

❏ 余りによる分類

❖ 261-061-005

整数の割り算について、 a を b で割ったときの商を q 、余りを r とします。すなわち、

$$a \div b = q \cdots r$$

とします。

このとき、上の式を変形すると、 $a = bq + r$ の形となります。

通常、 r は b より小さい数であり、 q と r は、ただ 1 通りに定まります。実はこの当たり前のことが、とても重要なのです。

さて、通常どんな整数でも、ある数によって割ったときの余りで分類することができます。たとえば、自然数 n を 3 で割った余りを考えてみましょう。 n が 1, 2, 3, 4, 5, 6, $\dots$ とすると、それらを 3 で割った余りは、1, 2, 0, 1, 2, 0, $\dots$ というように、余りが 0, 1, 2 で分類することができます。

3 で割った余りが 0 $\rightarrow$ 3, 6, 9, 12, 15, 18, 21, $\dots$

3 で割った余りが 1 $\rightarrow$ 1, 4, 7, 10, 13, 16, 19, $\dots$

3 で割った余りが 2 $\rightarrow$ 2, 5, 8, 11, 14, 17, 20, $\dots$

割り算の余りのことを**剰余**といいます。このように、ある数で割ったときの余りによって分類をする考え方全般を**剰余類**といいます。「余りを制するものは整数を制する」といわれるほど、重要な考え方です。

❏ 合同式

❖ 261-061-006

この内容は、完全にマスターする必要はありません。ですが、マスターできると、整数の剰余類の問題がいつきに解きやすくなります。余力のある人は取り組んでみましょう。今は飛ばして、時間を置いてから取り組んでも構いません。

合同式

m は正の整数とする。2つの整数 a, b について、 $a - b$ が m の倍数であるとき（すなわち、 a を m で割った余りと b を m で割った余りが等しいとき）、 a と b は m を**法として合同**であるといい、以下のように表す、また、これを**合同式**という。

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

さて、ただの記号のお約束なのですが、これがメチャクチャ役に立つのです。

たとえば、7 と 4 は、どちらも 3 で割った余りが 1 です ($7 - 4 = 3$)。なので、 $7 \equiv 4 \pmod{3}$ と表します。

合同式を知っていなくても問題は解けます。しかし、主に剰余類の問題を解くときには、式がとても煩雑になることがあり、ともすれば計算ミスを起こしたり、頭を整理することが困難になることもあります。合同式を知っていることで、表記が簡潔になり、問題に取り組みやすくなるというメリットがあります。合同式については、次の約束事を覚えておきましょう。

以下, a, b, c, d は整数とし, m と k は自然数とする。

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

$$(1) a + b \equiv c + d \pmod{m}$$

$$(2) a - b \equiv c - d \pmod{m}$$

$$(3) ab \equiv cd \pmod{m}$$

$$(4) a^k \equiv c^k \pmod{m}$$

要約すると, 除法 (割り算) を除いた四則演算で, 「 $\equiv$ 」と同じように扱うことができます。

それでは, 「合同式を使わない解き方」と「合同式を使う解き方」で, 簡単な例題を 2 問取り組んでみて, 比較しましょう。

《例 2-1》

15^{100} を 7 で割った余りを求めよ。

〈合同式を使わない解き方〉

$15 = (2 \cdot 7 + 1)$ より, 二項定理 (数学 II) を用いて,

$$\begin{aligned} 15^{100} &= (2 \cdot 7 + 1)^{100} \\ &= {}_{100}C_0 (2 \cdot 7)^{100} + {}_{100}C_1 (2 \cdot 7)^{99} + {}_{100}C_2 (2 \cdot 7)^{98} + \cdots + {}_{100}C_{99} \cdot 2 \cdot 7 + {}_{100}C_{100} \cdot 1^{100} \\ &= 7(2^{100} \cdot 7^{99} + {}_{100}C_1 \cdot 2^{99} \cdot 7^{98} + {}_{100}C_2 \cdot 2^{98} \cdot 7^{97} + \cdots + {}_{100}C_{99} \cdot 2) + 1 \end{aligned}$$

