

1日目

整数と合同式 (数A)

- § 1 概要・総論
- § 2 ユークリッドの互除法
- § 3 合同式
- § 4 合同式

□ 4つの特長で使いやすい!! 文章を美しく見せるなら「ロジカルノート」

大、小の文字が書ける!

植物の成長
 芽したインゲンマメが
 育って来ました。

- 1 行間が作れる、英文の記入にも最適**
- 1行の間に3分割のガイドラインを入れました。下側2分割に文字を記入することにより、1行に対して1/3の行間を確保することができます。これにより、読み返し易い、きれいな文章を記入することができます。
 - また3分割のガイドラインは、英文の記入にも活用が可能です。英習紙のように大文字と小文字が書き易くなります。

英文を書きやすい!

土曜日の朝に
 on Saturday morning

- 2 段落が揃う**
- タテの方向に、横書きに支障のない濃さのラインが印刷されています。このタテラインを目安に、タイトルと文章に段落を付けることができます。これを活用することで、文章が見やすくなります。

図、枠が描きやすい!

水 二酸化炭素
 water carbon dioxide

6×2=12

- 3 図、表の作成**
- タテとヨコのラインで方眼紙のような使い方ができます。数学、理科で記入の多い図形の作成に便利です。
 - 定規を使用しなくても手描きで容易に作表ができます。また、定規を使用すれば、より効率的に作表することが可能です。

● ページを2分割

● ページを3分割

● ページを3分割(4分目メモリ使用)

● ページを4分割

例) 数学、物理: 図、解答に分ける

例) 世界史: 国、地域ごとに分ける

例) 日本史: 年代ごとにまとめる

例) 英語: 単語帳として

- 4 ページを分割**
- ページ上下のメモリをタテラインに合わせることで、ページを3分割、又は4分割にすることが可能です。
 - 分割することにより、様々な科目、用途に活用できます。

§1. 整数の除法、約数・倍数、素数

10.1

(1) $25 \div 7 = 3 \dots 4$ 余り 4

(2) $-25 \div 7 = -3 \dots 4$ 余り 4

(3) 1, 2, 3, 4, 6, 8, 12, 24

(4) はい

(5) いいえ

解説

(1) 25 を 7 で割った余り

$$\Delta 25 \div 7 = 3 \dots 4$$

(あまり) の表現

② $25 = 7 \times 3 + 4$

(なるべくかけ算の形で)

余り 4 は

割る数 7 より小さく

0 以上で表す。

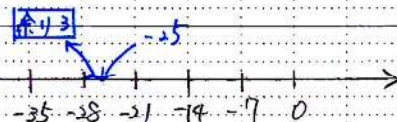
	3
7	25
21	
4	

筆算は OK

 $a \in \text{整数}, b \in \text{自然数}$ とするとき以下のような整数 q, r がただ 1 つ決まる。

$$a = bq + r$$

ただし、 $0 \leq r < b$

このとき q を商、 r を余りという。(2) -25 を 7 で割った余り

(3) 24 の約数を全て列挙せよ。← 負の約数もある

< 約数・倍数について >

整数 A, B に対して

$$A = Bk$$

を満たす整数が存在するとき

 B を A の約数
 A を B の倍数 と言う。

(解答)

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$$

(4) 0 は 6 の倍数か。

(解答: Yes)

(整数)

(約数)

$$0 = \Delta \times 6$$

ある? $\Rightarrow 0$

(0 は 6 の 0 倍)

(5) 0 は 6 の約数か。

(解答: No)

$$6 = \Delta \times 0$$

ここにはある整数ある?

(1x-ジとして、 $\frac{6}{0}$ とした整数は存在しない)

102

(1) 2, 3, 5, 7, 11, 13, 17, 19

(2) $108 = 2 \times 2 \times 3 \times 3 \times 3$

約数: 12個。

(3) 正の約数: 16個。 総和: 360。

解説

[素数]... 2以上の約数で

正の約数も1と自分自身しか持たないもの

(1) は素数には入らない

↑ 1が入ると、素因数分解が1通りに決まらない。

(1) 素数: 2, 3, 5, 7, 11, 13, 17, 19, ...

