Pisano-periódus és Arnold diszkrét macskája

Aranymetszés: $\phi := (1+\sqrt{5})/2$.

Fibonacci: $F_0 := 0,\ F_1 := 1, \quad n > 1 : F_n := F_{n-1} + F_{n-2}$;

Lucas: $L_0 := 2,\ L_1 := 1, \quad n > 1 : L_n := L_{n-1} + L_{n-2}$.

Mátrixok: $\mathsf{I} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathsf{F} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{Ł} := \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$.

Köztudomású:[1]

$$F_n = (\phi^n - \bar{\phi}^n)/\sqrt{5}; \quad L_n = \phi^n + \bar{\phi}^n. \ \ (\bar{\phi} = -\phi^{-1}.) \tag{1 a,b}$$

Indukcióval:

$$\mathsf{F}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}; \quad \begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} = \mathsf{Ł}\mathsf{F}^n = \mathsf{F}^{n-1} + \mathsf{F}^{n+1}. \tag{2 a,b}$$

Az előzőből (vagy közvetlenül indukcióval):

$$F_{-n} = (-1)^{n-1} F_n; \quad L_{-n} = (-1)^n L_n. \tag{3 a,b}$$

$$F_{n+k} - (-1)^k F_{n-k} = F_k L_n; \quad F_{n+k} + (-1)^k F_{n-k} = F_n L_k. \tag{4 a,b}$$

*

F_n viselkedését vizsgáljuk mod m, ahol m pozitív egész szám. A maradékosztályokat a legkisebb nem-negatív elemükkel reprezentáljuk. Mátrixra/vektorra a mod m komponensenként értendő. A „$\overset{\equiv}{m}$” jelölés mod m kongruenciát jelent. N hosszúságú tiszta periódusokat 1-től N-ig (nem pedig 0-tól $N-1$-ig) ábrázolunk.

(A) *Periodicitás*

F^n tisztán periodikus mod m. Ugyanis a mod m különböző mátrixok véges száma miatt van olyan N_1 és N_2, hogy $\mathsf{F}^{N_1} \overset{\equiv}{m} \mathsf{F}^{N_2}$, amiből $N := N_2 - N_1$-re $\mathsf{F}^N \overset{\equiv}{m} \mathsf{I}$. — Jelölje $P(m)$ a legkisebb pozitív N-et.

F^n-nel együtt F_n is periodikus mod m, hiszen F_n-ek állnak F^n mellékátlójában. F_n minimális periódusának hossza nyilván nem lehet nagyobb $P(m)$-nél, de kisebb sem lehet, mert ha $F_{n-1} \overset{\equiv}{m} 1$ és $F_n \overset{\equiv}{m} 0$ már korábban előfordulna, akkor $F_{n+1} = F_n + F_{n-1} \overset{\equiv}{m} 1$ miatt már F^n is kongruens lenne I-vel.

Ez a minimális periódus a „mod m Pisano-periódus”.

(B) *Periódushosszak*

$P(1) = 1$: a periódus 0.

$P(2) = 3$: a periódus 1, 1, 0.

$m > 2$-re $P(m)$ páros: $+1$ és -1 mod m különbözik, $\det \mathsf{F} = -1$, $\det \mathsf{F}^{P(m)} = +1$.

$P(m) = 2$ és $P(m) = 4$ nem fordul elő: $m \leq 2$-re láttuk, hogy nem; $m > 2$-re a periódus kezdetén az 1, 1, 2 nem csonkul, így az 1, 0 csak ezután jöhet.

[1] Megkapható $x^2 = x + 1$-re illesztéssel (cf. pl. Gelfond: *Исчисление конечных разностей*, V, 4), lánctörtekből (cf. Hardy–Wright: *An Introduction to the Theory of Numbers*, X,14); közvetlenül is verifikálható, a kulcslépés: $\phi^2 = \phi + 1$.

Minden más páros szám előfordul, véges sok m-re, mint $P(m)$:

Jelöljünk egy (nem okvetlenül minimális) periódushosszat $N = 2n$-nel; $n > 2$.

