4 Linear Recurrence Relations & the Fibonacci Sequence

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

\[
\begin{align*}
F_{n+2} &= F_{n+1} + F_n \\
F_1 &= F_2 = 1
\end{align*}
\]

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

1. How do we find a formula for the \( n \)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 (Some of) The Theory of Linear Recurrence Relations

**Definition 4.1.** A sequence \((x_n)_{n=1}^{\infty}\) of complex numbers satisfies a **linear recurrence relation of degree** \( r \in \mathbb{N} \) if, there exist functions \( a_0, \ldots, a_{r-1}, c \) with domain \( \mathbb{N} \) and a family of linear relations

\[
x_{n+r} + a_{r-1}(n)x_{n+r-1} + \cdots + a_0(n)x_n = c(n)
\]

satisfied for each \( n \in \mathbb{N} \).

There is nothing stopping us from changing the indices to have a sequence start at \( x_0 \), or anywhere else for that matter. In our examples, the coefficient functions will almost always be constants.

**Examples**

1. The Fibonacci sequence satisfies a linear recurrence of degree two.
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:

\[
(x_n) = (2, 3, 5, 9, 17, 33, 65, 129, \ldots)
\]

Observe that the ratio \( \frac{x_{n+1}}{x_n} \) appears to be approaching 2. We might guess therefore 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 \( x_1 = 2\alpha + 1 = 2 \iff \alpha = \frac{1}{2} \). Our solution is then

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

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

\(^1\)Typically real numbers or, for us, integers.
The general theory of solving linear recurrences is entirely analogous to that of linear differential equations, but the theorems are significantly easier to prove! We will give some of the discussion in the language of second-degree equations, though it should be obvious how the theory extends for higher-degree. Moreover, for a first-degree recurrence, only part 1 is strictly relevant.

Viewing the above example in the context of part 2 of the Theorem, note that
\[ x_n = x_1 2^n \]
is the general solution to the homogeneous relation \( x_{n+1} = 2x_n \) while \( x_n = 1 \) is a single solution to the full recurrence \( x_{n+1} = 2x_n - 1 \).

**Theorem 4.2.** Suppose that \( x_{n+2} + a(n)x_{n+1} + b(n)x_n = c(n) \) is a second-degree linear recurrence relation.

1. Given any values \( x_1, x_2 \), there is a unique solution \( (x_n)_{n=1}^\infty \).

2. If \((y_n)\) and \((z_n)\) are any two solutions, their difference \((y_n - z_n)\) is a solution to the associated homogeneous equation
   \[ x_{n+2} + a(n)x_{n+1} + b(n)x_n = 0 \]  

3. Let \((y_n)\) and \((z_n)\) be the solutions to (*) satisfying the initial conditions \((y_1, y_2) = (1, 0)\) and \((z_1, z_2) = (0, 1)\) respectively. The set of all solutions to (*) forms a two-dimensional vector space spanned by \((y_n)\) and \((z_n)\). Otherwise said, every solution is a linear combination
   \[ x_n = py_n + qz_n \]
   for unique constants \( p, q \in \mathbb{C} \). Indeed \( p = x_1 \) and \( q = x_2 \) are the first two terms of the sequence \((x_n)\).

**Proof.** Part 1 should be clear, while part 2 is a simple calculation: you should have seen an analogous result in a differential equations class.

For part 3: suppose \((x_n)\) is a solution and \((y_n), (z_n)\) are as defined. Compute the sequence
\[ w_n := x_n - x_0 y_n - x_1 z_n \]

It is clear that \( w_1 = w_2 = 0 \) and that \((w_n)\) satisfies
\[ w_{n+2} = -a(n)w_{n+1} - b(n)w_n, \quad \forall n \in \mathbb{N} \]

By induction we see that \( w_n = 0 \) for all \( n \).

### 4.2 Constant Coefficient Recurrences

Just as for linear differential equations, the theory is even simpler if the coefficients are constant…

**Theorem 4.3.** Suppose \( x_{n+2} + ax_{n+1} + bx_n = 0 \) is a constant coefficient homogeneous recurrence relation. Let \( \lambda_1, \lambda_2 \) be the roots, up to multiplicity, of the characteristic equation
\[ \lambda^2 + a\lambda + b = 0 \]

We have two cases: here \( \alpha, \beta \) are arbitrary constants.