(2) [素因数分解]

2以上の整数Nは

素数を小さい順に並べることで

T=1通りに積の形に表せる

→「素因数分解の一意性」

$$\begin{array}{l}
 2) 108 \\
 2) 54 \\
 3) 27 \\
 3) 9 \\
 3) 3
 \end{array}
 \quad
 \begin{array}{l}
 108 = 2 \times 2 \times 3 \times 3 \times 3 \\
 = 2^2 \times 3^3
 \end{array}$$

指数法則 (例で)

(1) $2^3 \times 2^5 = 2^{3+5} = 2^8$

(2) $(2^3)^4 = 2^{3 \times 4} = 2^{12}$

(3) $(3 \times 5)^5 = 3^5 \times 5^5$

[正の約数の個数・総和]

(注意) $2^0 = 1$ と決める。 $2^0 = 1$ に関して、

$$2^5 \div 2^3 = \frac{2 \times 2 \times 2 \times 2 \times 2}{2 \times 2 \times 2} = 2^{5-3} = 2^2 = 4$$

$$2^5 \div 2^5 = \frac{2 \times 2 \times 2 \times 2 \times 2}{2 \times 2 \times 2 \times 2 \times 2} = 1 = 2^{5-5} = 2^0$$

$$2^5 \div 2^6 = \frac{2 \times 2 \times 2 \times 2 \times 2}{2 \times 2 \times 2 \times 2 \times 2 \times 2} = \frac{1}{2} = 2^{5-6} = 2^{-1}$$

$$2^{-1} = \frac{1}{2} \text{ と定義できる。 } (2^{-n} = \frac{1}{2^n})$$

(2) の 108 を例に考える。

$108 = 2^2 \times 3^3$

108 の正の約数Dは、

$D = 2^a \times 3^b$ の形に表せる。

T=1で、 $a=0, 1, 2$

$b=0, 1, 2, 3$

例) $2 = 2^1 \times 3^0 \rightarrow 1$

$36 = 2^2 \times 3^2$

よって、Dの約数は $(2+1)(3+1) = 3 \times 4 = 12$ (個)

aの個数 bの個数

[実際に書いてみると]

[表1]

1, 2, 2^2

$1 \times 3, 2 \times 3, 2^2 \times 3$

$1 \times 3^2, 2 \times 3^2, 2^2 \times 3^2$

$1 \times 3^3, 2 \times 3^3, 2^2 \times 3^3$

の計12個。

[正の約数の総和] → 綺麗な形に整う。

108 で具体的に計算する。

表1を全て足すと、(総和をSとする)

$$\begin{aligned}
 S &= 1 + 2 + 2^2 \\
 &\quad + (1 + 2 + 2^2) \times 3 \\
 &\quad + (1 + 2 + 2^2) \times 3^2 \\
 &\quad + (1 + 2 + 2^2) \times 3^3 \\
 &= (1 + 2 + 2^2)(1 + 3 + 3^2 + 3^3) \\
 &= (1 + 2 + 4)(1 + 3 + 9 + 27) \\
 &= 7 \times 40 \\
 &= 280
 \end{aligned}$$

次のように、自然数 N が素因数分解されたとき

$$N = 2^a \times 3^b \times 5^c \times 7^d$$

正の約数の総和 S は

$$\begin{aligned}
 S &= (1 + 2^1 + 2^2 + \dots + 2^a)(1 + 3^1 + 3^2 + \dots + 3^b) \\
 &\quad \times (1 + 5^1 + 5^2 + \dots + 5^c)(1 + 7^1 + 7^2 + \dots + 7^d) \text{ と表せる。}
 \end{aligned}$$

$$(3) \quad 120 = 2^3 \times 3 \times 5$$

[正の約数の個数]

120 の正の約数 D は

$$D = 2^a \times 3^b \times 5^c$$

$$a = 0, 1, 2, 3$$

$$b = 0, 1$$

$$c = 0, 1$$

よって約数の個数は

$$(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16$$

[正の約数の総和 S]

全て正の約数を書く。

$$\begin{aligned}
 S &= \boxed{1 + 2 + 2^2 + 2^3} \quad \xrightarrow{\text{和は } (1+2+2^2+2^3) \times 3} \quad \text{2}^a \times 3^b \text{ の約数 (形)} \\
 &\quad \boxed{1 \times 3 + 2 \times 3 + 2^2 \times 3 + 2^3 \times 3} \\
 &\quad + \boxed{1 \times 5 + 2 \times 5 + 2^2 \times 5 + 2^3 \times 5} \quad \xrightarrow{\text{和は } (1+2+2^2+2^3+3+2 \times 3+2^2 \times 3+2^3 \times 3) \times 5} \quad \text{2}^a \times 3^a \times 5^b \text{ の約数 (形)} \\
 &\quad + \boxed{1 \times 3 \times 5 + 2 \times 3 \times 5 + 2^2 \times 3 \times 5 + 2^3 \times 3 \times 5} \\
 &\quad \xrightarrow{\text{和は } (1+2+2^2+2^3+3+2 \times 3+2^2 \times 3+2^3 \times 3) \times 5} \\
 &\quad = (1+2+2^2+2^3)(1+3) \times 5 \\
 \text{つまり、} S &= (1+2+2^2+2^3)(1+3) \times 1 \\
 &\quad + (1+2+2^2+2^3)(1+3) \times 5 \\
 &= (1+2+2^2+2^3)(1+3)(1+5) \\
 &= (1+2+4+8) \times 4 \times 6 \\
 &= 15 \times 4 \times 6 \\
 &= 360
 \end{aligned}$$

