# 指数と底の交換に関する考察

群馬県立高崎高等学校
山口凌生　山口眞人

## 要旨

正の整数を $a,b,k$ として合同式

$$a^b \equiv b^a \ (mod\ k) \quad (1)$$

が成り立つ際の $a,b,k$ の条件，成り立つ確率，および $b$ を 1 ずつ増加させたときの $a^b \ mod\ k$ と $b^a \ mod\ k$ の取る値の周期性について調べた。その結果，$a = 3$ と固定したとき，式 $(1)$ が成り立つ確率について，$k$ が 9 の倍数でないとき，$\frac{1}{k}$ となることが予想された。 また，$k$ が 3 と互いに素のとき，$3^b$ の周期は $\varphi(k)$ の約数，$b^3$ の周期は$k$ となり，$k$ が 9 の倍数のとき，$b^3$ の周期は $\frac{k}{3}$ であるとわかった。ただし，$\varphi(n)$ は $n$ 以下の自然数で $n$ と互いに素であるものの個数を表す。

## 1．はじめに

我々が行った本研究は，SSH 活動の一環として，2 年次より 継続してきたものである。その由来は中学生のときまで遡る。「正の実数の平方根」というものを習った中学 3 年生当時，よく出てきた 16 という数字に関して「$2^4$ と $4^2$ は等しい」という素朴な事実に気がついた。この指数部分の数と底の部分の数を交換しても成り立つという性質は，他の数字の組では見られないのではないかと思い，本研究を開始した。

### 1.1.予備調査

はじめに，正の整数 $a,b$ に関する次の等式 $(2)$ について考えた。

$$a^b = b^a \quad (2)$$

式 $(2)$ が成立する $a,b$ に関する条件を調べたところ，先行研究[1)]が見つかった。先行研究を参考に考えた結果，式 $(2)$ が成り立つための必要十分条件は，

$$a = b \text{ または } (a,b) = (2,4),(4,2) \quad (3)$$

であることがわかった。この先行研究では，関数 $f(x) = \frac{log\ x}{x}$ ($log\ x$ は $e = 2.718\ldots$ を底とする対数)を利用した，次のような証明がなされていた。

（先行研究における定理 $(3)$ の証明）

$f(x) = \frac{log\ x}{x}$ $(x > 0)$ に対して，$f'(x) = \frac{1-log\ x}{x^2}$ である。

$x > 0$ より，分母 $x^2 > 0$ なので，$f'(x) = 0$ となるとき，$x = e$ である。

よって，増減表を書くと次のようになる。

| $x$ | $0$ | $\cdots$ | $e$ | $\cdots$ |
|---|---|---|---|---|
| $f'(x)$ | | $+$ | $0$ | $-$ |
| $f(x)$ | | ↗ | $\frac{1}{e}$ | ↘ |

