, \ x_2 = -4 \end{cases}$$

2. Find a particular solution of the form $x_n^{(p)} = dn + e$ to the relation

$$\begin{cases} x_{n+2} - 4x_{n+1} + 4x_n = n \\ x_1 = 1, \ x_2 = -4 \end{cases}$$

   Using your answer to the previous question, find the general solution to the full recurrence.

   (*This is precisely the method of undetermined coefficients as seen in differential equations*)

3. Find the general solution to the recurrence relation

$$\begin{cases} x_{n+2} - 2x_{n+1} + 2x_n = 0 \\ x_1 = 1, \ x_2 = 0 \end{cases}$$

   (*The characteristic equation has complex roots: this is no matter! If you want a challenge, write your answer using binomial coefficients...*)

4. Prove all parts of Theorem 4.3.
   (*Hint: for part 3, consider* $w_n := x_n - \alpha y_n - \beta z_n$ *where* $\binom{\alpha}{\beta} = \begin{pmatrix} y_1 & z_1 \\ y_2 & z_2 \end{pmatrix}^{-1} \binom{x_1}{x_2}$)

### 4.2 The Fibonacci Sequence in $\mathbb{Z}_m$

If a solution to a recurrence relation is in integers, one can ask if there are any patterns with respect to a given modulus. It should be clear that any recurrence of the form

$$x_{n+2} = ax_{n+1} + bx_n$$

where $a, b \in \mathbb{Z}$ and with initial conditions $x_1, x_2 \in \mathbb{Z}$ necessarily produces a sequence of integers. The Fibonacci sequence ($a = b = x_1 = x_2 = 1$) is one of the simplest such, so we begin by hunting for patterns.

| | | | |
|---|---|---|---|
| $F_n$ | mod 2 | 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, ... | Period 3 |
| $F_n$ | mod 3 | 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, ... | Period 8 |
| $F_n$ | mod 4 | 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, ... | Period 6 |
| $F_n$ | mod 5 | 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, ... | Period 20 |
| $F_n$ | mod 6 | 1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1, ... | Period 24 |
| $F_n$ | mod 7 | 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, ... | Period 16 |
| $F_n$ | mod 8 | 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, ... | Period 12 |
| $F_n$ | mod 9 | 1, 1, 2, 3, 5, 8, 4, 3, 7, 1, 8, 0, 8, 8, 7, 6, 4, 1, 5, 6, 2, 8, 1, 0, 1, 1, ... | Period 24 |

As soon as we see a pair of 1's we know that the sequence repeats. Does this always happen? Are there any patterns in the periods? Can you guess what the period is modulo 10?

**Theorem 4.5.** *The Fibonacci sequence in $\mathbb{Z}_m$ is periodic.*

*Proof.* This is a simple box-principle argument. Let $\{(F_n, F_{n+1}) : n \in \mathbb{N}\}$ be the set of pairs of consecutive Fibonacci numbers modulo $m$. This is a subset of $\mathbb{Z}_m \times \mathbb{Z}_m$ (cardinality $m^2$). Since the sequence is infinite, the box-principle tells us that at least one pair occurs infinitely many times:

$$\exists n, N \in \mathbb{N} \text{ such that } F_n \equiv F_{n+N} \text{ and } F_{n+1} \equiv F_{n+1+N} \pmod{m} \tag{†}$$

Since the defining recurrence relation is second-order, the pairs $(F_n, F_{n+1})$ and $(F_{n+N}, F_{n+1+N})$ generate the *same sequence* modulo $m$. It follows that $(F_n)$ is eventually periodic.

To see that the entire sequence is periodic, observe that we can write

$$F_{n-1} = F_{n+1} - F_n$$

This defines the sequence in reverse, starting from any pair. In particular, the reverse sequences starting from the pairs $(F_n, F_{n+1})$ and $(F_{n+N}, F_{n+1+N})$ in (†) are identical, whence the periodicity continues back to the initial pair $(F_1, F_2)$. ∎

**Definition 4.6.** Denote by $N(m)$ the period of the Fibonacci sequence modulo $m$; that is, the value of the *smallest* $N$ such that $F_{N+1} \equiv F_{N+2} \equiv 1 \pmod{m}$.

By looking for patterns in the above table, you might hypothesize some elementary properties.

**Theorem 4.7.**
1. *$F_{k+S} \equiv F_k \pmod{m}, \forall k \in \mathbb{N} \iff N(m) \mid S$.*
2. *For any $m, n$ we have $N(m) \mid N(mn)$.*
3. *If $\gcd(m,n) = 1$ then $N(mn) = \operatorname{lcm}\big(N(m), N(n)\big)$.*

*Proof.*
1. The ($\Leftarrow$) direction is trivial. The ($\Rightarrow$) is just the division algorithm: there exist unique $q, r \in \mathbb{Z}$ such that

   $$S = qN(m) + r, \quad 0 \le r < N(m)$$

   from which the minimality of $N(m)$ forces $r = 0$.