10.3

$$a = 2^3 \times 3^5 \quad \text{全て偶数}$$

$$b = 2^2 \times 3^4 \times 5^2 \quad \text{「平方数」}$$

$$c = 3^6 \times 5^3 \quad \text{「平方数」「立方数」}$$

$$d = 5^2 \times 11^3 \quad \text{「立方数」}$$

(1) 平方数: 整数の2乗の形の整数。

$$\text{例) } 1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 9$$

$$\text{平方数 } M^2 = \boxed{} \rightarrow \text{整数 } M$$

$$a = 2^3 \times 3^5 = \begin{array}{l} \boxed{2 \times 2 \times 3 \times 3 \times 3} \\ \times \boxed{2 \times 3 \times 3 \times 3} \end{array} \quad \begin{array}{l} \text{平方数に素因数分解すると} \\ \text{各素数の指数は偶数} \end{array}$$

(2) 立方数: 整数の3乗の形の整数。

$$\text{立方数 } N^3 = \boxed{}$$

$$\times \boxed{}$$

$$\times \boxed{}$$

$$a = 2^3 \times 3^5 = \begin{array}{l} \boxed{2 \times 3 \times 3} \\ \times \boxed{2 \times 3 \times 3} \\ \times \boxed{2 \times 3 \times 3} \end{array} \quad \begin{array}{l} \text{立方数に素因数分解すると} \\ \text{各素数の指数は3の倍数} \end{array}$$

(3) $N = a \times b$

$$= 2^3 \times 3^5 \times 2^2 \times 3^{10} \times 5^2$$

$$= 2^{3+2} \times 3^{5+10} \times 5^2$$

$$= 2^5 \times 3^{15} \times 5^2$$

 N の約数 D は、

$$D = 2^a \times 3^b \times 5^c \quad (a, b, c \text{ は } 0 \text{ 以上の整数})$$

このうち平方数は、全ての指数が偶数のもの (0も偶数)

よって、 $a = 0, 2, 4 \quad (5 \text{ 以下})$ $b = 0, 2, 4, 6, 8, 10, 12, 14 \quad (15 \text{ 以下})$ $c = 0, 2 \quad (2 \text{ 以下})$

なので、平方数の約数の個数は

$$3 \times 8 \times 2 = 48 \quad \square$$

10.4

$$(1) M = 2^3 \times 3^2 \times 5$$

$$N = 2^5 \times 3^4 \times 5^2 \times 7$$

 M の倍数でかつ N の約数である正の整数 D は

$$D = 2^a \times 3^b \times 5^c \times 7^d$$

とおくと、

$$a = 3, 4, 5$$

$$b = 2, 3, 4$$

$$c = 1, 2$$

$$d = 0, 1$$

なので、個数は $n = 3 \times 3 \times 2 \times 2 = 36 \quad \square$

総和は、

$$\left(\begin{array}{l} \text{具体的に書くと、} 2^3 \times 3^2 \times 5 + 2^3 \times 3^2 \times 5 \times 7 \\ + 2^3 \times 3^2 \times 5^2 + 2^3 \times 3^2 \times 5^2 \times 7 \dots \end{array} \right)$$

$$2^3, 2^4, 2^5, 3^2, 3^3, 3^4, 5, 5^2, 1, 7$$

の組み合わせを考えると、

$$(2^3 + 2^4 + 2^5)(3^2 + 3^3 + 3^4)(5 + 5^2)(1 + 7)$$

を展開すると求める整数の和が、もれなく重複なく現れる。

よってこの値が S である。

$$\begin{aligned} S &= 2^3(1+2+4) \times 3^2(1+3+9) \times 5(1+5)(1+7) \\ &= 2^3 \times 7 \times 3^2 \times 13 \times 5 \times 2 \times 3 \times 2^3 \\ &= 2^7 \times 3^3 \times 5 \times 7 \times 13 \end{aligned}$$

2日目

指数法則

$$[1] 2^m \times 2^n = 2^{m+n}$$

$$[2] (2^m)^n = 2^{m \times n}$$

$$[3] (2 \times 3)^n = 2^n \times 3^n$$

練習

$$(1) 2^5 \times 2^4 = 2^{5+4} = 2^9$$

$$(2) (2^5)^4 = 2^{5 \times 4} = 2^{20}$$

$$(3) (2^3 \times 7^2)^4 = (2^3)^4 \times (7^2)^4 = 2^{12} \times 7^8$$

$$\begin{aligned} (4) (2^3 \times 3)^2 \times (2 \times 3^2)^3 &= (2^3)^2 \times 3^2 \times 2^3 \times (3^2)^3 \\ &= 2^6 \times 3^2 \times 2^3 \times 3^6 \\ &= 2^{6+3} \times 3^{2+6} \\ &= 2^9 \times 3^8 \end{aligned}$$

