暗号の数理問題解説 #3

河野

演習問題 1.4　関係 $\sim$ が次の 3 つを満たすとき同値関係と言う。

(1) $a \sim a$

(2) $a \sim b \implies b \sim a$

(3) $a \sim b \wedge b \sim c \implies a \sim c$

上で定義した $\equiv$ が同値関係であることを示せ。

(1) $a \in \mathbb{Z}$ に対し $a - a = 0 = n0$ となるので $a - a = 0 \in n\mathbb{Z}$ である。よって $a \equiv a \pmod{n}$ が成立する。
(2) $a \equiv b$ が成立しているとき $a-b \in n\mathbb{Z}$ より $\exists m \in \mathbb{Z}\ \ a-b = nm$ となるこのとき $b-a = n(-m)$ なので $b - a \in n\mathbb{Z}$ となり，$b \equiv a \pmod{n}$ が成立する。
(3) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n}$ が成立しているので $\big(\exists m_1 \in n\mathbb{Z}\ \ a - b = nm_1\big) \wedge \big(\exists m_2 \in n\mathbb{Z}\ \ b - c = nm_2\big)$ となる。このとき $a - c = (a - b) + (b - c) = nm_1 + nm_2 = n(m_1 + m_2)$ となるので，$a - c \in n\mathbb{Z}$ であり，$a \equiv c \pmod{n}$ となる。

演習問題 1.5　$\mathbb{Z}_{10}$ および $\mathbb{Z}_9$ の各元の位数を求めよ。

最初に Z_{10} について考える。[0] はすでに単位元 (零元) なので位数は 1 である。[1] は

$$2[1] = [1] + [1] = [2], 3[1] = [1] + [1] + [1] = [3], \ldots$$

と足して行くと $10[1] = [0]$ で 10 で初めて [0] になるので位数は 10 である。[2] は

$$2[2] = [2] + [2] = [4], 3[2] = [4] + [2] = [6], 4[2] = [6] + [2] = [8], 5[2] = [8] + [2] = [0]$$

なので位数は 5 である。[3] は

$$1[3] = [3], 2[3] = [6], 3[3] = [9], 4[3] = [2], 5[3] = [5], 6[3] = [8], 7[3] = [1], 8[3] = [4], 9[3] = [7], 10[3] = [0]$$

なので位数は 10 である。以下途中計算を省略すると [4] のとき

$$[4], [8], [2], [6], [0]$$

となり位数は 5 である。[5] のとき

$$[5], [0]$$

で位数は 2 である。[6], [7], [8], [9] は

$$[6], [2], [8], [4], [0]$$
$$[7], [4], [1], [8], [5], [2], [9], [6], [3], [0]$$
$$[8], [6], [4], [2], [0]$$
$$[9], [8], [7], [6], [5], [4], [3], [2], [1], [0]$$

なので $[6]$ の位数は 5，$[7]$ の位数は 10，$[8]$ の位数は 5，$[9]$ の位数は 10 である。

次に Z_9 について考える。$[0], [1], \ldots, [8]$ を累加していくと，

$$[0]$$
$$[1], [2], [3], [4], [5], [6], [7], [8], [0]$$
$$[2], [4], [6], [8], [1], [3], [5], [7], [0]$$
$$[3], [6], [0]$$
$$[4], [8], [3], [7], [2], [6], [1], [5], [0]$$
$$[5], [1], [6], [2], [7], [3], [8], [4], [0]$$
$$[6], [3], [0]$$
$$[7], [5], [3], [1], [8], [6], [4], [2], [0]$$
$$[8], [7], [6], [5], [4], [3], [2], [1], [0]$$

となるので $[1], [2], [4], [5], [7], [8]$ は位数 9，$[3], [6]$ は位数 3，$[0]$ は位数 1 である。

演習問題 1.6　$G = \mathbb{Z}_{12}$ とする。$H = \langle 9 \rangle$ とするとき剰余類分割を求めよ。また $N = \langle 2 \rangle$ とするとき，剰余類分割を求めよ。

