合同式

11と18を7で割ると，どちらも余りが4になりますが，これを記号「≡」を用いて合同式というもので表すと，$11 \equiv 18 \pmod 7$ となり『11と18は7を法として合同である』と言います。

簡単に言えば「11と18は7で割った余りが同じ」ということです。

一般的には，n (≧2) で割ったとき，余りが等しい２数 a, b について $a \equiv b \pmod n$ と表します。

合同式は等式と同じような以下の性質が成り立ちます。

$a \equiv b \pmod n$, $c \equiv d \pmod n$ のとき
１． $a+c \equiv b+d \pmod n$
２． $a-c \equiv b-d \pmod n$
３． $ac \equiv bd \pmod n$

〔証明〕 $a = np+k$, $b = nq+k$, $c = nr+h$, $d = ns+h$ とおく。

１． $a+c = np+k+nr+h = n(p+r)+k+h$， $b+d = nq+k+ns+h = n(q+s)+k+h$

２． $a-c = np+k-(nr+h) = n(p-r)+k-h$， $b+d = nq+k-(ns+h) = n(q-s)+k-h$

３． $ac = (np+k)(nr+h) = n(prn+hp+kr)+kh$， $bd = (nq+k)(ns+h) = n(nqs+hn+ks)+kh$

このことから

$a+b \equiv b+a$, $ab \equiv ba$, $a(b+c) \equiv ab+ac$, $(a+b)+c \equiv a+(b+c)$, $a(bc) \equiv (ab)c$ （mod n）

も成り立ちますので，加法・減法・乗法については，合同式と等式は同等なものになります。

■ 合同式を利用するメリット

合同式を使うと、簡潔な表現で解答を作ることができます。

【例題１】 5^{100} を7で割った余りを求めよ。

〔解答〕 $5^{100} \equiv (25)^{100} \equiv 4^{50} \equiv 16^{25} \equiv 2^{25} \equiv 32^5 \equiv 4^5 \equiv 16 \times 16 \times 4 \equiv 2 \times 2 \times 4 \equiv 16 \equiv 2 \pmod 7$ より 2

【例題２】 6^{100} を7で割った余りを求めよ。

〔解答〕 $6^{100} \equiv (-1)^{100} \equiv 1 \pmod 7$ より 1

【例題３】自然数 $m,n\ (m\neq n)$ について， $m^n+1,\ n^m+1$ がともに10の倍数となるような自然数の組 (m,n) を１組求めよ。

〔解答〕 m^n+1 が10の倍数 $\Rightarrow$ $m^n+1\equiv 0 \pmod{10}$ であり， $m^n\equiv -1 \pmod{10}$ であるから，

$m\equiv -1 \pmod{10}$ で n が奇数なら満たすことがわかる。

同様にして， $n^m\equiv -1 \pmod{10}$ から $n\equiv -1 \pmod{10}$ で m が奇数なら満たす。

したがって， $m\equiv n\equiv -1 \pmod{10}$ を満たせばよいので、

答えの１つとして、 $m=9,\ n=19$ が挙げられる。

■ 合成数が法のとき

合成数とは素数ではない数のことです。

いくつかの数の積で表される数が法となっているとき，どう考えればよいでしょうか。

【例題４】 23^{100} を55で割った余りを求めよ。

〔解答〕 $23^{100}\equiv 3^{100}\equiv (-2)^{100}\equiv 4^{50}\equiv (-1)^{50}\equiv 1 \pmod{5}$

