Recursion

Yan-Der Lu

July 6, 2013

1 Introduction

在數學上，遞迴 (Recursion)，是指在函式的定義中使用函式自身的方法，就是說，一種遞推地定義一個序列的方程式：序列的每一項是定義為前幾項的函數。

遞迴之所以重要，在研究層面上，有相當多的研究依循這樣的模式：遞迴是好觀察的，所以遞迴關係容易得到，接著再想辦法用種種數學的工具與方法得到一般項或其他結果。

遞迴最簡單的例子是等差數列和等比數列。舉例來說，首項為 a，公差為 d 的等差數列寫成遞迴就是：$a_{n+1} = a_n + d$, 其中 $a_1 = a$。而首項為 a，公比為 r 的等比數列寫成遞迴就是：$a_{n+1} = ra_n$, 其中 $a_1 = a$。更一般地，用數學符號描述的話，一個完整的遞迴關係是：

1. $a_{n+1} = f(a_1, a_2, \ldots, a_n)$ (即每一項由前面幾項所決定)。
2. 先給定了前幾項。

然而，可以看出這樣形容是非常模糊的。換句話說，知道遞迴關係跟知道一般項完全是兩碼子事。

解一個遞迴關係式，即是說求其解析解，在多數情況下是不可能辦得到的，某些簡單定義的遞迴關係式可能會表現出非常複雜的性質，他們屬於數學中的非線性分析領域。例如說邏輯映射 (Logistic Map)：$a_n = ra_{n-1}(1 - a_{n-1})$，其中 r 是一個事先給定的常數，初始值 $0 \leq a_0 \leq 1$。這是科學家在研究人口數量模型時所提出的，這個遞迴式看起來好可愛，卻非常難以分析和預測，由此遞迴式，引出一整個新的數學分支，稱為混沌 (Chaos)。這也是所謂蝴蝶效應 (butterfly effect) 的由來。

本文旨在介紹一些解遞迴式的方法及理論，另外如何從關係式中得到數列的某些性質，最後稍微提到兩個有趣的問題，而這些僅不過是數列理論中的一小部分罷了，希望在讀完後，或多或少都有些收穫。

2 Linear Recurrence Relations

2.1 Approach though Linear Algebra

在數學中，一個齊次系統 (homogeneous system) 象徵的是射影平面 (projection surface) 的概念，從許多面向來看，它通常是比較好處理的。我們定義 k 階

常係數線性齊次遞迴關係式 (order k linear homogeneous recurrence relation with constant coefficients) 為：

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}. \tag{1}$$

其中 $c_1, c_2, \ldots, c_k$ 為給定的常數。

舉例來說，等比數列就是這樣的遞迴：因為 $a_{n+1} = ra_n$。這是一個 1 階的齊次遞迴。而事實上，等差數列也可以寫出這樣的關係式，因為我們可以寫出

$$a_n = a_{n-1} + d \text{ 和 } a_{n-1} = a_{n-2} + d.$$

兩式相減就得到 $a_n - 2a_{n-1} = a_{n-2}$。這是一個 2 階的齊次遞迴。另外一個常見的東西就是 Fibonacci sequence：$F_n = F_{n-1} + F_{n-2}$。

要求出這類型遞迴的解析解之前，我們必須先了解它會有什麼樣好用的性質。假設說今天有許多數列 $\langle x_{i,j} \rangle_{j=1}^{\infty}$

$$\begin{cases} x_{1,1}, & x_{1,2}, & \ldots, & x_{1,n-1}, & \ldots \\ x_{2,1}, & x_{2,2}, & \ldots, & x_{2,n-1}, & \ldots \\ \vdots & \vdots & & \vdots \\ x_{m,1}, & x_{m,2}, & \ldots, & x_{m,n-1}, & \ldots \end{cases}$$

滿足遞迴關係 (1)，那麼由於他是齊次的，所以很快知道，對於常數 $d_1, d_2, \ldots, d_m$，數列 $\langle x_{m+1,j} \rangle_{j=1}^{\infty}$ 也會滿足滿足遞迴關係 (1)，其中 $x_{m+1,j} \equiv d_1 x_{1,j} + d_2 x_{2,j} + \cdots + d_m x_{m,j}$。也就是說，任意一些滿足某階常係數線性齊次遞迴關係式的數列們，他們的線性組合仍滿足同一個遞迴關係式！

這是一個好的方向，因為我們知道這樣的遞迴某項只會受到他前面 k 項的影響，而且他又是齊次系統，所以不太可能因為初始值的改變使得整個數列變得不可預測。事實上，你可以把這樣的數列每一項都寫成 $a_u = f_1(u)a_1 + f_2(u)a_2 + \cdots + f_{n-1}(u)a_{n-1}$，其中 $f_i(u)$ 是你應該有可能求出的係數。(試著寫寫看 Fibonacci sequence 的前幾項你就知道了，但千萬別把 $F_1 = 1, F_2 = 1$ 代進去 ...，用變數表示就好。) 這似乎告訴我們這樣的數列它的本質在於遞迴關係，而不是初始值。

現在讓我們把焦點放在遞迴關係上。對於這樣的遞迴式，我們有沒有可能先求出某些特殊數列的一般項？容易看出，如果 α 滿足 $\alpha^n = c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_k\alpha^{n-k}$，那麼數列 $\langle \alpha^j \rangle_{j=1}^{\infty}$ 就會滿足遞迴式 (1)。而這樣的數 α 共有 k 個 (去掉 0)，也就是說我們已經找到了 k 個一般式很好表達的遞迴數列。由於我們先前證明了任意一些滿足某階常係數線性齊次遞迴關係式的數列們，他們的線性組合仍滿足同一個遞迴關係式，所以自然會想到：有沒有可能用這 k 個數列來線性組合出其他所有滿足遞迴式 (1) 的數列？

為了方便，我們定義遞迴式 (1) 所對應到的特徵方程 (characteristic polynomial) 為：

$$x^k - c_1x^{k-1} - c_2x^{k-2} - \cdots - c_k = 0.$$

它的根為 $\alpha_1, \ldots, \alpha_k$。假設今天給定初始值 $a_i = b_i$，其中 $i = 1, 2, \ldots, k$。現在想一下，想用數列 $\langle\alpha_i^j\rangle_{j=1}^{\infty}$ 組合出 $\langle b_j\rangle_{j=1}^{\infty}$，所代表的就是希望找到常數 $d_1, d_2, \ldots, d_k$ 使得

$$b_i = d_1\alpha_1^i + d_2\alpha_2^i + \cdots + d_k\alpha_k^i. \tag{2}$$

對所有 i 都成立。然而事實上可以更簡單，因為這些數列滿足的遞迴關係都是相同的，所以如果式 (2) 已經對 $i = 1, 2, \ldots, k$ 都成立了，那麼顯然他對所有 i 都會成立！

寫清楚一些，對於任意的 b_i，我們只要找到常數 $d_1, d_2, \ldots, d_k$ 使得線性方程組

$$\begin{cases} b_1 = d_1\alpha_1 + d_2\alpha_2 + \cdots + d_k\alpha_k. \\ b_2 = d_1\alpha_1^2 + d_2\alpha_2^2 + \cdots + d_k\alpha_k^2. \\ \qquad\vdots \\ b_k = d_1\alpha_1^k + d_2\alpha_2^k + \cdots + d_k\alpha_k^k. \end{cases}$$

同時成立。而這看起來似乎是對的，因為我們有 k 個未知數以及 k 個方程式！事實上，線性代數告訴我們：

定理 1　(Cramer's Rule) 考慮 n 個變元 $(x_1, \ldots, x_n)$ 的 n 條式子的線性方程組，寫成矩陣 $Ax = b$，其中 A 是 $n\times n$ 方陣，x 和 b 都是行矩陣。那麼這個方程組有唯一解

$$x_i = \frac{\det(A_i)}{\det(A)}, \ \ \forall i.$$

其中 A_i 是把 A 的第 i 行以 b 代換之後的方陣。

定理 2　(Vandermonde matrix) 定義 $m\times n$ 階的 Vandermonde matrix 為:

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \ldots & \alpha_m^{n-1} \end{bmatrix}$$

那麼 n 階方陣的行列式值可以寫成 $\displaystyle\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)$。

