補 講4　合同式

4.0　はじめに

合同式 と呼ばれる考え方について簡単に解説しておきます。

この考え方も慣れておくと，入試問題などが簡単に解けるようになります。「演習編」への準備として，解説します。

4.1　合同式

4.1.1　合同式の定義

まずは定義から。

定義 (m を法とする合同)　m を与えられた一つの自然数とする。

$a,\ b$ を二つの整数とするとき，もし $a-b$ が m で割り切れるならば，a と b は m **を法として合同** であるといい，　**合同**

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

と表す。　**(定義終)**

4.1.2　合同式の性質

合同式について次の性質が成り立ちます。

定理 (同値関係であること)　m を法とするとき，次が成り立つ。

(1) $a \equiv a$ (反射律)

(2) $a \equiv b$ ならば $b \equiv a$ (対称律)

(3) $a \equiv b,\ b \equiv c$ ならば $a \equiv c$ (推移律)

証明　(1) $a-a=0=0\times m$。よって $a-a$ は m の倍数。ゆえに $a \equiv a$。

(2) $a \equiv b$ とすると，$a-b$ は m の倍数。つまり $a-b=mk$。

一方 $b-a=-mk=m(-k)$。つまり $b-a$ も m の倍数。ゆえに $b \equiv a$。

(3) $a \equiv b,\ b \equiv c$ ならば $a-b,\ b-c$ は m の倍数。よって $a-b=mk,\ b-c=mk'$ と書ける。

$$a-c=(a-b)+(b-c)=mk+mk'=m(k+k')$$

つまり $a-c$ も m の倍数。ゆえに $a \equiv c$。 **(証明終)**

さらに次の定理も成り立ちます。

定理 (合同式と加減乗) $a \equiv b,\ c \equiv d$ のとき，次の式が成り立つ。ただし，すべて m に関する法で考えているものとする。

(1) $a+c \equiv b+d$

(2) $a-c \equiv b-d$

(3) $ac \equiv bd$

(4) $a^k \equiv b^k$ (ただし k は自然数)

証明 (1) $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$ より，$a-b=mk,\ c-d=mk'$ と表すことができる。

$$(a+c)-(b+d)=(a-b)+(c-d)=mk+mk'=m(k+k')$$

よって $a+c \equiv b+d$。

(2) も同様。

(3) $a-b=mk$ より $a=b+mk$。同様に $c=d+mk'$ である。

$$ac-bd=(b+mk)(d+mk')-bd=m(bk'+dk+mkk')$$

よって $ac \equiv bd$。

(4) は (3) を繰り返し用いれば示せる。厳密には数学的帰納法による。**(証明終)**

演習編で合同式を使うと解答が簡単になる例をいくつか紹介しましょう。