よって, 15 を 7 で割った余りは 1 である。

〈合同式を使う解き方〉

$15 \equiv 1 \pmod{7}$ より, $15^{100} \equiv 1^{100} \pmod{7}$ なので, 15^{100} を 7 で割った余りは 1 である。

《例 2-2》

整数 n を 9 で割った余りが 4 であるとき, $n^2 + n + 1$ を 9 で割った余りを求めよ。

〈合同式を使わない解き方〉

$n = 9k + 4$ (k は整数) とおくと,

$$\begin{aligned} n^2 + n + 1 &= (9k + 4)^2 + (9k + 4) + 1 \\ &= 9^2 k^2 + 9 \cdot 8k + 16 + 9k + 4 + 1 \\ &= 9^2 k^2 + 9 \cdot 9k + 18 + 3 \\ &= 9(9k^2 + 9k + 2) + 3 \end{aligned}$$

よって, $n^2 + n + 1$ を 9 で割った余りは 3 である。

〈合同式を使う解き方〉

$n \equiv 4 \pmod{9}$ より, $n^2 \equiv 16 \equiv 7 \pmod{9}$ となるので,

$$n^2 + n + 1 \equiv 7 + 4 + 1 \equiv 12 \equiv 3 \pmod{9}$$

よって, $n^2 + n + 1$ を 9 で割った余りは 3 である。

どうでしょうか? 合同式の魅力が伝わりませんか? 使わなくても解けるので, 演習問題は合同式を使わなくても OK です。マスターしたい人は, 演習問題でも合同式を使ってみましょう!

□ □ 【12】 ◇ 261-062-012

n を自然数とすると、次のことを証明せよ。

- (1) $n^3 - n$ は 6 の倍数である。
- (2) $n^4 + 2n^2$ は 3 の倍数である。

□ □ 【13】 ◇ 261-062-013

$n + 2$ が 3 の倍数であるとき、 $7n + 4$ を 3 で割ったときの余りはいくらか。

□ □ 【14】 ◇ 261-062-014

- (1) 3 で割ると 2 余り、4 で割ると 3 余る正の整数のうち最小のものを求めよ。
- (2) 11 で割れば 3 余り、15 で割れば 7 余るような整数の中で最小の正の整数を求めよ。

□ □ 【15】 ◇ 261-062-015

n を 1 以上 200 以下の自然数とする。

- (1) n を 5 で割ったときの余りが 1 となるような n は全部で何個あるか。
- (2) n^2 を 5 で割ったときの余りが 1 となるような n は全部で何個あるか。

□ □ 【16】 ◇ 261-062-016

各位の数がすべて異なる 3 桁の 3 の倍数はいくつあるか。

□ □ 【17】 ◇ 261-062-017

自然数 n に対し、 $n^9 - n^3$ は 9 で割り切れることを示せ。

□ □ 【18】 ◇ 261-062-018

n を自然数とする。 $n^3 + 2n + 1$ を 3 で割ると 1 余ることを証明せよ。

演習問題
解答・解説



- (1) $a = 15a'$, $b = 15b'$ とすると, a' , b' は互いに素である。
最小公倍数が 180 より,
$$a' \times b' \times 15 = 180 \quad \therefore a'b' = 12$$

したがって,
 $(a', b') = (1, 12), (2, 6), (3, 4)$
このうち, $(2, 6)$ は互いに素ではないので,
 $(a', b') = (1, 12), (3, 4)$
以上から,
 $(a, b) = (15, 180), (45, 60)$

- (2) $a = 12a'$, $b = 12b'$ とすると, a' , b' は互いに素である。
最小公倍数が 216 より,
$$a' \times b' \times 12 = 216 \quad \therefore a'b' = 18$$

したがって,
 $(a', b') = (1, 18), (2, 9), (3, 6)$
このうち, $(3, 6)$ は互いに素ではないので,
 $(a, b) = (12, 216), (24, 108)$

【11】 ※ 261-062-011

- (1) 和が 180, 最大公約数が 12 である 2 つの自然数の組をすべて求めよ。
(2) 積が 3549, 最小公倍数が 273 である 2 つの自然数の組を求めよ。