(3 a) miatt $F_{N-k} \underset{N}{\equiv} F_{-k} \underset{N}{\equiv} (-1)^{k-1} F_k$. $\qquad (*)$

$2 \not| n$ —

(4 a)-ból $k = n-1$-re $F_{N-1} \underset{L_n}{\equiv} 1$; $k = n$-re $F_N \underset{L_n}{\equiv} 0$. $P(L_n)$ tehát osztója N-nek. De nem lehet valódi osztója: valódi osztó $\le n$, és $h \le n$-re nem lehet $F_h \underset{L_n}{\equiv} 0$, mert $F_h > 0$ és nem csonkul ($L_n > F_n \ge F_h$). Tehát $P(L_n) = N$.

Ha m olyan, hogy az N periódus mod m-re: $(*)$-ból $k = n-1$-re $m | F_{n+1} + F_{n-1}$, (4 a)-ból $F_{n+1} + F_{n-1} = L_n$; ezért $m | L_n$.

$2 | n$ —

(4 b)-ből $k = n-1$-re $F_{N-1} \underset{F_n}{\equiv} 1$; $k = n$-re $F_N \underset{F_n}{\equiv} 0$. $P(F_n)$ tehát osztója N-nek. Nem valódi osztó: $h < n$-re $F_h \underset{F_n}{\not\equiv} 0$, mert F_h nem csonkul ($F_n > F_h$), $h = n$-re pedig, ugyanebből az okból, $F_{h-1} \underset{F_n}{\not\equiv} 1$. Tehát $P(F_n) = N$.

Ha az N periódus mod m-re: $(*)$-ból $k = n-1$-re $m | F_{n+1} - F_{n-1}$, (4 b)-ből[1] $F_{n+1} - F_{n-1} = F_n$; ezért $m | F_n$.

Összefoglalva —

$$M_n := \begin{cases} L_n, & \text{ha } 2 \not| n; \\ F_n, & \text{ha } 2 \,|\, n. \end{cases}$$

$n > 2$-re $P(M_n) = N = 2n$. Ha $P(m) | N$, akkor $m | M_n$. Megfordítva, ha $m | M_n$, akkor nyilván $P(m) | N$; ha ez nem egyenlőség, akkor m már korábban is szerepelt (a „saját" N-jéhez tartozó $M_{N/2}$-nél vagy $P(2)$-nél).[2]

(C) *Redukáló relációk*

$P([m,n]) = \big[P(m), P(n)\big]$.

Ugyanis egyrészt $k | n \Longrightarrow P(k) | P(n)$ miatt $P(m)$ is, $P(n)$ is, és így $\big[P(m), P(n)\big]$ is osztja $P([m,n])$-et; másrészt $P([m,n])$ osztja $P(m)$ és $P(n)$ szorzatát, amelyben azonban a közös periódushossz-osztókat elég egyszeresen tekintetbe venni: $\dfrac{P(m)P(n)}{\big(P(m), P(n)\big)} = \big[P(m), P(n)\big]$.

Következmény: ha $m = p_1^{e_1} \cdots p_r^{e_r}$ akkor $P(m) = \big[P(p_1^{e_1}), \ldots, P(p_r^{e_r})\big]$.

$P(p^{e+1}) \,|\, p^e P(p)$; ha $P(p^2) \neq P(p)$,[3] akkor $P(p^{e+1}) = p^e P(p)$.

Ugyanis $\mathbf{F}^{P(p^e)} = \mathbf{I} + p^e \mathbf{R}_e$, $\mathbf{F}^{pP(p^e)} = \mathbf{I} + \binom{p}{1} p^e \mathbf{R}_e + \binom{p}{2} p^{2e} \mathbf{R}_e^2 + \cdots + p^{pe} \mathbf{R}_e^p$, $\mathbf{F}^{pP(p^e)} \underset{p^{e+1}}{\equiv} \mathbf{I}$, amiből $P(p^{e+1}) | pP(p^e)$; másrészt nyilván $P(p^e) | P(p^{e+1})$.

Ezért $P(p^{e+1})$ vagy $= P(p^e)$, vagy $= pP(p^e)$.

[1] Sőt már a definícióból is.

