

APÉRY数の合同性質

神戸大 理 味村 良雄

Apéryは、 $\zeta(3) = \sum n^{-3}$ の無理数性の証明 [1] のときに、次の漸化式で与えられる数列を扱っている。

$$n^3 a_n - (34n^3 - 51n^2 + 27n - 5)a_{n-1} + (n-1)^3 a_{n-2} \quad (n \geq 2) \quad (1)$$

彼は、初期条件 $A_0=1, A_1=5$ をもつ (1) の解 A_n ($n \geq 0$) が次で与えられることを示した。

$$A_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \quad (2)$$

S. Chowla-J. Cowles-M. Cowles [2] は、この A_n について

$$A_n \equiv 1 \pmod{2} \quad \text{for all } n \geq 0,$$

$$A_p \equiv 5 \pmod{p^2} \quad \text{for all primes } p$$

を証明し、次を予想した

$$A_n \equiv 1 + 4n \pmod{8} \quad \text{for all } n \geq 0,$$

$$A_n \equiv (-1)^n \pmod{3} \quad \text{for all } n \geq 0,$$

$$A_p \equiv 5 \pmod{p^3} \quad \text{for all primes } p > 3,$$

$$A_p \equiv 0 \pmod{5} \quad \text{for all primes } p > 2.$$

さらに，次の問題を提出した．

(1) の解 $a_n (n \geq 0)$ の各項 a_n が整数となるための初期条件は何か？

以下では，これに対する解答と，上の予想された合同式をすべて含む若干の合同式を証明する．

定理 1 a_0, a_1 は整数とする．このとき，(1) をみたす数列 $a_n (n \geq 0)$ の各項 a_n が整数である必要十分条件は， $a_1 = 5a_0$ となることである．

(証明) $f(x) = 5 - 27x + 51x^2 - 34x^3$ とおく． $1 \leq i \leq j$ に対して

$$\mathfrak{D}(i, j) = \begin{pmatrix} f(i) & i^3 & & & \\ i^3 & f(i+1) & (i+1)^3 & & \\ & (i+1)^3 & f(i+2) & \cdot & 0 \\ & & \cdot & \cdot & \cdot \\ & & & \cdot & f(j-1) & (j-1)^3 \\ & 0 & & & (j-1)^3 & f(j) \end{pmatrix} \quad \text{とおく.}$$

p を奇素数として， $p^* = p$ ($p > 3$)， $p^* = 9$ ($p = 3$) とする．明らかに

$$f(i) + f(j) \equiv 0 \pmod{p^*} \quad \text{if} \quad i+j = p+1. \quad (3)$$

行列 W を考える：

$$W = \begin{pmatrix} & & & 1 \\ & 0 & \cdot & \\ & \cdot & \cdot & \\ 1 & \cdot & 0 & \end{pmatrix}.$$

(3) から， $W\mathfrak{D}(i, j)W \equiv -\mathfrak{D}(i, j) \pmod{p^*} \quad \text{if} \quad i+j = p+1.$

$D(i, j) = \det \mathfrak{D}(i, j)$ とおくと, 次がえられる:

$$D(i, j) \equiv 0 \pmod{p^*} \quad \text{if } i+j = p+1. \quad (4)$$

$\mathfrak{D}(i, j)$ の定義と(4) から

$$\begin{aligned} D(2, p) &= f(p)D(2, p-1) - (p-1)^6 D(2, p-2) \\ &\equiv 1^3 \cdot (p-1)^3 \cdot D(2, p-2) \pmod{p^*} \\ &= 1^3 \cdot (p-1)^3 \cdot \{f(2)D(3, p-2) - 2 D(4, p-2)\} \\ &\equiv 1^3 \cdot (p-1)^3 \cdot 2^3 \cdot (p-2)^3 \cdot D(4, p-2) \pmod{p^*} \\ &\equiv \dots \equiv \{(p-1)!\}^3 \pmod{p^*} \end{aligned}$$