而這兩個定理保證了，只要特徵方程無重根，那麼對於任意的初始值，我們能寫出這個數列的一般項！

例題 1 求出 Fibonacci sequence：$F_n = F_{n-1} + F_{n-2}$，其中 $F_1 = F_2 = 1$ 的通項公式。

解: 首先它對應到的特徵方程為 $x^2 - x - 1 = 0$，兩個根為

$$\alpha_1 = \frac{1+\sqrt{5}}{2},\ \ \alpha_2 = \frac{1-\sqrt{5}}{2}.$$

現在我們要求出常數 d_1, d_2 使得

$$\begin{cases} 1 = F_1 = d_1\left(\dfrac{1+\sqrt{5}}{2}\right) + d_2\left(\dfrac{1-\sqrt{5}}{2}\right) \\ 1 = F_2 = d_1\left(\dfrac{1+\sqrt{5}}{2}\right)^2 + d_2\left(\dfrac{1-\sqrt{5}}{2}\right)^2. \end{cases}$$

解之得 $d_1 = \dfrac{1}{\sqrt{5}}, d_2 = -\dfrac{1}{\sqrt{5}}$，因此 Fibonacci sequence 的通項公式就是

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

然而，當特徵方程有重根時，又該怎麼求一般式？其中一個解決辦法是，假設以 $\alpha_2, \ldots, \alpha_k$ 為根的多項式為

$$x^{k-1} + c_1' x^{k-2} + c_2' x^{k-3} + \cdots + c_{k-1}' = 0 \tag{3}$$

那麼考慮數列 $\langle a_i' \equiv a_{i+1} - \alpha a_i \rangle$，會發現他的特徵方程剛好是式 (3)！如果我們能求出 $\langle a_i' \rangle_{i=1}^{\infty}$ 的通項公式，那代回去又可以得到 $\langle a_i \rangle_{i=1}^{\infty}$ 的通項公式。重複這個步驟，不管原本的特徵方程為何，總是有辦法求出原本遞迴數列的解。當然，在有重根時，你也可以選用其他數列當做基底 (basis)，去線性組合出所有滿足遞迴式的數列。例如 α 為 k 重根時，可以用

$$\begin{cases} 1, & \alpha, & \alpha^2, & \ldots, & \alpha^{n-1}, & \ldots \\ 0, & \alpha, & 2\alpha^2, & \ldots, & (n-1)\alpha^{n-1}, & \ldots \\ 0, & \alpha, & 2^2\alpha^2, & \ldots, & (n-1)^2\alpha^{n-1}, & \ldots \\ \vdots & \vdots & \vdots & & \vdots & \\ 0, & \alpha, & 2^{k-1}\alpha^2, & \ldots, & (n-1)^{k-1}\alpha^{n-1}, & \ldots \end{cases}$$

這些數列當做基底。總之，可以證明：

定理 3 一個多項式有 k_1 重根 α_1，k_2 重根 α_2，...，k_m 重根 α_m，那麼存在一個遞迴數列 $\langle a_n \rangle$ 以這個多項式為特徵方程當且僅當它的一般項可以寫成

$$a_n = g_1(n)\alpha_1^n + g_2(n)\alpha_2^n + \cdots + g_m(n)\alpha_m^n.$$

其中 $g_i(x)$ 是隨著原本多項式而決定的次數不高於 $k_i - 1$ 的多項式。

你可能還碰過一類問題，就是說對於滿足遞迴式 (1) 的數列，如果我們定義它的和分 S_n (summation) 為：

$$S_n = \sum_{i=1}^{n} a_n.$$

那麼可以證明他是 $k+1$ 階常係數線性齊次遞迴關係式，還可以直接算出他們的特徵函數長怎樣，這在像是求

$$\sum_{i=1}^{n} i^k.$$

這種數時很好用 (有興趣者可查詢 Bernoulli number)。這部分留給讀者當做練習。最後再提一個有趣的定理：

定理 4 (Skolem-Mahler-Lech Theorem) 若 $\langle a_i \rangle$ 是線性遞迴數列，那麼對於任一複數 c，總存在有限多個等差數列 $A_1, A_2, \ldots, A_m$ 以及有限集 S，使得讓 $a_k = c$ 的 k 值所成的集合會是這些集合的聯集。

2.2 Approach though Generating Function

從生成函數的角度來看，一切問題都變得簡單多了。對於同樣的遞迴式 (1)，我們先逆推回所謂的 a_0 這一項，然後考慮這個數列的生成函數：

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

由他的遞迴關係，我們可以寫出：

$$\begin{array}{rllll}
f(x) = a_0 + & a_1 x + & a_2 x^2 & + \cdots & \\
c_1 x f(x) = & (a_0 c_1) x + & (a_1 c_1) x^2 & + (a_2 c_1) x^3 + \cdots & \\
c_2 x^2 f(x) = & & (a_0 c_2) x^2 & + (a_1 c_2) x^3 + (a_2 c_2) x^4 + \cdots & \\
\vdots & & & & \\
c_k x^k f(x) = & & & & (a_0 c_k) x^k + (a_1 c_k) x^{k+1} + (a_2 c_k) x^{k+2} + \cdots
\end{array}$$

一直減下去馬上有

$$f(x) = \frac{a_0 + (a_1 - a_0 c_1) x + \cdots + (a_{k-1} - a_{k-2} c_1 - a_{k-3} c_2 - \cdots - a_0 c_{k-1}) x^{k-1}}{1 - c_1 x - \cdots - c_k x^k}.$$

假設 $1 - c_1 x - \cdots - c_k x^k = 0$ 的根是 k_1 重根 β_1，k_2 重根 β_2，...，k_m 重根 β_m，那麼我們將能把此分式寫成

$$f(x) = \sum_{i=1}^{m} \sum_{j=1}^{k_i - 1} \frac{g_{i,j}(x)}{(x - \beta_i)^j}.$$

的型式，其中 $g_{i,j}(x)$ 是次數不高於 j 次的多項式。再用 Tylor expansion 以及微分法則便可以表示出 $f(x)$ 的任一項的係數，即可求出原數列的通項公式。

例題 2 用生成函數求出 Fibonacci sequence：$F_n = F_{n-1} + F_{n-2}$，其中 $F_1 = F_2 = 1$ 的通項公式。

解: 首先寫出：

$$f(x) = \frac{f_0 + (f_1 - f_0)x}{1 - x - x^2} = \frac{x}{1 - x - x^2}.$$

分母對應到的方程為 $1 - x - x^2 = 0$，兩個根為

$$\beta_1 = \frac{-1+\sqrt{5}}{2}, \quad \beta_2 = \frac{-1-\sqrt{5}}{2}.$$

現在我們要求出常數 d_1, d_2 使得

$$f(x) = \frac{x}{1 - x - x^2} = \frac{d_1}{x - \beta_1} + \frac{d_2}{x - \beta_2}.$$

乘開得到 $x = -d_1(x - \beta_2) - d_2(x - \beta_1)$，解之得 $d_1 = \dfrac{1-\sqrt{5}}{2\sqrt{5}}, d_2 = \dfrac{-1-\sqrt{5}}{2\sqrt{5}}$。又由 Tylor expansion 知道

$$\frac{1}{x-c} = -\frac{1}{c}\left(1 + \left(\frac{1}{c}x\right) + \left(\frac{1}{c}x\right)^2 + \cdots\right).$$

因此 Fibonacci sequence 的通項公式就是

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

生成函數可以告訴我們一個快速而且直觀的做法，即使給的遞迴式不齊次還是什麼的，仍有辦法找到裡面的結構，所以請大家學會熟用。

可能有人會問：既然生成函數好做又好想，為什麼還要扯到線性代數去？這是有它的歷史背景在的。這背後的理論是 18 世紀的數學家 De Moivre 以及 Bernoulli Daniel 所建立的，而發展至今，一般遞迴關係我們都會寫成矩陣的形式，然後再利用矩陣對角化的方式直接求出數列通項公式。事實上，特徵多項式也源自於矩陣理論，當然，你也可以把特徵多項式和抽象代數中的極小多項式扯上關係。只能說，數學的世界太廣大了，唯有站在前人的肩膀上，才能看得更高、更遠。

Problems

1. Let $\langle a_n \rangle$ be a linear recursive sequence satisfying a recurrence with characteristic polynomial $f(x)$. Let $g(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0$ be a polynomial. Then every solution $\langle x_n \rangle$ to the inhomogeneous recurrence

$$c_k x_{n+k} + c_{k-1} x_{n+k-1} + \cdots + c_1 x_{n+1} + c_0 x_n = b_n.$$

   also satisfies a linear recurrence with characteristic polynomial $f(x)g(x)$.

2. Let $\langle a_n \rangle$ and $\langle b_n \rangle$ be two linear homogeneous recursive relations with constant coefficients. Prove that:

   (a) The sequence $\langle a_n + b_n \rangle$ is also a linear homogeneous recursive relation with constant coefficients.

   (b) The sequence $\langle a_n b_n \rangle$ is also a linear homogeneous recursive relation with constant coefficients.