したがって，グラフを書くと図 1 を得る。

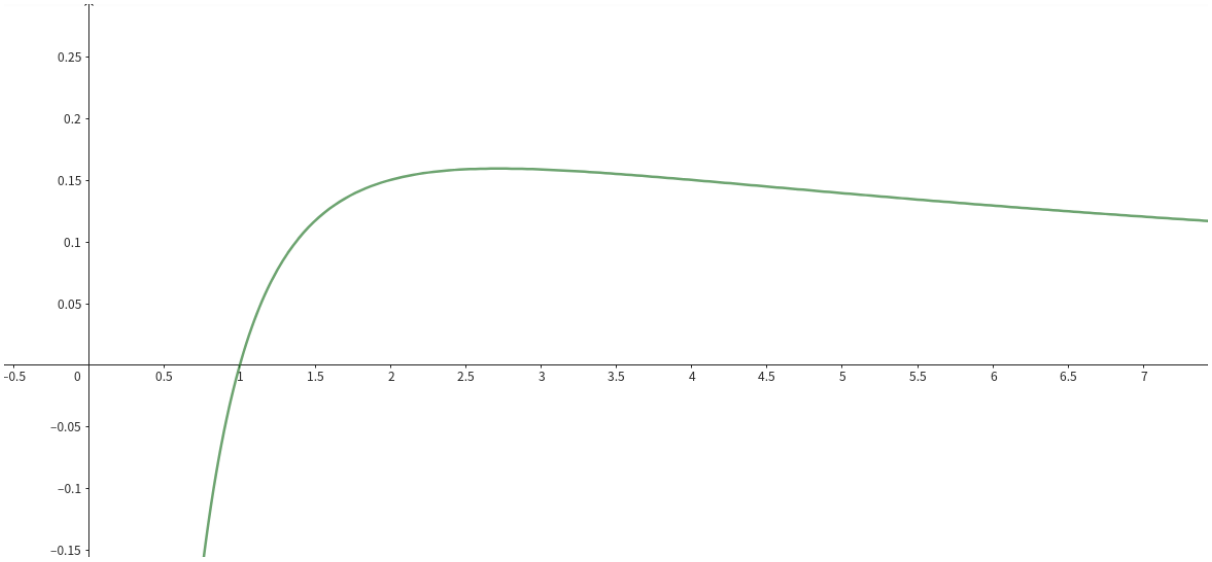



図 1　$y = f(x)$ のグラフ （GeoGebra[2)]により作成。）

ここで，$f(x)$ は増減表から，$0 < x < e$ において単調に増加し，$x = e$ で極大値 $\frac{1}{e}$，$e < x$ において単調に減少するので，$a, b$ が正の整数であることおよび $e = 2.718\ldots$ に注意すると，$a < b$ のもとでは $a = 2, b \geq 3 > e$ である。$f(2) = \frac{\log 2}{2}$ より，図 1 に直線 $y = \frac{\log 2}{2}$ のグラフを加えると図 2 のようになる。

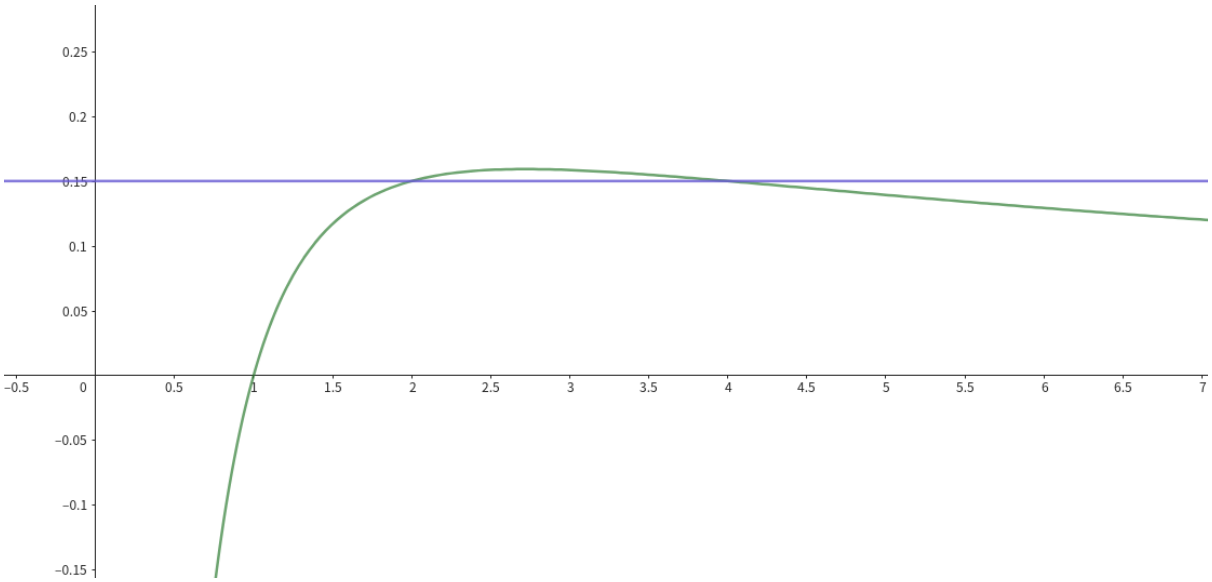



図 2　図 1 に直線 $y = \frac{\log 2}{2}$ のグラフを加えた図 （緑線が $y = \frac{\log x}{x}$，紫線が $y = \frac{\log 2}{2}$，GeoGebra[2)]により作成。）

ここで，$f(4) = \frac{\log 4}{4} = \frac{\log 2}{2} = f(2)$ と図 2 から，$x$ が正の整数のとき，$\frac{\log 4}{4} = \frac{\log 2}{2}$ のみ成り立つ。両辺に 8 を掛けると，$2\log 4 = 4\log 2 \quad \therefore \log 4^2 = \log 2^4$

