合同式の定義

整数 $a,\ b$, 自然数 m に対し, m が $a-b$ を割り切るとき,
「m を法として a と b は合同である」といい, 「$a \equiv b \pmod{m}$」と書く.

ここから以下の定理を得ます. 証明は略しますが, 感覚的にも納得できるでしょう.

合同式と余りの関係

整数 $a,\ b$, 自然数 m に対し,

$$a \equiv b \pmod{m} \Longleftrightarrow a \text{ と } b \text{ を } m \text{ で割った余りは等しい}$$

ここまでを基礎知識として, 改めて以下の問題を考えてみましょう.

整数 $a,\ b$ と自然数 $k,\ m$ に対し, 以下の $\square$ を埋めよ.

$$ak \equiv bk \pmod{m} \Longleftrightarrow a \equiv b \pmod{\square}$$

【コメント】

$42 \equiv 6 \pmod{9}$ では, 両辺を 6 で割ったと同時に法も変えて, 例えば $7 \equiv 1 \pmod{3}$ とすれば正しい合同式になります.
その他にもいくつか具体例を考えてみることで, 法をどう変化させればよいか予想することができるのです.
未知の問題に取り組むときは**「実験＆観察 → 予想 → 論証」**の流れが大切です.
特に**実験＆観察**は自分の手で行ってこそ技術が身につくので, 時間を割いて行ってほしいです.

【解答】

整数 $a,\ b$ と自然数 $k,\ m$ に対し,

$G = \gcd(k,\ m)$ (k と m の最大公約数) とおくと, $ak \equiv bk \pmod{m} \Longleftrightarrow a \equiv b \pmod{\boxed{\frac{m}{G}}}$

【証明】

$G = \gcd(k,\ m)$ より, $\begin{cases} k = n_1 G,\ m = n_2 G \quad (n_1,\ n_2 \text{は自然数}) \\ \gcd(n_1,\ n_2) = 1 \end{cases}$ と表せる.

(i) $\Longrightarrow$ 向きを示す.

$ak \equiv bk \pmod{m}$ より整数 l を用いて

$$\begin{aligned} ak - bk = lm &\Longleftrightarrow (a-b)n_1 G = l \cdot n_2 G \\ &\Longleftrightarrow (a-b)n_1 = l \cdot n_2 \quad (G \neq 0 \text{ より}) \end{aligned}$$

と表せる. これと $\gcd(n_1,\ n_2) = 1$ より n_2 は $a-b$ を割り切る.

よって $a \equiv b \pmod{n_2}$ つまり $a \equiv b \pmod{\frac{m}{G}}$ が成り立つことが示された.

(ii) $\Longleftarrow$ 向きを示す.

$a \equiv b \pmod{\frac{m}{G}}$ より整数 l を用いて

$$\begin{aligned} a - b = l \cdot \frac{m}{G} &\Longrightarrow ak - bk = k \cdot l \cdot \frac{m}{G} \\ &\Longleftrightarrow ak - bk = n_1 G \cdot l \cdot \frac{m}{G} \\ &\Longleftrightarrow ak - bk = n_1 lm \end{aligned}$$

と表せる. これと $n_1 l$ が整数であることから m は $ak - bk$ を割り切る.

よって $ak \equiv bk \pmod{m}$ が成り立つことが示された.

【この定理の利用例】

問) $6x \equiv 18 \pmod{10}$ を満たす整数 x を求めよ.

解) 合同式の両辺を 6 で割りたいが, そのときに法 10 がどう変化するのかを上の定理が教えてくれる.

$\gcd(6,\ 10) = 2$ より

$$\begin{aligned} 6x \equiv 18 \pmod{10} &\Longleftrightarrow \frac{6x}{6} \equiv \frac{18}{6} \pmod{\frac{10}{2}} \\ &\Longleftrightarrow x \equiv 3 \pmod{5} \\ &\Longleftrightarrow x \equiv 3,\ 8 \pmod{10} \quad (\text{元々の法に戻して答えた.}) \end{aligned}$$

よって求める整数 x は 10 で割った余りが 3 または 8 になるものである.