従って, $D(2, p) \equiv -1 \pmod{p^*}. \quad (5)$

(1) を満たす数列 a_n を考える. $t \geq 0$ として, ベクトル

$$\alpha_t = (a_{pt+1}, a_{pt+2}, \dots, a_{pt+p-1})$$

$$\beta_t = (-(pt+1)^3 a_{pt}, 0, \dots, 0, -(pt+p)^3 a_{pt+p})$$

を考える. (1) より

$$\alpha_t \mathfrak{D}(pt+2, pt+p) = \beta_t. \quad (6)$$

各 a_n は整数であるとする. $\mathfrak{D}(pt+2, pt+p) \equiv \mathfrak{D}(2, p) \pmod{p^*}$

だから, $\alpha_t \mathfrak{D}(2, p) \equiv \beta_t \pmod{p^*}.$

(5) から, $\mathfrak{D}(2, p) \pmod{p^*}$ の逆行列 $\mathfrak{D}_p^*$ が存在する. 従って

$$\alpha_t \equiv \beta_t \mathfrak{D}_p^* \pmod{p^*}.$$

$\mathfrak{D}_p^*$ の第一行を $(-d_p(1), \dots, -d_p(p-1))$ とすると,

$$a_{pt+j} \equiv d_p(j) a_{pt} \pmod{p^*} \quad (7)$$

が $j=0, 1, \dots, p-1$ に対して成立する. (但し, $d_p(0)=1$ とする)

(4) から, $0 \equiv D(1,p) = f(1)D(2,p) - 1^6 D(3,p) \pmod{p^*}.$

故に, $D(3,p) \equiv 5 \pmod{p^*}.$

従て, $-d_p(1) \equiv D(3,p)D(2,p)^{-1} \equiv -5 \pmod{p^*}.$

(7) から, $a_1 \equiv d_p(1)a_0 \equiv 5a_0 \pmod{p^*}$ となる。 $|a_1 - 5a_0|$ より大きい素数 p を初めにとりておけば, これは $a_1 = 5a_0$ を示す。逆は Apéry の結果を用いればよい。

注意 (Zagier) Let B_n be the solution of (1) with $B_0=0, B_1=1$. The main ingredients in Apéry's proof of the irrationality of (3) were the assertions

$$12N_n^3 B_n \in \mathbb{Z} \quad (N_n = \text{l.c.m.}\{1, 2, \dots, n\}) \quad (8)$$

$$\text{and} \quad B_n/A_n = \zeta(3)/6 + O((1+2)^{-8n}). \quad (9)$$

In fact the 12 can be omitted in (8) (though this is not quite trivial), but apart from that our argument shows that (8) is essentially best possible. Indeed, taking $a_n = B_n$ and $t=0$ in (6) and observing that $B_1, \dots, B_{p-1}$ are p -integral and $B_0=0$, we deduce from (6) and (5) the statement

$$p^3 B_p \in \mathbb{Z}_p \quad \text{and} \quad p^2 B_p \notin \mathbb{Z}_p.$$

$\mathbb{Z}_p$ denotes the ring of p -integers. Note that this statement actually implies Theorem 1, since any solution of (1) is a linear combination of $\{A_n\}$ and $\{B_n\}$.

以下, A_n の合同式について考える。

PROP.1. $A_n \equiv 1+4n \pmod{8}$ for all $n \geq 0$.

(証明) $[]$ は Gauss 記号とする。 k は正整数とし, e は,
 $2^e \mid \binom{2k}{k}$, $2^{e+1} \nmid \binom{2k}{k}$ で定まる整数とする。

$$e = \sum_{r=1}^{\infty} \left[\frac{2k}{2^r} \right] - 2 \sum_{r=1}^{\infty} \left[\frac{k}{2^r} \right] = k - \sum_{r=1}^{\infty} \left[\frac{k}{2^r} \right] > k - \sum_{r=1}^{\infty} \frac{k}{2^r} = 0.$$