底 $e$ は 1 より大きいので，$4^2 = 2^4$ に限る。

以上より，$a \neq b$ のとき，$(2) \Leftrightarrow (a, b) = (2, 4), (4, 2)$

また，式 $(2)$ は $a, b$ に関して対称な式なので，$a = b$ のとき，$a^a = a^a$ となり，常に成立する。

したがって, $(2) \Leftrightarrow a = b$ または $(a, b) = (2, 4), (4, 2)$ （証明終わり）

ところで, この証明は関数 $f(x)$ の定義域を実数として考えているが, 正の整数における定理であることから, 我々は定義域を正の整数としても証明が可能であると考え, 以下の証明1.2を行った。

### 1.2.正の整数を定義域としたときの式 $(3)$ の証明

*Proof:*

$a = b$ のとき, 式 $(2)$ は $a, b$ に関して対称な式なので, $a = b$ のとき, $a^a = a^a$ となり, 常に成立する。

以下, $a > b$とする。

(i) $b = p^e$ ($p$ は素数, $e$ は正の整数)と表せるとき,

$a^b = b^a$ は, $a^{(p^e)} = (p^e)^a$ と表現できるので,

$$a \cdot a \cdot a \cdot \cdots\cdots \cdot a\,(p^e \text{ 個の } a \text{ の積}) = p^e \cdot p^e \cdot p^e \cdot \cdots\cdots \cdot p^e\,(a \text{ 個の } p^e \text{ の積}) \quad (4)$$

と考えることができる。

左辺は因数 $a$, 右辺は因数 $p$ のみを含むため, 仮定から, $2$ 以上の自然数 $n$ を用いて

$$a = p^n \quad (5)$$

と表すことができる。

式 $(5)$ を式 $(2)$ に代入して, $(p^n)^{(p^e)} = (p^e)^{(p^n)}$

ゆえに, $p^{np^e} = p^{ep^n}$

底 $p$ は $1$ でない自然数なので, $np^e = ep^n \quad (6)$

【1】式 $(6)$ で, $e = 1$ のとき, $pn = p^n$

両辺を $p(\neq 0)$ で割って, 左辺と右辺を入れ替えると,

$$p^{n-1} = n \quad (7)$$

$n = 2$ のとき式 $(7)$ より, $p^{2-1} = 2$ なので, $p = 2$ のとき, $2^{2-1} = 2$ は成立する。

$p \geq 3$ のとき式 $(7)$ より, $p^{2-1} \geq 3^{2-1} > 2$ であり, 成立しない。

ここで, $n \geq 3$ のとき

$$p^{n-1} > n \quad (8)$$

であることを数学的帰納法を用いて示す。

(A) $n = 3$ のとき, (左辺) $= p^{3-1} = p^2 \geq 2^2 = 4$, (右辺) $= 3$

$p^{3-1} \geq 4 > 3$より, 式 $(8)$ は成り立つ。

(B) $n = k\ (k \geq 3)$ のとき, 式 $(8)$ が成り立つと仮定すると, $p^{k-1} > k \quad (9)$

$n = k + 1$のとき, (左辺) $= p^{(k+1)-1} = p^k$, (右辺) $= k + 1$

よって, (左辺) − (右辺) $= p^k - (k + 1) = p \cdot p^{k-1} - (k + 1)$

式 $(9)$ より (左辺) − (右辺) $> pk - (k + 1) = (p - 1)k - 1 \geq (2 - 1) \cdot 3 - 1 = 2 > 0$

ゆえに, (左辺) − (右辺) $> 0$ なので, (左辺) $>$ (右辺)

したがって, 式 $(8)$は成り立つ。

(A), (B) より, $n \geq 3$のとき, 式 $(8)$ は成り立つ。

つまり, $n \geq 3$ のとき $p^{n-1} \neq n$ である。

これと $n = 2, p \geq 3$ における式 $(7)$ の考察から，式 $(7)$ を満たす自然数の組 $(p, n)$ は，$(p, n) = (2, 2)$ のみである。
よって，式 $(5)$ より，$a = 4$ なので，$b = p$ から $(a, b) = (4, 2)$