3. Suppose that $\langle a_n \rangle$ and $\langle b_n \rangle$ are linear recursive sequences. Prove that

$$a_1, b_1, a_2, b_2, a_3, b_3, \ldots$$

   is also a linear recursive sequence.

4. (Iran MO 2003) Find all homogeneous linear recursive sequences such that it is periodic.

5. Prove that if a sequence is periodic, then it is also a homogeneous linear recursive sequence.

6. Let θ be a fixed real number, and let $a_n = \cos(n\theta)$ for integers $n \geq 1$. Prove that $\langle a_n \rangle$ is a linear recursive sequence, and find the minimal characteristic polynomial.

7. (KöMaL 2000) A sequence of numbers is called of Fibonacci-type if each term, after the first two, is the sum of the previous two. Prove that the set of positive integers can be partitioned into the disjoint union of infinite Fibonacci-type sequences.

8. Given a finite set S of positive integers, show that there exists a linear recursive sequence

$$a_1, a_2, a_3, \ldots$$

   such that $\{n \mid a_n = 0\} = S$.

3 In Algebra

例題 3 考慮數列：$a_n = a_{n-1} + 2n$，其中 $a_0 = 0$。試求出它的通項公式。

解: 首先我們想把問題化簡為學過的，因此考慮

$$a_n = a_{n-1} + 2n \text{ 以及 } a_{n-1} = a_{n-2} + 2(n-1).$$

相減可以得到 $a_n - a_{n-1} = a_{n-1} - a_{n-2} + 2$。又可以再寫出

$$a_n - a_{n-1} = a_{n-1} - a_{n-2} + 2 \text{ 以及 } a_{n-1} - a_{n-2} = a_{n-2} - a_{n-3} + 2.$$

再次相減可以得到 $a_n - 2a_{n-1} + a_{n-2} = a_{n-1} - 2a_{n-2} + a_{n-3}$。這剛好是一個常係數齊次遞迴數列！因此我們知道一般項可以寫成很多個次方數的和。可是仔細看一下，一般項不過就只是 $a_n = (n)(n+1)$ 而已嗎？哪邊出了問題呢？

其實大家都看得出來沒有錯，考慮遞迴數列特例的情況：特徵方程是 $(x-1)^k$ 的形式。這時候帶回公式，會發現一般項其實可以寫成一個多項式。在這時候，我們定義它的差分 Δ (difference) 為：

$$\Delta(a_n) = a_{n+1} - a_n.$$

那麼會發現他剛好是 $k-1$ 階齊次遞迴。這是有用的，因為有些數列可能是很高階遞迴，你看不出來，這時候就可以一直求差分，最後就可以求出一般式。(可以對照 Bernoulli number)

其實上面完全不是我想提的。在競賽數學裡你大概不會看到有要求差分算一般式的情況。多數時候你會遇到的問題大概是：

- 給遞迴式及初始值，問這數列有沒有上下界。
- 給遞迴式及初始值，問這數列會不會收斂。
- 給遞迴式，證明某個不等式。
- 已知某數列有週期，求出它滿足的條件。

之類的，這些大都是非線性分析的範疇，沒有一般性的做法。這邊簡介一些題目，讓大家了解主要是如何運作的。

總而言之，多練基本功，多觀察，多去猜測，多用變數變換，多用數學歸納法，這些動作在基本的遞迴題裡都是必要的。

例題 4 (ISL 2006 A1) 設 $a_0, a_1, a_2, \ldots$ 是個實數數列，滿足如下的遞迴關係：

$$a_{n+1} = [a_n] \cdot \{a_n\}.$$

試證存在正整數 j 使得對任意 $i \geq j$，總有 $a_{i+2} = a_i$.

證明： 我們分兩種情況討論：

Case I. $a_0 \geq 0$.

注意到由於 $a_{n+1} = [a_n] \cdot \{a_n\}$，其中 $\{a_n\} < 1$，因此 $[a_{n+1}] < [a_n]$。所以必從在某個 k 使得 $0 \leq a_k < 1$。而這蘊含了 $a_{k'} = 0 \ \forall k' > k$。

Case II. $a_0 < 0$.

同樣由 $a_{n+1} = [a_n]\cdot\{a_n\}$，可以知道 $|[a_{n+1}]| \leq |[a_n]|$。現在考慮數列 $|[a_0]|, |[a_1]|, \ldots$，我們知道它是遞減的整數數列，並且有下界 0，因此存在某兩正整數 j, k 使得 $|[a_i]| = k \ \forall i \geq j$。第一種情況是 $k > 1$，此時假設

$$a_j = -k + b, \ \ 0 \leq b < 1.$$

那麼由 $|[a_{j+1}]| = k$ 可以得到

$$a_{j+1} = -k(b) < -k + 1 \ \ \Rightarrow \ \ b > \frac{k-1}{k}.$$

又由 $|[a_{j+2}]| = k$ 可以得到

$$a_{j+2} = -k(-kb + k) < -k + 1 \ \ \Rightarrow \ \ 1 - b > \frac{k-1}{k^2}.$$

經過數學歸納法後我們可以宣稱可以由 $|[a_{j+3}]| = k, |[a_{j+4}]| = k, \ldots$ 依序得到：

$$b > \frac{(k-1)(1+k^2+k^4+\cdots+k^{2n})}{k^{2n+1}}.$$
$$1 - b > \frac{(k-1)(1+k^2+k^4+\cdots+k^{2n})}{k^{2n+2}}.$$

兩邊取極限有

$$b \geq \frac{k}{k+1} \quad \text{以及} \quad 1 - b \geq \frac{1}{k+1}.$$

由於兩邊和一樣，故只有 $b = k/(k+1)$，這時易驗證 $a_j = a_{j+1} = \cdots$。

第二種情況是 $k = 1$，代表 $-1 \leq a_j < 0$。此時 $a_{j+1} = -b = -a_j + 1$，且仍有 $-1 \leq a_{j+1} < 0$，故 $a_{j+2} = -a_{j+1} + 1 = a_j$。同理 $a_j = a_{j+2} = \cdots$, $a_{j+1} = a_{j+3} = \cdots$。綜上得證。 □

例題 5 (ISL 2006 A2) 設 $a_0, a_1, a_2, \ldots$ 是個實數數列，滿足 $a_0 = -1$ 以及

$$a_n + \frac{a_{n-1}}{2} + \frac{a_{n-2}}{3} + \ldots + \frac{a_1}{n} + \frac{a_0}{n+1} = 0 \quad \text{對所有 } n \geq 1.$$

試證對所有 $n \geq 1$ 總有 $a_n > 0$。

證明： 我們用數學歸納法證明：首先有 $a_1 > 0$，並且假設 $a_m > 0\ \forall m \leq n$。我們考慮：

$$(n+1)a_n + \frac{n+1}{2}a_{n-1} + \ldots + a_0 = 0.$$

$$(n+2)a_{n+1} + \frac{n+2}{2}a_n + \ldots + a_0 = 0.$$

這兩式，直接相加便得到

$$(n+2)a_{n+1} = \sum_{i=0}^{n} a_i \left(\frac{n+1}{n+1-i} - \frac{n+2}{n+2-i} \right) = \sum_{i=0}^{n} a_i \frac{i}{(n+1-i)(n+2-i)} > 0.$$

綜上由數學歸納法得證。 □

例題 6 (ARO 2006) 兩個正實數數列 $\langle x_n \rangle$ 和 $\langle y_n \rangle$ 滿足各自的遞迴關係：$x_{n+2} = x_{n+1}^2 + x_n$ 和 $y_{n+2} = y_{n+1} + y_n^2$，對所有自然數 n。試證如果 x_1, x_2, y_1, y_2 全都大於 1，那麼存在正整數 k 使得 $x_k > y_k$。

證明： 看得出來這兩個數列的是嚴格遞增的，所以容易分析為什麼一定要有 k 使得 $x_k > y_k$：因為 x_n 的遞迴式含有 x_{n-1}^2，但 y_n 只有 y_{n-1}。

首先估計 x_n：$x_3 = x_2^2 + x_1 > 2$，且 $x_{n+1} = x_n^2 + x_{n-1} > x_n^2$，因此數歸可以知道 $x_n > 2^{2^{n-3}}$。接著估計 y_n：由於 $y_n = y_{n-1} + y_{n-2}^2$，因此 $y_{n+1} = y_n + y_{n-1}^2 = y_{n-1}^2 + y_{n-1} + y_{n-2}^2 < y_n^2$，代入遞迴式中便有 $y_{n+2} = y_{n+1} + y_n^2 < 2y_n^2$ 了！因此當 n 是偶數時，$y_n < 2^{2^{(\frac{n}{2}-1)}-1} y_2^{2^{(\frac{n}{2}-1)}}$。

綜合 $x_n > 2^{2^{n-3}}$ 以及 $y_n < 2^{2^{(\frac{n}{2}-1)}-1} y_2^{2^{(\frac{n}{2}-1)}}$，就知道一定有 k 使得 $x_k > y_k$。 □

Comment. 像這類型 (這兩道例題) 給定遞迴式，要證明不等式成立，不管有沒有給數列初始值，通常都是直接從它的遞迴關係式下手。特別像這題就是經由數列本身的縮放得到的不等關係，這基本上是利用一些代數變換或者觀察遞迴式的形式得來的，基本功要練好才容易做出來。

Problems

1. (ELMO 2012) Let a_0, b_0 be positive integers, and define $a_{n+1} = a_n + \lfloor b_n \rfloor$ and $b_{n+1} = b_n + \lfloor a_n \rfloor$ for all n. Show that there exists a positive integer k such that $a_k = b_k$.

