Ciąg Fibonacciego

Pierścienie

1. **Definicja** *Pierścieniem (z jedynką) będę nazywać zbiór R, z określonymi działaniami $+$ i $\cdot$ takimi, że*

   (a) R jest grupą ***przemienną*** *ze względu na $+$, której element neutralny oznaczam 0.*

   (b) Dla wszystkich $a, b \in R$ mamy $a \cdot b \in R$.

   (c) Działanie $\cdot$ jest łączne, tj. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dla wszystkich $a, b, c \in R$.

   (d) Istnieje element neutralny mnożenia $e \in R$:

   $$ea = ae = a$$

   dla wszystkich $a \in R$. Element ten jest jedyny (dowód jak w grupach, patrz poprzednie kółko), oznaczamy go 1 i nazywamy jedynką.

   (e) Działanie $\cdot$ jest rozdzielne względem $+$:

   $$(a+b)c = ac + bc$$

   $$c(a+b) = ca + cb$$

   dla wszystkich $a, b, c \in R$.

   Dla każdego $a \in R$ zachodzi
   $$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$
   odejmujemy $a \cdot 0$ stronami i otrzymujemy $0 = a \cdot 0$.
   Dla każdych $a, b \in R$ zachodzi
   $$-ab = (-a)b = a(-b)$$
   Dowód: $ab - ab = 0 = a0 = a(b + (-b)) = ab + a(-b)$, stąd $-ab = a(-b)$. Analogicznie $ab - ab = 0 = (a + (-a))b = ab + (-a)b$, więc $-ab = (-a)b$.

2. Tak naprawdę warunki na bycie pierścieniem są bardzo słabe i większość zbiorów z działaniami, jakie znane są w liceum jest pierścieniami: liczby rzeczywiste, wymierne, całkowite, wielomiany o współczynnikach np. rzeczywistych itd.

3. **Definicja** *Niech R będzie pierścieniem. Jeżeli dla elementu $a \in R$ istnieje $b \in R$ takie, że*

   $$a \cdot b = b \cdot a = 1$$

   to powiemy, że element a jest odwracalny. Odwrotność elementu a oznaczamy wtedy a^{-1}.

   Uwaga: Jeżeli pierścień nie jest przemienny, to odwrotności nie piszemy jako $\frac{1}{a}$, żeby nie popełnić błędu: $b\frac{1}{a} = \frac{b}{a} = \frac{1}{a}b$. Błąd polega na tym, że środkowy obiekt b/a nie jest zdefiniowany.

4. **Definicja** *Niech R będzie pierścieniem. Powiemy, że R jest przemienny, jeżeli*

   $$a \cdot b = b \cdot a$$

   dla wszystkich $a, b \in R$.

5. **Lemat (Suma ciągu geometrycznego)** *Niech $a \in R$. Załóżmy, że element $1-a$ pierścienia R jest odwracalny. Zachodzi wtedy*

$$1 + a + \cdots + a^{n-1} = (a^n - 1)(a-1)^{-1}$$

DOWÓD. Mamy

$$(1 + a + \cdots + a^{n-1})(a-1) = a^n - 1$$

domnażamy z prawej strony przez $(a-1)^{-1}$:

$$1 + a + \cdots + a^{n-1} = (1 + a + \cdots + a^{n-1})(a-1)(a-1)^{-1} = (a^n - 1)(a-1)^{-1}$$

■

Teoria macierzy

1. **Definicja** *Macierzą o wymiarach 2×2 o elementach ze pierścienia R nazywamy układ $2 \cdot 2 = 4$ liczb $a, b, c, d \in R$ zapisany w postaci*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Zbiór wszystkich macierzy oznaczamy $\mathbb{M}_2(R)$.
Na początku, jeżeli wygląda to zbyt okropnie weź $R = \mathbb{R}$, czyli macierze o wyrazach rzeczywistych.