従って, $\binom{2k}{k}$ は偶数であり, $\binom{n+k}{k} \binom{n}{k} = \binom{n+k}{2k} \binom{2k}{k}$ は偶数。

$$\text{ゆえに, } \binom{n+k}{k} \binom{n}{k} \equiv (-1)^k \binom{n+k}{k} \binom{n}{k} \pmod{4}.$$

$$\begin{aligned} \text{ゆえに, } A_n &= 1 + \sum_{k=1}^n \binom{n+k}{k}^2 \binom{n}{k}^2 \equiv 1 + \left\{ \sum_{k=1}^n \binom{n+k}{k} \binom{n}{k} \right\}^2 \pmod{8} \\ &\equiv 1 + \left\{ \sum_{k=1}^n (-1)^k \binom{n+k}{k} \binom{n}{k} \right\}^2 \pmod{8}. \end{aligned}$$

$$[2] \text{ の Lemma より, } T(n) = \sum_{k=0}^n (-1)^k \binom{n+k}{k} \binom{n}{k} = (-1)^n \quad \text{だから}$$

$$A_n \equiv 1 + ((-1)^n - 1)^2 \equiv 1 + 4n \pmod{8}$$

$$\text{LEMMA. } \binom{pm}{pk} \equiv \binom{m}{k} \pmod{p^3} \quad \text{for all primes } p \geq 5,$$

$$\binom{pm}{pk} \equiv \binom{m}{k} \pmod{p^2} \quad \text{for all primes } p.$$

(証明) p を 3 より大きい素数とする。

$$\binom{pm}{pk} = \prod_{i=1}^{pk} \frac{p(m-k)+i}{i} = \binom{m}{k} \prod_{h=0}^{k-1} U_h, \quad U_h = \prod_{j=1}^{p-1} \frac{p(m-k+h)+j}{ph+j}.$$

$$\prod_{j=1}^{p-1} (pt+j) = \left(\prod_{j=1}^{p-1} j \right) \left(\prod_{j=1}^{p-1} \left(1 + \frac{pt}{j} \right) \right)$$

$$\equiv (p-1)! \left(1 + pt \sum_{j=1}^{p-1} \frac{1}{j} + p^2 t^2 \sum_{0 < i < j < p} \frac{1}{ij} \right) \pmod{p^3}.$$

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2}, \quad \text{また} \quad \sum_{0 < i < j < p} \frac{1}{ij} \equiv 0 \pmod{p} \quad \text{だから, } \prod_{j=1}^{p-1} (pt+j) \equiv$$

$$(p-1)! \pmod{p^3}. \quad U_h \equiv 1 \pmod{p^3}, \quad \text{則ち, } \binom{pm}{pk} \equiv \binom{m}{k} \pmod{p^3}.$$

$p=2, 3$ は, 直接に確かめられる。

PROP.2. $A_{pm} \equiv A_m \pmod{p^3}$ for all primes $p \geq 5$,

$A_{pm} \equiv A_m \pmod{p^2}$ for all primes p .

(証明) $m=0$ のときは明らか。 $m>0$ とする。 $p=3$ 或は $p>3$ に

応じて, $e=2$ 或は $e=3$ とする。 Lemma より

$$\begin{aligned} A_{pm} &= \sum_{i=0}^m \binom{pm}{pi}^2 \binom{p(m+i)}{pi}^2 + \sum_{t=0}^{m-1} \sum_{i=1}^{p-1} \binom{pm}{pt+i}^2 \binom{pm+pt+i}{pt+i}^2 \\ &\equiv A_m + \sum_{t=0}^{m-1} \sum_{i=1}^{p-1} \binom{pm}{pt+i}^2 \binom{pm+pt+i}{pt+i}^2 \pmod{p^e} \end{aligned}$$

一方, $\binom{pm+pt+i}{pt+i} = \prod_{j=1}^{pt+i} \frac{pm+j}{j} \equiv \prod_{i=1}^t \frac{m+i}{i} = \binom{m+t}{t} \pmod{p}$.