【2】式 $(6)$ で，$e \geq 2$ のとき，$a \neq b$ なので，(i) の仮定と式 $(5)$ から，$n \neq p$
　このとき，式 $(4)$ において，左辺と右辺で素因数 $p$ の個数が一致しないので，$e \geq 2$ は不適である。

(ii) $b = {p_1}^{e_1}{p_2}^{e_2}{p_3}^{e_3}\cdots\cdots{p_i}^{e_i}$（$p_1, p_2, p_3, \cdots\cdots, p_i$ は異なる素数，$e_1, e_2, e_3, \cdots\cdots, e_i$ は非負整数，$i \geq 2$）と表せるとき，(i) と同様の操作をすると，素因数分解の一意性より，
ある $p_k$ $(1 \leq k \leq i)$ について，${n_k}{p_k}^{e_k} = e_k{p_k}^{n_k}$ である。
これを，(i) と同様に考えると，$(p_k, n_k) = (2, 2)$ と $1$ つに定まるので，素数 $p_i$ は存在できない。
よって，$b = p$ と表すことができ，(i) に帰着する。

(i), (ii) より，$(a, b) = (4, 2)$
$a < b$ の場合も考えると，$(a, b) = (2, 4), (4, 2)$である。
したがって，$(2) \Leftrightarrow a = b$ または $(a, b) = (2, 4), (4, 2)$　（証明終わり）

## ２．実験

### 2.1.実験の動機

予備調査で示した式 $(2)$ に関しては証明がなされたので，次に等号(=)を合同記号(≡)に置き換え，合同式にした式 $(1)$ について研究することにした。本実験では，式 $(1)$ において $a = 3$ として研究した。すなわち，正の整数を $b, k$ として合同式

$$3^b \equiv b^3 \pmod{k} \quad (10)$$

について考えた。

### 2.2.用語の定義

本実験で用いる用語について定義する。なお，$N$ は任意の非負整数とする。
「周期」とは，式 $(10)$ において，$b$ の値を $1$ ずつ増加させたとき，左辺と右辺のそれぞれで現れる最小正剰余の最小の繰り返し単位を指す。また，左辺，右辺の周期の長さをそれぞれ $C(3^b), C(b^3)$ と表すことにする。例として，正の整数を出力する関数 $g(b), h(b)$ が次の表 1 のようになったとする。このとき，$g(b)$ の周期は $3N + 2 \leq b \leq 3N + 4$ における「$7, 2, 8$」であり，$C(g(b)) = 3$ である。$h(b)$ の周期は $2N + 1 \leq b \leq 2N + 2$ における「$1, 2$」であり，$C(h(b)) = 2$ である。なお，$g(1) = 5$ については，$b \geq 2$ において繰り返し単位に含まれないので $g(b)$ の周期から除外して考える。本実験では式 $(10)$ のように，法を $k$ とした合同式について調べるため，$k$ が大きいところでは $b$ が小さいところで剰余ではなく真の値になってしまい，実験の趣旨にそぐわないと判断した。
　また，「全体の周期」とは式 $(10)$ において，左辺と右辺ともに剰余が繰り返されている部分におけるそれぞれの繰り返しの最小公倍数の長さをもつ繰り返し単位のことをいう。表 1 においては，$g(b)$ は $b \geq 2$ で，$h(b)$ は $b \geq 1$ でそれぞれ繰り返しが始まっているので，$b \geq 2$ において $6N + 2 \leq b \leq 6N + 7$ が全体の周期となる。このとき，全体の周期の長さは $LCM(3, 2) = 6$ である。

ただし，$LCM(A,B)$ は 2 自然数 $A$, $B$ の最小公倍数を表す。

さらに，「確率」とは，全体の周期における式 (10) が成り立つ確率を指す。すなわち，

$$\frac{(\text{全体の周期における式}(10)\text{ が成り立つ}\boldsymbol{b}\text{ の値の個数})}{(\text{全体の周期の長さ})} \quad (11)$$

である。表 1 では，全体の周期における $g(b) = h(b)$ となる $b$ の値は $b = 6N + 6$ のみである。したがって，式 (11) より確率は $\frac{1}{6}$ である。

表 1　$b$ と $g(b), h(b)$ の対応

| $b$ | $g(b)$ | $h(b)$ |
|---|---|---|
| 1 | 5 | 1 |
| 2 | 7 | 2 |
| 3 | 2 | 1 |
| 4 | 8 | 2 |
| 5 | 7 | 1 |
| 6 | 2 | 2 |
| 7 | 8 | 1 |
| 8 | 7 | 2 |
| … | 以下，2,8,7,2,8,7,… と続く。 | 以下，1,2,1,2,… と続く。 |