2. Macierze z danego zbioru możemy dodawać:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{bmatrix}$$

i mnożyć, nieco bardziej skomplikowanie (polecam http://pl.wikipedia.org/wiki/Mnożenie_macierzy):

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}$$

dodatkowo możemy na macierzach zdefiniować mnożenie przez stałą $r \in R$.

$$r \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} := \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} ra_{11} & ra_{12} \\ ra_{21} & ra_{22} \end{bmatrix}$$

3. **Twierdzenie** *Dla dowolnego pierścienia R macierze $\mathbb{M}_2(R)$ tworzą pierścień z działaniami $+$ i $\cdot$. Elementem neutralnym tego pierścienia jest macierz*

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Jeżeli ponadto pierścień R jest przemienny, to zachodzi

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} A = A \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} A$$

dla wszystkich macierzy $A \in \mathbb{M}_2(R)$.

DOWÓD. Aby udowodnić, że macierze są pierścieniem wystarczy przeliczyć wszystkie własności pierścienia. Podobnie można policzyć, że I jest jedynką.

Przeliczę tylko ostatnie stwierdzenie. Niech $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathbb{M}_2(R)$ oraz $r \in R$ wtedy

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} ra_{11} & ra_{12} \\ ra_{21} & ra_{22} \end{bmatrix} = \begin{bmatrix} a_{11}r & a_{12}r \\ a_{21}r & a_{22}r \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$$

■

4. Aby uprościć robotę nieinteresujące mnie elementy macierzy będę oznaczać $*$. Nigdy nie będę ich wyliczać, **ich wartość nie będzie miała wpływu na przekształcenia**. Przykład:

$$\begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} = I = \dots$$

elementy $*$ należy rozumieć jako elementy macierzy sąsiedniej (tutaj I).

Teoria ciągu Fibonacciego

1. **Definicja** *Ciągiem* ***Fibonacciego*** *nazywamy ciąg rekurencyjny* (F_n) *dany równaniami:*

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \text{ dla } n \geq 2$$

Kolejne wyrazy ciągu Fibonacciego to:

n	0	1	2	3	4	5	6	7	8
F_n	0	1	1	2	3	5	8	13	21

Dla wygody zdefiniujemy również wyrazy o indeksach ujemnych, tak, żeby zachowana była własność $F_n = F_{n-1} + F_{n-2}$. *W tym celu należy wziąć* $F_{-n} = (-1)^{n+1}F_n$.

n	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8
F_n	5	-3	2	-1	1	0	1	1	2	3	5	8	13	21

Macierzą ciągu Fibonacciego nazywamy macierz

$\mathbb{F} := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Jest ona odwracalna w $\mathbb{M}_2(\mathbb{Z})$, jej odwrotnością jest $\mathbb{F}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$

Równanie: Bezpośrednio przeliczamy, że

$$\mathbb{F}^2 - \mathbb{F} - I = 0 \text{ stąd wynika po podzieleniu } \mathbb{F} = \frac{1}{\mathbb{F} - I} \text{ a więc } (\mathbb{F} - I)^{-1} = \mathbb{F}$$

Ważna uwaga/metatwierdzenie: Jeżeli rozpatrujemy tylko wyrażenia zawierające $\mathbb{F}$ oraz rI, gdzie $r \in \mathbb{R}$, to każde dwa takie wyrażenia będą przemienne ze sobą, w szczególności możemy pisać odwrotności w normalnej postaci ułamka.

2. **Lemat (Postać macierzowa ciągu)** *Dla każdego* n *całkowitego*

$$\mathbb{F}^n = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$$

Dowód. Zauważmy, że $F^0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} F_1 & F_0 \\ F_0 & F_{-1} \end{bmatrix}$, a więc dla $n = 0$ równość jest prawdziwa. Równość udowodnimy najpierw dla $n \geq 0$, przez indukcję, której bazę właśnie udowodniliśmy. Krok indukcyjny wygląda następująco:

$$\mathbb{F}^{n+1} = \mathbb{F}^n \cdot \mathbb{F} = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} F_{n+1} + F_n & F_{n+1} \\ F_n + F_{n-1} & F_n \end{bmatrix} = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}$$

Pozostaje udowodnić tę równość także dla $n < 0$. Dowód przebiega przez indukcję względem malejącego n, której rdzeniem jest równość

$$\mathbb{F}^{-(n+1)} = \mathbb{F}^{-n}\mathbb{F}^{-1} = \begin{bmatrix} F_{-n+1} & F_{-n} \\ F_{-n} & F_{-n-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} F_{-n} & F_{-n+1} - F_{-n} \\ F_{-n-1} & F_{-n} - F_{-n-1} \end{bmatrix} = \begin{bmatrix} F_{-n} & F_{-n-1} \\ F_{-n-1} & F_{-n-2} \end{bmatrix}.$$