2. (Brazil MO 2004) Let $x_1, x_2, ..., x_{2004}$ be a sequence of integer numbers such that $x_{k+3} = x_{k+2} + x_k x_{k+1}$ $\forall 1 \leq k \leq 2001$. Is it possible that more than half of the elements are negative?

3. (ISL 2004 A2) Let $a_0, a_1, a_2, \ldots$ be an infinite sequence of real numbers satisfying the equation $a_n = |a_{n+1} - a_{n+2}|$ for all $n \geq 0$, where a_0 and a_1 are two different positive reals. Can this sequence be bounded?

4. (KöMaL 2003) Let $a_1 = 1$ and
$$a_{n+1} = a_n + \frac{1}{s_n}.$$
with $s_n = a_1 + a_2 + \cdots + a_n$. Is the sequence bounded?

5. (ARO 1978) Show that there exists an infinite bounded sequence $\langle a_n \rangle_{n=1}^{\infty}$ such that for every two distinct positive integers m, n, it satisfies:
$$|a_m - a_n| > \frac{1}{m-n}.$$

6. (ISL 2010 A4) A sequence $x_1, x_2, \ldots$ is defined by $x_1 = 1$ and $x_{2k} = -x_k$, $x_{2k-1} = (-1)^{k+1} x_k$ for all $k \geq 1$. Prove that $x_1 + x_2 + \ldots + x_n \geq 0$ holds for all $n \geq 1$.

7. (KöMaL 2003) Assume that the sequence $\langle a_n \rangle$ defined by the recurrence
$$a_n = \frac{1}{1-a_n} - \frac{1}{1+a_n}.$$
is periodic. Find the first term of this sequence.

8. (KöMaL 2003) Let $x_1 = 1, y_1 = 2, z_1 = 3$, and let
$$x_{n+1} = y_n + \frac{1}{z_n},\ y_{n+1} = z_n + \frac{1}{x_n},\ z_{n+1} = x_n + \frac{1}{y_n}.$$
for every positive integer n. Prove that at least one of the numbers x_{200}, y_{200} and z_{200} is greater than 20.

9. Suppose $\langle a_n \rangle$ is a bounded integer sequence, which satisfies
$$a_n = \frac{a_{n-1} + a_{n-2} + a_{n-3}a_{n-4}}{a_{n-1}a_{n-2} + a_{n-3} + a_{n-4}}.$$
Prove that $\langle a_n \rangle$ is periodic.

4 In Combinatoric

你可能以前常聽爸媽說:「遞迴是你的好夥伴。」在許多組合計數的問題中,常常可以看到遞迴的影子。然而,這時候出現的就沒有像先前提的那麼簡單的形式了,舉例來說,你遇到的遞迴數列不只一個,而是很多個,而且他們的關係式還像搞基一樣惺惺相惜。像是:

$$\begin{cases} a_{n+1} = b_n + c_n. \\ b_{n+1} = a_n + c_n. \\ c_{n+1} = a_n + b_n. \end{cases}$$

要怎麼解呢?一個好的辦法是依序代換掉數列,比方先把 $\langle c_n \rangle$ 消掉,我們可寫成

$$\begin{cases} a_{n+1} = b_n + a_{n-1} + b_{n-1}. \\ b_{n+1} = a_n + a_{n-1} + b_{n-1}. \end{cases}$$

現在要把 $\langle b_n \rangle$ 消掉就比較麻煩了。我們先改寫成

$$b_{n+1} - b_{n-1} = a_n + a_{n-1}.$$

然後為了運用此式代換,把第一式寫兩遍變成

$$\begin{cases} a_{n+1} = b_n + a_{n-1} + b_{n-1}. \\ a_{n-1} = b_{n-2} + a_{n-3} + b_{n-3}. \end{cases}$$

相減得到:

$$a_{n+1} - a_{n-1} = (a_{n-1} + a_{n-2}) + (a_{n-1} - a_{n-3}) + (a_{n-2} + a_{n-3}).$$

就回到常係數線性齊次遞迴了!

當然,你應該有更快的方法。我們可以將原遞迴式寫成矩陣的形式:

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 0 \\ 2 & -4 & 2 \end{bmatrix} \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}$$

(我換了遞迴式,因為剛剛的對應矩陣不能對角化 ...,由此了解多會一些基本方法還是很重要的),然後我們要求的就是這 3×3 矩陣的冪次。所以對角化:

$$\text{令 } P = \begin{bmatrix} -1 & 0 & -1 \\ -1 & 0 & 0 \\ 2 & 1 & 2 \end{bmatrix}$$

那麼我們會有

$$PAP^{-1} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

此時可以算出

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 0 \\ 2 & -4 & 2 \end{bmatrix}^n \begin{bmatrix} a_1 \\ b_1 \\ c_1 \end{bmatrix} = \left(P^{-1} \begin{bmatrix} 3^n & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 1 \end{bmatrix} P \right) \begin{bmatrix} a_1 \\ b_1 \\ c_1 \end{bmatrix}$$

這時候可以輕易表達這三個數列的通式。

但是，大家都知道人生不是那麼輕鬆的，有時候光是只有一個數列做遞迴就可以嚇死人了。以下是幾個例子。

例題 7 (The Bernoulli-Euler Problem of Misdressed Envelops) 現在有 n 個寫好名字的信封袋，還有對應到的 n 封信，試求出所有信都被裝錯的可能情況數。

解: 我們將裝錯的可能情況數記為 a_n。首先易見 $a_1 = 0, a_2 = 1$。現在我們考慮任一種所有信都被裝錯的情況，假設第 n 封信被裝錯到第 i 個袋 (i 有 $n-1$ 種可能)。

Case I. 第 i 封信不是被裝錯到第 n 個袋。
這時候可以看成“第 i 封信不能被裝到第 n 個袋”以及“第 j 封信不能被裝到第 j 個袋 $\forall j \neq i, n$”，所以裝錯的可能情況數是 a_{n-1}。

Case II. 第 i 封信被裝錯到第 n 個袋。
這時候 n 和 i 就沒用了，剩下的 $n-2$ 個袋袋和信都被裝錯的可能情況數就是 a_{n-2}。

綜上，有遞迴式 $a_n = (n-1)(a_{n-1} + a_{n-2})$。這時候就要一點高超的技巧了：

$$\begin{aligned} a_n - na_{n-1} &= -\Big[a_{n-1} - (n-1)a_{n-2}\Big] \\ &= (-1)^2\Big[a_{n-2} - (n-2)a_{n-3}\Big] \\ &= \cdots \\ &= (-1)^{n-2}\Big[a_2 - 2a_1\Big] \\ &= (-1)^n. \end{aligned}$$

現在，你就可以展開看出 $\langle a_n \rangle$ 的通項表達式了：

$$\begin{aligned} a_n &= na_{n-1} + (-1)^n \\ &= n(n-1)a_{n-2} + n(-1)^{n-1} + (-1)^n \\ &= n(n-1)(n-2)a_{n-3} + n(n-1)(-1)^{n-2} + n(-1)^{n-1} + (-1)^n \\ &= \cdots \\ &= n!\left(\frac{(-1)^0}{0!} + \frac{(-1)^1}{1!} + \cdots + \frac{(-1)^n}{n!}\right). \end{aligned}$$

如果仔細看，你會發現這根本就是 $n!e^{-1}$ 的近似值，事實上：

$$|a_n - n!e^{-1}| = |n! \sum_{k \geq n+1} \frac{(-1)^k}{k!}| < \frac{1}{2}.$$

所以 a_n 就是最接近 $n!e^{-1}$ 的整數！

例題 8 (Catalan Numbers) 現在給定 n 個符號排成一串，我們可以加許多小括號以表示這些數字的運算順序，試問有幾種不同的運算方法？以下是前幾個例子：

n	運算方法數	實際排法
1	1	x_1
2	1	x_1x_2
3	2	$x_1(x_2x_3)$, $(x_1x_2)x_3$
4	5	$x_1(x_2(x_3x_4))$, $x_1((x_2x_3)x_4)$, $(x_1x_2)(x_3x_4)$, $(x_1(x_2x_3))x_4$, $((x_1x_2)x_3)x_4$