- (1) 2 つの自然数を A, B ($A < B$) とすると,
 $A = 12a$, $B = 12b$ (a, b は互いに素)
となる。
 $A + B$ が 180 となるので,
$$12a + 12b = 180$$
$$12(a + b) = 180$$
$$a + b = 15$$

よって, a, b の組合せは $a < b$ より,
 $(a, b) = (1, 14), (2, 13), (3, 12),$
 $(4, 11), (5, 10), (6, 9), (7, 8)$
このうち, a, b が互いに素になるものは,
 $(1, 14), (2, 13), (4, 11), (7, 8)$
である。よって,
 $(A, B) = (12, 168), (24, 156),$
 $(48, 132), (84, 96)$

- (2) 2 つの自然数を A, B ($A < B$) とし, 最大公約数を g とすると,
 $A = ag$, $B = bg$ (a, b は互いに素)
となる。
 $AB = 3549$ であることから,
$$abg^2 = 3549 \quad \cdots \cdots \textcircled{1}$$

 A, B の最小公倍数が 273 であることから,
$$abg = 273 \quad \cdots \cdots \textcircled{2}$$

 $\textcircled{1}, \textcircled{2}$ より $g = 13$
これを $\textcircled{2}$ に代入し, $ab = 21$
よって, a, b の組合せは $a < b$ より,
 $(a, b) = (1, 21), (3, 7)$
どちらも互いに素であるから,
 $(A, B) = (13, 273), (39, 91)$

Section 2 剰余類

【12】 ※ 261-062-012

n を自然数とすると, 次のことを証明せよ。

- (1) $n^3 - n$ は 6 の倍数である。
(2) $n^4 + 2n^2$ は 3 の倍数である。

- (1) $n^3 - n = n(n^2 - 1)$
$$= n(n+1)(n-1)$$
$$= (n-1) \times n \times (n+1)$$

よって, $n^3 - n$ は 3 連続している整数の積であるので, 少なくとも 1 つの偶数と 3 の倍数を含む。
したがって, $n^3 - n$ は 6 の倍数である。 ■
(注) n が 1 のときは, $n^3 - n$ が 0 になってしまうが, これも 6 の倍数として考えている。
(2) $n^4 + 2n^2 = n^2(n^2 + 2) \quad \cdots \cdots \textcircled{1}$
 k を 0 以上の整数としたとき, すべての自然数は $3k, 3k+1, 3k+2$ の形で表すことができる。

- (i) $n = 3k$ のとき
$$\textcircled{1} = (3k)^2 \{(3k)^2 + 2\}$$
$$= 9k^2(9k^2 + 2)$$

よって, 3 の倍数となる。
(ii) $n = 3k+1$ のとき
$$\textcircled{1} = (3k+1)^2 \{(3k+1)^2 + 2\}$$
$$= (3k+1)^2(9k^2 + 6k + 3)$$
$$= 3(3k+1)^2(3k^2 + 2k + 1)$$

よって, 3 の倍数となる。

(iii) $n = 3k + 2$ のとき、

$$\begin{aligned} \textcircled{1} &= (3k+2)^2 \{(3k+2)^2 + 2\} \\ &= (3k+2)^2 (9k^2 + 12k + 6) \\ &= 3(3k+2)^2 (3k^2 + 4k + 2) \end{aligned}$$

よって、3 の倍数となる。

(i), (ii), (iii) より、すべての自然数 n に関して、 $n^4 + 2n^2$ は

3 の倍数である。■

〈別解〉

合同式で場合分けをしてもよい。

(i) $n \equiv 0 \pmod{3}$

$$n^4 + 2n^2 \equiv 0 + 0 \equiv 0 \pmod{3}$$

(ii) $n \equiv 1 \pmod{3}$

$$n^4 + 2n^2 \equiv 1 + 2 \equiv 3 \equiv 0 \pmod{3}$$

(iii) $n \equiv 2 \pmod{3}$

$$\begin{aligned} n^4 + 2n^2 &\equiv 2^4 + 2 \cdot 2^2 \equiv 24 \\ &\equiv 0 \pmod{3} \end{aligned}$$

