合同式

城北中学校・高等学校　数学科
清水団（しみず・だん）

余りの定義

Aを整数，Bを自然数とするとき，
AをBで割ったときの余りRとは，

$$A = BQ + R,\ 0 \leqq R < B$$

となる負でない整数Rをさす。（商Qは整数とする）

例 $A = -9$，$B = 4$とすると，

$$-9 = 4 \times (-3) + 3$$

となり，-9を4で割った余りは3である。

合同式の定義

a，bは整数，mは自然数とする。$a-b$がmの倍数であるとき，

$$a \equiv b \pmod{m}$$

と表し，『aとbはmを法として合同である』という。
（a合同b modulo mなどと読む）

合同式の例

- **例1**　$7-4=3$より，$7 \equiv 4 \pmod 3$
- **例2**　$10-4=6=2\cdot 3$より，$10 \equiv 4 \pmod 3$
- **例3**　$13-4=9=3\cdot 3$より，$13 \equiv 4 \pmod 3$
- **例4**　$4-13=-9=-3\cdot 3$より，$4 \equiv 13 \pmod 3$
- **例5**　$4-(-2)=6=2\cdot 3$より，$4 \equiv -2 \pmod 3$

合同式の例

法を3とすると,

- **3で割って余り0のグループ**

$$\cdots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots$$

- **3で割って余り1のグループ**

$$\cdots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots$$

- **3で割って余り2のグループ**

$$\cdots \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots$$

と3つのグループにわかれ，このループ内の数字は同じとみることになる。

合同式の例

次の3つのは同値である。

- $a \equiv b \pmod{m}$
- $a - b$はmで割り切れる
- aとbをmで割ったときの余りは一致する。

合同式の性質

同値律

$\mod m$として,

- [反射律] $a \equiv a$
- [対称律] $a \equiv b \quad$ ならば $\quad b \equiv a$
- [推移律] $a \equiv b,\ \ b \equiv c \quad$ のとき, $\ a \equiv c$

合同式の性質

性質

$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$のとき,

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$
4. $a^n \equiv b^n \pmod{m}$

合同式の性質

【1の証明】 $a+c \equiv b+d \pmod{m}$

$a-b=km,\ \ c-d=lm,$ ($k,\ l$は整数)とおくと,

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= km+lm\\ &= (k+l)m\end{aligned}$$

$$\therefore a+c \equiv b+d \pmod{m}$$

合同式の性質

【2の証明】 $a - c \equiv b - d \pmod{m}$

$a - b = km,\ \ c - d = lm,$ ($k,\ l$は整数)とおくと,

$$\begin{aligned}(a-c)-(b-d) &= (a-b)-(c-d) \\ &= km - lm \\ &= (k-l)m\end{aligned}$$

$$\therefore a - c \equiv b - d \pmod{m}$$

合同式の性質

【3の証明】 $ac \equiv bd \pmod{m}$

$a-b=km,\ c-d=lm,$ ($k,\ l$は整数)とおくと,

$$
\begin{aligned}
ac-bd &= (b+km)(d+lm)-bd \\
&= bd+(k+l)m+klm^2-bd \\
&= (k+l+klm)m
\end{aligned}
$$

$$\therefore ac \equiv bd \pmod{m}$$

合同式の性質

【4の証明】 $a^n \equiv b^n \pmod{m}$

$$
\begin{aligned}
a^2 &\equiv b^2 \pmod{m} \\
a^3 &\equiv b^3 \pmod{m} \\
a^4 &\equiv b^4 \pmod{m} \\
&\vdots
\end{aligned}
$$

帰納的に，自然数nに対して，

$$a^n \equiv b^n \pmod{m}$$

合同式の性質

例1

$40 \equiv 4 \pmod 6$, $8 \equiv 2 \pmod 6$であるので,

$$40+8 \equiv 4+2 \pmod 6 \qquad \therefore 48 \equiv 6 \pmod 6$$

$$40-8 \equiv 4-2 \pmod 6 \qquad \therefore 32 \equiv 2 \pmod 6$$

$$40 \times 8 \equiv 4 \times 2 \pmod 6 \qquad \therefore 320 \equiv 8 \pmod 6$$

しかし，割り算は成り立たない。

$40 \div 8 = 5$, $4 \div 2 = 2$であるが, $5 \equiv 2 \pmod 6$ではない。

合同式の性質

例2

$37 \equiv 2 \pmod 7$, $61 \equiv 5 \pmod 7$を用いると,

$$37 \times 61 \equiv 2 \times 5 \equiv 10 \equiv 3 \pmod 7$$

$$37^2 + 61^2 \equiv 2^2 + 5^2 \equiv 29 \equiv 1 \pmod 7$$

などがわかる。

合同式の性質

例3

$10 \equiv 1 \pmod 3$を用いると，nを自然数として，

$$10^n \equiv 1^n \equiv 1 \pmod 3$$

$$\begin{aligned} 794 &\equiv 7 \times 10^2 + 9 \times 10 + 4 \\ &\equiv 1 \times 1 + 0 \times 1 + 1 \\ &\equiv 2 \pmod 3 \end{aligned}$$

$$\begin{aligned} 56734 &\equiv 5 + 6 + 7 + 3 + 4 \\ &\equiv 2 + 0 + 1 + 0 + 1 \\ &\equiv 4 \\ &\equiv 1 \pmod 3 \end{aligned}$$

