MATEMATICAMENTE

Divisibilidade em Recursões Lineares

Prof. Victor Bitarães
bitaraesv@gmail.com

Vamos olhar nesta lista para as clássicas sequências de Fibonacci e de Lucas; a primeira é dada por $F_1 = 1$, $F_2 = 1$ e $F_{n+2} = F_{n+1} + F_n, \forall n \in \mathbb{N}$, e a outra por $L_1 = 1$, $L_2 = 3$ e $L_{n+2} = L_{n+1} + L_n, \forall n \in \mathbb{N}$. As duas estão intimamente relacionadas.

1 Fatos clássicos

1. Se α, β são as raízes de $x^2 - x - 1$, vale $F_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ e $L_n = \alpha^n + \beta^n$;
2. Todo inteiro positivo tem um múltiplo na sequência Fibonacci;
3. $F_{m+n} = F_{m+1}F_n + F_mF_{n-1}$
4. $\text{mdc}(F_m, F_n) = F_{\text{mdc}(m,n)}$

2 Problemas

1. Prove que todo primo da forma $4k - 1$ divide algum termo da sequência de Lucas.
2. Seja $n > 5$ um inteiro. Suponha que F_n é primo. Prove que n é primo, e que $n | F_n^2 - 1$.
3. **(MEMO 2010)** Há uma fortaleza em cada vértice de um n-ágono regular. Num dado momento, cada fortaleza atira contra exatamente uma das suas vizinhas, atingindo-a. O *resultado do tiroteio* é o conjunto das fortalezas atingidas, não importando a quantidade de vezes que se atingiu cada uma. Seja $P(n)$ o número de possíveis resultados do tiroteio. Prove que, para todo inteiro positivo $k \geq 3$, são coprimos os números $P(k)$ e $P(k+1)$.
4. **(Treinamento Cone Sul)** Considere a sequência dada por $a_1 = 43$, $a_2 = 142$ e $a_{n+2} = 3a_{n+1} + a_n, \forall n \in \mathbb{N}$. Prove que, para todo inteiro positivo m, existem infinitos naturais n tais que $a_n - 1$ e $a_{n+1} - 1$ são ambos múltiplos de m.
5. **(Balcânica 2002)** Dada a sequência $a_1 = 20$, $a_2 = 30$, $a_{n+2} = 3a_{n+1} - a_n$, ache todos os índices n tais que $1 + 5a_na_{n+1}$ é um quadrado perfeito.
6. **(ISL 2004, N4)** Seja k um inteiro fixado maior do que 1, e seja $m = 4k^2 - 5$. Mostre que existem inteiros positivos a e b para os quais a sequência x_n definida por

$$x_0 = a, x_1 = b, x_{n+2} = x_{n+1} + x_n, \forall n \in \mathbb{N}$$

tem todos os seus termos coprimos com m.

Problema 1: Prove que $(\exists m \mid p \mid L_m,)\ \forall p = 4K-1$ primo.

Folha 1/2

$$L_p \underset{p}{\equiv} \left(2^{-1}\cdot(1+\sqrt{5})\right)^p + \left(2^{-1}\cdot(1-\sqrt{5})\right)^p$$

$$\underset{p}{\equiv} (2^{-1})^p \cdot \left(\sum_{i=0}^{\frac{p-1}{2}} 2\binom{p}{2i} 5^i \right).$$

Mas $\binom{p}{i} \underset{p}{\equiv} \begin{cases} 1, & \text{se } i=0 \text{ ou } i=p \\ & \text{ou} \\ 0, & \text{c.c} \end{cases}$,

$$\Rightarrow L_p \equiv (2^{-1})^p \cdot (2 \cdot 5^0).$$

Pelo, P.T.F., $2^{-1} \underset{p}{\equiv} (2^{-1})^p \Rightarrow$

$$\Rightarrow \boxed{L_p \underset{p}{\equiv} 1}.$$

$$L_{p+1} \underset{p}{\equiv} (2^{-1})^{p+1} \cdot \left(\sum_{i=0}^{\frac{p+1}{2}} 2 \cdot \binom{p+1}{2i} 5^i \right)$$

