Another conjecture on Markov triples

— Markov triples $\mathbf{mod}\ N$ —

T. Asai ($Yaizu$)

Aichi N.T. Seminar / May 19, 2018

Markov triple vector : $[x, y, z] \in \mathbf{Z}^3$

$$\overset{def}{\iff} \quad x^2 + y^2 + z^2 - 3xyz = 0,$$
$$\& \quad x > 0,\ y > 0,\ z > 0.$$

$$\odot \qquad x^2 + y^2 + z^2 - 3xyz = 0$$
$$\iff \quad x^2 + y^2 = z \cdot z',\ z' = 3xy - z.$$

$$\odot \qquad x > y > z \implies x' < y < x < y' < z'.$$

$\mathcal{M} \doteq$ "the set of all Markov triple vectors"

$\mathfrak{S}(\mathcal{M}) \ni A, J, K,\ Q = AK, P = A^2K$:

$$[x, y, z]A \doteq [y, z, x],\ [x, y, z]J \doteq [z, y, x],$$

$$[x, y, z]K \doteq [z, y', x],\ y' = 3zx - y.$$

$$[x, y, z]Q \doteq [x, z', y],\ [x, y, z]P \doteq [y, x', z].$$

$$[1, 1, 1] \underset{P}{\overset{Q}{\rightarrow}} [1, 2, 1] \xrightarrow{Q} [1, 5, 2] \xrightarrow{P} [5, 29, 2]$$

Markov numbers with Farey index

$$[\mathbf{1},\mathbf{1},\mathbf{1}] = [m(\tfrac{\mathbf{-1}}{\mathbf{1}}), m(\tfrac{\mathbf{0}}{\mathbf{1}}), m(\tfrac{\mathbf{1}}{\mathbf{0}})] = \ddot{m}(\tfrac{\mathbf{0}}{\mathbf{1}})$$
$$\xrightarrow{P} [\mathbf{1},\mathbf{2},\mathbf{1}] = [m(\tfrac{\mathbf{0}}{\mathbf{1}}), m(\tfrac{\mathbf{1}}{\mathbf{1}}), m(\tfrac{\mathbf{1}}{\mathbf{0}})] = \ddot{m}(\tfrac{\mathbf{1}}{\mathbf{1}})$$
$$\xrightarrow{Q} [\mathbf{1},\mathbf{5},\mathbf{2}] = [m(\tfrac{\mathbf{0}}{\mathbf{1}}), m(\tfrac{\mathbf{1}}{\mathbf{2}}), m(\tfrac{\mathbf{1}}{\mathbf{1}})] = \ddot{m}(\tfrac{\mathbf{1}}{\mathbf{2}})$$
$$\xrightarrow{P} [\mathbf{5},\mathbf{29},\mathbf{2}] = [m(\tfrac{\mathbf{1}}{\mathbf{2}}), m(\tfrac{\mathbf{2}}{\mathbf{3}}), m(\tfrac{\mathbf{1}}{\mathbf{1}})] = \ddot{m}(\tfrac{\mathbf{2}}{\mathbf{3}}),$$

$m(\frac{0}{1})$=**1**, $m(\frac{1}{1})$=**2**, $m(\frac{1}{2})$=**5**, $m(\frac{1}{3})$=**13**, $m(\frac{2}{3})$=**29**,
$m(\frac{1}{4})$=**34**, $m(\frac{1}{5})$=**89**, $m(\frac{3}{4})$=**169**, $m(\frac{2}{5})$=**194**, $\cdots$

$$\mathcal{F} \doteq \{r \in \mathbf{Q} \mid \mathbf{0} \le r \le \mathbf{1}\} \ni r \longmapsto m(r),\ \ddot{m}(r)$$

The Uniqueness Conjecture (Frobenius 1913)
The mapping "$\mathcal{F} \ni r \longmapsto m(r)$" is injective.