■

Ten dowód przeprowadzony jest wprost, gdyż wydaje mi się pouczający. Poniżej szkic (prostszego) dowodu alternatywnego korzystającego z $\mathbb{F}^2 = \mathbb{F} + I$:
Dowód. Bezpośrednio przeliczamy, że dla $n = 0$ i $n = 1$ równość jest prawdziwa. Przeprowadzamy, jak wyżej, indukcję po n rosnącym i malejącym. Przykładowo – krok indukcyjny w indukcji po n rosnącym

$$\mathbb{F}^{n+2} = \mathbb{F}^n\mathbb{F}^2 = \mathbb{F}^n(\mathbb{F} + I) = \mathbb{F}^{n+1} + \mathbb{F}^n = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix} + \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} =$$

$$\begin{bmatrix} F_{n+2} + F_{n+1} & F_{n+1} + F_n \\ F_{n+1} + F_n & F_n + F_{n-1} \end{bmatrix} = \begin{bmatrix} F_{n+3} & F_{n+2} \\ F_{n+2} & F_{n+1} \end{bmatrix}$$

co było do udowodnienia. Ten dowód korzysta bardzo mocno ze struktury algebraicznej macierzy. ■

Własności ciągu Fibonacciego – zadania prostsze

1. Uzasadnić (elementarnie jest prościej :), że każde dwa kolejne wyrazy ciągu Fibonacciego są są względnie pierwsze.
   Rozwiązanie. Niech $n, d \in \mathbb{Z}_+$ będą takie, że, że $d|F_n,\ d|F_{n+1}$. Wtedy $d|F_{n+1} - F_n = F_{n-1}$. Analogicznie wnioskując $d|F_n - F_{n-1} = F_{n-2}$, itd. Dochodzimy do $d|F_1 = 1$. Tym samym $d = 1$.

2. Uzasadnić, że dla wszystkich liczb naturalnych n, m zachodzi

$$F_{n+1}F_m + F_nF_{m-1} = F_{m+n}$$

   Rozwiązanie.

$$\begin{bmatrix} * & F_{n+m} \\ * & * \end{bmatrix} = \mathbb{F}^{n+m} = \mathbb{F}^n\mathbb{F}^m = \begin{bmatrix} F_{n+1} & F_n \\ * & * \end{bmatrix} \begin{bmatrix} * & F_m \\ * & F_{m-1} \end{bmatrix} = \begin{bmatrix} * & F_{n+1}F_m + F_nF_{m-1} \\ * & * \end{bmatrix}$$

3. W szczególności dla wszystkich liczb naturalnych n zachodzi

$$F_n^2 + F_{n+1}^2 = F_{2n+1}$$

   Rozwiązanie. Równość z poprzedniego zadania dla $m := n + 1$.

4. Niech n będzie liczbą naturalną. Uzasadnić, że

$$F_0 + F_1 + \cdots + F_n = F_{n+2} - 1$$

   Rozwiązanie. Zastosujemy wzór na sumę ciągu geometrycznego

$$\begin{bmatrix} * & F_0 + F_1 + \cdots + F_n \\ * & * \end{bmatrix} = \mathbb{F}^0 + \mathbb{F}^1 + \cdots + \mathbb{F}^n = \frac{\mathbb{F}^{n+1} - I}{\mathbb{F} - I} = \mathbb{F}^{n+2} - \mathbb{F} = \begin{bmatrix} * & F_{n+2} - 1 \\ * & * \end{bmatrix}$$

   Z równości macierzy wynika teza.