106

[最大公約数・最小公倍数]

[G.C.D.] [L.C.M.]

$$(1) \begin{cases} 120 = 2^3 \times 3 \times 5 \\ 1260 = 2^2 \times 3^2 \times 5 \times 7 \end{cases}$$

[G.C.D.] 共通の約数で最大のもの。

$$A \text{ の約数: } 2^{\textcircled{3}} \times 3^{\textcircled{1}} \times 5^{\textcircled{1}} \times \dots \textcircled{1}$$

$$B \text{ の約数: } 2^{\textcircled{2}} \times 3^{\textcircled{2}} \times 5^{\textcircled{1}} \times 7^{\textcircled{1}} \times \dots \textcircled{2}$$

と書く。(1に1は、①、②の各指数はそれぞれ A, B の指数以下)

A, B の G.C.D. は、各指数の小さい方 (最小のもの)

をとって、各底に対してかければ良い。

$$\textcircled{2} 2 \rightarrow \begin{cases} a \leq 3 \\ p \leq 2 \end{cases} \Rightarrow 2^2 \text{ とする。}$$

$$\textcircled{3} 3 \rightarrow \begin{cases} b \leq 1 \\ q \leq 2 \end{cases} \Rightarrow 3^1 \text{ とする。}$$

$$\textcircled{4} 5 \rightarrow \begin{cases} c \leq 1 \\ r \leq 1 \end{cases} \Rightarrow 5^1 \text{ とする。}$$

$$\textcircled{5} 7 \rightarrow 7 \text{ は } A \text{ の約数ではないのでとらない。}$$

(7⁰ = 1 と考えても良い)

よって G.C.D. は

$$2^2 \times 3 \times 5$$

[L.C.M.]

A, B の公倍数を素因数分解すると

A, B の素因数分解を (両方とも必ず) 含む。

⇒ 各底に対して、指数の大きい方を

公倍数は約数として必ず含む。

⇒ A, B の L.C.M. は (最小性を考えると)

A, B の各素因数を比較して

指数の大きい方をとって、かけあわせれば良い。

$$A = 2^{\textcircled{3}} \times 3^{\textcircled{1}} \times 5^{\textcircled{1}} \times \dots \textcircled{1}$$

$$B = 2^{\textcircled{2}} \times 3^{\textcircled{2}} \times 5^{\textcircled{1}} \times 7^{\textcircled{1}} \times \dots \textcircled{2}$$

$$L.C.M. \text{ は } 2^3 \times 3^2 \times 5 \times 7$$

$$(2) \begin{cases} 240 = 2^4 \times 3 \times 5 \\ 252 = 2^2 \times 3^2 \times 7 \end{cases}$$

$$G.C.D. = 2^2 \times 3$$

$$L.C.M. = 2^4 \times 3^2 \times 5 \times 7$$

$$(3) \begin{cases} 432 = 2^4 \times 3^3 \\ 1225 = 5^2 \times 7^2 \end{cases}$$

$$G.C.D = 2^0 \times 3^0 \times 5^0 \times 7^0 = 1$$

$$L.C.M = 2^4 \times 3^3 \times 5^2 \times 7^2$$

$$(4) \begin{cases} 7^5 \\ 7^9 \end{cases}$$

$$G.C.D = 7^5$$

$$L.C.M = 7^9$$

108

[大きな数の素因数分解]

$$\begin{aligned} (1) 10! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 2 \times 3 \times 2^2 \times 5 \times (2 \times 3) \times 7 \times 2^3 \times 3^2 \times (2 \times 5) \\ &= 2^8 \times 3^4 \times 5^2 \times 7 \end{aligned}$$

10!の2の個数を数える。

	2	2 ² =4	2 ³ =8	2 ⁴
1				
2	○			
3				
4	○	○		
5				
6	○			
7				
8	○	○	○	
9				
10	○			

このように

2^a (a:自然数)

(2の累乗の形)

でいくつ割れるか(商)

を計算して

合計すれば良い。

10÷2, 10÷4, 10÷8の商の

合計が、10!の素因数分解

した時の2の指数。

$$5 + 2 + 1 = 8$$

[計号の紹介~カウス記号~]

[x] = 「xをこえない最大の整数」

= 「x>0のときは、xの整数部分」

$$\text{例)} [3.14] = 3, [12] = 1$$

よって、10!の素因数2の指数は

$$\begin{aligned} \left[\frac{10}{2} \right] + \left[\frac{10}{4} \right] + \left[\frac{10}{8} \right] &= [5] + [2.5] + [1.25] \\ &= 5 + 2 + 1 \\ &= 8 \end{aligned}$$

と書ける。

(2) 2の指数

$$\begin{aligned} \left[\frac{50}{2} \right] + \left[\frac{50}{4} \right] + \left[\frac{50}{8} \right] + \left[\frac{50}{16} \right] + \left[\frac{50}{32} \right] &= 25 + 12 + 6 + 3 + 1 \\ &= 47 \end{aligned}$$