Markov triple Descent ($\rightsquigarrow$ "transitivity")

$$[\mathbf{194},\mathbf{13},\mathbf{5}] \xrightarrow{A^2} [\mathbf{5},\mathbf{194},\mathbf{13}] \xrightarrow{K} [\mathbf{13},\mathbf{1},\mathbf{5}] \xrightarrow{A^2} [\mathbf{5},\mathbf{13},\mathbf{1}]$$
$$\xrightarrow{K} [\mathbf{1},\mathbf{2},\mathbf{5}] \xrightarrow{A} [\mathbf{2},\mathbf{5},\mathbf{1}] \xrightarrow{K} [\mathbf{1},\mathbf{1},\mathbf{2}] \xrightarrow{A} [\mathbf{1},\mathbf{2},\mathbf{1}].$$
$$\therefore [\mathbf{194},\mathbf{13},\mathbf{5}] = [\mathbf{1},\mathbf{2},\mathbf{1}]\boldsymbol{A^2KA^2KAKA}.$$

Observations : $m(r) \pmod N$?

$\mathcal{F}_n \doteq \{r = \frac{h}{k} \in \mathcal{F} \mid 1 \le k \le n\}$

$N = 4,\ r \in \mathcal{F}_{500},\ \sharp = 76117$

$m(r) \pmod 4$	0	1	2	3
times	0	57047	19070	0
ratio	0	0.749	0.251	0

$\because\ m(\frac{h}{k}) \equiv 0 \pmod 2 \Leftrightarrow h \equiv k \equiv \pm 1 \pmod 3.$

$N = 5,\ r \in \mathcal{F}_{1000},\ \sharp = 304193$

$m(r) \pmod 5$	0	1	2	3	4
times	60800	76068	45657	45598	76070
ratio	0.200	0.250	0.150	0.150	0.250

$N = 7,\ r \in \mathcal{F}_{1000},\ \sharp = 304193$

$m(r) \pmod 7$	0	1	2	3	4	5	6
times	0	87945	64683	0	0	65745	85820
ratio	0	0.289	0.213	0	0	0.216	0.282

Observations : $\ddot{m}(r)\,(\mathbf{mod}\ N)$?

$N = 7,\ \ddot{m}(r)(\mathbf{mod}\,7)$ -table

$[1,1,1]$,	$[1,1,2]$,	$[1,2,1]$,	$[1,2,5]$,
$[1,5,2]$,	$[1,5,6]$,	$[1,6,5]$,	$[1,6,6]$,
$[2,1,1]$,	$[2,1,5]$,	$[2,2,6]$,	$[2,5,1]$,
$[2,6,2]$,	$[2,6,6]$,	$[5,1,2]$,	$[5,1,6]$,
$[5,2,1]$,	$[5,5,6]$,	$[5,6,1]$,	$[5,6,5]$,
$[6,1,5]$,	$[6,1,6]$,	$[6,2,2]$,	$[6,2,6]$,
$[6,5,1]$,	$[6,5,5]$,	$[6,6,1]$,	$[6,6,2]$.

$m(\mathbf{mod}\ 7)$	0	1	2	3	4	5	6
times	0	8	6	0	0	6	8
ratio	0	0.286	0.214	0	0	0.214	0.286

times of $\ddot{m}(r)(\mathbf{mod}\ 7),\ r \in \mathcal{F}_{1000}$

11233,	11474,	11338,	10968,
11660,	10676,	11537,	11271,
11063,	11056,	10199,	11217,
9846,	9855,	11507,	10840,
10935,	10854,	11303,	11047,
10881,	9891,	10250,	10993,
10451,	10887,	11034,	9927.

uniform ?