[2] Fordított paritással (4 b,a)-ból látni, hogy $2n$-re nem ér véget a periódus ($F_{2n} \equiv 0$ ugyan most is, de $F_{2n-1} \equiv -1$ mindkét esetben), viszont $4n$-re véget ér. Ezzel nem kapunk új periódusokat (a fentiekben már mind szerepelt), de pl. kapunk egy felső becslést és némi szerkezeti információt.

[3] Ez fennáll, ha $p < 10^{14}$; nem tudom, hogy mindig-e.

Ha $P(p^2)\neq P(p)$, akkor $P(p^2)=pP(p)$ és $p\not|\,\mathbf{R}_1$, továbbá $p\not|\,\mathbf{R}_2$: $p=2$-re (számolásból) $\mathbf{R}_2=\mathbf{F}^3$, $p\neq 2$-re pedig $\mathbf{F}^{P(p^2)}=\mathbf{F}^{pP(p)}\underset{p^3}{\equiv}\mathbf{I}+p^2\mathbf{R}_1$. Ha $e>1$, ez öröklődik e-ről $e+1$-re: $P(p^{e+1})=pP(p^e)$, $\mathbf{F}^{P(p^{e+1})}\underset{p^{e+2}}{\equiv}\mathbf{I}+p^{e+1}\mathbf{R}_e$,[1] $p\not|\,\mathbf{R}_{e+1}$.

(D) *Ingadozás*

$P(m)\in\left(2\dfrac{\log m}{\log\phi},6m\right]$; $P(m)$ az alsó értéket tetszőlegesen megközelíti, a felsőt végtelen sokszor felveszi:[2]

$2\not|\,n$-re $P(L_n)\searrow 2\dfrac{\log L_n}{\log\phi}$; L_n-mentes m-sorozatra $P(m)$ határozottan nagyobb:

(1 b)-ben $\bar\phi^n\to 0$ és $2\not|\,n$-re negatív. — $P(m)=N=2n\implies m|M_n;\ M_n\leq L_n$.

$P(m)=6m$, ha $m=2\cdot 5^e,\ e>0$; más m-re $P(m)<6m$:

m felbontása $p_1^{e_1}\cdots p_r^{e_r}$; $\widehat m:=p_1\cdots p_r$.

$P(\widehat m)=[P(p_1),\ldots,P(p_r)]$; $P(m)\,\big|\,P(\widehat m)\cdot p_1^{e_1-1}\cdots p_r^{e_r-1}$.[3] $P(m)/m\leq P(\widehat m)/\widehat m$.

$p\neq 2,5$ —

$F_p\underset{\bar p}{\equiv}\pm1$: (1 a)-t kifejtve $F_p=2^{1-p}\Big(p+\binom{p}{3}5+\binom{p}{5}5^2+\ldots+5^{(p-1)/2}\Big)$; $2^{p-1}\underset{\bar p}{\equiv}1$, $5^{(p-1)/2}\underset{\bar p}{\equiv}\left(\frac{5}{\bar p}\right)$, a többi tag osztható p-vel.

$-1=\det\mathbf{F}^p=F_{p+1}F_{p-1}-F_p^2$; $p\,|\,F_{p+1}F_{p-1}$. $\bar p:=\begin{cases}p-1, & \text{ha } p|F_{p-1};\\ p+1 & \text{különben.}\end{cases}$[4]

$F_{\bar p-1}\underset{\bar p}{\equiv}F_{\bar p+1}\underset{\bar p}{\equiv}\pm1$. Ha $+1$: $\mathbf{F}^{\bar p}\underset{\bar p}{\equiv}\mathbf{I}$, $P(p)\,|\,\bar p$; ha -1: $\mathbf{F}^{\bar p}\underset{\bar p}{\equiv}-\mathbf{I}\implies\mathbf{F}^{2\bar p}\underset{\bar p}{\equiv}\mathbf{I}$, $P(p)\,|\,2\bar p$; mindenképp $P(p)\,|\,2\bar p=4\cdot\bar p/2$ ($\bar p$ páros).