解: 我們將不同的運算方法數記為 c_n，現在考慮這 n 個符號，它們會被我們加的小括號切成兩段，因此遞迴式就是：

$$c_n = c_1c_{n-1} + c_2c_{n-2} + \cdots + c_1c_{n-1}.$$

啊哈哈，然後就算不出來了。我們只好考慮它的生成函數：

$$f(x) = c_1x + c_2x^2 + \cdots .$$

由遞迴式，我們可以考慮

$$\begin{aligned}(f(x))^2 &= (c_1^2)x^2 + (c_1c_2 + c_2c_1)x^3 + \cdots + (c_1c_{n-1} + c_2c_{n-2} + \cdots + c_1c_{n-1})x^n + \cdots \\ &= c_2x^2 + c_3x^3 + \cdots + c_nx^n + \cdots \\ &= f(x) - c_1x\end{aligned}$$

所以就得到了 $(f(x))^2 - f(x) + x = 0$。解這個二次方程，再用 Tylor expansion 可以知道

$$a_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

Comment. 這種組合數又稱為 Catalan number，在組合、拓撲等等領域中常常會碰到，其重要性讓它已自成一理論。試作另外幾題：

1. 圓上有 $2n$ 個等分點，依序記為 $P_1, Q_1, P_2, Q_2, \ldots, P_n, Q_n$，現在連出 n 條弦，每兩條弦不相交，每條弦的頂點都是某對 P_i, Q_j，問有幾種連法。
2. 有 n 個 1 及 n 個 -1 排成一數列，這數列從第一項開始加到任意一項的和都是非負的，求這樣的排法數。

Problems

1. (ISL 1997) In town A there are there are n girls $g_1, \ldots, g_n$ and $2n-1$ boys $b_1, \ldots, b_{2n-1}$. The girl g_i, $i = 1, \ldots, n$ knows the boys $b_1, \ldots, b_{2i-1}$ and no others. For all $r = 1, \ldots, n$ denote by $A(r)$ the number of different ways in which r girls can dance with r boys , forming r pairs, each girl with a boy she knows. Prove that $A(r) = \binom{n}{r}^2$ for each $r = 1, \ldots, n$.

2. (ISL 1998 A4) For any two nonnegative integers n and k satisfying $n \geq k$, we define the number $c(n,k)$ as follows:

   ▼ $c(n,0) = c(n,n) = 1$ for all $n \geq 0$.

   ▼ $c(n+1,k) = 2^k c(n,k) + c(n,k-1)$ for $n \geq k \geq 0$.

   Prove that $c(n,k) = c(n,n-k)$ for all $n \geq k \geq 0$.

3. (USAMO 2013) For a positive integer $n \geq 3$ plot n equally spaced points around a circle. Label one of them A, and place a marker at A. One may move the marker forward in a clockwise direction to either the next point or the point after that. Hence there are a total of $2n$ distinct moves available; two from each point. Let a_n count the number of ways to advance around the circle exactly twice, beginning and ending at A, without repeating a move. Prove that $a_{n-1} + a_n = 2^n$ for all $n \geq 4$.

4. (ISL 2003 C4) Given n real numbers $x_1, \ldots, x_n$ and n further real numbers $y_1, \ldots, y_n$. The entries a_{ij} (with $1 \leq i,j \leq n$) of an $n \times n$ matrix A are defined as follows:
$$a_{ij} = \begin{cases} 1, & \text{if } x_i + y_j \geq 0 \\ 0, & \text{if } x_i + y_j < 0. \end{cases}$$
   Further, let B be an $n \times n$ matrix whose elements are numbers from the set $\{0,1\}$ satisfying the following condition: The sum of all elements of each row of B equals the sum of all elements of the corresponding row of A ; the sum of all elements of each column of B equals the sum of all elements of the corresponding column of A. Show that $A = B$.

5. (ISL 2009 C3) Let n be a positive integer. Given a sequence $\varepsilon_1, \ldots, \varepsilon_{n-1}$ with $\varepsilon_i = 0$ or 1 for each i. The sequences $a_0, \ldots, a_n$ and $b_0, \ldots, b_n$ are constructed by the following rules: $a_0 = b_0 = 1$, $a_1 = b_1 = 7$,
$$a_{i+1} = \begin{cases} 2a_{i-1} + 3a_i, & \text{if } \varepsilon_i = 0 \\ 3a_{i-1} + a_i, & \text{if } \varepsilon_i = 1. \end{cases}$$

$$b_{i+1} = \begin{cases} 2b_{i-1} + 3b_i, & \text{if } \varepsilon_{n-i} = 0 \\ 3b_{i-1} + b_i, & \text{if } \varepsilon_{n-i} = 1. \end{cases}$$

Prove that $a_n = b_n$.

6. (USAMO 1996) An n-term sequence $\langle x_1, x_2, \ldots x_n \rangle$ in which each term is either 0 or 1 is called a *binary sequence of length* n. Let a_n be the number of binary sequences of length n containing no three consecutive terms equal to $0, 1, 0$ in that order. Let b_n be the number of binary sequences of length n that contain no four consecutive terms equal to $0, 0, 1, 1$ or $1, 1, 0, 0$ in that order. Prove that $b_{n+1} = 2a_n$ for all positive integers n.

7. (MOSP 2006) Consider a convex n-gon with vertices $P_1, P_2, \ldots, P_n$ with all of its edges and diagonals drawn in. Each line between two vertices is assigned a number. Among any 3 vertices, the lines joining them have two numbers that are the same and one that is different, and the different one must be smaller than the other two. We wish to know two things:
   (a) What is the least number of distinct numbers that allow such a situation (in terms of n)?
   (b) In how many ways can this minimal arrangement be achieved?

8. (ISL 2010 C4) Each of the six boxes $B_1, B_2, B_3, B_4, B_5, B_6$ initially contains one coin. The following operations are allowed:

   Type 1) Choose a non-empty box B_j, $1 \le j \le 5$, remove one coin from B_j and add two coins to B_{j+1}.

   Type 2) Choose a non-empty box B_j, $1 \le j \le 4$, remove one coin from B_j and swap the contents (maybe empty) of the boxes B_{j+1} and B_{j+2}.

   Determine if there exists a finite sequence of operations of the allowed types, such that the five boxes B_1, B_2, B_3, B_4, B_5 become empty, while box B_6 contains exactly $2010^{2010^{2010}}$ coins.

5 In Geometry

"*Clouds are not spheres, mountains are not cones, and lightening does not travel in a straight line. The complexity of nature's shapes differs in kind, not merely degree, from that of the shapes of ordinary geometry, the geometry of fractal shapes.*"

–Benoit B. Mandelbrot

1872 年，Karl Weierstrass 給出了一個具有處處連續但處處不可微這種非直觀性質的函數例子，其圖像在現今被認為是碎形。1904 年，Koch 不滿意 Weierstrass 那抽象且解析的定義，用更加幾何化的定義給出一個類似的函數，今日稱之為 Koch 雪花。1915 年 Wacław Sierpiński 造出了 Sierpiński 三角；隔年，又造出了 Sierpiński 地毯。Georg Cantor 也給出一個具有不尋常性質的實直線上的子集－Cantor 集，今日也被認為是碎形。

複數平面的迭代函數在 19 世紀末 20 世紀初被許多數學家所研究，但直到現在有電腦繪圖的幫忙，許多他們所發現的函數才顯現出其美麗來。

1960 年代，Benoit Mandelbrot 開始研究自相似，最終在前人的工作之上，寫下論文《How Long Is the Coast of Britain? Statistical Self-Similarity and Fractional Dimension》。並在 1975 年提出了「碎形 (fraction)」一詞，來標記 Hausdorff-Besicovitch Dimesion。Mandelbrot 以顯著的電腦繪製圖像來描繪此一數學定義，它們中許多都基於遞迴，導致了大眾對「碎形」的通俗理解。