$H = \langle [9] \rangle$ と書くべきでしたね。$2[9] = [6], 3[9] = [3], 4[9] = [0]$ なので $H = \{ [0], [3], [6], [9] \}$ である。$[1] \notin H$ である。

$$[1] + [0] = [1], \quad [1] + [3] = [4], \quad [1] + [6] = [7], \quad [1] + [9] = [10]$$

なので $1 + H = \{ [1], [4], [7], [10] \}$ となるがこの集合を H_1 と書く。$[2] \notin H \cup H_1$ である。

$$[2] + [0] = [2], \quad [2] + [3] = [5], \quad [2] + [6] = [8], \quad [2] + [9] = [11]$$

なので $2 + H = \{ [2], [5], [8], [11] \}$ となるがこの集合を H_2 と書く。$H \cup H_1 \cup H_2 = G$ なのでこれが求める剰余類分割である。即ち

$$G = \{ [0], [3], [6], [9] \} \cup \{ [1], [4], [7], [10] \} \cup \{ [2], [5], [8], [11] \}$$

となる。

$2[2] = [4], 3[2] = [6], 4[2] = [8], 5[2] = [10], 6[2] = [0]$ なので $N = \{ [0], [2], [4], [6], [8], [10] \}$ である。$[1] \notin N$ である。

$$[1] + [0] = [1], [1] + [2] = [3], [1] + [4] = [5], [1] + [6] = [7], [1] + [8] = [9], [1] + [10] = [11]$$

なので $[1] + N = \{ [1], [3], [5], [7], [9], [11] \}$ となる。

$$G = \{ [0], [2], [4], [6], [8], [10] \} \cup \{ [1], [3], [5], [7], [9], [11] \}$$

が剰余類分割である。

$[1] \notin N$ で剰余類分割を作ったが，他の元で作っても同じ結果になる。例えば $[3] \notin N$ なので

$$[3] + [0] = [3], [3] + [2] = [5], [3] + [4] = [7], [3] + [6] = [9], [3] + [8] = [11], [3] + [10] = [1]$$

となる剰余類分割は

$$G = \{\,[0],[2],[4],[6],[8],[10]\,\} \cup \{\,[1],[3],[5],[7],[9],[11]\,\}$$

である。

演習問題 1.7　$|\langle g\rangle| = |g|$ を示せ。

$|g| = n$ とすると $g^n = e$ (単位元) であり，$m < n$ となる自然数に対しては $g^m \neq e$ である。$H = \{\,g, g^2, g^3, \ldots, g^n\,\}$ であり，$\ell \leqq n, m \leqq n$ となる自然数 ℓ, m に対し $g^\ell \neq g^m$ が言えれば $|H| = n$ となる。

$H = \{\,g, g^2, g^3, \ldots, g^n, g^{n+1}, \ldots, g^k, \ldots\,\}$ なので k を $k > n$ となる任意の自然数とする。このとき $k = pn + r$ となる整数 p, r $(0 \leqq r < n)$ が存在する。$r = 0$ のとき $k = pn$ なので $g^k = g^{pn} = (g^n)^p = e^p = e = g^n$ である。$0 < r$ のときは $g^k = g^{pn+r} = g^{pn} g^r = (g^n)^p\, g^r = e^p g^r = g^r$ となる。いずれの場合も

$$g^k \in \{\,g, g^2, \ldots, g^n\,\}$$

となる。

今 $\ell, m \leqq n$ となる異なる自然数 ℓ, m に対し $g^\ell = g^m$ が成立していたとする。$\ell > m$ のときは g^{-1} を m 個かけることにより $g^{\ell-m} = e$ を得る。$\ell - m < n$ なので n の定義に矛盾する。$\ell < m$ のときは g^{-1} を ℓ 個かけることにより $e = g^{m-\ell}$ を得る。$m - \ell < n$ なので n の定義に矛盾する。よって $g^\ell \neq g^m$ なので $|H| = n$ である。