Mas, $\binom{p+1}{i} \underset{p}{\equiv} \begin{cases} 1, & \text{se } i=0 \text{ ou } 1 \text{ ou } p \text{ ou } p+1 \\ 0, & \text{c.c.} \end{cases}$

Logo: $L_{p+1} \underset{p}{\equiv} (2^{-1})^p \cdot \left(5^0 + 5^{\frac{p+1}{2}}\right)$

$$\underset{p}{\equiv} (2^{-1}) \cdot \left(1 + 5\left(\frac{5}{p}\right)\right) \underset{p}{\equiv} (2^{-1}) \cdot \left(1 + 5\left(\frac{p}{5}\right)\right) = \begin{cases} \xrightarrow{\left(\frac{p}{5}\right)=1} 3 \\ \xrightarrow{\left(\frac{p}{5}\right)=-1} -2 \end{cases}$$

Logo: $L_{p-1} = \begin{cases} \xrightarrow{\left(\frac{p}{5}\right)=1} 2 \\ \xrightarrow{\left(\frac{p}{5}\right)=-1} -3 \end{cases}$

Problema 1 - Folha 2/2

Mas: $L^2_{\frac{p\pm1}{2}} = \left(\alpha^{\frac{p\pm1}{2}} + \beta^{\frac{p\pm1}{2}}\right)^2 = \alpha^{p\pm1} + \beta^{p\pm1} + 2(\alpha\beta)^{\frac{p\pm1}{2}}$

$= L_{p\pm1} + 2(-1)^{\frac{p\pm1}{2}}.$

- Se $\left(\frac{p}{5}\right) = +1 \Rightarrow$

$$L^2_{\frac{p-1}{2}} = L_{p-1} + 2(-1)^{\frac{p-1}{2}} \equiv 2 + 2\cdot(-1)$$
$$\equiv 0 \pmod p$$

$\Rightarrow \quad p \mid L_{\frac{p-1}{2}}.$

- Se $\left(\frac{p}{5}\right) = -1 \Rightarrow$

$$L^2_{\frac{p+1}{2}} = L_{p+1} + 2\cdot(-1)^{\frac{p+1}{2}} \equiv -2 + 2$$
$$\equiv 0 \pmod p$$

$\Rightarrow p \mid L_{\frac{p+1}{2}}$

$\square$

Problema 2: Folha 1/1

Seja $n>5$ um inteiro. Suponha que F_n é primo.

Prove que n é primo e que $n \mid F_n^2-1$.

- Se $n>5$ é composto $\Rightarrow n=p\cdot q$, $p>2$ e $q>1$.

Logo: $F_p \mid F_n = \text{primo} \Rightarrow F_p = F_n$ ou $F_p=1$.

Mas $p>2 \Rightarrow F_p>1$ e $n>p>2 \Rightarrow F_n>F_p$. Absurdo!

Logo, n é primo.

$$F_n = \frac{\alpha^n-\beta^n}{\alpha-\beta} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

$$= \frac{2}{2^n}\cdot\left[\sum_{i=0}^{\frac{n-1}{2}}\binom{n}{2i+1}\cdot 5^i\right] \circledast$$

$$\underset{n}{\equiv} (2^{-1})^{n-1}\left[5^{\frac{n-1}{2}}\right] \underset{n}{\equiv} 5^{\frac{n-1}{2}}$$

$$\Rightarrow F_n^2 \underset{n}{\equiv} 5^{n-1} \underset{n}{\equiv} 1 \Rightarrow n \mid F_n^2-1.$$

$\square$

$\circledast$ $\binom{n}{i} \underset{n}{\equiv} \begin{cases} 1, & \text{se } i=0 \text{ ou } i=n \\ 0, & \text{c.c} \end{cases}$

Problema 3 Folha 1/3

(MEMO 2010) Há uma fortaleza em cada vértice de um n-ágono regular. Num dado momento, cada fortaleza atira em uma de suas vizinhas. O "resultado do torneio" é o conjunto das fortalezas atingidas, sem contar multiplicidade. Seja $P(n)$ o # de possíveis resultados do torneio.

Prove que $\forall K \geq 3$, $P(K)$ e $P(K+1)$ são coprimos.

Sol.

Seja $Q_L(K)$ o # de formas de pintar elementos em uma lista de tamanho K, sem que haja consecutivos pintados.

