

学籍番号		氏名	
------	--	----	--

- [1] **(同値関係)** 集合 X の 2 つの元の間定義された関係 $\sim$ が、次の 3 つの条件を満たすとき、この関係 $\sim$ を**同値関係**という。

(1) **反射律** $x \sim x \ (\forall x \in X)$,

(2) **対称律** $x \sim y$ ならば $y \sim x \ (\forall x, y \in X)$,

(3) **推移律** $(\forall x, y, z \in X)$,

定理. 集合 X に同値関係 $\sim$ を定めると、同値類 $C(a) = [a]$ によって X の類別が得られる。

- [2] $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$ を考える。但し、 $[a] = a + m\mathbb{Z} = \{a + mn \mid n \in \mathbb{Z}\} = \bar{a}$ である。
ここで、集合 $\mathbb{Z}/m\mathbb{Z}$ に 2 つの演算、加法 $+$ と乗法 $\cdot$ を以下の様に定義する。

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := \span style="border: 1px solid black; padding: 2px 10px;">.$$

この同値類に対して定義された演算 $(+, \cdot)$ が、代表元の取り方に依らずに定まっていること、すなわち $[a] = [a']$ かつ $[b] = [b']$ ならば $[a + b] = [a' + b']$ 及び $[ab] = [a'b']$ が成り立つことを、

w から始まる英単語 1 つを用いて、演算は であるという。

- [3] $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ に対して、 $\bar{a} = [a]$ として、演算表を書いてみる：

$m = 2$			$m = 3$			$m = 4$				$m = 5$					$m = 6$									
$\cdot$	$\bar{0}$	$\bar{1}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
				$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
								$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
												$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

よって、 $m = 2, 3, 4, 5, 6$ のうち、 $\mathbb{Z}/m\mathbb{Z}$ が**体**となる m は である。

- [4] $(\mathbb{Z}/m\mathbb{Z})^\times := \{[a] \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$ に対して、 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ は**位数** $\varphi(m)$ の可換群をなす。群 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ を 群、 $\varphi(m)$ を**オイラー関数**と呼ぶ。

$$\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = \span style="border: 1px solid black; padding: 2px 10px;">, \varphi(9) = 6.$$

- [5] **(オイラーの定理)** 整数 $m \geq 2$ と $\gcd(a, m) = 1$ なる整数 $a \in \mathbb{Z}$ に対して、以下が成り立つ：

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

素数 p に対して、 $m = p$ の場合、 $\varphi(m) = \span style="border: 1px solid black; padding: 2px 10px;"> であるから、**オイラー** (1707–1783) の$

定理は、数学者 (1601–1665) の名前が付いた の**小定理**の拡張になっている。

(1) 19^7 を 7 で割った余りは , (2) 19^7 を 8 で割った余りは .