1. If \( \lambda_1 \neq \lambda_2 \), then the general solution is
   \[ x_n = \alpha \lambda_1^n + \beta \lambda_2^n \]

2. If \( \lambda_1 = \lambda_2 \), then the general solution is
   \[ x_n = (\alpha + \beta n)\lambda_1^n \]
Examples

1. Solve the homogeneous recurrence relation

\[
\begin{align*}
x_{n+2} - 4x_{n+1} + 4x_n &= 0 \\
x_1 &= 1, \quad x_2 = -4
\end{align*}
\]

The characteristic equation \(\lambda^2 - 4\lambda + 4 = 0\) has repeated root \(\lambda = 2\) and thus the homogeneous equation has general solution

\[x_n = (\alpha + \beta n)2^n\]

Applying the initial conditions gives us

\[
\begin{align*}
1 &= 2(\alpha + \beta) \\
-4 &= 4(\alpha + 2\beta)
\end{align*} \implies \alpha = 2, \beta = -\frac{3}{2} \implies x_n = (3 - 2n)2^n
\]

2. Solve a similar recurrence relation to part (a):

\[
\begin{align*}
x_{n+2} - 4x_{n+1} + 4x_n &= n \\
x_1 &= 1, \quad x_2 = -4
\end{align*}
\]

We have the same homogeneous solution as in (a). For a particular solution, guess \(x_n = an + b\)

Substituting into the recurrence, we obtain

\[n = a(n + 2) + b - 4(a(n + 1) + b) + 4(an + b) = an - 2a + b \implies a = 1, \ b = 2\]

The general solution is then

\[x_n = (\alpha + \beta n)2^n + n + 2\]

which, after applying the initial conditions gives us

\[
\begin{align*}
1 &= 2(\alpha + \beta) + 3 \\
-4 &= 4(\alpha + 2\beta) + 4
\end{align*} \implies \alpha = 0, \beta = -1 \implies x_n = n + 2 - n2^n
\]

3. Solve the recurrence relation

\[
\begin{align*}
x_{n+2} - 2x_{n+1} + 2x_n &= 0 \\
x_1 &= 1, \quad x_2 = 0
\end{align*}
\]

The characteristic equation \(\lambda^2 - 2\lambda + 2 = 0\) has roots \(\lambda = 1 \pm i\), whence the solution to the homogeneous equation is

\[x_n = \alpha(1 + i)^n + \beta(1 - i)^n\]

The initial conditions yield

\[
\begin{align*}
1 &= \alpha(1 + i) + \beta(1 - i) \\
0 &= 2i\alpha - 2i\beta
\end{align*} \implies \alpha = \beta = \frac{1}{2} \implies x_n = \frac{1}{2} [(1 + i)^n + (1 - i)^n]
\]

\[\text{This is precisely the method of undetermined coefficients as seen in ODEs: if the right hand side is a polynomial in } n, \text{ guess an arbitrary polynomial of the same degree.}\]
The Fibonacci Sequence and Binet’s Formula

We apply the above discussion to the Fibonacci sequence: the characteristic equation is

\[ \lambda^2 = \lambda + 1 \implies \lambda = \frac{1 \pm \sqrt{5}}{2} = \phi, \hat{\phi} \]

where we use \( \phi = \frac{1 + \sqrt{5}}{2} \) to represent the golden ratio, and \( \hat{\phi} = \frac{1 - \sqrt{5}}{2} = -\frac{1}{\phi} \). Choosing the constants to force \( F_1 = F_2 = 1 \), we conclude:

**Theorem 4.4** (Binet’s Formula). If \( (F_n)_{n=1}^\infty = (1, 1, 2, 3, 5, 8, 13, \ldots) \) is the Fibonacci sequence, then

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

4.3 The Fibonacci Sequence Modulo \( m \)

If a solution to a recurrence relation is in integers, then one can ask if there are any patterns to the solution 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 second-degree examples, so we begin by hunting for patterns.

<table>
<thead>
<tr>
<th>( F_n \mod m )</th>
<th>( 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots )</th>
<th>Period 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F_n \mod 3 )</td>
<td>( 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, \ldots )</td>
<td>Period 8</td>
</tr>
<tr>
<td>( F_n \mod 4 )</td>
<td>( 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, 1, 1, \ldots )</td>
<td>Period 6</td>
</tr>
<tr>
<td>( F_n \mod 5 )</td>
<td>( 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, \ldots )</td>
<td>Period 20</td>
</tr>
<tr>
<td>( F_n \mod 6 )</td>
<td>( 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, \ldots )</td>
<td>Period 24</td>
</tr>
<tr>
<td>( F_n \mod 7 )</td>
<td>( 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, \ldots )</td>
<td>Period 16</td>
</tr>
<tr>
<td>( F_n \mod 8 )</td>
<td>( 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, \ldots )</td>
<td>Period 12</td>
</tr>
<tr>
<td>( F_n \mod 9 )</td>
<td>( 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, \ldots )</td>
<td>Period 24</td>
</tr>
</tbody>
</table>