Markov triple vectors $\mathbf{mod}\ N$

$$\boldsymbol{\mathcal{M}_N \doteq \{[x,y,z] \in (\mathbf{Z}/N\mathbf{Z})^3 \mid \text{(i) \& (ii) \& (iii)}\},}$$

(i) $\boldsymbol{x^2+y^2+z^2-3xyz \equiv 0\ (\mathbf{mod}\ N),}$

(ii) $\boldsymbol{(x,y,z,N)=1,}$

(iii) $\boldsymbol{[x,y,z] \equiv [1,1,1],[2,1,1],[1,2,1]}$
or $\boldsymbol{[1,1,2]\ (\mathbf{mod}\,4)}$ if $\boldsymbol{4|N.}$

$\odot$ $\boldsymbol{\ell(N) \doteq \sharp\,\mathcal{M}_N = \prod \ell(p^e),}$

$\boldsymbol{\ell(p^e) = \ell(p)p^{2e-2}\ \ (p \neq 2),}$

$\boldsymbol{\ell(p) = p(p+3)\ \ (p \equiv 1\ (\mathbf{mod}\ 4)),}$

$\boldsymbol{\ell(p) = p(p-3)\ \ (p \equiv 3\ (\mathbf{mod}\ 4),\ \ p \neq 3),}$

$\boldsymbol{\ell(2) = 2^2,\ \ell(2^e) = 2^{2e-2}\ (e>1),\ \ell(3) = 2^3.}$

The reduction map $\boldsymbol{\pi_N : \mathcal{M} \longrightarrow \mathcal{M}_N}$ is well defined by $\boldsymbol{\pi_N([x,y,z]) = [x,y,z]\,(\mathbf{mod}\ N).}$

$\odot$ $\boldsymbol{\pi_N(\mathcal{M}) = \pi_N(\mathcal{M}_{\mathcal{F}}),\ \mathcal{M}_{\mathcal{F}} = \{\ddot{m}(r) \mid r \in \mathcal{F}\}.}$

$\because$ It is shown by using some finite group action.

$\boldsymbol{\Gamma \doteq \langle A, K, J\rangle \subset \mathfrak{S}(\mathcal{M}),}$

$\boldsymbol{A^3 = K^2 = J^2 = I,\ JA = A^2J,\ JK = KJ.}$

$\boldsymbol{PGL_2(\mathbf{Z})} \xrightarrow{\exists\, hom} \boldsymbol{\Gamma}$ by $\begin{bmatrix} & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$

and $\begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \longmapsto \boldsymbol{A, K}$ and $\boldsymbol{J}$, respectively.

$\therefore \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} \longmapsto \boldsymbol{AK = Q}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \longmapsto \boldsymbol{A^2K = P.}$

⊙ The representation $\boldsymbol{PGL_2(\mathbf{Z}) \longrightarrow \mathfrak{S}(\mathcal{M})}$ is faithful.

⊙ The actions of $\boldsymbol{PGL_2(\mathbf{Z}) \cong \Gamma = \langle A, K, J\rangle}$ and $\boldsymbol{PSL_2(\mathbf{Z}) \cong \langle A, K\rangle}$ on $\boldsymbol{\mathcal{M}}$ are both transitive.

For $\boldsymbol{r \in \mathrm{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}}$, $(\,\boldsymbol{\infty = \pm 1/0}\,)$
the indexed Markov number $\boldsymbol{m(r)}$ is well defined by

$$\boldsymbol{[m(r),\ *,\ *] = [1, 2, 1]S,}$$

where $\boldsymbol{S(0) = r,\ S \in PGL_2(\mathbf{Z})}$; being consistent with the Farey index when $\boldsymbol{r \in \mathcal{F}}$. Also it is valid

⊙ $\boldsymbol{[1, 2, 1]S = [m(S(0)),\ m(S(1)),\ m(S(\infty))].}$

Similarly, $\boldsymbol{\Gamma = \langle A, K, J\rangle = PGL_2(\mathbf{Z}) \overset{act}{\curvearrowright} \mathcal{M}_N.}$

$\boldsymbol{\psi_N \ : \ \Gamma \xrightarrow{hom} \mathfrak{S}(\mathcal{M}_N) = \mathfrak{S}_\ell, \ \ \ell = \ell(N).}$

$\boldsymbol{G_N \doteq \psi_N(\Gamma) = \psi_N(\langle A, K, J\rangle) = \langle a, k, j\rangle.}$

Example. $\boldsymbol{G_7 \subset \mathfrak{S}_{28}}$, $\boldsymbol{|G_7|}$ = 123863040 = $2^{10}\, 4!\, 7!$,

$\boldsymbol{G_7 \triangleright \exists N_7,\ G_7/N_7 \cong \mathfrak{S}_7 \therefore \ker \psi_7}$ is non-congruence.