3の指数

$$\begin{aligned} \left[\frac{50}{3} \right] + \left[\frac{50}{9} \right] + \left[\frac{50}{27} \right] &= 16 + 5 + 1 \\ &= 22 \end{aligned}$$

5の指数

$$\begin{aligned} \left[\frac{50}{5} \right] + \left[\frac{50}{25} \right] &= 10 + 2 \\ &= 12 \end{aligned}$$

(3) 10 = 2 × 5 より

2と5両方で10がでる。

よって5の素因数の個数

(2の素因数より少ない)

12が0が並ぶ。

よって、0は12個並ぶ。

§2. ユークリッドの互除法

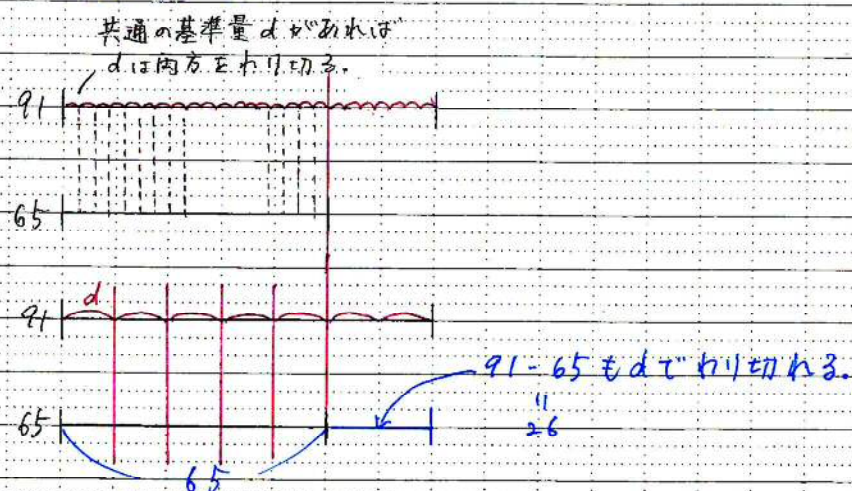
[ユークリッドの互除法]

素因数分解を使わずに

2 整数の最大公約数を求める方法。

例) 202(2) 91 と 65 の G.C.D を求める。

2 数の最大公約数は、

2 数を割り切る最大の基準量とみなす
(共通に測れる)整数 A, B に対して

A, B の公約数 d は
$A-B$ の公約数でもある。

↑[互除法の原理]

整数 A, B に対して、 A, B の最大公約数を $\text{GCD}(A, B)$ と書く。

互除法の原理

$$\text{GCD}(A, B) = \text{GCD}(B, A-B)$$

以下これを証明する。

 $P = [A \text{ と } B \text{ の公約数の集合}]$ $Q = [B \text{ と } A-B \text{ の公約数の集合}]$ とおいて、集合 P と Q が一致することを示す。(i) P の要素が Q に属すること $d \in P$ (d が P に属する)つまり $\begin{cases} A = da \cdots ① \\ B = db \cdots ② \end{cases} \begin{matrix} \swarrow \\ \searrow \end{matrix} \begin{matrix} d \text{ は } A, B \text{ の公約数} \\ (a, b \text{ は整数}) \end{matrix}$

①-②より

$$A - B = d(a - b) \cdots ③$$

整数

②, ③より d は $A-B$ と B の公約数である。 $\therefore d \in Q$ (d は Q に属する)(ii) Q の要素が P に属すること $d \in Q$ つまり $B = db \cdots ④$