### 2.3.方法

Google スプレッドシートを用いて，以下の手順で実験を行った。

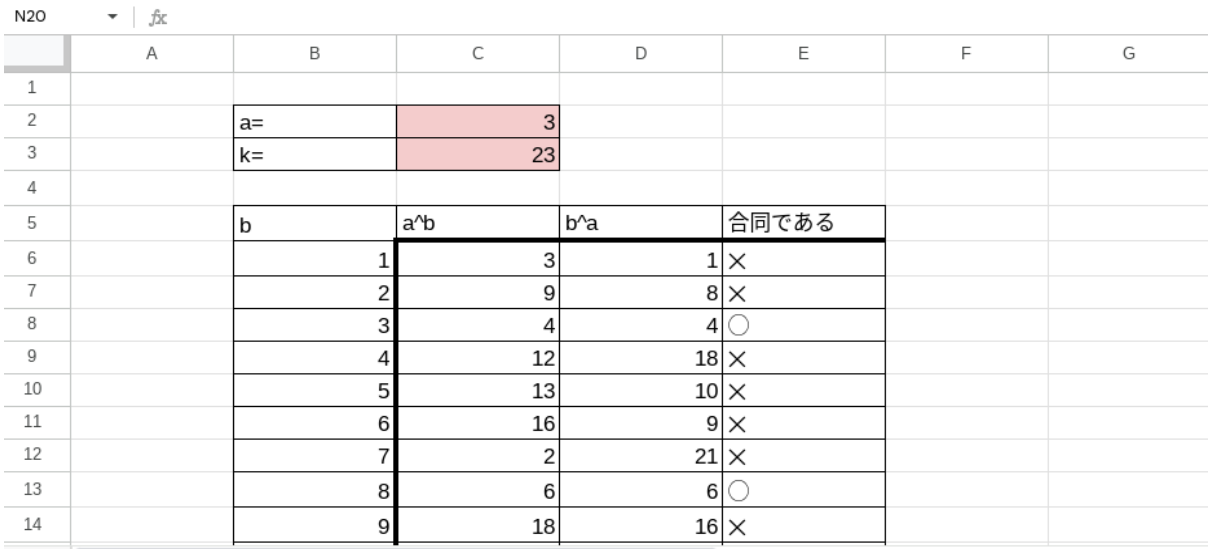
手順1　C2に $a$ の値である 3，C3に $k$ の値を入力する。図 3 中では，赤背景の部分を指す。

手順2　6 行目以降，B列に $b$ の値を入力する。

手順3　i≧6としてCiに「=mod(C(i−1)*$C$2,$C$3)」，Diに「=mod(Bi^$C$2,$C$3)」を入力する。

手順4　Eiに「=if(Ci=Di,"○","×")」を入力する。

手順5　手順1の $k$ の値を変化させ，周期および確率を確認，計算する。



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 2 | | a= | 3 | | | | |
| 3 | | k= | 23 | | | | |
| 4 | | | | | | | |
| 5 | | b | a^b | b^a | 合同である | | |
| 6 | | 1 | 3 | 1 | × | | |
| 7 | | 2 | 9 | 8 | × | | |
| 8 | | 3 | 4 | 4 | ○ | | |
| 9 | | 4 | 12 | 18 | × | | |
| 10 | | 5 | 13 | 10 | × | | |
| 11 | | 6 | 16 | 9 | × | | |
| 12 | | 7 | 2 | 21 | × | | |
| 13 | | 8 | 6 | 6 | ○ | | |
| 14 | | 9 | 18 | 16 | × | | |

図 3　実験に用いたGoogle スプレッドシート(ここでは, $a = 3, k = 23$ の場合を示した。)

### 2.3.結果

実験によって得られたデータのうち, $k, C(3^b), C(b^3)$, 全体の周期, 確率について, $1 \leq k \leq 10$ の範囲で $k$ を変化させたときの結果を以下の表 2 に示す。また, $k$ が $9$ の倍数であるときに $9 \leq k \leq 54$ の範囲で $k$ を変化させたときの結果を以下の表 3 に示す。

