合同記号は「アタリマエ」記号

1　アタリマエのこと

例えば，6 と 11 は異なる整数ですが，共に 5 で割った余りは 1 に等しいので，5 で割った余りの分類では同じグループに属します．このことを

$$6 \equiv 11 \pmod 5$$

と表記し，「6 と 11 は 5 を法として合同である」といいます．一般に，ある 2 つの整数 a，b を自然数 m で割った余りが等しいとき，a，b は m を法として合同であるといい，

$$a \equiv b \pmod m$$

と表します．つまり，ある整数で割ったとき，余りが同じになる数は全部「同じ」と考えるのです．

記号 $\equiv$ を合同記号といい，合同記号を使った式を合同式といいます．

【例】$10 \equiv 3 \pmod 7$，$4 \equiv -1 \pmod 5$

2 つの整数 a，b を自然数 m で割った余りが等しいとき，$a-b$ は m で割り切れるから，合同式は次のように変形できます．

意味をしっかり考えよう

$$\begin{aligned} & a \equiv b \pmod m \\ \iff & a,\ b \text{ を } m \text{ で割った余りが等しい} \\ \iff & a-b \text{ が } m \text{ で割り切れる} \\ \iff & a-b \text{ を } m \text{ で割った余りが } 0 \\ \iff & a-b \equiv 0 \pmod m \end{aligned}$$

つまり．始めの合同式の右辺を左辺に移項したに過ぎません．このように，合同式では普通の等式に似た式変形が可能です．

▷Point◁(合同式の性質 Ⅰ)

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

$a+c \equiv b+d \pmod m$

$a-c \equiv b-d \pmod m$

$ac \equiv bd \pmod m$

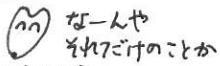
$ka \equiv kb \pmod m$

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

とくに違和感ないね

フツー

つまり，合同記号 (≡) は加法，減法，乗法については通常の等号 (=) と全く同じです．



3 つめの合同式だけ証明してみます．他の合同式は各自で証明しておいてください．

解

$a \equiv b \pmod m \iff a-b \equiv 0 \pmod m$

より，$a-b=mk$，つまり，$a=mk+b$ とおける

$c \equiv d \pmod m \iff c-d \equiv 0 \pmod m$

より，$c-d=mk$，つまり，$c=mk+d$ とおける

よって，

$$\begin{aligned} ac &= (mk+b)(mk+d) \\ &= m^2k^2+mkd+mkb+bd \\ &= m(mk^2+kd+kb)+bd \end{aligned}$$

なので，$ac-bd \equiv 0 \pmod m$．

よって，$ac \equiv bd \pmod m$ が成立する．

■

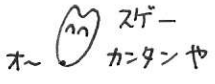
それでは，合同式を利用して問題を解いてみよう．比較のために，合同式を用いた解法と合同式を用いない解法を両方やってみます．

例題 1.　a，b，c は，それぞれ 5 で割った余りが 1, 2, 3 となる正の整数である．$a+2b+3c$ を 5 で割った余りを求めよ．

合同式を用いた解法

$a \equiv 1 \pmod 5$，$b \equiv 2 \pmod 5$，$c \equiv 3 \pmod 5$ より，

$$\begin{aligned} a+2b+3c &\equiv 1+2\cdot 2+3\cdot 3 \pmod 5 \\ &\equiv 14 \pmod 5 \\ &\equiv 4 \pmod 5 \end{aligned}$$



よって，$a+2b+3c$ を 5 で割った余りは 4 である．

合同式を用いない解法

$a=5p+1$，$b=5q+2$，$c=5r+3$ とおく．このとき，

$$\begin{aligned} a+2b+3c &= 5p+1+2(5q+2)+3(5r+3) \\ &= 5p+10q+15r+1+4+9 \\ &= 5p+10q+15r+14 \\ &= 5(p+2q+3r+2)+4 \end{aligned}$$