$$A - B = dc \cdots ⑤ \quad (b, c \text{ は整数})$$

④, ⑤より

$$B + A - B = db + dc$$

$$\therefore A = d(b + c) \cdots ⑥$$

整数

④, ⑥より $d \in P$ (i), (ii) より、 P と Q は集合として一致する。 $P = Q$ より、 P, Q の最大の値も一致するので

$$\text{GCD}(A, B) = \text{GCD}(B, A-B) \cdots *$$

が言える。

次に $A \div B$ でわって余りを R とする。

$$\text{すなわち } A = BQ + R$$

商

$$\text{このとき、} \text{GCD}(A, B) = \text{GCD}(B, R)$$

理由 ④をくり返しを用いる。

$$\text{GCD}(A, B) = \text{GCD}(B, A-B)$$

$$= \text{GCD}(B, A-2B)$$

$$= \text{GCD}(B, A-QB) = \text{GCD}(B, R)$$

201

$$(2) \text{GCD}(1008, 1001) \\ = \text{GCD}(1001, 7) \\ \text{7} \times 143$$

$$= 7$$

$$(4) \text{GCD}(437, 299) = \text{GCD}(299, 138) = \text{GCD}(138, 23) = 23$$

$$\begin{array}{r} 299 \overline{) 437} \\ \underline{299} \\ 138 \end{array}$$

$$\begin{array}{r} 138 \overline{) 299} \\ \underline{276} \\ 23 \end{array}$$

$$\begin{array}{r} 23 \overline{) 138} \\ \underline{138} \\ 0 \end{array}$$

$\boxed{23} \times 6$
↑
求める
最大公約数

202

$$(2) \begin{array}{r} 65 \overline{) 91} \\ \underline{65} \\ 26 \end{array} \quad \begin{array}{r} 26 \overline{) 65} \\ \underline{52} \\ 13 \end{array} \quad \begin{array}{r} 13 \overline{) 26} \\ \underline{26} \\ 0 \end{array}$$

求める
GCD

$$\left(\begin{array}{l} \text{GCD}(91, 65) \\ = \text{GCD}(65, 26) \\ = \text{GCD}(26, 13) = 13 \end{array} \right)$$

$$(1) \begin{array}{r} 391 \overline{) 713} \\ \underline{391} \\ 322 \end{array} \quad \begin{array}{r} 322 \overline{) 391} \\ \underline{322} \\ 69 \end{array} \quad \begin{array}{r} 69 \overline{) 322} \\ \underline{276} \\ 46 \end{array} \quad \begin{array}{r} 46 \overline{) 69} \\ \underline{46} \\ 23 \end{array} \quad \begin{array}{r} 23 \overline{) 46} \\ \underline{46} \\ 0 \end{array}$$

よって、GCDは23

(3)

$$\begin{array}{r} 5891 \overline{) 9179} \\ \underline{5891} \\ 3288 \end{array} \quad \begin{array}{r} 3288 \overline{) 5891} \\ \underline{3288} \\ 2603 \end{array} \quad \begin{array}{r} 2603 \overline{) 3288} \\ \underline{2603} \\ 685 \end{array} \quad \begin{array}{r} 685 \overline{) 2603} \\ \underline{2055} \\ 548 \end{array}$$

$$\begin{array}{r} 548 \overline{) 685} \\ \underline{548} \\ 137 \end{array} \quad \begin{array}{r} 137 \overline{) 548} \\ \underline{548} \\ 0 \end{array}$$

よって、GCDは137

203

$$(1) \text{GCD}(n+1, n) = \text{GCD}(n, n+1-n) \\ = \text{GCD}(n, 1) \\ = 1$$

n と $n+1$ の最大公約数は1

$$(2) \text{GCD}(n+4, n) = \text{GCD}(n, n+4-n) \\ = \text{GCD}(n, 4)$$

n と 4 の最大公約数は 4 の正の約数。

ここで、 n を 4 で割った余りで考えると、

$$n = 4k \text{ のとき } \text{GCD}(n, 4) = 4$$

$$n = 4k+2 \text{ のとき } \text{GCD}(n, 4) = 2 \\ = 2(2k+1)$$

$$n = 4k+1, 4k+3 \text{ のとき } \text{GCD}(n, 4) = 1 \\ (k=0, 1, 2, \dots \text{は整数})$$

$$(3) n^2 + 4n + 12 \text{ を } n+1 \text{ で割ると、}$$

$$\begin{array}{r} n+3 \\ n+1 \overline{) n^2+4n+12} \\ \underline{n^2+n} \\ 3n+12 \end{array}$$

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

$$\begin{array}{r} 3n+12 \\ 3n+3 \\ \hline 9 \end{array}$$

3日目

$$\text{GCD}(n^2 + 4n + 12, n + 1)$$

$$= \text{GCD}((n+1)(n+3) + 9, n+1)$$

$$= \text{GCD}(n+1, 9)$$

$$n+1 = 9k \text{ とすると, GCD は } 9$$

$$n+1 = 3k \text{ とすると, GCD は } 3$$

以上より,

$$n = 9k - 1 \text{ のとき } 9$$

$$n = 3(3k+1) - 1 = 9k+2$$

$$= 3(3k+2) - 1 = 9k+5 \text{ のとき } 3$$

n が上記以外の場合, 1

110

AB : 2桁の数

CD : 2桁の数

$$AB \times CD = EFFF \text{ となった。}$$

($A \sim F$ は異なる $0 \sim 9$ の数)

$$AB \times CD = EFFF \dots \textcircled{1} \text{ は計算間違い}$$

$\textcircled{1}$ の右辺は特徴的

$\Rightarrow$ 何かの倍数とみられるか?