5. Niech n będzie liczbą naturalną. Uzasadnić, że

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$$

   Rozwiązanie. Jak w poprzednim przykładzie stosujemy ciąg geometryczny

$$\begin{bmatrix} * & F_1 + F_3 + F_5 + \cdots + F_{2n-1} \\ * & * \end{bmatrix} = \mathbb{F} + \mathbb{F}^3 + \cdots + \mathbb{F}^{2n-1} = \mathbb{F}(\mathbb{F}^0 + \mathbb{F}^2 + \cdots + \mathbb{F}^{2n-2}) =$$

$$\mathbb{F}\frac{\mathbb{F}^{2n} - I}{\mathbb{F}^2 - I} = \mathbb{F}\frac{\mathbb{F}^{2n} - I}{\mathbb{F}} = \mathbb{F}^{2n} - I = \begin{bmatrix} * & F_{2n} \\ * & * \end{bmatrix}$$

6. Niech n będzie liczbą naturalną. Udowodnić, że

$$\sum_{i=1}^{n} iF_i = nF_{n+2} - F_{n+3} + 2$$

   Rozwiązanie.

$$\sum_{i=1}^{n} i\mathbb{F}^i = \sum_{i=1}^{n}(\mathbb{F}^i + \mathbb{F}^{i+1} + \cdots + \mathbb{F}^n) = \sum_{i=1}^{n} \mathbb{F}^i \frac{\mathbb{F}^{n+1-i} - I}{\mathbb{F} - I} = \sum_{i=1}^{n} \mathbb{F}^i(\mathbb{F}^{n+1-i} - I)\mathbb{F} = \sum_{i=1}^{n} \mathbb{F}^{n+2} - \mathbb{F}^{i+1} =$$

$$n\mathbb{F}^{n+2} - \sum_{i=1}^{n} \mathbb{F}^{i+1} = n\mathbb{F}^{n+2} - \mathbb{F}^2\frac{\mathbb{F}^n - I}{\mathbb{F} - I} = n\mathbb{F}^{n+2} - \mathbb{F}^2(\mathbb{F}^n - I)\mathbb{F} = n\mathbb{F}^{n+2} - \mathbb{F}^{n+3} + \mathbb{F}^3$$

   jak zwykle porównujemy współczynniki w prawym górnym rogu, uzyskując tezę (z ostatniej macierzy uzyskamy $F_3 = 2$).

7. Uzasadnić, że dla wszystkich n naturalnych zachodzi

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

ROZWIĄZANIE. Trik. Wiemy, że $\mathbb{F}^n\mathbb{F}^{-n} = I$. Ale można to spróbować policzyć bezpośrednio:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I = \mathbb{F}^n\mathbb{F}^{-n} = \begin{bmatrix} F_{n+1} & F_n \\ * & * \end{bmatrix} \begin{bmatrix} F_{-n+1} & * \\ F_{-n} & * \end{bmatrix} = \begin{bmatrix} F_{n+1}F_{-n+1} + F_nF_{-n} & * \\ * & * \end{bmatrix}$$

wynika stąd $1 = F_{n+1}F_{-n+1} + F_nF_{-n}$. Podstawiamy, korzystając z definicji, $F_{-n+1} = (-1)^n F_{n-1}$, $F_{-n} = (-1)^{n+1}F_n$ i uzyskujemy

$$1 = (-1)^n F_{n+1}F_{n-1} + (-1)^{n+1}F_n^2$$

mnożymy obie strony przez $(-1)^n$:

$$(-1)^n = (-1)^{2n}F_{n+1}F_{n-1} + (-1)^{2n+1}F_n^2 = F_{n+1}F_{n-1} - F_n^2$$

Dalsze własności pierścieni

1. **Definicja** *Niech R będzie pierścieniem. Podzbiór J pierścienia R nazywamy ideałem jeżeli:*

   (a) I jest podgrupą przemienną ze względu na $+$.

   (b) Dla dowolnego $r \in R, i \in I$ zachodzi

   $$r \cdot i \in I \text{ oraz } i \cdot r \in I$$

   J jest ideałem R oznaczamy przez $J \lhd R$.

