数学と人間の活動【合同式】 p.174～176

青チャートA: 例題129～132

【態度目標】しゃべる、質問する、説明する、動く、協力する、貢献する

【内容目標】性質を用いて、条件を満たす自然数の組を求めよう

発展 補足 合同式

2つの整数 a，b を5で割ったときの余りが，それぞれ2，4であるとき，$a+b$，$a-b$，ab を5で割ったときの余りは，それぞれ $2+4$，$2-4$，$2\cdot4$ を5で割ったときの余りに等しかった。

一般に，m を正の整数とし，2つの整数 a，b を m で割ったときの余りを，それぞれ r，r' とすると，次のことが成り立つ。

1 $a+b$ を m で割った余りは，余りの和 $r+r'$ を m で割った余りに等しい。
2 $a-b$ を m で割った余りは，余りの差 $r-r'$ を m で割った余りに等しい。
3 ab を m で割った余りは，余りの積 rr' を m で割った余りに等しい。

更に，k を正の整数とするとき，次のことが成り立つ。

4 a^k を m で割った余りは，r^k を m で割った余りに等しい。

整数の割り算やその余りについて考察するとき，「**合同式**」を用いると，表記が簡潔になり，考察もしやすくなる。

m は正の整数とする。2つの整数 a，b について a を m で割ったときの余りと，b を m で割ったときの余りが等しいとき，余りの差 $r-r'$ は0であり，$a-b$ は m の倍数である。

$a-b$ が m の倍数であるとき，a と b は m を **法** として **合同** であるといい，式で

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

a 合同 b モッド m

と表す。このような式を **合同式** という。a と b が m を法として合同であるとは，

『a を m で割った余りと，b を m で割った余りが等しい』

ということと同じである。

ガウスが1801年(24歳のとき)「Disquisitiones Arithmeticae (ガウス整数論)」にて発表

補足 mod はラテン語で寸法あるいは標準を，英語では法や対数係数，絶対値を意味する modulus を略したものである。

補足 証明 $a=mq+r$, $b=mq'+r'$ …… ① とすると

1 $r+r'$ を m で割ったときの商を s，余りを u とすると
$r+r'=ms+u$, $0 \leqq u < m$ …… ②
①②により $a+b=m(q+q')+r+r'$
$=m(q+q')+ms+u$
$=m(q+q'+m)+u$
したがって $a+b$ を m で割ったときの余りは u
すなわち $r+r'$ を m で割ったときの余りに等しい
(2も同様)

3 rr' を m で割ったときの商を v，余りを w とすると
$rr'=mv+w$, $0 \leqq w < m$ …… ③
①③により $ab=(mq+r)(mq'+r')$
$=m(mqq'+qr'+q'r)+rr'$
$=m(mqq'+qr'+q'r)+mv+w$
$=m(mqq'+qr'+q'r+v)+w$
したがって ab を m で割ったときの余りは w
すなわち rr' を m で割ったときの余りに等しい

4 c, d を整数とし $b=mc+d$ とする。
d は必ずしも $0 \leqq d < m$ を満たさなくてもよい。
このとき①より
$ab=m(mqc+qd+cr)+rd$ ……④
となり
$ab \div m$ の余り $= rd \div m$ の余り ……⑤
となる
④において $b=a$, $c=q$, $d=r$ とすれば
$a^2=m(mq^2+2qr)+r^2$ ……⑥
となり⑤より
$a^2 \div m$ の余り $= r^2 \div m$ の余り
がわかる。また，④において，⑥のように
$b=a^2$, $c=mq^2+2qr$, $d=r^2$ とすると⑤より
$a^3 \div m$ の余り $= r^3 \div m$ の余り
がわかる。
同様にして任意の自然数 k について4が成り立つ

数学と人間の活動【合同式】 p.174～176

青チャートA: 例題129～132

以下では，a，b，c，d は整数，m，k は正の整数とする。

合同式について，次のことが成り立つ。

[1] $a \equiv a \pmod{m}$【反射律】

[2] $a \equiv b \pmod{m}$ のとき　$b \equiv a \pmod{m}$【対称律】

[3] $a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$ のとき　$a \equiv c \pmod{m}$【推移律】

} まとめて同値律

【注意】$a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$ を $a \equiv b \equiv c \pmod{m}$ と書いてもよい。