由於碎形的美感建立在大量圖像上，本文並不去介紹，只推薦給大家一本書。《動手玩碎形》–由淺入深廣泛的描述了碎形的結構。另外 amazon 上面也有不錯的原文書籍。

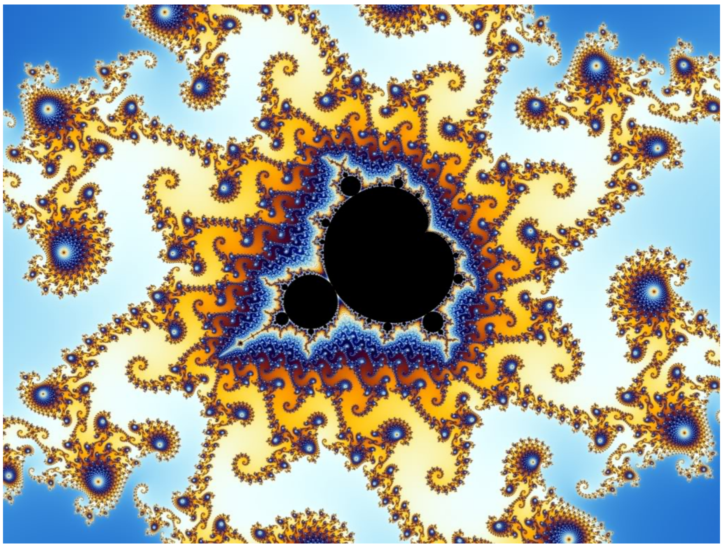

Figure 1: A View of the Entire Universe

6 In Number Theory

競賽數學裡關於遞迴關係中的數論問題大概可以分為兩類：

- 遞迴關係中含有取最大公因數、開根號等等，感覺有東西會變少 (小) 的。
- 隱藏得很好，讓你不知道有好的遞迴式存在：題目通常出現平方後再開根號關係。

處理的方式也都蠻固定的。第一種明顯就是要你對其中一個東西賦值，可能是某數質因數分解式中所有質數冪次總和啊、寫成分數形式後分子加分母的和之類的，然後進行無窮遞降法，這就多多練習抓感覺。至於第二種，就是典型的 Vieta jumping 題，你把數列前幾項寫出來後，大概就會發現他有 2 階的齊次遞迴，例如：$a_1 = 1$, $a_{n+1} = 2a_n + \sqrt{3a_n^2+1}$. 證明每項都是整數。

今天我們要介紹的主要是整數遞迴數列中的整除關係。你明年可能碰到這樣的問題：試求出 Fibonacci sequence 第 2014 項的十位跟個位是多少。當你算到某一項時，你好像發現了這個數列的末兩位數好像會循環！哼哼，這其實是有原因的，事實上：

定理 5 如果遞迴數列 $\langle a_n \rangle$ 的遞迴關係是

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}).$$

其中 f 是多項式。那麼對任意正整數 m，數列 $\langle a_n \pmod m \rangle$ 都是循環的。

證明： 我們觀察數列 $\langle a_n \pmod m \rangle$ 中的連續 k 項，由於在 $\bmod m$ 下只有有限種可能 (最多就 m^k 種)，因此由鴿籠原理知道必定有兩段連續 k 項是相等的，這個數列每一項都可由它前面的連續 k 項依同樣的規則決定，因此數列 $\langle a_n \pmod m \rangle$ 必是循環的。 □

Comment. 注意到這說明了 Fibonacci sequence 對模任意正整數是循環數列，又因為這個數列每一項都可由它前面 (或後面) 的連續兩項決定，且 $f_0 = 0$，所以對模任意正整數都有無窮多項是 0，也就是說對任意正整數 m，Fibonacci sequence 裡有無窮多項是 m 的倍數！

為方便研究，我們定義說：

定義 1 對於循環數列 $\langle a_n \rangle$，假設說正整數 T 使得

$$a_{n+T} = a_n.$$

對所有 n 都成立 (事實上只要對足夠大的 n 成立就好，不過這邊感興趣的是對所有 n 都成立的情況)，那麼我們稱 T 為這個數列的**週期** (period)。並且稱這些 T 裡面最小的那個為**最小週期**。(在 Fibonacci sequence 中又稱做 **Pisano period**)

定義完之後會發現一件比較麻煩的事，我們在研究的週期不只一個，這時候搞不好這些週期還有各自的性質，可我們又不可能一一去研究。然而你想到數論問題裡面很多時候都會有最小週期整除週期的情況發生 (比如某數對 $\mathbb{Z}/\mathbb{Z}_p$ 的 order)，會不會循環數列也有這種性質呢？

定理 6　如果循環數列 $\langle a_n \rangle$ 的最小週期是 T，而 T' 是任一週期，那麼 $T \mid T'$。

證明： 由定義，必須要有

$$a_{n+T} = a_n \text{ 以及 } a_{n+T'} = a_n \; \forall n.$$

又由輾轉相除法，我們可以找到整數 d, d' 使得 $dT + d'T' = \gcd(T, T')$。這時候會有

$$a_n = a_{n+T} = a_{n+2T} = \cdots = a_{n+dT} = \cdots = a_{n+dT+d'T'} = a_{n+\gcd(T,T')} \; \forall n.$$

然而我們已宣稱 T 是最小週期，因此 $\gcd(T, T') = T$，即 $T \mid T'$。 □

先讓我們回到一開始的問題：Fibonacci sequence 第 2014 項的十位跟個位是多少？由中國剩餘定理可以知道，事實上你只需分別求出第 2014 項 mod 4 和 mod 25 是多少就好了。這時候你很快會發現：其實 mod 100 的最小週期就是 mod 4 和 mod 25 的最小週期的最小公倍數吧！而且這命題還可以再加強一點：

定理 7　假設一數列 $\langle a_n \rangle$ 在模任何正整數下都是循環的，且計 mod x 下的最小週期是 $T(x)$。那麼當 $(m, n) = 1$ 時，$T(mn) = \text{lcm}[T(m), T(n)]$。

證明： 首先由定義有 $a_{x+\text{lcm}[T(m),T(n)]} \equiv a_x \pmod{m}$，對 mod n 也成立，因此 $T(mn) \mid \text{lcm}[T(m), T(n)]$。再來由於 $a_{x+T(mn)} \equiv a_x \pmod{mn}$ 對所有 x 都要成立，因此

$$a_{x+T(mn)} \equiv a_x \pmod{m}$$

$$a_{x+T(mn)} \equiv a_x \pmod{n}$$

這兩式對所有 x 都必須要成立。由**定理 6** 就知道 $T(m), T(n) \mid T(mn)$，所以 $\text{lcm}[T(m), T(n)] \mid T(mn)$。綜上 $T(mn) = \text{lcm}[T(m), T(n)]$。 □

有了這個定理，如果說你想要研究某一遞迴數列在模 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 的最小週期時，實際上只要求出模 p^i 的週期就好了！在計算之前，我們先定義 $\phi = (1+\sqrt{5})/2, \bar{\phi} = (1-\sqrt{5})/2$。我們先討論最簡單的情況：模 p 的週期。

首先你可能會迷惘，怎麼可能求的出週期呢？我們對 Fibonacci sequence 就強力的了解就是它的封閉式，難道你要我真的用那個一般式去炸週期嗎，不好笑啊。現在我們要介紹一點抽象代數的結構：Field Extenstion, Splitting Field。

Field 我們在此假定各位至少知道它的定義，以及會把一些像同餘運算、指數原根二次剩餘等寫成 $\mathbb{F}_p$ 的形式表達了。首先介紹 Field Extenstion。

回顧數學的發展過程，依次引入了正整數、非負整數、有理數、實數、複數。在這過程中，都是因為“某個方程在有的代數結構中找不到解”。因為 $x+1=2$ 無正整數解，所以引入負整數和 0。因為 $2x=1$ 無整數解，所以引入有理數。因為 $x^2=2$ 無有理數解，所以引入根號。因為 $x^2=-1$ 無實數解，所以引入複數。那麼，什麼叫做“引入新的代數結構”？

這其實純粹是個理想化數學的方法，因為現在找不到，所以我們加新東西進去讓它更完美。比如說從正整數再引入非負整數的過程中，我們讓方程式 $x+1=2$ 有解了，但那個所謂的“解”，它所有的性質完全就和“正整數”這個結構無關，因為它並不是在這個結構下產生的。這造成了一個奇怪的現象，明明在想法上是“擴張”的概念，但如果要用嚴謹的數學式去定義時，我們卻必須先有那個“擴張後的結構”，才能說從“原本的結構”去生成“擴張後的結構”。

定義 2 如果 $\mathbb{L}$ 是一個 field，並且 $\mathbb{K}$ 是 $\mathbb{L}$ 的一個 subfield (即 $\mathbb{K}$ 對 $\mathbb{L}$ 上定義的加法跟乘法封閉，且 $\mathbb{K}$ 中每個元素對加法跟乘法的逆都還是在 $\mathbb{K}$ 中)，則說 $\mathbb{L}$ 是 $\mathbb{K}$ 的 extension。