2. Pojęcie ideału rozszerza pojęcie kongruencji:
   Piszemy $a \equiv b \mod I$ jeżeli $b - a \in I$. Załóżmy, że

   $$a \equiv b \mod I, \quad c \equiv d \mod I$$

   Wtedy (m. in.)

   $$b \equiv a \mod I$$
   $$a + c \equiv b + d \mod I$$
   $$a - c \equiv b - d \mod I$$
   $$ac \equiv bd \mod I$$

   Udowodnię dla przykładu ostatnią (najtrudniejszą) własność.

   $$a \equiv b \mod I \Rightarrow a - b \in I \Rightarrow (a-b)c \in I$$
   $$c \equiv d \mod I \Rightarrow d - c \in I \Rightarrow b(d-c) \in I$$
   $$(a-b)c \in I,\ b(d-c) \in I \Rightarrow ac - bd = (a-b)c - b(d-c) \in I \Rightarrow ac \equiv bd \mod I$$

3. Naturalne w tym kontekście jest zauważenie, że dla ustalonego $n \in \mathbb{Z}$ zbiór postaci

   $$I_n := \{kn \mid k \in \mathbb{Z}\}$$

   jest ideałem w $\mathbb{Z}$. Kongruencje $\mod I_n$ to znane nam kongruencje $\mod n$.

4. **Lemat** *Rozważmy macierze $\mathbb{M}_2(R)$ i niech $I \lhd R$. Zdefiniujmy*

   $$\mathbb{M}_2(I) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R \mid a, b, c, d \in I \right\}$$

   Wtedy $\mathbb{M}_2(I)$ jest ideałem w $\mathbb{M}_2(R)$.

Dowód. Na początku udowodnimy, że $\mathbb{M}_2(I)$ jest podgrupą przemienną. Wystarczy (patrz kółko o grupach) udowodnić, że

$$A, B \in \mathbb{M}_2(I) \Rightarrow A + B \in \mathbb{M}_2(I) \text{ oraz } -A \in \mathbb{M}_2(I)$$

Rozważmy $A := \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, B := \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$. Z definicji $\mathbb{M}_2(I)$ wynika, że $a_i, b_i \in I$. W związku z tym również (z własności ideału I):

$$a_{11} - b_{11} \in I, a_{12} - b_{12} \in I \ldots$$

a stąd

$$A - B = \begin{bmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & a_{22} - b_{22} \end{bmatrix} \in \mathbb{M}_2(I)$$

z definicji $\mathbb{M}_2(I)$. $-A \in \mathbb{M}_2(I)$ udowadniamy analogicznie.

Pozostaje udowodnić drugą własność ideałów. Rozważmy dowolną $C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \in \mathbb{M}_2(R)$ i dowolną $\begin{bmatrix} i_{11} & i_{12} \\ i_{21} & i_{22} \end{bmatrix} \in \mathbb{M}_2(R)$:

$$\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} i_{11} & i_{12} \\ i_{21} & i_{22} \end{bmatrix} = \begin{bmatrix} c_{11}i_{11} + c_{12}i_{21} & c_{11}i_{12} + c_{12}i_{22} \\ c_{21}i_{11} + c_{22}i_{21} & c_{21}i_{12} + c_{22}i_{22} \end{bmatrix}$$

Widać, że np. w pierwszej komórce $i_{11} \in I$ stąd $c_{11}i_{11} \in I$, analogicznie $c_{12}i_{21} \in I$, więc $c_{11}i_{11} + c_{12}i_{21} \in I$. Pozostałe wartości również należą do I, więc cała macierz należy do $\mathbb{M}_2(I)$ (z definicji $\mathbb{M}_2(I)$).
Drugą część drugiej własności udowadniamy analogicznie. ■

Własności ciągu Fibonacciego – zadania trudniejsze

1. Uwaga: poniższe dwa zadania można zrobić elementarnie, korzystając z tożsamości $F_{n+1}F_m + F_nF_{m-1} = F_{m+n}$ oraz z lematu w zadaniu drugim, ale dowody są (moim zdaniem) *trudniejsze* do wymyślenia i *mniej naturalne*, oczywiście z dokładnością do pewnego zrozumienia pojęć abstrakcyjnych.