また $(p(m-t)-i) \binom{pm}{pt+i} = pm \prod_{s=1}^{pt+i} \frac{pm-s}{s}$

$$\begin{aligned} &= pm \prod_{h=0}^{t-1} \left(\prod_{j=1}^{p-1} \frac{p(m-h)-j}{ph+j} \right) \cdot \prod_{h=1}^t \frac{p(m-h)}{ph} \prod_{j=1}^i \frac{p(m-t)-j}{pt+j} \\ &\equiv pm(-1)^{(p-1)t+i} \binom{m-1}{t} \pmod{p^2}. \end{aligned}$$

ゆえに, $\binom{pm}{pt+i}^2 \equiv p^2 m^2 \binom{m-1}{t}^2 \frac{1}{i^2} \pmod{p^3}$, $\binom{pm}{pt+i}^2 \equiv 0 \pmod{p^2}$.

結局, $\sum_{i=1}^{p-1} \binom{pm}{pt+i}^2 \binom{pm+pt+i}{pt+i}^2 \equiv \sum_{i=1}^{p-1} \binom{pm}{pt+i}^2 \binom{m+t}{t}^2 \pmod{p^3}$

$$\equiv p^2 m^2 \binom{m-1}{t}^2 \binom{m+t}{t}^2 \sum_{i=1}^{p-1} \frac{1}{i^2} \pmod{p^3} \equiv 0 \pmod{p^e}.$$

系.1. $A_p \equiv 5 \pmod{p^3}$ for all primes $p \geq 5$,

$A_p \equiv 5 \pmod{p^2}$ for all primes p .

(証明) Prop. 2. で $m=1$ として得られる。

定理 2. p は奇素数で, $n = \sum_{j=0}^{\infty} e_j p^j$ ($0 \leq e_j \leq p-1$) とする。このとき

$$A_n \equiv \prod_{j=0}^{\infty} d_p(e_j) \pmod{p^*}.$$

(証明) Prop. 2 と (7) から出る。

系 1. $A_n \equiv (-1)^n \pmod{3}$ for all $n \geq 0$.

(証明) $n = \sum_{j=0}^{\infty} e_j 3^j$ ($e_j = 1, 2, 3$) と書く。 $n \equiv \sum_{j=0}^{\infty} e_j \pmod{2}$ である。一方, $d_3(0)=d_3(2)=1, d_3(1)=5$ だから, 定理 2 によつて

$$A_n \equiv \prod_{j=0}^{\infty} d_3(e_j) \equiv \prod_{j=0}^{\infty} (-1)^{e_j} = (-1)^{\sum e_j} \equiv (-1)^n \pmod{3}.$$

系 2. $A_n \equiv 0 \pmod{5}$ for all odd n .

(証明) $d_5(0)=d_5(4)=1, d_5(1)=d_5(3)=0, d_5(2)=3$ に注意する。
 $n = \sum_{j=0}^{\infty} e_j 5^j$ ($0 \leq j \leq 4$) と書く。 n は奇数だから, $e_j \equiv 1 \pmod{2}$ となる j が少なくとも一つあり, この j に対しては, $d_5(e_j) = 0$ だから, $A_n \equiv \prod_{j=0}^{\infty} d_5(e_j) \equiv 0 \pmod{5}$.

注意. 定理 2 によつて, $d_p(j)$ ($0 \leq j \leq p-1$) が計算されているなら, n に対する $A_n \pmod{p}$ が計算できる。 $10000 = "41104"$ (7 進法で表示) だから, 付録の表より, $A_{10000} \equiv 3 \cdot 1 \cdot 5 \cdot 3 \equiv 1 \pmod{7}$

となる。同様にして, $A_{5t+1} \equiv A_{5t+3} \equiv 0 \pmod{5}$ $A_{11t+5} \equiv 0 \pmod{11}$, $A_{17t+3} \equiv A_{17t+13} \equiv 0 \pmod{17}$ 等がえられる。

Prop.3. $A_{p-1} \equiv 1 \pmod{p^3}$ for all primes $p \geq 5$,

$A_{p-1} \equiv 1 \pmod{p^2}$ for all primes p .