2. For any $k, m, n$, we have

   $$F_{k+N(mn)} \equiv F_k \pmod{mn} \implies F_{k+N(mn)} \equiv F_k \pmod{m}$$

   By part 1, we conclude that $N(m) \mid N(mn)$.

3. When $\gcd(m,n) = 1$, observe

   $$F_{k+N} \equiv F_k \pmod{mn} \iff \begin{cases} F_{k+N} \equiv F_k \pmod{m} & \text{and,} \\ F_{k+N} \equiv F_k \pmod{n} \end{cases}$$

   Suppose this holds for all $k$. By definition $N = N(mn)$ is the least positive integer satisfying the LHS. By part 2, $\operatorname{lcm}(N(m), N(n))$ is the least positive integer satisfying the RHS. ∎

Remarkably, even for such a simple sequence, the period $N(m)$ is not fully understood.

**Conjecture 4.8.** *$N(p^n) = p^{n-1}N(p)$ when $p$ is prime: no counter-example has been found among all primes $p < 2.8 \times 10^{16}$.*

Using this, one could, for example, compute

$$N(2304) = N(2^8 \cdot 3^2) = \operatorname{lcm}(2^7 N(2), 3N(3)) = \operatorname{lcm}(128 \cdot 3, 3 \cdot 8) = 384$$

**Binet's formula modulo $p$**

For roughly half the primes, we can obtain a modular version of Binet's formula.

**Theorem 4.9.** *If $p$ is a prime congruent to either 1 or 4 modulo 5 (equivalently $p \equiv \pm 1 \mod 10$), then $\exists c \in \mathbb{Z}_p^\times$ such that*

$$\forall n \in \mathbb{N},\ F_n \equiv c^{-1}\left[\left(\frac{1+c}{2}\right)^n - \left(\frac{1-c}{2}\right)^n\right] \pmod{p}$$

*Proof.* The idea is to look for a value $c$ that plays the role of $\sqrt{5}$: otherwise said, we want $c^2 \equiv 5$ modulo $p$. Computing Legendre symbols and recalling quadratic reciprocity, we see that

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = 1$$

The congruence $c^2 \equiv 5$ therefore has a solution, which we may assume is odd, for otherwise we could choose the other solution $p - c$. Now define the sequence

$$J_n \equiv c^{-1}\left[\left(\frac{1+c}{2}\right)^n - \left(\frac{1-c}{2}\right)^n\right] \pmod{p}$$

It is easily checked that $J_n \equiv J_{n-1} + J_{n-2}$ and $J_1 \equiv J_2 \equiv 1$, whence $J_n \equiv F_n$ modulo $p$. ■

It is easy to see that $\frac{1\pm c}{2}$ are both non-zero modulo $p$, so we always get both terms in Binet's formula.

**Example 4.10.** If $p = 11$, then $c^2 \equiv 5 \iff c^2 \equiv 16 \iff c \equiv \pm 4$. We choose $c = 7$, which yields $c^{-1} \equiv 8$. Therefore

$$F_n \equiv 8(4^n - 8^n) \equiv 3(8^n - 4^n) \pmod{11}$$

Binet's formula gives us more: by Fermat's Little Theorem,

$$F_{n+10} \equiv 3(8^{n+10} - 4^{n+10}) \equiv 3(8^n - 4^n) \equiv F_n \pmod{11}$$

whence the period $N(11)$ divides 10. This is true in general. . .

**Theorem 4.11.** *Let $p$ be a prime congruent to either 1 or 4 modulo 5. Then $N(p) \mid p - 1$.*

*Proof.* Write $\alpha := \frac{1+c}{2}$ and $\beta := \frac{1-c}{2}$ to obtain

$$F_{n+(p-1)k} \equiv c^{-1}\left[\alpha^n\alpha^{(p-1)k} - \beta^n\beta^{(p-1)k}\right] \equiv c^{-1}\left[\alpha^n - \beta^n\right] \equiv F_n \pmod p$$

since $\alpha, \beta \not\equiv 0$. By Theorem 4.7, we conclude $N(p) \mid p-1$. ∎

It is harder to prove, but the following can also be shown:

- If $p \equiv 2, 3$ modulo 5, then $N(p) \mid 2p+2$. We shouldn't expect a discrete version of Binet's formula since there are no values $c$ which satisfy $c^2 \equiv 5$.
- $N(m) \begin{cases} = 6m & \text{if } m = 2 \cdot 5^k \text{ for some } k \geq 1 \\ \leq 4m & \text{otherwise} \end{cases}$

**Other Recurrence Relations: Lucas Sequences**

It is reasonable to ask if the solution to *any* linear constant coefficient recurrence relation is periodic modulo $m$. Suppose that the recurrence has order $r$ and that

$$x_{n+r} + a_{r-1}x_{n+r-1} + \cdots + a_1x_{n+1} + a_0x_n = 0$$

has *integer* coefficients $a_k$. By considering the $r$-tuples

$$(x_N, x_{N+1}, \ldots, x_{N+r-1})$$

modulo $m$ and applying the box-principle argument of Theorem 4.5, we see that any solution is therefore *eventually periodic* modulo $m$: with a trivial modification, the gcd result (Theorem 4.7) also holds. We don't necessarily get full periodicity however, for example

$$\begin{cases} x_{n+1} = 2x_n \\ x_1 = 1 \end{cases} \implies (x_n) \equiv (1, 2, 0, 0, 0, 0, 0, 0, 0, \ldots) \pmod 4$$

To obtain full periodicity, it is enough that $a_0$ be a unit modulo $m$.