2. **Twierdzenie (*)** *Jeżeli liczby $n, m \in \mathbb{Z}_+$ oraz $n \mid m$ to*

$$F_n \mid F_m$$

Dowód. Niech $m = nk$.
Wiemy (patrz część teoretyczna), że zbiór

$$J := \mathbb{M}_2(I_{F_n})$$

jest ideałem w $\mathbb{M}_2(\mathbb{Z})$. Rozpatrzmy kongruencje $\mod J$.

$$\mathbb{F}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \equiv \begin{bmatrix} F_{n+1} & 0 \\ 0 & F_{n-1} \end{bmatrix} \mod J$$

Tym samym

$$\begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} = \mathbb{F}^m = (\mathbb{F}^n)^k \equiv \begin{bmatrix} F_{n+1} & 0 \\ 0 & F_{n-1} \end{bmatrix}^k = \begin{bmatrix} F_{n+1}^k & 0 \\ 0 & F_{n-1}^k \end{bmatrix} \mod J$$

Tak więc (wyrazy nieprzydatne w rozumowaniu oznaczam $*$):

$$J \ni \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} - \begin{bmatrix} F_{n+1}^k & 0 \\ 0 & F_{n-1}^k \end{bmatrix} = \begin{bmatrix} * & F_m \\ F_m & * \end{bmatrix}$$

Z definicji J znaczy to, że $F_m = bF_n$ dla pewnego $b \in \mathbb{Z}$, $F_n \mid F_m$. ■

3. **Twierdzenie (*)** *Dla wszystkich liczb naturalnych n, m zachodzi równość*

$$NWD(F_n, F_m) = F_{NWD(n,m)}$$

Dowód.

Lemat *Jeżeli $a, b \in \mathbb{Z}_+$, $d = NWD(a, b)$, to istnieją takie $k, l \in \mathbb{Z}$, $k, l > 0$, że*

$$ak - bl = d$$

Dowód. Liczby $a/d, b/d$ są całkowite i względnie pierwsze, tj. $NWD(a/d, b/d) = 1$. Niech $a' := a/d, b' := b/d$.
Rozważmy wszystkie liczby względnie pierwsze z b' ze zbioru $\{1, 2, \ldots, n\}$. Niech będą to liczby $c_1, \ldots, c_s$. Liczby $c_1a' \mod b', \ldots, c_sa' \mod b'$ należą do tego zbioru (bo są względnie pierwsze z b'), ponadto

$$c_ia' \equiv c_ja' \mod b' \Rightarrow (c_i - c_j)a' \equiv 0 \mod b' \text{ a skoro } NWD(a', b') = 1, \text{ to } c_i \equiv c_j \mod b, c_i = c_j$$

tym samym liczby $c_1a' \mod b', \ldots, c_sa' \mod b'$ są parami różne.
Zachodzi $\{c_1a' \mod b', \ldots, c_sa' \mod b'\} \subseteq \{c_1, \ldots, c_s\}$ i $|\{c_1a' \mod b', \ldots, c_sa' \mod b'\}| = |\{c_1, \ldots, c_s\}|$, a więc $\{c_1a' \mod b', \ldots, c_sa' \mod b'\} = \{c_1, \ldots, c_s\} \ni 1$, w szczególności istnieje c_i: $c_ia' \equiv 1 \mod b'$, czyli istnieje takie $t \in \mathbb{Z}$, że

$$c_ia' + tb' = 1$$

$$c_ia/d + tb/d = 1$$

$$c_ia - (-t)b = d$$

Wiemy, że $c_i > 0$. Pozostaje doprowadzić do stanu, gdy $-t > 0$ czyli gdy $t < 0$. Robimy to następująco: $d = c_ia + tb = (c_i + sb)a + (t - sa)b$. Wybieramy na tyle duże $s > 0$, że $t - sa < 0$. *Tak tak, ten cały dowód to jeszcze raz przeliczenie, że coś jest grupą – stale to robię....* ■

Z poprzedniego twierdzenia wnioskujemy, że

$$F_{NWD(n,m)} \mid F_n \text{ i } F_{NWD(n,m)} \mid F_m \text{ a więc } F_{NWD(n,m)} \mid NWD(F_n, F_m)$$

pozostaje wykazać, że

$$NWD(F_n, F_m) \mid F_{NWD(n,m)}.$$

Niech dla zwięzłości $d := NWD(n, m)$ oraz $D := NWD(F_n, F_m)$.
Korzystamy z lematu i wybieramy takie $k, l \in \mathbb{Z}$, że $nk - ml = d$.
Rozważmy ideał $\mathbb{M}_2(I_D) \lhd \mathbb{M}_2(\mathbb{Z})$. Przypominam, jest to ideał