補足 証明 [1] $a-a=m\cdot 0$ から　$a \equiv a \pmod{m}$

[2] $a-b=ml$（l は整数）から　$b-a=m(-l)$　よって　$b \equiv a \pmod{m}$

[3] $a-b=ml$，$b-c=ml'$（l，l' は整数）から

$a-c=(a-b)+(b-c)=ml+ml'=m(l+l')$

よって　$a \equiv c \pmod{m}$

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

1　$a+b \equiv c+d \pmod{m}$　　2　$a-b \equiv c-d \pmod{m}$

3　$ab \equiv cd \pmod{m}$　　4　$a^k \equiv c^k \pmod{m}$

【1の証明】

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

整数 l，l' を用いて

$a-c=ml$ ……①，

$b-d=ml'$ ……②

と表される。①，② から

$(a+b)-(c+d)=(a-c)+(b-d)$

$=ml+ml'$

$=m(l+l')$

したがって　$a+b \equiv c+d \pmod{m}$　終

【2の証明】

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

整数 l，l' を用いて

$a-c=ml$ ……①

$b-d=ml'$ ……②

と表される。①，② から

$(a-b)-(c-d)=(a-c)-(b-d)$

$=ml-ml'$

$=m(l-l')$

したがって　$a-b \equiv c-d \pmod{m}$　終

【3の証明】

①，② から

$ab-cd=a(b-d)+d(a-c)$

$=aml'+dml$

$=m(al'+dl)$

したがって　$ab \equiv cd \pmod{m}$　終

【4の証明】

3で $b=a$，$d=c$ とすると，

$a^2 \equiv c^2 \pmod{m}$，

$a^3 \equiv c^3 \pmod{m}$，

$a^4 \equiv c^4 \pmod{m}$，

…… が成り立ち，

4が成り立つことがわかる。　終

補足 割り算について

3で $b=d$ としたもの逆演算を割り算とみることができるが，両辺を b で割って良いのは

b と m （割る数と法とする数）が互いに素であるときに限られるので注意が必要

数学と人間の活動【合同式】 p.174～176

青チャートA: 例題129～132

合同式を利用して，整数の割り算の余りを求めてみよう。

例１） (1) 15^{100} を 7 で割った余りを求める。

$15 \equiv 1 \pmod 7$ であるから　$15^{100} \equiv 1^{100} \equiv 1 \pmod 7$

よって，15^{100} を 7 で割った余りは 1 である。

(2) 3^{2222} を 5 で割った余りを求める。

$3^4 = 81$ であるから　$3^4 \equiv 1 \pmod 5$

よって　$3^{2222} \equiv (3^4)^{555} \cdot 3^2 \equiv 1^{555} \cdot 9 \equiv 4 \pmod 5$