Jelöljük $\widetilde m$-mel az $\widehat m$ 2-től és 5-től különböző prímtényezőinek szorzatát, $\overline m$-mel a megfelelő $\bar p/2$-k szorzatát; $\overline m/\widetilde m<1$, mert minden tényezője <1. $P(\widetilde m)$ osztja a $4\cdot\bar p/2$-k legkisebb közös többszörösét. A 4 kiemelhető, a legkisebb közös többszöröst majorálja a szorzat, $P(\widetilde m)/\widetilde m\leq 4\overline m/\widetilde m<4$.

$2\,|\,\widehat m$ vagy $5\,|\,\widehat m$ —

Ha $\widetilde m$ nem üres: 2 miatt $P(\widetilde m)/\widetilde m$ legfeljebb $P(2)/2=3/2$-vel szorzódik, 5 miatt — $P(5)=4\cdot5$, de a 4-et már kiemeltük — legfeljebb 1-gyel szorzódik, tehát $P(\widehat m)/\widehat m<6$. Ha $\widetilde m$ üres: $P(2)/2=3/2$, $P(5)/5=4$, $P(2\cdot5)/2\cdot5=6$.

$\widehat m=2\cdot5\implies m=2^{1+e_2}\cdot5^{1+e_5},\ e_2,e_5\geq0$.

Explicit számolásból $P(2)=3$ és $P(2^2)\neq P(2)$, $P(5)=20$ és $P(5^2)\neq P(5)$; így $P(2^{1+e_2}\cdot5^{1+e_5})=[3\cdot2^{e_2},20\cdot5^{e_5}]=2^{\max\{e_2,2\}}\cdot3\cdot5^{1+e_5}$.

$e_2=0$-ra $P(m)=6m$, $e_2=1$-re $P(m)=3m$, $e_2\geq2$-re $P(m)=1.5m$.

Tehát $P(m)/m\leq6$; egyenlőség akkor és csak akkor van, ha $m=2\cdot5^e,\ e>0$.[5]

---

[1] Akkor is, ha $p=2$.

[2] Pl. $P(10420180999117162549)=182$, $P(50)=300$,

[3] „|” helyett „=” igaz, ha minden 1-nél nagyobb kitevőjű p-re $P(p^2)\neq P(p)$.

[4] Nem fog kelleni, de igaz: $p=5k\pm1$-re $\bar p=p-1$, $p=5k\pm2$-re $\bar p=p+1$.

[5] Ez is igaz: $P(m)=m\iff m=1\vee m=2^3\cdot3\cdot5^e,\ e\geq0$.

(E) mod m *zérusok*

A periódus zérussal zárul.[1]

$m = 1, 2$-re nincs több. A továbbiakban $m > 2$.

Legyen h a legkisebb pozitív index, amelyre $m|F_h$; $r := F_{h-1} \bmod m$. Ha $r = 1$, akkor $h = P(m)$ és nincs több zérus. Ellenesetben is $F_{h+1} \underset{m}{\equiv} r$ (a rekurzióból); $r^2 \underset{m}{\equiv} \det \mathbf{F}^h = (-1)^h$. Ha $2|h$, akkor $r^2 \underset{m}{\equiv} 1$, $\mathbf{F}^{2h} \underset{m}{\equiv} \mathbf{I}$, $2h = P(m)$ és két zérus van. Ha $2\not|h$, akkor $r^2 \underset{m}{\equiv} -1$, $r^4 \underset{m}{\equiv} 1$, $\mathbf{F}^{4h} \underset{m}{\equiv} \mathbf{I}$, $4h = P(m)$ és négy van. Mind a két többlet-zérusos esetben $\det \mathbf{F}^{P(m)/2} = 1$.

$P(m)/2$ egész szám, jelöljük n-nel; $n > 2$. Ha van többlet-zérus, F_n mindenesetre az. $2\not|n$ esetén $\det \mathbf{F}^n = -1$, többlet-zérus nincs. $2|n$ esetén (B) miatt $m|F_m$, tehát eleve van (legalább egy) többlet-zérus.[2] Három többlet-zérus csak akkor lehet, ha $2\|n$ $(2\not|h)$.[3]

(F) *Macska-transzformáció*

$E := [0,1) \times [0,1)$ — a féligzárt egységnégyzet; $(x, y) \in E$.