As soon as we see a pair of 1’s we know that the sequence repeats. There are some obvious questions: 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 modulo \( m \) is always 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 must be a subset of \( \mathbb{Z}_m \times \mathbb{Z}_m \) (a finite set of cardinality \( m^2 \)). Since the Fibonacci sequence is infinite, by the box-principle, at least one pair occurs infinitely many times. It follows that there is some pair \( n, N \in \mathbb{N} \) for which

\[ F_n \equiv F_{n+N} \quad \text{and} \quad F_{n+1} \equiv F_{n+1+N} \mod m \]  

(†)

Since the sequence is defined by a recurrence relation applied to two successive terms, the pairs \( (F_n, F_{n+1}) \) and \( (F_{n+N}, F_{n+1+N}) \) must generate the same sequence modulo \( m \). It follows that \( (F_n) \) is eventually periodic.
In fact the entire sequence is periodic. To see this, observe that we can write
\[ F_{n-1} = F_{n+1} - F_n \]

This uniquely 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 \((\dagger)\) must be identical, whence the periodicity continues all the way back to the initial pair \((F_1, F_2)\).

**Definition 4.6.** We denote by \(N(m)\) the period of the Fibonacci sequence modulo \(m\); that is, the value of the smallest \(N\) satisfying \((\dagger)\) for all \(n \in \mathbb{N}\).

The division algorithm quickly proves that any potential period is a multiple of \(N(m)\):

**Lemma 4.7.** \(\forall k \in \mathbb{N}, F_{k+r} \equiv F_k \mod m \iff N(m) \mid r.\)

Now we look for a pattern in the sequence of periods. Staring at the table of values eventually leads to a conjecture...

**Theorem 4.8.** Let \(N(m)\) be the period of the Fibonacci sequence modulo \(m\).

1. For any \(m, n\) we have \(N(m) \mid N(mn)\), thus \(N(mn)\) is always a common multiple of \(N(m)\) and \(N(n)\).
2. If \(\gcd(m, n) = 1\) then \(N(mn) = \lcm(N(m), N(n))\).

**Proof.**

1. Observe that for any \(k, m, n\), we have

\[ F_{k+N(mn)} \equiv F_k \mod mn \implies F_{k+N(mn)} \equiv F_k \mod m \]

By the Lemma, we conclude that \(N(m) \mid N(mn)\).

2. When \(\gcd(m, n) = 1\), we observe\(^3\)

\[ F_{k+N} \equiv F_k \mod mn \iff \begin{cases} F_{k+N} \equiv F_k \mod m \\ F_{k+N} \equiv F_k \mod n \end{cases} \]

Suppose this holds for all \(k\). By definition \(N = N(mn)\) is the least positive integer satisfying the LHS. By 1., \(\lcm(N(m), N(n))\) is the least positive integer satisfying the RHS.

**Conjecture 4.9.** \(N(p^n) = p^{n-1}N(p)\) 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

\[ N(2304) = N(2^8 \cdot 3^2) = \lcm(2^7N(2), 3N(3)) = \lcm(128 \cdot 3, 3 \cdot 8) = 384 \]

\(^3\)The \((\Rightarrow)\) direction requires \(\gcd(m, n) = 1\). If \(\gcd(m, n) \geq 2\), the best we can conclude is that \(N(mn)\) is a common multiple of \(N(m)\) and \(N(n)\).
Binet’s formula modulo $p$

For roughly half the primes, it is possible to obtain a discrete version of Binet’s formula.

**Theorem 4.10.** 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

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

**Proof.** The idea is to look for a value $c$ that plays the role of $\sqrt{5}$: otherwise said, we want $c^2 \equiv 5 \mod p$. Computing Legendre symbols, we see that $(\frac{5}{p}) = (\frac{p}{5}) = 1$ since $p \equiv 1, 4 \mod 5$. This says that we can solve $c^2 \equiv 5 \mod p$. Moreover, we may assume that $c$ is odd, for otherwise we can choose the other solution $p - c$. Now define the sequence

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

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

It is easy to see that $\frac{1+\sqrt{5}}{2}$ are both non-zero modulo $p$, so we always get both terms in Binet’s formula.

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

$$F_n \equiv 8(4^n - 8^n) \equiv 3(8^n - 4^n) \mod 11$$

Binet’s formula actually gives us something else: by Fermat’s Little Theorem, it is immediate that the period $N(11)$ divides 10, for

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

This is, in fact, true in general.

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

**Proof.** Simply compute: writing $\alpha := \frac{1+c}{2}$ and $\beta := \frac{1-c}{2}$, we see that

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

by Fermat’s Little Theorem (since $\alpha, \beta \not\equiv 0 \mod p$). It immediately follows that $N(p) | p - 1$.

