整数問題【中級編】

初級編をマスターした人は，中級編にトライしていきましょう．ここでは，合同式の知識を学習し，より快適に整数問題を攻略する術を身につけていきます．なお，合同式は大学の教養課程で学習するものですが，大学入試で取り上げられることもあり，整数問題を頻出とする大学を受験する人は是非とも知っておきたい方法です．

【合同式】

整数 a をある数 n で割ったとき，その余りによって n 通りに分類することができます．

例： 整数 を 5 で割ったときの余りについて分類すると，

余り 0 ☞ … -10, -5, 0, 5, 10 …

余り 1 ☞ … -9, -4, 1, 6, 11 …

余り 2 ☞ … -8, -3, 2, 7, 12 …

余り 3 ☞ … -7, -2, 3, 8, 13 …

余り 4 ☞ … -6, -1, 4, 9, 14 …

となります．負の数の余りは少し違和感があるかもしれませんが …．このように，無限個の整数を有限個に分類することは非常に大切な考え方なのです．そこで，余りに着目して等式を考えてみることにしましょう．

a, b を整数, n を自然数とするとき, a を n で割った余りと b を n で割った余りが等しいならば,「a と b は n を法として**合同**である」といい，次のように表します．

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

このような式を**合同式**といいます．mod はモッド（英語読み）とかモデュロ（仏語読み）と読みます．このように合同式を定義すると，合同式には次のような性質があることがわかります．

a, b, c, d を整数, n, m を自然数とするとき, $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ が成り立つとき，次の関係式が成り立つ．

（ i ） $a+c \equiv b+d \pmod{n}$　　（ ii ） $a-c \equiv b-d \pmod{n}$

（iii） $ac \equiv bd \pmod{n}$　　（iv） $a^m \equiv b^m \pmod{n}$

合同式は加法・減法・乗法に関しては，＝（イコール）の場合と同じ関係が成り立つ．

簡単に証明しておきましょう．

【証明】

a, b, c, d を n で割ったときの商をそれぞれ q_a, q_b, q_c, q_d とし，余りをそれぞれ r_a, r_b, r_c, r_d とする．このとき，$a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ が成り立つことから，

$$r_a = r_b \text{ かつ } r_c = r_d$$

が成り立つ．よって，

$$a = nq_a + r_a,\quad b = nq_b + r_a,\quad c = nq_c + r_c,\quad d = nq_d + r_c$$

と置くことができる.

（ｉ）の**【証明】**

$$a+c=nq_a+r_a+nq_c+r_c=n(q_a+q_c)+r_a+r_c$$

$$b+d=nq_b+r_a+nq_d+r_c=n(q_b+q_d)+r_a+r_c$$

となることからいずれも n で割った余りは r_a+r_c となるので，$a+c\equiv b+d\pmod n$ が成り立つ.

（ii）の**【証明】**

$$a-c=nq_a+r_a-nq_c-r_c=n(q_a-q_c)+r_a-r_c$$

$$b-d=nq_b+r_a-nq_d-r_c=n(q_b-q_d)+r_a-r_c$$

となることからいずれも n で割った余りは r_a-r_c となるので，$a-c\equiv b-d\pmod n$ が成り立つ.

（iii）の**【証明】**

$$ac=(nq_a+r_a)(nq_c+r_c)=n(nq_aq_c+q_ar_c+r_aq_c)+r_ar_c$$

$$bd=(nq_b+r_a)(nq_d+r_c)=n(nq_bq_d+q_br_c+r_aq_d)+r_ar_c$$

となることからいずれも n で割った余りは r_ar_c となるので，$ac\equiv bd\pmod n$ が成り立つ.