(証明) $p=2,3$ のときは容易に分る。 $p>3$ とし, $0 < k <$

p に対し, $\binom{p-1+k}{k} = \frac{p}{k} \prod_{i=1}^{k-1} \frac{p+i}{i} \equiv \frac{p}{k} \pmod{p^2}$

だから, $\binom{p-1+k}{k}^2 \equiv \left(\frac{p}{k}\right)^2 \pmod{p^3}$, $\binom{p-1+k}{k}^2 \equiv 0 \pmod{p^2}$.

また, $\binom{p-1}{k} = \prod_{i=1}^k \frac{p-i}{i} \equiv (-1)^k \pmod{p}$, $\binom{p-1}{k}^2 \equiv 1 \pmod{p}$.

故に, $A_{p-1} = 1 + \sum_{k=1}^{p-1} \binom{p-1}{k}^2 \binom{p-1+k}{k}^2 \equiv 1 + \sum_{k=1}^{p-1} \frac{p^2}{k^2}$
 $\equiv 1 + p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 1 \pmod{p^3}$.

Prop.2, Prop.3 及び (2) から, 次のような合同式が得られる。

$$A_{p+1} \equiv 25+60p \pmod{p} \quad \text{for all primes } p \geq 5,$$

$$A_{p+2} \equiv 365+1050p+360p^2 \pmod{p} \quad \text{for all primes } p \geq 5,$$

$$A_{p-2} \equiv 5-12p \pmod{p} \quad \text{for all primes } p \geq 5, \text{ etc.}$$

Prop.4. $i \geq 0, j \geq 0, t \geq 0, i+j=p-1$ とすると,

$$d_p(i) \equiv d_p(j) \pmod{p^*}, \quad A_{pt+i} \equiv A_{pt+j} \pmod{p^*}.$$

(証明) i に関する帰納法によって, $A_i \equiv A_{p-i-1} \pmod{p^*}$ を示そう。すでに, $A_0 \equiv A_{p-1} \pmod{p^*}$ と $A_1 \equiv A_{p-2} \pmod{p^*}$ は示してある。 $0 < i < p-1$ として, (1), (3) 及び帰納法の仮定により,

$$\begin{aligned} (i+1)^3 A_{i+1} &\equiv -f(i+1)A_i - i^3 A_{i-1} \\ &\equiv f(p-i)A_i + (p-i)^3 A_{i-1} \\ &\equiv f(p-i)A_{p-i-1} + (p-i)^3 A_{p-i} \\ &\equiv -(p-i-1)^3 A_{p-i-2} \equiv (i+1)^3 A_{p-i-2} \pmod{p^*}. \end{aligned}$$

従って, $A_{i+1} \equiv A_{p-i-2} \pmod{p^*}$. (7)より, $d_p(i) \equiv d_p(j) \pmod{p^*}$ (但し, $i+j=p+1$), 再び (7)より, $A_{pt+i} \equiv A_{pt+j} \pmod{p^*}$ となる.

付録:

$$\underline{d_p(j) \pmod{p^*}}$$

$$\begin{aligned} d_3(0)=1, d_3(1)=5; d_5(0)=1, d_5(1)=0, d_5(2)=3; d_7(0)=1, d_7(1)=5, \\ d_7(2)=d_7(3)=3; d_{11}(0)=1, d_{11}(1)=5, d_{11}(2)=7, d_{11}(3)=4, d_{11}(4)=1, \\ d_{11}(5)=0; d_{13}(0)=1, d_{13}(1)=5, d_{13}(2)=8, d_{13}(3)=2, d_{13}(4)=7, \\ d_{13}(5)=5, d_{13}(6)=9; d_{17}(0)=1, d_{17}(1)=5, d_{17}(2)=5, d_{17}(3)=0, \\ d_{17}(4)=4, d_{17}(5)=13, d_{17}(6)=8, d_{17}(7)=8, d_{17}(8)=16; \dots \end{aligned}$$

参考文献:

- [1] A. van der Poorten, A Proof That Euler Missed..., Math. Intell. 1 (1979), 195-203.
- [2] S. Chowla-J. Cowles-M. Cowles, Congruence Properties of Apéry Numbers, J. Number Theory 12 (1980), 188-190.
- [3] Y. Mimura, --- to appear in J. Number Theory.