$23^{100}\equiv 1^{100}\equiv 1 \pmod{11}$

となることから、23^{100} は「5 で割っても、11 で割っても 1 余る数」ということになり、55 で割ると１余る数になることがわかります。

★ 合成数のときは小さい数を法として分析し，後で総合するという解析的な手法が有効です。

【例題５】 $13^n-9^n-4^n$ は36で割り切れることを証明せよ。

〔解答〕 $13^n-9^n-4^n\equiv 4^n-0^n-4^n\equiv 0 \pmod{9}$

$13^n-9^n-4^n\equiv 1^n-1^n-0^n\equiv 0 \pmod{4}$

であるから，$13^n-9^n-4^n$ は 9 でも 4 でも割り切れることがわかり，36 で割り切れる。

★ 数学的帰納法を使っての証明をよく目にする問題ですが，合同式の威力が感じられます。

【例題６】 a,b を互いに素な整数とするとき、$(a-1)$ 個の数 $b,\ 2b,\ 3b,\ \cdots,\ (a-1)b$ を

それぞれ a で割った余りはすべて異なることを示せ。

〔解答〕背理法で示す。

$1 \leqq i < j \leqq a-1$　$ib \equiv jb \pmod{a}$ なる２数 $i,\ j$ が存在すると仮定する。

すると，$(j-i)b \equiv 0 \pmod{a}$　…（＊） となる。

ここで，$0 < j-i < a$，a と b が互いに素であることから（＊）は成立しない。

よって，このような２数 $i,\ j$ は存在せず，題意は成り立つ。

■ $ax+by=1$

【例題６】の結果により，次の定理が導かれます。

【例題７】 a,b を互いに素な整数とするとき，

$ax+by=1$ を満たすような整数の組 (x,y) が必ず存在することを証明せよ。

〔解答〕【例題６】の結果より、$b,\ 2b,\ 3b,\ \cdots,\ (a-1)b$ をそれぞれ a で割った余りは

すべて異なるので，これらは $1,\ 2,\ \cdots,\ (a-1)$ の並べ替えである。

したがって，その中には $bi \equiv 1 \pmod{a}$ $\left(1 \leqq i \leqq a-1\right)$ となるような i が存在する。

この i を y と書き換えると，$by \equiv 1 \pmod{a}$

よって，$1-by$ は a の倍数なので ax とおけ，

このような x について $ax+by=1$ となる。

■ フェルマーの小定理

【例題６】の結果として $a \to p$（p は素数）とすると，p と互いに素な任意の整数 b に対し，

$b,\ 2b,\ \cdots,\ (p-1)b$ を p で割った余りは，$1,\ 2,\ \cdots,\ (p-1)$ の並べ替えだけということになります。

このことから，次の「フェルマーの小定理」が導かれます。

＜フェルマーの小定理＞

素数 p と互いに素な任意の数について、その数を $(p-1)$ 乗した数を p で割ると１余る。

〔証明〕

a を素数 p と互いに素な任意の数とする。

このとき
$$\begin{aligned} a &\equiv r_1 \\ 2a &\equiv r_2 \\ &\vdots \\ (p-1)a &\equiv r_{p-1} \end{aligned}$$
いずれも $(\mathrm{mod}\ p)$ であり，

右辺の $r_1 \sim r_{p-1}$ は $1 \sim (p-1)$ の並べ替えであるから，これらの式を辺々かけて

$$(p-1)!a^{p-1} \equiv r_1 \cdots\cdots r_{p-1} \left(= (p-1)! \right) \ (\mathrm{mod}\ p)$$

よって　$(p-1)!(a^{p-1}-1) \equiv 0 \ \ (\mathrm{mod}\ p)$

ここで，$(p-1)!$ は p と互いに素であるから　$a^{p-1}-1 \equiv 0 \qquad \therefore a^{p-1} \equiv 1$

〔わかりにくいので，具体化してみると〕

素数 11 について，$1^{10}, 2^{10}, 3^{10}, \cdots, 10^{10}$ を 11 で割った余りはすべて 1 になり

素数 17 について，$1^{16}, 2^{16}, 3^{16}, \cdots, 16^{16}$ を 17 で割った余りはすべて 1 になります。

このことを応用すると【例題１】は次のように解くこともできます。

$5^{100} \equiv (5^6)^{16} \cdot 5^4 \equiv 1^{16} \cdot 5^4 \equiv 5^4 \equiv 2 \ (\mathrm{mod}\ 7)$

フェルマーの小定理より　$5^6 \equiv 1 \ (\mathrm{mod}\ 7)$　を利用しています。