これまで通りの解答ですね

つまんねー

よって，$a+2b+3c$ を 5 で割った余りは 4 である．

■

例題 2.　任意の整数 n に対し，n^3+2n は 3 の倍数であることを示せ．

合同式を用いた解法

$n \equiv 0 \pmod 3$ のとき，
$n^3+2n \equiv 0^3+2\cdot 0 \equiv 0 \pmod 3$
$n \equiv 1 \pmod 3$ のとき，
$n^3+2n \equiv 1^3+2\cdot 1 \equiv 3 \equiv 0 \pmod 3$
$n \equiv 2 \pmod 3$ のとき，
$n^3+2n \equiv 2^3+2\times 2 \equiv 12 \equiv 0 \pmod 3$

よって，いずれの場合においても，$n^3+2n \equiv 0 \pmod 3$ となるので任意の整数 n で n^3+2n は 3 で割り切れる．

➪注　$n \equiv 0 \pmod 3$，$n \equiv \pm 1 \pmod 3$ とすれば少しだけ計算がラクになります．

合同式を用いない解法

$n=3m$ のとき，
$n^3+2n=(3m)^3+2(3m)=3(9m^2+2m)$
$n=3m+1$ のとき，
$n^3+2n=(3m+1)^3+2(3m+1)$
$=3(9m^3+9m^2+5m+1)$
$n=3m+2$ のとき，
$n^3+2n=(3m+2)^3+2(3m+2)$
$=3(9m^3+18m^2+12m+4)$

よって，いずれの場合においても 3 の倍数になるので，任意の整数 n で n^3+2n は 3 の倍数である．

➪注　$n=3k$，$n=3k\pm 1$ とすれば少しだけ計算がラクになります．

■

➪注　なお，この問題は，次のように式変形でも解くことができます．

$$\begin{aligned} n^3+2n &= n^3-n+3n \\ &= n(n^2-1)+3n \\ &= n(n+1)(n-1)+3n \end{aligned}$$

$n(n+1)(n-1)$ は連続 3 整数の積なので 6 の倍数（つまり 3 の倍数）．よって，n^3+2n は 3 の倍数．

■

2 つの解答を比較してどうでしょうか．合同式を用いない解答では細かくきちんと計算していますが，合同式を用いた解法では，要するに 5 や 3 で割り切れる部分は最初から無視して，影響のある箇所のみに注目して計算しています．

言い換えれば，合同式とはただ単にそれだけのことで，合同式について取り立てて大騒ぎする必要はありません．使い慣れない人はこれまで通りの方法で解けば良いですが，使いこなせるととても便利なのでぜひともマスターしておこう．

特に，合同式は次のような指数タイプの問題で威力を発揮します．

例題 3.
2007^{2007} を 17 で割った余りを求めよ．

考え方　当然，(mod 17) で考えます．

解　$2007=17\times 118+1$ だから，
$2007 \equiv 1 \pmod{17}$．したがって，
$2007^{2007} \equiv 1^{2007} \equiv 1 \pmod{17}$
となるので，余りは 1 である．

$$\begin{array}{r} 118 \\ 17\overline{)2007} \\ 17 \\ \hline 30 \\ 17 \\ \hline 137 \\ 136 \\ \hline 1 \end{array}$$

■

例題 4.
(1)　4^{200} を 9 で割った余りを求めよ．
(2)　7^{251} の下 2 桁を求めよ．

考え方　(1) は (mod 9) で，(2) は (mod 100) で考えます．4 や 7 を何回かかけて，(mod 9) や (mod 100) でうまく計算できる瞬間を探します．

解
(1)　$4^3=64$ より，$4^3 \equiv 1 \pmod 9$．
したがって，
$4^{200} \equiv (4^3)^{66}\cdot 4^2 \equiv 4^2 \equiv 16 \equiv 7 \pmod 9$
となるので，余りは 7 である．
(2)　$7^4=2401$ より，$7^4 \equiv 1 \pmod{100}$．
したがって，
$7^{251} \equiv (7^4)^{62}\cdot 7^3 \equiv 343 \equiv 43 \pmod{100}$
となるので，下 2 桁は 43 である．

※ なぜ $7^4 \equiv 1 \pmod{100}$ に気付いたのか？

$7^2=49=50-1$ と考えると
$7^4=(50-1)^2=2500-100+1$
となります．$7^4 \equiv 1 \pmod{100}$ となるのは明らかですね．

■