< 円上のビリヤードの原理 >

正の整数 N, M に対し「N を M で割った余りが K」であることを

$$\boxed{N(\mathrm{mod}\ M) = K} \quad \left(\Leftrightarrow N - K(\mathrm{mod}\ M) = 0 \ \Leftrightarrow \ \text{「}N - K \text{ は } M \text{ で割り切れる」} \right)$$

という記号で表す。例えば $42\ (\mathrm{mod}\ 36) = 6$ である。

例 前ページの例は

$x_1 = 7\ (\mathrm{mod}\ 36) = 7,\ x_2 = 14\ (\mathrm{mod}\ 36) = 14,\ \cdots,\ x_6 = 42\ (\mathrm{mod}\ 36) = 6,$

$x_7 = 49\ (\mathrm{mod}\ 36) = 13,\ \cdots,\ x_n = 7n\ (\mathrm{mod}\ 36)$

で定まる数列 $\{x_n\}$ に対し, 集合 $\{x_1, x_2, \cdots, x_{35}\}$ は 1 から 35 までの全ての自然数の集合と一致する。一般に次の定理が成り立つ。

[定理]　a と M は共に正の整数で, $a < M$ とする。また

「a と M は互いに素」$\left(\Leftrightarrow a \text{ と } M \text{ の共通の約数は 1 だけである} \right)$

とする。このとき

$x_1 = \ a\ (\mathrm{mod}\ M)$

$x_2 = 2a\ (\mathrm{mod}\ M)$

$\quad \vdots$

$x_n = na\ (\mathrm{mod}\ M)$

で定まる数列 $\{x_n\}$ に対し, 集合 $\{x_1, x_2, \cdots, x_{M-1}\}$ は 1 から $M-1$ までの全ての自然数の集合と一致する。

[証明]　$\{x_1, x_2, \cdots, x_{M-1}\}$ は全て異なる数であることを示せば良い。背理法を使う。

もしそうでないとすれば, ある自然数 n と ℓ $(1 \leqq n < \ell \leqq M-1)$ が存在して, $x_n = x_\ell$ となる。$x_n = na\ (\mathrm{mod}\ M),\ x_\ell = \ell a\ (\mathrm{mod}\ M)$

$$x_\ell - x_n = (\ell - n)a\ (\mathrm{mod}\ M) = 0$$

より $(\ell - n)a$ は M で割り切れる。よってある自然数 k が存在して,

$$(\ell - n)a = kM$$

ここで a と M は互いに素だから k は a を約数にもつ。したがってある自然数 j が存在して, $k = aj$ と表される。

$(\ell - n)a = jaM \quad \Rightarrow \quad \ell - n = jM \ \geqq \ M \quad \cdots ①$

一方 $1 \leqq n < \ell \leqq M - 1$ より

$$\ell - n \leqq M - 1 - n < M - 1 \quad \cdots ②$$

①と②は矛盾している。よって仮定 $x_n = x_\ell$ は間違っている。　(証明終)