$\odot$ $\boldsymbol{\pi_N}$ is surjective $\Longleftrightarrow$ $\boldsymbol{G_N}$ is transitive.

Conjecture (ver.1)

$\boldsymbol{\pi_N : \mathcal{M} \to \mathcal{M}_N}$ is surjective for every $\boldsymbol{N > 1.}$

or equivalently,

Conjecture (ver.2)

$\boldsymbol{\mathfrak{S}_{\ell(N)} \supset G_N}$ is transitive for every $\boldsymbol{N > 1.}$

- Yes for $\boldsymbol{N < 200.}$ (checked by `PARI/GP`)
- surjective $\Rightarrow$ transitive $\Rightarrow$ "uniform" (?)

Theorem. Let p be a prime. In both the cases below,

$\mathfrak{S}_{\ell(N)} \supset G_N$ is transitive for $N = p^e, e > 0$.

(1) G_p is transitive and $p \equiv 1 \pmod 4$,

(2) G_{p^2} (or G_{2^3} if $p = 2$) is transitive.

Corollary.

The map $\pi_{p^e} : \mathcal{M} \longrightarrow \mathcal{M}_{p^e}$ is surjective for each prime $p < 300$ with $p \equiv 1 \pmod 4$, and $p = 2, 3, 7, 11, 19$. (and more !?)

$\pi = \pi_{e+1,\, e} : \mathcal{M}_{p^{e+1}} \longrightarrow \mathcal{M}_{p^e}$, (natural reduction)

$$\mathcal{M}_{p^{e+1}} = \bigcup_{X_1 \in \mathcal{M}_{p^e}} \pi^{-1}(X_1), \quad \sharp\, \pi^{-1}(X_1) = p^2.$$

Condition (A). $\exists X_0 \in \mathcal{M}_{p^e}$ and $\exists \Delta \subset \Gamma$:

Δ stabilizes X_0, and Δ acts on $\pi^{-1}(X_0)$ transitively.

Proof of Theorem under (A).

Let $\boldsymbol{X_0' \in \mathcal{M}_{p^{e+1}}}$ be suitably fixed, and $\boldsymbol{X_0 \doteq \pi(X_0')}$.

$\boldsymbol{\forall X \in \mathcal{M}_{p^{e+1}}, \exists T \in \Gamma : \pi(X)T = X_0}$ (by Ind.Hyp.)

$\boldsymbol{\pi(XT) = \pi(X)T = X_0 \therefore XT, X_0' \in \pi^{-1}(X_0)}$.

$\boldsymbol{\therefore \exists S \in \Delta \subset \Gamma : X(TS) = (XT)S = X_0'}$ (by (A))

Condition (A) is satisfied when we put

Case (1) : $\boldsymbol{X_0 \doteq [x_0, y_0, z_0]}$ where $\boldsymbol{3x_0 \equiv 3z_0 \equiv 2}$.

(for the existence we need $\boldsymbol{p \equiv 1 \pmod 4}$)

$$\boldsymbol{\Delta \doteq \langle\, Q^{p^e},\ P^{p^e} \,\rangle.\ (e \geq 1)}$$

Case (2) : $\boldsymbol{X_0 \doteq [1, 1, 1] \pmod{p^e}}$.

$$\boldsymbol{\Delta \doteq \langle\, Q^{rp^{e-1}},\ P^{rp^{e-1}} \,\rangle.\ (e \geq 2,\ p \neq 2)}$$

($\boldsymbol{2r}$ is a period of Fibonacci number $\boldsymbol{\bmod p}$)

$$\boldsymbol{\Delta \doteq \langle\, Q^{3 \cdot 2^{e-2}},\ P^{3 \cdot 2^{e-2}} \,\rangle.\ (e \geq 3,\ p = 2)}$$

In both cases the image of ϕ is abelian of type (p, p) :

$\boldsymbol{\Delta \xrightarrow{\phi} \mathfrak{S}(\pi^{-1}(X_0)) = \mathfrak{S}_{p^2}}$ i.e. simply transitive.