0を補って考えると良い

$$\text{例 } AB = A0 + B \rightarrow A \times 10 + B \text{ と書くのが正式}$$

$$EFFF = EE \times 100 + FF$$

$$EFFF = E0F0 + E0F$$

$$= E0F \times 10 + E0F$$

$$= (10+1) \times E0F$$

$$= 11 \times E0F$$

$$EFFF = 11 \times E0F \text{ と書けるので}$$

整数

$\textcircled{1}$ の右辺は11の倍数である。

一方、左辺は

AB, CD 共に一の位と十の位の数が異なるため

11の倍数でないので

積 $AB \times CD$ も11の倍数でない。

$\textcircled{1}$ の両方は整数なので

一方が11の倍数で他方が11の倍数でないことはありえない。

(素因数分解の一意性に反する)

したがって、この計算は間違いである。

205

<用語の解説>

「互いに素」

整数 a, b に対して、① a, b が2以上の公約数を持たないとき「互いに素」という。「 a, b が互いに素」の別の表現② a と b の最大公約数が1 ($\text{GCD}(a, b) = 1$)③ a と b が素数の公約数をもたない。

(1) $\begin{cases} 35 = 5 \times 7 \\ 63 = 9 \times 7 \end{cases} \rightarrow 2 \text{以上の公約数「7」をもつ。}$
 $\Rightarrow$ 互いに素でない。

(2) $\begin{cases} 64 = 8^2 = (2^3)^2 = 2^6 \\ 27 = 9 \times 3 = 3^3 \end{cases} \rightarrow \text{素数の公約数をもたない。}$
 $\Rightarrow$ 「互いに素」

(3) $\begin{cases} 1 \\ 20 \end{cases} \rightarrow \text{GCD} = 1 \text{ より、「互いに素」}$

(4) n を自然数とする n と $n+2$ は? $\Rightarrow$ GCDを計算する

$$\text{GCD}(n+2, n) = \text{GCD}(n, 2)$$

$\uparrow$
 $n+2-n$

 n が偶数のとき、 $\text{GCD} = 2$ より「互いに素でない」 n が奇数のとき、 $\text{GCD} = 1$ より「互いに素」

(注) となり合う2つの自然数は「互いに素」

206

[方程式の整数解] 基本形

⑧ $8x + 11y = 1$... ① の整数解 (x, y) を全て求めたい。
係数が互いに素であるのも基本形

(方針)

[1] まず、①を満たす整数解を

(何でも良いから) 1組みつける。

この解を「特殊解」と呼ぶ。

[2] 「特殊解」を用いて、全ての解を求める。

「一般解」と呼ぶ。

$$8x + 11y = 1 \quad \dots \text{①}$$

(1) $\begin{matrix} 8x \text{ (8の倍数)} & 8, 16, 24, \boxed{32}, 40, 48, 56, \dots \\ 11y \text{ (11の倍数)} & 11, 22, \boxed{33}, 44, 55, 66, \dots \end{matrix} \left\{ \begin{array}{l} \text{これらの差を} \\ \text{考える} \end{array} \right.$

$$8 \times (-4) + 11 \times 3 = 1 \quad \dots \text{②}$$

$$(x, y) = (-4, 3)$$

がみつかる (採用)

(2) ~ (4) まとめて

[1] $\rightarrow$ [2] へのステップ $(x, y) = (-4, 3)$ より ②式が成り立つ。

$$8x + 11y = 1 \quad \dots \text{①}$$

$$\rightarrow 8(-4) + 11 \times 3 = 1 \quad \dots \text{②}$$

$$8(x+4) + 11(y-3) = 0$$

$$\text{移項して、} \underbrace{8(x+4)}_{\text{整数}} = - \underbrace{11(y-3)}_{\text{整数}} \quad \dots \text{③} \quad (\text{両辺は整数})$$

③の左辺は8の倍数、右辺は11の倍数なので

③の各辺は8の倍数かつ11の倍数なので、 $8 \times 11k$ の倍数

$$\therefore 8(x+4) = -11(y-3) = 8 \times 11k \quad \dots \text{④} \quad (k \text{ は整数})$$

$$\textcircled{4} \text{より} \begin{cases} 8(x+4) = 8 \times 11k & \dots \textcircled{5} \\ -11(y-3) = 8 \times 11k & \dots \textcircled{6} \end{cases}$$

$$\textcircled{5} \text{より} \begin{aligned} x+4 &= 11k \\ \therefore x &= 11k-4 \end{aligned}$$

$$\textcircled{6} \text{より} \begin{aligned} -(y-3) &= 8k \\ y-3 &= -8k \\ \therefore y &= -8k+3 \end{aligned}$$

$$\text{以上より} \begin{cases} x = 11k-4 \\ y = -8k+3 \end{cases} \quad (k \text{ は整数})$$