（iv）の**【証明】**

$$\begin{aligned}a^m&=(nq_a+r_a)^m\\&={}_m\mathrm{C}_0(nq_a)^m+{}_m\mathrm{C}_1(nq_a)^{m-1}r_a+{}_m\mathrm{C}_2(nq_a)^{m-2}(r_a)^2+\cdots+{}_m\mathrm{C}_{m-1}nq_a(r_a)^{m-1}+{}_m\mathrm{C}_m(r_a)^m\end{aligned}$$

$$\begin{aligned}b^m&=(nq_b+r_a)^m\\&={}_m\mathrm{C}_0(nq_b)^m+{}_m\mathrm{C}_1(nq_b)^{m-1}r_a+{}_m\mathrm{C}_2(nq_b)^{m-2}(r_a)^2+\cdots+{}_m\mathrm{C}_{m-1}nq_b(r_a)^{m-1}+{}_m\mathrm{C}_m(r_a)^m\end{aligned}$$

となることからいずれも n で割った余りは $(r_a)^m$ となるので，$a^m\equiv b^m\pmod n$ が成り立つ.

このようにして，性質が証明されますが，この証明で次のような事実が判明します.

和の余りは，余りの和

積の余りは，余りの積

もちろん，差や累乗に関しても同様の結果が得られていることがわかります．実は，余りに関する問題を扱うときに非常に大切な考え方なので，必ず理解しておいてください．これに関しては，整数問題**【初級編】**の p.9, 10 でも解説しているので，参考にしてください.

次に，今後よく利用する式を紹介して証明しておきましょう．

x, a, b, n を自然数とするとき，次の合同式が成り立つ．

$$(ax+b)^n \equiv b^n \pmod{x}$$

【証明】

二項定理を用いて左辺を展開すると，

$$\begin{aligned}(ax+b)^n &= {}_n\mathrm{C}_0(ax)^n + {}_n\mathrm{C}_1(ax)^{n-1}b + {}_n\mathrm{C}_2(ax)^{n-2}b^2 + \cdots\cdots + {}_n\mathrm{C}_{n-1}(ax)b^{n-1} + {}_n\mathrm{C}_n b^n \\ &= ax({}_n\mathrm{C}_0(ax)^{n-1} + {}_n\mathrm{C}_1(ax)^{n-2}b + {}_n\mathrm{C}_2(ax)^{n-3}b^2 + \cdots\cdots + {}_n\mathrm{C}_{n-1}b^{n-1}) + b^n\end{aligned}$$

となるので，左辺を x で割った余りは b^n となるので，

$$(ax+b)^n \equiv b^n \pmod{x}$$

が成り立つことが示された． **【証明終】**

さて，まずはこの式が自由自在に使えるようになっておく必要があるので，その練習から始めましょう．

例題 **類題演習** ☞ p.20

次の各問いに答えよ．

(1) 12^{65} を 11 で割った余りを求めよ．

(2) 2^{65} を 11 で割った余りを求めよ．

(3) n を自然数とするとき，$13^{2n}+6$ は 7 で割り切れることを示せ．

(1) は $12 = 11+1$ と分解し，(2) では $2^{65} = (2^5)^{13} = (33-1)^{13}$ と変形し，(3) では $13 = 14-1$ と変形します．なんとかして 11 の倍数との和や差に変形することが大切です．

♣ ♠

解答 と **解説**

(1) $12^{65} = (11+1)^{65} \equiv 1^{65} \pmod{11}$

ゆえに，求める余りは **1**……(**答**)

(2) $2^{65} = (2^5)^{13} = (33-1)^{13} \equiv (-1)^{13} \pmod{11}$

$= -1 \equiv 11-1 \pmod{11}$

$= 10$

ゆえに，求める余りは **10**……(**答**)

(3) **【証明】**

$13^{2n}+6 = (14-1)^{2n}+6 \equiv (-1)^{2n}+6 \pmod{7}$

$= 1+6 \equiv 0 \pmod{7}$

ゆえに，示された． **【証明終】**

♣ ♠

注意したいのは，合同式を用いたときは 解答 にあるように，必ず （mod n）を書くということです．何を法として合同なのかがわからないと意味がないからです．このように，合同式を使うとあっという間に証明できることがわかります．整数問題**【初級編】**の p.8 の 例題 や p.11 の **5** の問題もこれと同じ方法で計算できるのでやってみて下さい．それでは，類題を解いてみましょう．