Sketch of the proof of Condition (A) in Case (1)

$[x_0, y_0, z_0]Q = [x_0, 3x_0y_0 - z_0, y_0]$

$\longleftrightarrow \quad (3x_0y_0 - z_0, y_0) = (y_0, z_0)C,\ C = \begin{bmatrix} 3x_0 & 1 \\ -1 & 0 \end{bmatrix}.$

$\therefore$ To obtain $[x_0, y_0, z_0]Q^n$, we need a formula for C^n.

Let $3x_0 \equiv 3z_0 \equiv 2 \pmod{p^{e+1}}$, and
$X_0' \doteq [x_0, y_0, z_0] \in \mathcal{M}_{p^{e+1}}, \quad X_0 \doteq \pi(X_0') \in \mathcal{M}_{p^e}.$
(For the existence of such X_0' we need $p \equiv 1 \pmod 4$.)

Then $C_0 = \begin{bmatrix} 2 & 1 \\ -1 & \end{bmatrix} = I + B, \quad B \doteq \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}.$

$\therefore C_0^n = I + nB.$ We need a closer formula $\bmod p^e$:

$C_\ell \equiv \begin{bmatrix} 2 + \ell p^e & 1 \\ -1 & 0 \end{bmatrix} \pmod{p^{e+1}},\ \ell \pmod p,\ e > 0.$

Then we have

$(*)\ \ {C_\ell}^n \equiv I + nB + \ell p^e W_n \pmod{p^{e+1}},$

where $W_n \doteq \begin{bmatrix} \binom{n+2}{3} & \binom{n+1}{3} \\ -\binom{n+1}{3} & -\binom{n}{3} \end{bmatrix}$, and $(*)$ follows from

$W_{n+1} = (I + B)W_n + W_1(I + nB).$

Since $W_p \equiv O \pmod{p}$, $C_\ell{}^p \equiv I + pB \pmod{p^{e+1}}$:

$(\star)$ $C_\ell{}^{jp^e} \equiv I + jp^eB \pmod{p^{e+1}}$.
The right hand no longer depends on ℓ.

$V \doteq Q^{p^e}$, $U \doteq P^{p^e} = JVJ$. $\because$ $P = JQJ$.
Using $(\star)$ it is now immediately observed

$$[x_0, y_0, z_0]V^j \equiv [x_0, y_0 + ju_0p^e, z_0 + ju_0p^e] \pmod{p^{e+1}},$$
$$[x_0, y_0, z_0]U^j \equiv [x_0 + ju_0p^e, y_0 + ju_0p^e, z_0] \pmod{p^{e+1}},$$
where $u_0 = y_0 - z_0 = y_0 - x_0 \not\equiv 0 \pmod{p}$. Similarly,

$$[x_0, y_0, z_0]U^jV^k \equiv [x_0, y_0, z_0]V^kU^j$$
$$\equiv [x_0+ju_0p^e, y_0+(j+k)u_0p^e, z_0+ku_0p^e] \pmod{p^{e+1}}.$$

Thus we have
$\pi^{-1}(X_0) = \{\, X_0'U^jV^k \mid 0 \le j,\, k < p \,\}$,
namely, $\pi^{-1}(X_0)$ is a single Δ-orbit with $\Delta = \langle U,\, V \rangle$.

The details of Case (2) are omitted. 2018.5.19 / t.a.

Reference : See the reference of Aigner's book,
Martin Aigner, Markov's Theorem etc., Springer, 2013.