表 2　$1 \leq k \leq 10$ の範囲における $k, C(3^b), C(b^3)$, 全体の周期, 確率

| $k$ | $C(3^b)$ | $C(b^3)$ | 全体の周期の長さ | 確率 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 2 | $\frac{1}{2}$ |
| 3 | 1 | 3 | 3 | $\frac{1}{3}$ |
| 4 | 2 | 4 | 4 | $\frac{1}{4}$ |
| 5 | 4 | 5 | 20 | $\frac{1}{5}$ |
| 6 | 1 | 6 | 6 | $\frac{1}{6}$ |
| 7 | 6 | 7 | 42 | $\frac{1}{7}$ |

| | | | | |
|---|---|---|---|---|
| 8 | 2 | 8 | 8 | $\frac{1}{8}$ |
| 9 | 1 | 3 | 3 | $\frac{1}{3}$ |
| 10 | 4 | 10 | 20 | $\frac{1}{10}$ |

表 3　$3 \leq k \leq 54$ における $k, C(3^b), C(b^3)$, 全体の周期, 確率

| $k$ | $C(3^b)$ | $C(b^3)$ | 全体の周期の長さ | 確率 |
|---|---|---|---|---|
| 9 | 1 | 3 | 3 | $\frac{1}{3}$ |
| 18 | 1 | 6 | 6 | $\frac{1}{6}$ |
| 27 | 1 | 9 | 9 | $\frac{1}{3}$ |
| 36 | 2 | 12 | 12 | $\frac{1}{12}$ |
| 45 | 4 | 15 | 60 | $\frac{1}{15}$ |
| 54 | 1 | 18 | 18 | $\frac{1}{6}$ |

### 2.4.考察

$k = 1$ のとき, $C(3^b), C(b^3)$, 全体の周期, 確率はすべて 1 である。1 を法とした合同式では任意の整数が 0 と合同であるからだと思われる。

$k$ が 3 と互いに素であるとき, $C(3^b)$ は $\varphi(k)$ の約数であると考えられる。ただし, $\varphi(n)$ は $n$ 以下の自然数で $n$ と互いに素であるものの個数を表す。

また, $k$ が 3 を因数にもつとき, $C(3^b)$ は不規則である[3)]と考えられる。一方, $C(b^3) = k$ だと思われる。そして, 確率は $\frac{1}{k}$ であると考えられる。

$k$ が 9 の倍数のとき, $C(b^3) = \frac{k}{3}$ であると思われる。確率については規則性が確認できなかった。

我々は, この考察に基づいて以下の命題 1, 2, 3 を立てた。

命題1　$k$ が 3 と互いに素のとき, $C(3^b)$ は $\varphi(k)$ の約数である。

命題2　$k$ が 9 の倍数でないとき, $C(b^3) = k$ である。

命題3　$k$ が 9 の倍数のとき, $C(b^3) = \frac{k}{3}$ である。

## 2.5.証明

2.4.考察 において立てた命題1, 2, 3 について証明する。

命題1

*Proof:*

$3$ と $k$ は互いに素なので, 補題1(オイラーの定理)より, $3^{\varphi(k)} \equiv 1 \pmod{k}$ ･･･①

また, $\varphi(k) = k_1 k_2$ ($k_1, k_2$ は自然数) と因数分解できるとすると, ①より,

$3^{\varphi(k)} = 3^{k_1 k_2} = \left(3^{k_i}\right)^{k_j} \equiv 1 \pmod{k}$ $((i,j) = (1,2),(2,1))$ が成り立つ。

これは, $3^{k_i} \equiv 1 \pmod{k}$ または $3^{k_1 k_2} = 3^{\varphi(k)} \equiv 1 \pmod{k}$ と同値である。

したがって, $3^{b}$ の周期は $k$ が $3$ と互いに素のとき, $\varphi(k)$ の約数となる。■

補題1(オイラーの定理)

自然数 $a, n$ $(n \geq 2)$ があって, $GCD(a,n) = 1$ ならば, $a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つ。

($GCD(a,n) :=$ Greatest Common Divisor of $a$ and $n$)

*Proof:*

まず, $n$ と互いに素で $n$ 以下の自然数で相異なるものの集合を $M = \left\{m_1, m_2, \cdots, m_{\varphi(n)}\right\}$ $(|M| = \varphi(n))$ とする。