【13】◇261-062-013

$n+2$ が 3 の倍数であるとき、 $7n+4$ を 3 で割ったときの余りはいくらか。

$n+2 = 3k$ (k は整数) とおくと、 $n = 3k - 2$
よって、

$$\begin{aligned} 7n+4 &= 7(3k-2)+4 \\ &= 21k-10 \\ &= 3(7k-4)+2 \end{aligned}$$

ゆえに、 $7n+4$ を 3 で割ったときの余りは **2**

〈別解〉

$n+2 \equiv 0 \pmod{3}$ より、 $n \equiv 1 \pmod{3}$ なので、

$$7n+4 \equiv 7+4 \equiv 11 \equiv 2 \pmod{3}$$

【14】◇261-062-014

- (1) 3 で割ると 2 余り、4 で割ると 3 余る正の整数のうち最小のものを求めよ。
(2) 11 で割れば 3 余り、15 で割れば 7 余るような整数の中で最小の正の整数を求めよ。

(1) 3 で割ると 2 余る自然数は「3 で割ると 1 不足」と考えることもできる。

同様に、4 で割ると 3 余る自然数も「4 で割ると 1 不足」している数である。

よって、求める数は 3 と 4 の最小公倍数から 1 を引いた **11**

(2) 求める正の整数を n とすると、 n は 11 で割っても、15 で割っても 8 不足する。

よって、 $n+8$ は、11 でも 15 でも割り切れる。

したがって、 $n+8$ は 11、15 の公倍数である。

$$n+8 > 8 \text{ より } n+8 = 11 \cdot 15$$

よって、 $n = \mathbf{157}$

【15】◇261-062-015

n を 1 以上 200 以下の自然数とする。

- (1) n を 5 で割ったときの余りが 1 となるような n は全部で何個あるか。
(2) n^2 を 5 で割ったときの余りが 1 となるような n は全部で何個あるか。

(1) n を 5 で割ったとき、余りが 1 となる 200 以下の自然数 n は、

$$1, 5 \cdot 1 + 1, 5 \cdot 2 + 1, \dots, 5 \cdot 39 + 1$$

よって、**40** 個

(2) $n = 5k + m$ (k は 0 以上の整数; $m = 1, 2, 3, 4, 5$) とすると、

$$\begin{aligned} n^2 &= (5k+m)^2 = 25k^2 + 10km + m^2 \\ &= 5(5k^2 + 2km) + m^2 \end{aligned}$$

n^2 を 5 で割ると 1 余るのは $m = 1, 4$ のときである。

よって、 $n = 5k + 1$ のとき、(1) から 40 個。

$n = 5k + 4$ のときも (1) と同様に考えて 40 個。

したがって、全部で、

$$40 + 40 = \mathbf{80} \text{ (個)}$$

〈別解〉

(2) で合同式を用いる。

$n \equiv 0, 1, 2, 3, 4 \pmod{5}$ であるとき、 $n^2 \equiv 0, 1, 4, 9, 16 \pmod{5}$ であり、 $n^2 \equiv 9 \equiv 4$ 、 $n^2 \equiv 16 \equiv 1 \pmod{5}$ であるから、 $n \equiv 1, 4 \pmod{5}$ である n を数えればよい。

(以下省略)

【16】◇261-062-016

各位の数がすべて異なる 3 桁の 3 の倍数はいくつあるか。

0~9 の数を, 3 で割った余りで分類する。

A グループ: {3, 6, 9} 余り 0

B グループ: {1, 4, 7} 余り 1

C グループ: {2, 5, 8} 余り 2

D グループ: {0}

3 の倍数を作るためには, ① {A, B, C}, ② {A, A, A}, ③ {B, B, B}, ④ {C, C, C}, ⑤ {A, A, D}, ⑥ {B, C, D} の組み合わせであればよい。

① のとき, $3 \times 3 \times 3 \times 3! = 162$ (個)

② のとき, $3! = 6$ (個)