我們知道 field extenstion 也分很多種，比方集合 $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ 是 $\mathbb{Q}$ 的擴張，而擴張次數 $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]=2$ 是有限的。然而像集合 $\mathbb{R}$ 是 $\mathbb{Q}$ 的擴張，擴張次數 $[\mathbb{R}:\mathbb{Q}]=\mathfrak{c}$ 卻是無限的。在數論中，我們真正感興趣的是所謂的代數擴張 (algebraic extension)，這是用在某個 field 上的多項式的根當做基底產生的擴張。比方 $\mathbb{Q}[\sqrt{2}]$ 就是一個代數擴張，因為多項式 $x^2-2=0$ 的係數都在 $\mathbb{Q}$ 中，然後 $\sqrt{2}$ 是 $x^2-2=0$ 的根。

接下來要介紹 Splitting Field。這時候又更凸顯出多項式實在很重要了。

定義 3 給定某個 field $\mathbb{K}$，以及一個係數都在那個 field 上的多項式 $f(x)$，我們稱 $f(x)$ 對 $\mathbb{K}$ 的 splitting field 指的是 $\mathbb{K}$ 的一個最小 extension field $\mathbb{L}$，使得 $f(x)$ 在 $\mathbb{L}$ 中可以完全被分解成線性因式。

舉例來說，現在有一個 field，就是 $\mathbb{Q}$，然後有個係數都在 $\mathbb{Q}$ 上的多項式 $f(x)=x^3-2$，那麼 $f(x)$ 對 $\mathbb{Q}$ 的 splitting field 就是 $\mathbb{Q}[\sqrt[3]{2},\omega]$，其中 ω 是三次單位根。有時候 splitting field 不唯一，但可以確定它們都是 isomorphism 的。

現在我們回到 Fibonacci sequence 模 p 的週期 (以下計 Fibonacci sequence 模正整數 m 的週期為 $l(m)$)。我們證明以下定理：(其實剛剛說的你都可以不要管，這些定理完全可以用二項式展開以及二次剩餘的基本性質做出來)

定理 8 假設一質數 $p\equiv\pm1 \pmod 5$，則 $l(p)\mid p-1$。

證明： 這時候我們知道 $\mathbb{F}_p$ 中有個元素扮演了 $\sqrt{5}$ 的角色 (就是說 5 是模 p 的二次

剩餘)，所以 $\phi, \bar{\phi}$ 都是 $\mathbb{F}_p$ 中的元素。由 Fermat's theorem 有：

$$\phi^{p-1} = 1 \text{ 以及 } \bar{\phi}^{p-1} = 1.$$

因此

$$F_{p-1} = \frac{1}{\sqrt{5}}\left(\phi^{p-1} - \bar{\phi}^{p-1}\right) = 0.$$

$$\begin{aligned} F_p &= \frac{1}{\sqrt{5}}\left(\phi^p - \bar{\phi}^p\right) = \frac{1}{\sqrt{5}}\left(\phi - \bar{\phi}\right) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = 1. \end{aligned}$$

綜上我們有

$$\begin{cases} F_{p-1} = 0 = F_0 \\ F_p = 1 = F_1. \end{cases}$$

故 $p-1$ 是 Fibonacci sequence 模 p 的週期，由**定理 6** 就知道 $l(p) \mid p-1$。 □

定理 9 假設一質數 $p \equiv \pm 2 \pmod 5$，則 $l(p) \mid 2p+2$，且 $(2p+2)/l(p)$ 是奇數。

證明： 這時候 $\mathbb{F}_p$ 中就沒有 $\sqrt{5}$ 了，但我們還是要用通項公式計算啊，怎麼辦呢？所以考慮 x^2-5 在 $\mathbb{F}_p$ 上的 splitting field:

$$\mathbb{F}_p[\sqrt{5}] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{F}_p\right\}.$$

(可以驗證有模逆等等)，而且此時 $5^{\frac{p-1}{2}} = -1$。計算可知

$$\begin{aligned} \phi^p &= \left(\frac{1+\sqrt{5}}{2}\right)^p = \left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^p = \left(\frac{1}{2}\right)^p + \left(\frac{\sqrt{5}}{2}\right)^p \\ &= \left(\frac{1}{2}\right)^p \left(1 + \sqrt{5}^p\right) = \frac{1}{2}\left(1 + 5^{\frac{p-1}{2}}\sqrt{5}\right) \\ &= \frac{1}{2}\left(1 - \sqrt{5}\right) = \bar{\phi}. \end{aligned}$$

因此也有

$$(\bar{\phi})^p = \overline{(\phi^p)} = \bar{\bar{\phi}} = \phi.$$

綜合以上兩式，我們得到：

$$\begin{aligned} F_p &= \frac{\phi^p - \bar{\phi}^p}{\sqrt{5}} = \frac{\bar{\phi} - \phi}{\sqrt{5}} = -1. \\ F_{p+1} &= \frac{\phi^{p+1} - \bar{\phi}^{p+1}}{\sqrt{5}} = \frac{\phi\bar{\phi} - \bar{\phi}\phi}{\sqrt{5}} = 0. \end{aligned}$$

這告訴我們 $F_p = -1, F_{p+1} = 0, F_{p+2} = -1$，所以 $F_{2p+1} = 1, F_{2p+2} = 0, F_{2p+3} = 1$，即有 $l(p) \mid 2p+2$。並且 $l(p) \nmid p+1$，所以 $(2p+2)/l(p)$ 是奇數。 □

我們發現雖然有一些漂亮的結果了，可惜還是解不出一般的週期。事實上可以證明若 n 是奇數，那麼 $l(n)$ 就是 ϕ 在 $\mathbb{Z}_n^\times[\sqrt{5}]$ 中的 order，而在抽象代數中要處理某數在 field 的 order 這類型的問題都是難的。我們知道它的結構其實和 order 有關，自然會聯想到：指數原根二次剩餘的一些性質能不能套用上來呢？

我們計算 Fibonacci sequence 模 p^i 的週期時，會發現一個和指數性質完全一樣的結論：(讀者可以想想看，模正整數的週期會不會有像 primitive roots 和 Carmichael function 類似的結果呢)

定理 10 如果 k 是最大的正整數使得 $l(p^k) = l(p)$，那麼對所有 $k_0 > k$，有 $l(p^{k_0}) = p^{k_0-k}l(p)$。

證明是簡單的，可以用和證指數性質時的一樣方法：二項式展開再加上數學歸納法，只是有點煩所以在此略去，讀者請自行練習。

現在研究 Fibonacci sequence 模正整數的週期已有許多成果，這邊礙於筆者能力以及篇幅只介紹了一小段，有興趣鑽研者可以自行 google。另外這種計算模正整數的週期亦可當作一種質數檢驗法。

例題 9 (Italy MO 2007) 考慮以下給定的數列：$x_1 = 2,\ x_{n+1} = 2x_n^2 - 1$，對所有 $n \geq 1$。證明對所有 $n \geq 1$，n 和 x_n 都是互質的。

證明： 首先當 $n = 1$ 時結論是成立的。現在我們考慮 n 的任一質因數 p，我們想要證明的就是 p 和 x_n 互質，而 n 可以是 p 的任何一個倍數，因此會想到去分析 $\langle x_n \pmod p\rangle$ 的週期。

我們考慮數列 $\langle x_n \pmod p\rangle_{n=1}^{p-1}$。只要當中有任何一個數是 0 或 1，那麼我們知道 $x_{p-t} \bmod p$ 只能是 -1 或 1，此時結論成立。如果當中沒有任何一個數是 0 或 1，那麼這 $p-1$ 個數只能有 $p-2$ 種取值，因此有兩個數是一樣的，那麼顯見這時候產生了一個週期，一個週期中任一數又不能是 0 (否則變成 $0, -1, 1, 1, \ldots$)，此時結論亦成立。綜上得證。 □

例題 10 (ISL 1998 Q1) 整數數列 $\langle a_n\rangle$ 是由以下的遞迴關係所定義：

$$a_0 = 0,\ a_1 = 1,\ a_{n+2} = 2a_{n+1} + a_n.$$

試證 2^k 整除 a_n 當且僅當 2^k 整除 n。

證明： 我們先宣稱他和 Fibonacci sequence 有相同的性質：(1)$a_{m+n} = a_{m-1}a_n + a_m a_{n+1}$、(2) 如果 $m \mid n$，那麼 $a_m \mid a_n$。其中 (1) 可以對 $m + n$ 做數學歸納法證明，或是用矩陣證。(2) 的話則是使用輾轉相除法。