このとき, 集合 $M$ の要素 $m_i, m_j$ について, $am_i \equiv am_j \pmod{n}$ $(1 \leq i < j \leq \varphi(n))$ とすると, $a(m_i - m_j) \equiv 0 \pmod{n}$ となる。

$a, n$ は互いに素なので, $m_i - m_j \equiv 0 \pmod{n}$ すなわち $m_i \equiv m_j \pmod{n}$ となる。

ここで, $m_i, m_j$ の定義から, $0 < m_i \leq n, 0 < m_j \leq n, m_i \neq m_j$ であるので, 矛盾が生じる。

よって, 集合 $aM = \left\{am_1, am_2, \cdots, am_{\varphi(n)}\right\}$ の各要素を $n$ で割った余りが等しい組は存在しない(つまり, すべて異なる)。

また, $GCD(a,n) = 1$ なので, $n \geq 2$ より, $\varphi(n) \leq n - 1 < n$ であること, および集合 $M$ の任意の要素が $n$ より小さいことを考慮すると, 鳩の巣原理から, 集合 $aM$ の各要素を $n$ で割った余りの集合は集合 $M$ に一致する。

ゆえに, $\prod_{k=1}^{\varphi(n)} am_k \equiv \prod_{k=1}^{\varphi(n)} m_k \pmod{n}$ $\therefore a^{\varphi(n)} \prod_{k=1}^{\varphi(n)} m_k \equiv \prod_{k=1}^{\varphi(n)} m_k \pmod{n}$

集合 $M$ の定義により, $\prod_{k=1}^{\varphi(n)} m_k$ と $n$ は互いに素なので, $a^{\varphi(n)} \equiv 1 \pmod{n}$ (証明終わり)

命題2

*Proof:*

$k$ が $9$ の倍数のとき, $k = 9m$ ($m$ は自然数) と表すことができる。

以下, 法を $9m$ とした合同式を考える。

自然数を $i, j$ $(j = 0, 1, \cdots, 3m - 1)$ として, $b = 3im + j$ とおくと,

$$b^3 = (3im + j)^3 = 27i^3m^3 + 27i^2jm^2 + 9ij^2m + j^3$$
$$= 9m(3i^3m^2 + 3i^2jm + ij^2) + j^3 \equiv j^3 \pmod{9m}$$

$(3m - 1) - 0 + 1 = 3m$ であるから, $j$ のとりうる値は, $3m$ 通り存在する。

$3m = \frac{9m}{3} = \frac{k}{3}$ なので，$k$ が $9$ の倍数のとき，$b^3$ の周期は $\frac{k}{3}$ である。（証明終わり）

命題3

*Proof:*

$k \equiv 0 \,(mod\ k)$ であるので，周期としてとりうる値の最大値は $k$ である。

以下，最小値が $k$ に一致していることを示す。

$(k+1)l \equiv 1 \,(mod\ k)$ より，周期を $1 \leq b < k$ において考えても一般性を失わない。

$0 \leq r < \left[\frac{k}{2}\right]$ を満たす自然数 $r$ を定めると，$-k < -\frac{k}{2} < r-k < 0$ であり，$r \equiv r-k \,(mod\ k)$ が成り立っている（$\left[\frac{k}{2}\right]$ は $\frac{k}{2}$ 以下で，最大の整数を表す）。

このとき，$(r-k)^3 = -(k-r)^3 \,(0 \leq k-r < k)$ であるが，$-(k-r)^3 \equiv (k-r)^3 \,(mod\ k)$ は成り立たない。

よって，周期が最小の繰り返し単位であることに注意すると，周期は $k$ となる。（証明終わり）

## ３．展望

式 (*10*) が成り立つ確率について，より深く考察したいと考える。

謝辞

群馬県立高崎高等学校教諭の國富充敏先生には，本研究の遂行にあたり，終始熱心なご指導をいただきました。ここに深く感謝申し上げます。

参考文献

1) aのb乗=bのa乗の整数解と大小比較と類題 ｜ 数学の偏差値を上げて合格を目指す
https://math-juken.com/kijutu/bnoajou/

2024/07/08閲覧

2) GeoGebra スイート
https://www.geogebra.org/calculator

2024/07/16使用

3) 冪剰余 - Wikipedia
https://ja.wikipedia.org/wiki/%E5%86%AA%E5%89%B0%E4%BD%99

2024/07/09閲覧