Several generalizations of the Fibonacci sequence are important in number theory. In particular:

**Definition 4.12.** A *Lucas sequence* $(x_n)$ is a solution to the recurrence $x_{n+2} = Px_{n+1} - Qx_n$, where $P$ and $Q$ are given integers. It is typical to start these sequences from $x_0$ and to consider two independent solutions

- $U(P, Q)$ satisfies $(x_0, x_1) = (0, 1)$
- $V(P, Q)$ satisfies $(x_0, x_1) = (2, P)$

The Fibonacci sequence is therefore $U(1, -1)$. In line with the above discussion, these sequences are eventually periodic modulo $m$ and the gcd theorem for periods also holds. Most examples seem to satisfy $N(p^k) = p^{k-1}N(p)$, although counter-examples are known (Exercise 4.2.6).

**Example 4.13.** The Lucas sequences $U(2,-1)$ and $V(2,-1)$ are known, respectively, as the *Pell numbers* and *Pell-Lucas numbers*. If we write the first few,

$$U_{n+1} = 2U_n + U_{n-1}, \quad U_0 = 0,\ U_1 = 1$$
$$V_{n+1} = 2V_n + V_{n-1}, \quad V_0 = 2,\ V_1 = 2$$

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $U_n(2,-1)$ | 0 | 1 | 2 | 5 | 12 | 29 | 70 | 169 |
| $V_n(2,-1)$ | 2 | 2 | 6 | 14 | 34 | 82 | 198 | 478 |

you should start to see the pattern: the ratio $\frac{\frac{1}{2}V_n}{U_n} = \frac{p_n}{q_n}$ is the sequence of convergents of the continued fraction $\sqrt{2} = [1, 2, 2, 2, 2, 2, \ldots]$.

**Exercises** 1. Consider the recurrence $x_{n+1} = 2x_n$.

(a) Solve this modulo 4, given *any* initial condition $x_1 \equiv a$: what do you observe?

(b) Solve the congruence modulo 5 with the initial condition $x_1 = 1$: what happens this time?

2. Solve the following linear recurrence relations using the characteristic equation method.

(a) $a_n = 3a_{n-1} + 10a_{n-2}, \quad a_1 = 1,\ a_2 = 3$

(b) $b_n = 2b_{n-1} - 5b_{n-2}, \quad b_1 = 1,\ b_2 = -3$

(c) $c_n = 4c_{n-1} - c_{n-2} - 6c_{n-3}, \quad c_1 = 0,\ c_2 = 0,\ c_3 = 1$

3. For each of the recurrences in the previous question, find the (eventual) periods modulo 2, modulo 3 and modulo 6. Check that $N(2 \cdot 3) = \operatorname{lcm}(N(2), N(3))$ in each case.

4. Find a Binet-type formula for the Fibonacci sequence modulo 19.

5. Let $(F_n)$ be the Fibonacci sequence.

(a) Prove that for all $n \geq k+2$ we have $F_n = F_{k+1}F_{n-k} + F_kF_{n-k-1}$

(b) Prove that $F_k \mid F_{2k}$ for all $k$.

(c) More generally, prove that $k \mid n \implies F_k \mid F_n$.

(d) Make a hypothesis and prove it: If $F_n$ is prime, then $n$ is…

6. Write a program or use a computer algebra package to find the period of the Lucas sequence with $(P, Q) = (2, -1)$ modulo 13 and modulo $169 = 13^2$. Hence show that $N(p^k)$ need not equal $p^{k-1}N(p)$.

7. (a) Suppose that $\lambda$ and $\mu$ are distinct roots of the characteristic equation for the Lucas sequences $(U_n)$ and $(V_n)$. Prove that

$$U_n = \frac{\lambda^n - \mu^n}{\lambda - \mu} \quad \text{and} \quad V_n = \lambda^n + \mu^n$$

(b) What are the solutions if the roots are repeated; that is, if $P^2 = 4Q$?

8. (a) Solve the recurrence relations for the Pell numbers and the Pell-Lucas numbers $U_n, V_n$.

(b) Use part (a) to find an explicit expression for the $n^{\text{th}}$ convergent of $\sqrt{2}$ and an alternative proof that the convergents really do converge to $\sqrt{2}$.

(c) For which primes $p$ will it be possible to find an explicit Binet-type formula for $U_n$ and $V_n$ modulo $p$? Find an explicit formula modulo $p = 7$.
(*Hint: think about quadratic residues*)

(d) Compute the periods of $U_n$ and $V_n$ modulo 2, 3, 5, and 7. What do you expect the period modulo 210 to be? If you have the time, check it!