◀類題演習▶

6

解答 ☞ p.21

次の各問いに答えよ．

（1） 7^{100} を 5 で割った余りを求めよ．

（2） 3^{52} を 11 で割った余りを求めよ．

（3） n が自然数のとき，$2^{n+1}+3^{2n-1}$ は 7 で割り切れることを証明せよ．

7 （′00　熊本県立大）

解答 ☞ p.22

今日は金曜日であるとする．

（1） 10^6 日後は何曜日か．

（2） 10^{100} 日後は何曜日か．

（3） 3^{100} 日後は何曜日か．

8

解答 ☞ p.23

3^{15} および $(3^{15})^{15}$ の 1 の位を求めよ．

9

解答 ☞ p.24

n を自然数とするとき，次の各問いに答えよ．

（1） $3^{n+1}+4^{2n-1}$ は 13 で割り切れることを示せ．

（2） $3^{4n+2}+5^{2n+1}$ は 14 で割り切れることを示せ．

6 解答 と 解説

(1) $7^{100} = (5+2)^{100} \equiv 2^{100} \pmod 5$

$= 4^{50} = (5-1)^{50}$

$\equiv (-1)^{50} \pmod 5$

$= \mathbf{1}$……(**答**)

(2) $3^{52} = 9^{26} = (11-2)^{26}$

$\equiv (-2)^{26} \pmod{11}$

$= 2^{26} = 2\cdot 2^{25} = 2\cdot 32^5 = 2(33-1)^5$

$\equiv 2(-1)^5 \pmod{11}$

$= -2$

$\equiv 9 \pmod{11}$

ゆえに，求める余りは，**9**……(**答**)

(3) **【証明】**

$2^{n+1} + 3^{2n-1} = 2^{n+1} + 3\cdot 3^{2n-2}$

$= 2^{n+1} + 3\cdot 9^{n-1}$

$\equiv 2^2\cdot 2^{n-1} + 3\cdot 2^{n-1} \pmod 7$

$= 7\cdot 2^{n-1}$

$\equiv 0 \pmod 7$

ゆえに，7 で割り切れることが示された． **【証明終】**

♣ ♢ ♠ ♡

解説

(1) は 5 を法として合同な式を作るので，できるだけ底を 5 に近い数になるように変形することを考えます．
なお，a^n において，a のことを底(てい)といいます．

(2) に関しても同様に 11 を法として合同式を作るので，底を 11 に近い数になるよう指数部分を使って変形をします．ただし，指数部分が分数になってはいけないので，

$$2^{26} = 32^{\frac{26}{5}}$$

のような変形をしてはいけません．このような事態を回避するために，$2^{26} = 2\cdot 2^{25}$ として，$2\cdot 32^5$ としているのです．

(3) は，底が統一されていないので，合同式を用いて底を統一することを考えます．最初の変形で $3^{2n-1} = 3\cdot 3^{2n-2}$ としているのは，$3^{2n-2} = (3^2)^{n-1}$ という変形がしたいからです．$3^2 = 9$ が 7 に近い数であることから 7 を法として合同式を作ることを考えます．このことから，このような変形をするのです．

7 解答 と 解説

(1) 7 で割った余りを計算すればよい.

$$\begin{aligned} 10^6 &= (7+3)^6 \\ &\equiv 3^6 \pmod 7 \\ &= 9^3 = (7+2)^3 \\ &\equiv 2^3 \pmod 7 \\ &\equiv 1 \pmod 7 \end{aligned}$$

よって, 10^6 日後は, **土曜日**……(**答**)

(2) (1) より, $10^6 \equiv 1 \pmod 7$ であるから,

$$\begin{aligned} 10^{100} &= (10^6)^{16} \cdot 10^4 \\ &\equiv 10^4 \pmod 7 \\ &\equiv 3^4 \pmod 7 \\ &\equiv 4 \pmod 7 \end{aligned}$$

よって, 10^{100} 日後は, **火曜日**……(**答**)

(3)

$$\begin{aligned} 3^{100} &\equiv (7+3)^{100} \pmod 7 \\ &\equiv 4 \pmod 7 \quad (\because (2)) \end{aligned}$$

よって, 3^{100} 日後は, **火曜日**……(**答**)

♣ ♢ ♠ ♡

解説

1 週間は 7 日なので, 7 を法とした合同式を考えます. 前問の結果をうまく使えば, 計算が幾分か省略できることに気付きましょう.