Egy (x_0, y_0) pont k-adik transzformáltja $(x_k, y_k) := \big((x_{k-1}, y_{k-1})\mathbf{F}\big) \bmod 1$.[4]

A transzformáció önmagára képezi le E-t; az inverze $\big((x_k, y_k)\mathbf{F}^{-1}\big) \bmod 1$.[5]

$(x_k, y_k) = \big((x_0, y_0)\mathbf{F}^k\big) \bmod 1$ (minden k-ra).

A transzformáció V. I. Arnoldtól való.[6]

Világos, hogy hogy a racionális pontokból álló véges részhalmazok, és csak azok, véges számú lépésben újra pontonként az eredeti helyükre kerülnek, mégpedig ha a legkisebb közös nevező m, akkor $P(m)$ lépésben (és annak többszöröseiben).

A diszkrét feladat: adott m-re vizsgálni az m-nevezőjű racionális pontok transzformációit.

Egész számokkal dolgozhatunk, ha egységnégyzet helyett $m \times m$-es „pixel”-négyzetet és mod 1 helyett mod m-et használunk. E most $[0, m-1] \times [0, m-1]$; $(x_k, y_k) := (x_{k-1} + y_{k-1} \bmod m, x_{k-1})$.

---

[1] L_n is minden m-re periodikus, de végtelen sok szám, köztük végtelen sok prím, nem osztja semelyiket sem (a legkisebb nem-osztók: 5, 8, 10, 12, 13); nincs is *egy* mátrix, amely generálná L_n-t.

[2] Pontosan egy, ha $m = F_n$ (a kisebb indexű F-ek nem csonkulnak).

[3] Fordítva nem következik: $m = F_{2k+1}$-re négy zérus van (az első negyed végén F_{2k+1} áll); $m = F_{4k+2}$-re (noha $2^2 \| P(F_{4k+2}) = 8k+4$) csak egy (a korábbi F-ek nem csonkulnak).

[4] $\mathbf{F}$ előáll így is: $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ (rendre x irányú átrendezés, x tengelyre tükrözés, y irányú átrendezés).

[5] E-t tórusznak tekinthetjük; ekkor a leképezés oda-vissza folytonos stb. stb.

[6] Valójában ő nem $\mathbf{F}$-fel, hanem $\mathbf{F}^2$-tel transzformál. $\mathbf{F}^2 = \left(\begin{smallmatrix}2&1\\1&1\end{smallmatrix}\right)$ periódushossza $m = 1, 2$-re megegyezik $P(m)$-mel, $m > 2$-re feleannyi. Az F_{2k} mod m periódusban 1 vagy 2 zérus van (a teljes periódusban egy felező zérus páros, egy negyedelős zérus páratlan indexű, cf. (E)). — $\mathbf{F}^2$ előáll így is: $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ (*ebben* a sorrendben).

Legyen $T = T(x_0, y_0)$ az E-n értelmezett függvény, a k-adik transzformáltja, $T^{(k)}$ pedig $T(x_k, y_k)$.

A „macska” név onnan ered, hogy a diszkrét esetet demonstráló első programban T egy macska képe volt.

Példa[1] — $m = 75$, $P(m) = 200$:

$T^{(0)}$

$T^{(18)}$

$T^{(k)}$ általában látszólag kaotikus, zagyvazajos vagy pacarácsos, T-vel semmiféle kapcsolatban nem álló mintázatot mutat (noha nem az, hiszen $P(m) - k$-szor transzformálva visszaadja T-t).[2]

Most jönne, de még nincs leírva, a lényeg: a transzformáltak statisztikai tulajdonságai és megkülönböztethetőségük az igazi-véletlen mintázatoktól.

[1] Az eredeti macskát a Wikipedia szerint szerzői jog védi; védetlen tigrissel helyettesítem.

[2] Ha $\mathbf{F}^k \underset{m}{\equiv} -\mathbf{I}$, és csak akkor, ott újra megjelenik T, de fejjel lefelé. Ez csak periódusközépen történhetik meg. Megtörténik, ha $m = F_{2h+1}$ vagy L_{2h} (cf. a lábjegyzetet (B) végén), valamint ha $4 | P(m)$ (vagyis van többlet-zérus) és m prím (prímre $\sqrt{1}$ vagy 1, vagy -1).