分析一下題目要求證的：$v_2(a_n) = v_2(n)$，我們可能會希望用數學歸納法的想法證明。首先我們把這數列模 2 和模 4，易看出週期分別是 $0, 1$ 和 $0, 1, 2, 1$，因此題目的結論在 $k = 1, 2$ 時是成立的。再來在 (1) 中帶入 $m = n$，得到 $a_{2n} = a_n(a_{n-1} + a_{n+1}) = 2a_n(a_{n-1} + a_n)$，所以 $v_2(a_{2n}) = v_2(2a_n(a_{n-1} + a_n)) = v_2(a_n) + 1$（因為 $a_{n-1} + a_n$ 是奇數），因此用數學歸納法就知道結論在 k 為任意正整數時都成立。 $\square$

Comment. 這種利用恆等式去求出對某個質數的冪次在 2 階齊次遞迴中很常見，然後證明中所用的輾轉相除法還可以做出一般 2 階遞迴很多好用的整除或最大公因數等等的性質。如果想練習更多這類型的題目，可以參考 PEN。

例題 11 (German TST 2009) 數列 $\langle a_n \rangle$ 定義為：$a_1 = 1$ 且 $a_{n+1} = a_n^4 - a_n^3 + 2a_n^2 + 1$，對所有 $n \geq 1$。試證存在無窮多個質數 p 使得任一個 a_n 都不被 p 整除。

證明： 首先注意到我們可以用 $a_0 = 0$ 生出同樣的數列。然後看一下我們剛剛學的：這樣的數列 $\langle a_n \pmod p \rangle$ 必定是循環的。那麼你會發現，題目其實是要我們證明無窮多個質數 p，使得 $\langle a_n \pmod p \rangle$ 的循環節裡不包含 0。

先觀察一下遞迴式，因為有一項係數是 2 跟其他人不一樣很奇怪，所以你可能會想移項成

$$a_{n+1} - a_n = (a_n^2 + 1)(a_n^2 - a_n + 1).$$

然後我們想證的是 $\langle a_n \pmod p \rangle$ 的循環節裡不包含 0，可是我們又有 $a_0 = 0$，所以我們知道要取的 p 一定不能讓循環節包含 a_0。這代表知道要取的 p 會讓 $\langle a_n \pmod p \rangle = \langle b_0, b_1, \ldots, \overline{c_1, \ldots, c_i} \pmod p \rangle$（就是說 $\langle a_n \rangle$ 前幾項不在循環節裡）。為了讓數列循環，你可能會想到取 $p \mid a_{m+1} - a_m$。

我們說明一下這樣的 p 為什麼會滿足題意：首先看出 $(a_{m+1}, a_m) = 1$，再來因為 $a_{m+1} \pmod p = a_m \pmod p$，因此由同樣的遞迴公式可以得到 $a_m \pmod p = a_{m+1} \pmod p = a_{m+2} \pmod p = \cdots$！而如果有某項 a_i 滿足 $a_i \pmod p = 0$，又因為 $a_0 \pmod p = 0$，這會代表 $\langle a_n \pmod p \rangle$ 的循環節裡包含 0，但我們知道循環節剛好是 $\overline{a_m}$，矛盾！因此這樣的 p 會滿足要求。

接著還要證明可以取到無窮多個 p。這是簡單的，因為假設 $q^s \mid\mid a_{m+1} - a_m$（其中 q 為奇質數），那麼帶入移項過後的遞迴式我們仍有 $q^s \mid\mid a_{k+1} - a_k \ \forall k \geq m$。而易計算 $v_2(a_{m+1} - a_m) = v_2\big((a_m^2 + 1)(a_m^2 - a_m + 1)\big) = 2$（因為數列每項都是奇數）。且 $\langle a_{n+1} - a_n \pmod p \rangle$ 又是嚴格遞增的，因此 p 要有無窮多個。 $\square$

Problems

1. (ARO 2003) Let a_0 be a natural number. The sequence $\langle a_n \rangle$ is defined by $a_{n+1} = a_n/5$ is a_n is divisible by 5, and $a_{n+1} = [\sqrt{5}a_n]$ otherwise. Show that the sequence a_n is increasing starting from some term.

2. (HIBMC 2002) Let $p(x)$ be a polynomial with rational coefficients, of degree at least 2. Suppose that a sequence $\langle r_n \rangle$ of rational numbers satisfies $r_n = p(r_{n+1})$ for every $n \geq 1$. Prove that the sequence $\langle r_n \rangle$ is periodic.

3. (ISL 2010 A5) Denote by $\mathbb{Q}^+$ the set of all positive rational numbers. Determine all functions $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ which satisfy the following equation for all $x, y \in \mathbb{Q}^+$:
$$f\left(f(x)^2 y\right) = x^3 f(xy).$$

4. (ISL 2008 N3) Let $a_0, a_1, a_2, \ldots$ be a sequence of positive integers such that the greatest common divisor of any two consecutive terms is greater than the preceding term; in symbols, $\gcd(a_i, a_{i+1}) > a_{i-1}$. Prove that $a_n \geq 2^n$ for all $n \geq 0$.

5. Show that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \in \mathbb{N}$. And conclude that no Fibonacci number can be factored into a product of two smaller Fibonacci numbers, each greater than 1.

6. Let $P(x)$ be a nonzero polynomial with integer coefficients. Let $a_0 = 0$ and for $i \geq 0$ define $a_{i+1} = P(a_i)$. Show that $\gcd(a_m, a_n) = a_{\gcd(m,n)}$.

7. (ELMO 2010 N4) Let r and s be positive integers. Define $a_0 = 0, a_1 = 1$, and $a_n = ra_{n-1} + sa_{n-2}$ for $n \geq 2$. Let $f_n = a_1 a_2 \cdots a_n$. Prove that $\dfrac{f_n}{f_k f_{n-k}}$ is an integer for all integers n and k such that $n > k > 0$.

8. (USA 1993) Let a and b be odd positive integers. Define the sequence $\langle f_n \rangle$ by putting $f_1 = a$, $f_2 = b$, and by letting f_n for $n \geq 3$ be the greatest odd divisor of $f_{n-1} + f_{n-2}$. Show that f_n is constant for sufficiently large n and determine the eventual value as a function of a and b.

9. (ISL 1994 N6) Let x_1 and x_2 be relatively prime positive integers. For $n \geq 2$, define $x_{n+1} = x_n x_{n-1} + 1$.

   (a) Prove that for every $i > 1$, there exists $j > i$ such that x_i^i divides x_j^j.

   (b) Is it true that x_1 must divide x_j^j for some $j > 1$?

10. (Brazil MO 2004) Consider the sequence $\langle a_n \rangle_{n=0}^{\infty}$ given by $a_0 = a_1 = a_2 = a_3 = 1$ and
$$a_n a_{n-4} = a_{n-1} a_{n-3} + a_{n-2}^2.$$
Prove that all its terms are integers.

11. (FKMO 2013) Two coprime positive integers a, b are given. Integer sequence $\langle a_n \rangle$, $\langle b_n \rangle$ satisties
$$(a + b\sqrt{2})^{2n} = a_n + b_n\sqrt{2}$$
Find all prime numbers p such that there exist positive integer $n \le p$ satisfying $p \mid b_n$.

12. (KöMaL 1997) Suppose that $a_1, a_2, \dots$ and $b_1, b_2, \dots$ are integer sequences such that $a_1 = b_1 = 0$, and
$$a_n = nb_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1.$$
holds for $n \ge 1$. Prove that, for any prime number p, a_p is divisible by p.

13. The Lucas sequence $\langle L_n \rangle$ is given by $L_0 = 2$, $L_1 = 1$ and $L_{n+1} = L_n + L_{n-1}$ for $n \ge 1$. Prove that if a prime number p divides $L_{2k} - 2$ for $k \in \mathbb{N}$, then p also divides $L_{2k+1} - 1$.

14. (ISL 2003 N7) The sequence $a_0, a_1, a_2, \dots$ is defined as follows: $a_0 = 2$, $a_{k+1} = 2a_k^2 - 1$ for $k \ge 0$. Prove that if an odd prime p divides a_n, then 2^{n+3} divides p.

15. Prove that there exists a Fibonacci primitive root(remember?) modulo p iff $p \equiv 1 \text{ or } 9 \pmod{10}$ and $l(p) = p - 1$.

16. (Lucas–Lehmer primality test) Let $M_p = 2^p - 1$ be the Mersenne number. Define a sequence $\langle s_n \rangle$ for all $n \ge 0$ by
$$s_0 = 4, \quad s_{n+1} = s_n^2 - 2 \ \ \forall n \ge 0.$$
Then M_p is prime if and only if $s_{p-2} \equiv 0 \pmod{M_p}$.