8 解答 と 解説

(1) 10 で割った余りを計算すればよい.

$$\begin{aligned} 3^{15} &= 3\cdot(3^2)^7 \\ &\equiv 3\cdot(-1)^7 \pmod{10} \\ &= -3 \\ &\equiv 7 \pmod{10} \end{aligned}$$

よって, 3^{15} の 1 の位は, **7**……(**答**)

(2) (1) より, $3^{15}\equiv 7 \pmod{10}$ であるから,

$$\begin{aligned} (3^{15})^{15} &\equiv 7^{15} \pmod{10} \\ &= (10-3)^{15} \pmod{10} \\ &\equiv (-3)^{15} \pmod{7} \\ &= -3^{15} \\ &\equiv -7 \pmod{10} \quad (\because (1)) \\ &\equiv 3 \pmod{10} \end{aligned}$$

よって, $(3^{15})^{15}$ の 1 の位は, **3**……(**答**)

♣ ♢ ♠ ♡

解説

1 の位を考えるので, 地道に計算してもそれほど大変ではありません. 合同式を使うのであれば, 10 を法として考えましょう.

9 解答 と 解説

(1) **【証明】**

$$\begin{aligned}(\text{与式}) &= 3^2\cdot 3^{n-1}+4\cdot 4^{2(n-1)}\\ &\equiv 9\cdot 3^{n-1}+4\cdot 3^{n-1} \pmod{13}\\ &= 13\cdot 3^{n-1}\\ &\equiv 0 \pmod{13}\end{aligned}$$

ゆえに，13 で割り切れることが示された． **【証明終】**

(2) **【証明】**

$$\begin{aligned}(\text{与式}) &= 9^{2n+1}+5^{2n+1}\\ &\equiv (-5)^{2n+1}+5^{2n+1} \pmod{14}\\ &= -5^{2n+1}+5^{2n+1}\\ &= 0\end{aligned}$$

ゆえに，14 で割り切れることが示された． **【証明終】**

♣ ◇ ♠ ♡

解説

底をそろえることを考えます．(1), (2) ともに大きな数で割るので，よく考えて底をそろえましょう．

合同式に関しての基本的な計算などができるようになれば，後は実戦に取り組んでいきましょう．合同式が題材になった入試問題を紹介するので，解いてみてください．

10 （'00　名古屋大） 解答 ☞ p.25

自然数 x, y に対して，それぞれを 100 で割った余りが等しいとき，$x \equiv y$ と書くことにする．

(1)　自然数 m に対して，$76^m \equiv 76$ を証明せよ．

(2)　$2^n \equiv 76$ をみたす最小の自然数 n を求めよ．

(3)　2^{1001} を 100 で割った余りを求めよ．

10 解答 と 解説

(1) **【証明】**

$76^2 = 5776 \equiv 76$ より，$76^3 \equiv 76^2 \equiv 76$ となるので，以後これを繰り返し用いると，

$$76^m \equiv 76$$

となることがわかるので，示された． **【証明終】**

(2) 2^n の下 2 桁を $f(n)$ で表すことにすると，下表を得る．

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$f(n)$	2	4	8	16	32	64	28	56	12	24	48	96	92	84	68	36	72	44	88	76

ゆえに，$\boldsymbol{n = 20}$……(**答**)

(3) (2) より，$2^{20} \equiv 76$ であるから，

$$2^{1000} = (2^{20})^{50} \equiv 76^{50} \equiv 76 \quad (\because \ (1))$$

よって，$2^{1001} \equiv 2 \cdot 76 = 152 \equiv 52$ より，求める余りは **52**……(**答**)

♣ ♢ ♠ ♡

解説

(1) は，厳密には数学的帰納法で証明する方がよいでしょうが，明らかに規則性がわかるので，解答では省略しました．(2) は，答えの書き方で迷いますが，思い切って表をかき，地道に探すのが一番早いでしょう．ただ，考えるのは下 2 桁だけでよいので，$f(n)$ という関数を作りました．(3) は，(1), (2) で得られた事実をどのように利用するかがポイントになります．