Defina $Q_C(K)$ analogamente, trocando "lista" por "ciclo".

- $Q_L(0) = 1$
- $Q_L(1) = 2$, $Q_L(2) = 3$; $Q_L(3) = 5$
- $Q_L(K) = \underbrace{Q_L(K-1)}_{\text{sem escolher o } 1^\circ} + \underbrace{Q_L(K-2)}_{\text{escolhendo o } 1^\circ}$

Logo, $\underline{Q_L(K) = F_{K+2}}$.

- $Q_C(K) = \underbrace{Q_L(K-1)}_{\text{sem escolher o } 1^\circ} + \underbrace{Q_L(K-3)}_{\text{escolhendo o } 1^\circ}$, $\forall K \geq 3$.

$$= F_{K+1} + F_{K-1} = L_K .$$

Logo, $\underline{Q_C(K) = L_K}$.

Todo resultado de tiroteio ímpar, considerando o ciclo de fortalezas, $a_1, a_3, a_5, \dots, a_n, a_2, a_4, \dots, a_{n-1}$, satisfaz que, para duas fortalezas consecutivas nesse ciclo não há duas vivas (*) (pois a_i atira em a_{i-1} ou a_{i+1}).

Problema 3 - Folha 2/3

Além disso, para toda seleção de fortalezas vivas que satisfaz a propriedade (*), há como construir um resultado de tiroteio correspondente.

Basta:

$$a_i \text{ atirar em } \begin{cases} a_{i+1}, & \text{se } a_{i-1} \text{ é marcado p/ ficar vivo.} \\ a_{i-1}, & \text{c.c.} \end{cases}$$

(Estratégia)

Isso funciona pois a_j continua vivo $\iff$ a_{j-1} não atira em a_j e a_{j+1} não atira em a_j $\iff$

$\iff$ a_{j-1} atira em a_{j-2} e a_{j+1} atira em a_{j+2} $\iff$ a_{j-2} não é marcado p/ ficar vivo e a_j é marcado p/ ficar vivo.

$\iff$ a_j é marcado p/ ficar vivo (pois a_j é marcado p/ ficar vivo $\Downarrow$ a_{j-2} não é marcado p/ ficar vivo)

Logo, $P(2K+1) = Q_c(2K+1) = L_{2K+1}$.

Num torneio par, podemos fazer a mesma observação anterior para esses dois ciclos:

- $a_1, a_3, \dots, a_{n-1}$
- $a_2, a_4, \dots, a_n$.

(*')

I.e., em cada um desses ciclos, dois adjacentes não permanecem vivos.

Usando a mesma Estratégia, podemos obter qualquer seleção de fortalezas vivas com a condição em (*').

Logo: $P(2K) = Q_c(K)^2 = L_K^2$.

Basta provar que $L_{2k\pm1}$ e L_k são coprimos.

Mas, $L_{2k\pm1} = F_{k\pm1} L_{k\pm1} + F_k L_k$

Logo: $\text{mdc}(L_{2k\pm1}, L_k) =$

$$= \text{mdc}(F_{k\pm1} L_{k\pm1}, L_k) =$$
$$= \text{mdc}(F_{k\pm1}, L_k) =$$
$$= \text{mdc}(F_{k\pm1}, F_{k-1} + F_{k+1}) =$$
$$= \text{mdc}(F_{k+1}, F_{k-1}) =$$
$$= \text{mdc}(F_{k+1}, F_k) = 1.$$

$\square$

Problema 4

A sequência é periódica (mod m), pois, por P.C.P.,

o par (a_i, a_{i+1}) e (a_j, a_{j+1}) são iguais, com $i \neq j$.

Mas, dois termos consecutivos definem unicamente a sequência "para frente" e "para trás". Logo, $i-j$ é período.

Mas, $a_0 = 13 \Rightarrow a_{-}$ $\Rightarrow a_{-2} = 1 \Rightarrow a_{-3} = 1$.

Como o par $(a_{3}, a_{-2}$ $(1,1) \equiv (1,1) \pmod{m}$.

e

a sequência é periódica

temos infinitos n's t.q.: $a_n \equiv 1$ e $a_{n+1} \equiv 1 \pmod{m}$.

$\square$