倍数判定法

3の倍数　各位の和が3の倍数

$$\boxed{abcdef} \equiv a+b+c+d+e+f \pmod 3$$

倍数判定法

3の倍数　各位の和が3の倍数

$$\boxed{abcdef} \equiv a + b + c + d + e + f \pmod 3$$

倍数判定法

pr.)　$\mathrm{mod}\ 3$とする。

$10 \equiv 1$より,

$$10^n \equiv 1^n = 1 \cdots ☆$$

$$\begin{aligned} \therefore \boxed{abcdef} &= a \times 10^5 + b \times 10^4 + c \times 10^3 \\ &\quad + d \times 10^2 + \cdots + e \times 10 + f \\ &\equiv a \times 1 + b \times 1 + c \times 1 \\ &\quad + d \times 1 + \cdots + e \times 1 + f \\ &= a + b + c + d + e + f \end{aligned}$$

倍数判定法

4の倍数　下2桁が4の倍数

$$\boxed{abcdef} \equiv \boxed{ef} \pmod 2$$

倍数判定法

pr.)　$\mathrm{mod}\ 4$とする。

$$10^2 = 100 \equiv 0 \cdots \bigstar$$

$$\begin{aligned} \therefore \boxed{abcdef} &= \boxed{abcd} \times 10^2 + \boxed{ef} \\ &\equiv \boxed{abcd} \times 0 + \boxed{ef} \quad (\because \bigstar) \\ &= \boxed{ef} \end{aligned}$$

倍数判定法

7の倍数（その1）

$$\boxed{abcdefgh} \equiv \boxed{ab} - \boxed{cde} + \boxed{fgh} \pmod 7$$

倍数判定法

pr.) $\mathrm{mod}\ 7$とする。

$$10^3 \equiv -1 \quad \therefore 10^6 \equiv 1 \cdots ◎$$

$$\begin{aligned} \therefore \quad & \boxed{abcdefgh} \\ &= \boxed{ab} \times 10^6 + \boxed{cde} \times 10^3 + \boxed{fgh} \\ &\equiv \boxed{ab} \times 1 + \boxed{cde} \times (-1) + \boxed{fgh} \quad (\because ◎) \\ &= \boxed{ab} - \boxed{cde} + \boxed{fgh} \end{aligned}$$

倍数判定法

7の倍数（その2）

$$\boxed{abc} \equiv 0 \Leftrightarrow \boxed{ab} - 2c \equiv 0 \pmod 7$$

倍数判定法

pr.)　$\bmod 7$とする。

$$10 \equiv 3,\ 100 \equiv 9 \equiv 2$$

(⇒)

$$\begin{aligned} \boxed{abc} &= a \times 10^2 + b \times 10 + c \\ &\equiv 2a + 3b + c \\ &\equiv 0 \end{aligned}$$

$$\therefore c \equiv -2a - 3b$$

$$
\begin{aligned}
\boxed{ab} - 2c &= a \times 10 + b - 2c \\
&\equiv 3a + b - 2c \\
&= 3a + b - 2(-2a - 3b) \\
&= 7(a + b) \\
&\equiv 0
\end{aligned}
$$

(⇐)

$$\begin{aligned}\boxed{ab} - 2c &= a \times 10 + b - 2c \\ &\equiv 3a + b - 2c \\ &\equiv 0\end{aligned}$$

$$\therefore b \equiv -3a + 2c$$

$$
\begin{aligned}
\boxed{abc} &= a \times 10^2 + b \times 10 + c \\
&\equiv 2a + 3b + c \\
&\equiv 2a + 3(-3a + 2c) + c \\
&= 7(c - a) \\
&\equiv 0
\end{aligned}
$$

倍数判定法

8の倍数　下3桁が8の倍数

$$\boxed{abcdef} \equiv \boxed{def} \pmod 8$$

倍数判定法

pr.)　$\mathrm{mod}\ 8$とする。

$$10^3 = 1000 \equiv 0 \cdots \bigstar$$

$$\begin{aligned} \therefore\ \boxed{abcdef} &= \boxed{abc} \times 10^3 + \boxed{def} \\ &\equiv \boxed{abc} \times 0 + \boxed{def} \quad (\because \bigstar) \\ &= \boxed{def} \end{aligned}$$

倍数判定法

9の倍数　各位の和が9の倍数

$$\boxed{abcdef} \equiv a+b+c+d+e+f \pmod 9$$

pr.)　$\bmod 9$とする。あとは3の倍数と同じ。

倍数判定法

11の倍数

$$\boxed{abcdef} \equiv -a + b - c + d - e + f \pmod{11}$$

pr.) $\mod 11$とする。

$10 \equiv -1$より,

$$10^n \equiv (-1)^n \cdots ※$$

$$\begin{aligned}
\therefore \boxed{abcdef} &= a \times 10^5 + b \times 10^4 + c \times 10^3 \\
&\quad + d \times 10^2 + \cdots + e \times 10 + f \\
&\equiv a \times (-1) + b \times 1 + c \times (-1) \\
&\quad + d \times 1 + \cdots + e \times (-1) + f \quad (\because ※) \\
&= -a + b - c + d - e + f
\end{aligned}$$