③, ④ のときもそれぞれ 6 (個)

⑤ のとき, A グループからの 2 つの数の選び方が ${}_3C_2$ 通りであり, 0 は百の位におけないので, 並べ方は 4 通り。よって,

$${}_3C_2 \times 4 = 12 \text{ (個)}$$

⑥ のとき, $3 \times 3 \times 4 = 36$ (個)

よって, ①~⑥ より,

$$162 + 6 \times 3 + 12 + 36 = 228 \text{ (個)}$$

【17】◇ 261-062-017

自然数 n に対し, $n^9 - n^3$ は 9 で割り切れることを示せ。

任意の自然数 n は, 自然数 k を用いて $n = 3k - 2$ または $n = 3k - 1$ または $n = 3k$ で表される。

ここで,

$$\begin{aligned} n^9 - n^3 &= n^3(n^6 - 1) \\ &= n^3(n^3 - 1)(n^3 + 1) \end{aligned}$$

(i) $n = 3k - 2$ のとき

$$\begin{aligned} n^3 - 1 &= 27k^3 - 54k^2 + 36k - 8 - 1 \\ &= 9(3k^3 - 6k^2 + 4k - 1) \end{aligned}$$

(ii) $n = 3k - 1$ のとき

$$\begin{aligned} n^3 + 1 &= 27k^3 - 27k^2 + 9k - 1 + 1 \\ &= 9(3k^3 - 3k^2 + k) \end{aligned}$$

(iii) $n = 3k$ のとき

$$n^3 = 27k^3 = 9 \times 3k^3$$

(i), (ii), (iii) より, $n^3 - 1$, $n^3 + 1$, n^3 のいずれかが 9 の倍数となる。

よって, $n^9 - n^3$ は 9 で割り切れる。 ■

【18】◇ 261-062-018

n を自然数とする。 $n^3 + 2n + 1$ を 3 で割ると 1 余ることを証明せよ。

(i) $n = 3m(m = 1, 2, \dots)$ のとき

$$\begin{aligned} n^3 + 2n + 1 &= 27m^3 + 6m + 1 \\ &= 3(9m^3 + 2m) + 1 \end{aligned}$$

よって, 3 で割ると 1 余る。

(ii) $n = 3m + 1(m = 0, 1, 2, \dots)$ のとき

$$\begin{aligned} n^3 + 2n + 1 &= (3m + 1)^3 + 2(3m + 1) + 1 \\ &= 27m^3 + 27m^2 + 9m + 1 + 6m + 3 \\ &= 3(9m^3 + 9m^2 + 5m + 1) + 1 \end{aligned}$$

よって, 3 で割ると 1 余る。

(iii) $n = 3m + 2(m = 0, 1, 2, \dots)$ のとき

$$\begin{aligned} n^3 + 2n + 1 &= (3m + 2)^3 + 2(3m + 2) + 1 \\ &= 27m^3 + 54m^2 + 36m + 8 + 6m + 5 \\ &= 3(9m^3 + 18m^2 + 14m + 4) + 1 \end{aligned}$$

よって, 3 で割ると 1 余る。

(i), (ii), (iii) より, すべての自然数 n において, $n^3 + 2n + 1$ を 3 で割ると 1 余る。 ■

<別解>

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

$(n - 1)n(n + 1)$ は 3 連続整数の積で 3 の倍数であるから, $n^3 + 2n + 1$ は 3 で割ると 1 余る。

Section 3 ユークリッドの互除法

【19】◇ 261-062-019

$\frac{148953}{298767}$ を約分して既約分数にせよ。

$298767 \div 148953 = 2 \cdots 861$ が成立する。また, $148953 \div 861 = 173$ が成り立つ。よって, 298767 と 148953 の最大公約数は 861 となるので,

$$148953 = 861 \times 173$$

$$298767 = 148953 \times 2 + 861$$

$$= 861 \times 173 \times 2 + 861$$

$$= 861 \times (346 + 1)$$

$$= 861 \times 347$$

$$\text{ゆえに, } \frac{148953}{298767} = \frac{173}{347}$$