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

- If $p \equiv 2, 3 \mod 5$ (but not 2 or 3), then $N(p) | 2p + 2$. One shouldn’t expect a discrete version of Binet’s formula, since there are no values $c$ which satisfy $c^2 \equiv 5 \mod p$.

- $N(m) \begin{cases} = 6m & \text{if } m = 2 \cdot 5^k \text{ for some } k \geq 1 \\ \leq 4m & \text{otherwise} \end{cases}$
4.4 Other Recurrence Relations (non-examinable)

It is reasonable to ask if the solution to any linear constant coefficient recurrence relation is periodic modulo $m$. Supposing that the recurrence is of degree $r$ and $x_{n+r}$ is an integer linear combination of the previous $r$ terms in the sequence, then one could look at $r$-tuples

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

modulo $m$ and apply the box-principle argument of Theorem 4.5. Any solution is therefore eventually periodic modulo $m$.

We cannot quite claim that the entire sequence is periodic however. For example, consider the simple recurrence

$$\begin{align*}
x_{n+1} &= 2x_n \\
x_1 &= 1
\end{align*}$$

Modulo 4, we obtain

$$(x_n) \equiv (1, 2, 0, 0, 0, 0, 0, 0, 0, \ldots)$$

which is not periodic, only eventually so. The problem is that, once we’ve found a repetition using the box principle, we cannot reverse the calculation to define $x_n$ in terms of $x_{n+1}$, because $x_n = \frac{1}{2}x_{n+1}$ is not an equation in integers. In practice this means that the same eventually periodic string may be obtained from different initial conditions. For instance, the initial condition $x_1 = 3$ in the above, yields the same repeating string modulo 4, but a different initial segment:

$$(x_n) \equiv (3, 2, 0, 0, 0, 0, 0, 0, 0, \ldots)$$

The thing that makes the Fibonacci sequence different is that the coefficient in front of the $x_n$ is 1, so we can reverse the recurrence to obtain a sequence $x_n = x_{n+2} - x_{n+1}$ which is still defined in integers. This means that we can work backwards modulo any $m$. In general, one will be able to claim periodicity modulo $m$ of any sequence defined by

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

where $b$ is a unit modulo $m$.

Even given this caveat, it is an impressive fact that any sequence coming from such a recurrence must be eventually periodic modulo any $m$.

Lucas Sequences

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

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

$$\begin{align*}
U(P, Q) &\text{ satisfying } (x_0, x_1) = (0, 1) \\
V(P, Q) &\text{ satisfying } (x_0, x_1) = (2, P)
\end{align*}$$
The Fibonacci sequence is \( U(1, -1) \). These sequences are always eventually periodic modulo \( m \). Moreover, the gcd theorem for periods also holds. We usually appear to have the conjecture \( N(p^k) = p^{k-1}N(p) \), although counter-examples are known. For example, the sequences with \( (P, Q) = (2, -1) \) modulo 13 have period 28, which is the same as their period modulo \( 13^2 = 169 \). By contrast, \( N(169) = 364 = 13N(13) \) for the Fibonacci sequence.

**Pell numbers and continued fractions**  The two sequences \( U(2, -1) \) and \( V(2, -1) \) are known as the *Pell numbers* and *Pell-Lucas numbers* respectively. If we write the first few,

| \( n \) | 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. Indeed the definitions of these sequences

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

are almost identical to those that form the sequence of convergents for \( \sqrt{2} = [1, 2, 2, 2, 2, \ldots] \).

\[
\begin{array}{c|cccccc}
 n & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
c_n & 1 & 2 & 2 & 2 & 2 & 2 \\
p_n & 1 & 1 & 3 & 7 & 17 & 41 \\
q_n & 0 & 1 & 2 & 5 & 12 & 29 \\
\end{array}
\]

Indeed the sequence of convergents is precisely \( \frac{p_n}{q_n} = \frac{1}{2} \frac{V_n}{U_n} \). This explains the *Pell numbers* sobriquet.

It is reasonable to ask why the Pell-Lucas numbers are *twice* the numerators of the convergents of \( \sqrt{2} \): why didn’t we use the initial condition \( (1, 1) \) instead? Partly it is convention, though there are some concrete reasons. For instance, they have very similar Binet-type formulæ

\[
U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \\
V_n = \alpha^n + \beta^n
\]

where \( \alpha, \beta \) are the roots of the characteristic equation \( \lambda^2 - P\lambda + Q = 0 \). A second reason is that the Pell-Lucas numbers can be related to the Pell numbers in another way:

\[
V_n = U_{n-1} + U_{n+1}
\]

See if you can prove this...