$$\mathbb{M}_2(I_D) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \; : \; a_{11}, a_{12}, a_{21}, a_{22} \in I_D \right\} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \; : \; D \mid a_{11}, a_{12}, a_{21}, a_{22} \right\}$$

$$\begin{bmatrix} F_{d+1} & F_d \\ F_d & F_{d-1} \end{bmatrix} = \mathbb{F}^d = \mathbb{F}^{nk}\mathbb{F}^{-ml} = \begin{bmatrix} F_{nk+1} & F_{nk} \\ F_{nk} & F_{nk-1} \end{bmatrix} \begin{bmatrix} F_{-ml+1} & F_{-ml} \\ F_{-ml} & F_{-ml-1} \end{bmatrix} \equiv$$

$$\begin{bmatrix} F_{nk+1} & 0 \\ 0 & F_{nk-1} \end{bmatrix} \begin{bmatrix} F_{-ml+1} & 0 \\ 0 & F_{-ml-1} \end{bmatrix} = \begin{bmatrix} F_{nk+1}F_{-ml+1} & 0 \\ 0 & F_{nk-1}F_{-ml-1} \end{bmatrix} \mod \mathbb{M}_2(I_D)$$

Wykorzystujemy tutaj fakt, że $D|F_m|F_{-ml}$ oraz $D|F_n|F_{nk}$. Z definicji $\mathbb{M}_2(I_D)$ jest $F_d \equiv 0 \mod D$, $D \mid F_d$, a jeżeli przypomnimy definicje d, D, otrzymujemy $NWD(F_n, F_m) \mid F_{NWD(n,m)}$.
■

4. **Twierdzenie (**Wzór Bineta)** *Niech $\phi_1 := \dfrac{1+\sqrt{5}}{2}$, $\phi_2 := \dfrac{1-\sqrt{5}}{2}$, innymi słowy, niech będą to pierwiastki równania $x^2 - x - 1 = 0$. Wtedy*

$$F_n = \frac{1}{\sqrt{5}}(\phi_1^n - \phi_2^n)$$

dla wszystkich liczb całkowitych n.

Dowód. **Uwaga:** W tym zadaniu, w przeciwieństwie do pozostałych, rozważamy macierze o wyrazach rzeczywistych, a nie całkowitych.
Rozważmy macierz

$$S := \begin{bmatrix} \phi_1 & \phi_2 \\ 1 & 1 \end{bmatrix}, \text{ wtedy } S^{-1} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\phi_2 \\ -1 & \phi_1 \end{bmatrix}$$

Obliczamy

$$S^{-1}\mathbb{F}S = \begin{bmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{bmatrix}$$

cała operacja nie jest przypadkowa i nazywa się diagonalizacją macierzy. Obliczamy

$$S^{-1}\mathbb{F}^n S = S^{-1}\mathbb{F}\mathbb{F}\dots\mathbb{F}S = S^{-1}\mathbb{F}SS^{-1}\mathbb{F}S\dots\mathbb{F}S = (S^{-1}\mathbb{F}S)^n = \begin{bmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{bmatrix}^n = \begin{bmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{bmatrix}$$

Wyliczamy (w końcowej fazie obliczam tylko potrzebną mi część, pozostałe wyrazy oznaczam $*$):

$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \mathbb{F}^n = S(S^{-1}\mathbb{F}^n S)S^{-1} = S \begin{bmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{bmatrix} S^{-1} =$$

$$\begin{bmatrix} \phi_1 & \phi_2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \phi_1^n & 0 \\ 0 & \phi_2^n \end{bmatrix} \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\phi_2 \\ -1 & \phi_1 \end{bmatrix} = \begin{bmatrix} \phi_1^{n+1} & \phi_2^{n+1} \\ * & * \end{bmatrix} \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\phi_2 \\ -1 & \phi_1 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} \phi_1^{n+1} - \phi_2^{n+1} & * \\ * & * \end{bmatrix}$$

Stąd $F_{n+1} = \frac{1}{\sqrt{5}}(\phi_1^{n+1} - \phi_2^{n+1})$, z czego wynika teza. ■