したがって，3^{2222} を 5 で割った余りは 4 である。　終

『 $\equiv 1$ 』を作るのがポイント

合同式を利用して，百五減算について考察してみよう。

問題　私の年齢を 3 で割った余りは 2，5 で割った余りは 3，7 で割った余りは 4 である。私の年齢は何歳か。ただし，105 歳より下である。

求める年齢 x を 3，5，7 で割った余りがそれぞれ a，b，c であるとき，

$n = 70a + 21b + 15c$ とする。

$x \equiv a \pmod 3$，$x \equiv b \pmod 5$，$x \equiv c \pmod 7$ であり

$n \equiv 70a \equiv 1 \cdot a \equiv a \equiv x \pmod 3$

$n \equiv 21b \equiv 1 \cdot b \equiv b \equiv x \pmod 5$

$n \equiv 15c \equiv 1 \cdot c \equiv c \equiv x \pmod 7$

$n - x$ は 3，5，7 で割り切れる，すなわち 3，5，7 の最小公倍数 105 で割り切れる。

よって，整数 k を用いて $n - x = 105k$ と表される。

すなわち　$x = n - 105k$

この k が n から 105 を引く回数である。

$a = 2$，$b = 3$，$c = 4$ となるから

$n = 140 + 63 + 60 = 263$

よって　$x = 263 - 105k$

$k = 2$ とすると　$x = 53$

例） n は整数とする。n を 5 で割った余りが 3 であるとき，次のものを求めよ。

$n = 5k + 3$（k は整数）とおいて代入してもよい

(1) n^4 を 5 で割った余り　　(2) $n^2 + n + 1$ を 5 で割った余り

解答 (1) $n \equiv 3 \pmod 5$ のとき

$n^4 \equiv 81 \pmod 5$

$81 \equiv 1 \pmod 5$ より

$n^4 \equiv 1 \pmod 5$

よって，n^4 を 5 で割った余りは 1 である。

(2) $n \equiv 3 \pmod 5$ のとき

$n^2 + n + 1 \equiv 3^2 + 3 + 1 \pmod 5$

$3^2 + 3 + 1 = 13$，$13 \equiv 3 \pmod 5$ より

$n^2 + n + 1 \equiv 3 \pmod 5$

よって，$n^2 + n + 1$ を 5 で割った余りは 3 である。

数学と人間の活動【合同式】 p.174～176

青チャートA: 例題129～132

補充問題）

1． n は整数とする。n を 11 で割った余りが 5 であるとき， $2n^2-5n+4$ を 11 で割った余りを求めよ。

解答 $2n^2-5n+4 \equiv 2\cdot 5^2-5\cdot 5+4$

$\equiv 29 \equiv 7 \pmod{11}$

よって，求める余りは 7 である

別解 $n=11k+5$（k は整数）とおくと

$2n^2-5n+4$

$=2(11k+5)^2-5(11k+5)+4$

$=2\cdot 11^2k^2+15\cdot 11k+29$

$=11(22k^2+15k+2)+7$

と変形できるので，求める余りは 7 である。

2． n は整数とする。合同式を用いて，次のことを証明せよ。

「n^4 を 3 で割ったときの余りは， 0 か 1 である。」

解答 $n\equiv 0$ のとき $n^4\equiv 0^4\equiv 0 \pmod{3}$

$n\equiv 1$ のとき $n^4\equiv 1^4\equiv 1 \pmod{3}$

$n\equiv 2$ のそき $n^4\equiv 2^4\equiv 16\equiv 1 \pmod{3}$

よって， n^4 を 3 で割ったときの余りは， 0 か 1 である

別解 すべての整数 n は

$n=3k$，$n=3k+1$，$n=3k+2$（k は整数）

のいずれかの形で表される。

$n^4=(3m)^4=3\cdot 27m^4$

$n^4=(3m+1)^4$

$=81m^4+108m^3+54m^2+12m+1$

$=3(27m^4+36m^3+18m^2+4m)+1$

$n^4=(3m+2)^4$

$=81m^4+216m^3+216m^2+96m+16$

$=3(27m^4+72m^3+72m^2+32m+5)+1$

と変形できるので，

n^4 を 3 で割ったときの余りは， 0 か 1 である

3． a，b，c は整数で $a^2+b^2=c^2$ が成り立つとき， a，b の少なくとも 1 つは 3 の倍数であることを証明せよ。

解答 整数 n について， 3 を法として

$n\equiv 0$，$n\equiv 1$，$n\equiv 2$ のいずれかが成り立ち，

$n\equiv 0$ のとき $n^2\equiv 0$

$n\equiv 1$ のとき $n^2\equiv 1^2\equiv 1$

$n\equiv 2$ のとき $n^2\equiv 2^2\equiv 4\equiv 1$

である。

a，b はともに 3 の倍数でないと仮定する。

上で調べたことから， 3 を法として

$a^2\equiv 1$，$b^2\equiv 1$

よって $a^2+b^2\equiv 1+1\equiv 2$

ところが $c^2\equiv 2$ とはなり得ない。

したがって， a，b の少なくとも 1 つは

3 の倍数である。

解答 a，b はともに 3 の倍数でないと仮定する。

3 の倍数でない整数は $3k+1$，$3k+2$（k は整数）のどちらかで表され

$(3k+1)^2=9k^2+6k+1=3(3k^2+2k)+1$

$(3k+2)^2=9k^2+12k+4=3(3k^2+4k+1)+1$

ゆえに，3 の倍数でない整数の 2 乗を 3 で割った余りは 1 となるから，a^2，b^2 を 3 で割った余りはともに 1 となる。

よって，a^2+b^2 を 3 で割った余りは 2 ……①

一方，c が 3 の倍数のとき，c^2 は 3 で割り切れ，c が 3 の倍数でないとき，c^2 を 3 で割った余りは 1 となる。

よって，c^2 を 3 で割った余りは 0 か 1 ……②

①，② は $a^2+b^2=c^2$ であることに矛盾する。

したがって，a，b のうち少なくとも 1 つは 3 の倍数である。