剰余定理（Division theorem）

任意の $x, n \in \mathbb{Z}, (n \neq 0)$ に対し

$$x = nq + r$$
$$0 \leqq r < |n|$$

となる $q, r \in \mathbb{Z}$ が一意に存在する

q：商（quotient）　r：剰余（remainder）

とよぶ

$x, y \in \mathbb{Z}$ を正整数 n で割った剰余が等しいとき x と y は「n を法として合同である（congruent modulo n）」といい，次のように書く

$$x \equiv y \pmod{n}$$

上記のような式を合同式（cogruence）とよぶ

命題

$$x \equiv y \pmod{n} \leftrightarrow (x-y) \text{は } n \text{ の倍数}$$

同値類の例（Example of equivalence class）

Z: 整数全体の集合

Z 上の同値関係: R_3

$R_3 = \{ (x,y) \mid x \equiv y \pmod 3 \}$

$[0] = \{ x \mid (0, x) \in R_3 \}$

$0 \equiv x \pmod 3$ より $x=3k, \quad k \in Z$

$[0] = \{ \cdots, -6, -3, 0, 3, 6, \cdots \}$

同様に

$[1] = \{ \cdots, -2, 1, 4, 7, \cdots \}$

$[2] = \{ \cdots, -1, 2, 5, 8, \cdots \}$

$[3] = \{ x \mid (3,x) \in R_3 \}$

$3 \equiv x \pmod 3$ より $x=3k, \quad k \in Z$

となるので $[3] = [0]$

同様に

$[4] = [1]$

$[-1] = [2]$

$[-2] = [1]$

・

・

互いに素である同値類は

$$[0], [1], [2]$$

従って

$Z/R_3 = \{ [0], [1], [2] \}$

$[0], [1], [2]$は互いに素であり，かつ

$$Z = [0] \cup [1] \cup [2]$$

なので，確かに Z/R_3 =は Z の分割になっている