← 特殊解が残る

$$\textcircled{注} k=0 \text{ のとき} (x, y) = (-4, 3)$$

$$k=1 \text{ のとき} (x, y) = (11-4, -8+3) \\ = (7, -5)$$

207

$$(1) 3x-10y=1 \quad \dots \textcircled{1}$$

特殊解として $(x, y) = (7, 2)$ を用いる

$$3x-10y=1 \quad \dots \textcircled{1}$$

$$\rightarrow 3 \times 7 - 10 \times 2 = 1 \quad \dots \textcircled{2}$$

$$3(x-7) - 10(y-2) = 0$$

$$\therefore 3(x-7) = 10(y-2) \quad \dots \textcircled{3}$$

3と10は互いに素なので、③の各辺は30の倍数

$$\therefore \begin{cases} 3(x-7) = 3 \times 10k \\ 10(y-2) = 3 \times 10k \end{cases} \quad (k \text{ は整数})$$

$$\begin{cases} x-7 = 10k \\ y-2 = 3k \end{cases}$$

$$\therefore \begin{cases} x = 10k+7 \\ y = 3k+2 \end{cases} \quad (k \text{ は整数})$$

$$(2) 2x+5y=3 \quad \dots \textcircled{1}$$

特殊解として $(x, y) = (4, -1)$ を用いる。

$$2 \times 4 + 5 \times (-1) = 3 \quad \dots \textcircled{2}$$

$$\textcircled{1} - \textcircled{2} \text{より}$$

$$2(x-4) + 5(y+1) = 0$$

$$\therefore 2(x-4) = -5(y+1) \quad \dots \textcircled{3}$$

2と5は互いに素なので、③の各辺は10の倍数

$$\begin{cases} 2(x-4) = 10k \\ -5(y+1) = 10k \end{cases} \quad (k \text{ は整数})$$

$$\begin{cases} x-4 = 5k \\ y+1 = -2k \end{cases}$$

$$\therefore \begin{cases} x = 5k+4 \\ y = -2k-1 \end{cases} \quad (k \text{ は整数})$$

$$(3) 6x+15y=1$$

$$3(x+5y)=1 \quad \dots \textcircled{*}$$

整数

整数解 (x, y) が存在すると、

④の左辺は3の倍数だが右辺はそうではない

これは矛盾なので、整数解は存在しない。

208

[特殊解を求めにくい場合]

⇒ より簡単な方程式に帰着させる方法

(互除法を用いて特殊解を求める)

$$81x + 35y = 1 \quad \dots ①$$

(1) $81 = 35 \times 2 + 11$ に注目。(①に代入して)

$$① \Leftrightarrow (35 \times 2 + 11)x + 35y = 1$$

$$\Leftrightarrow 35(\underbrace{2x+y}_Y) + 11\underbrace{x}_X = 1$$

$$\text{ここで、} \begin{cases} 2x+y=Y & \dots ② \\ x=X & \dots ③ \end{cases}$$

とみると、
 $①' \Leftrightarrow 35Y + 11X = 1 \quad \dots ④$ と表せる。

$$35 = 11 \times 3 + 2$$

を④に代入して、

$$(11 \times 3 + 2)Y + 11X = 1$$

$$\Leftrightarrow 11(3Y+X) + 2Y = 1$$

Zとみると

$$11Z + 2Y = 1 \quad \dots ⑤$$

$$Z = 3Y + X \quad \dots ⑥$$

⑤の整数解として、

$$(Y, Z) = (-5, 1) \text{ を得る。}$$

(あとは⑥③②を用いて x, y の整数解が求まる)

$$⑥より、1 = 3(-5) + X$$

$$\therefore X = 16 = x$$

$$②より、2 \times 16 + y = -5$$

$$\therefore y = -37$$

よって、①の特殊解 $(x, y) = (16, -37)$ がみつける。これを用いて、(例えば) $\begin{cases} x = 35k + 16 \\ y = -81k - 37 \end{cases}$

が求まる。(kは整数)

[特殊解の別の求め方]

$$81x + 35y = 1 \quad \dots ①$$

81と35に互除法を行う。

$$\begin{array}{r} 2 \qquad 3 \qquad 5 \\ 35 \overline{) 81} \quad 11 \overline{) 35} \quad 2 \overline{) 11} \\ \underline{70} \quad \underline{33} \quad \underline{10} \\ 11 \quad 2 \quad 1 \end{array} \quad \text{⑦} \leftarrow 81 \text{ と } 35 \text{ の GCD}$$

これをかけ算の形で書くと、

$$81 = 35 \times 2 + 11 \quad \Leftrightarrow \quad 11 = 81 - 35 \times 2 \quad \dots ③$$

$$35 = 11 \times 3 + 2 \quad \Leftrightarrow \quad 2 = 35 - 11 \times 3 \quad \dots ②$$

$$11 = 2 \times 5 + 1 \quad \Leftrightarrow \quad 1 = 11 - 2 \times 5 \quad \dots ①$$

↓を用いて、
 $1 = 81 \times () + 35 \times ()$
 の式が作れる。

$$= 11 - (35 - 11 \times 3) \times 5 \quad (② \text{ を } ① \text{ に代入})$$

$$= 11 - 35 \times 5 + 11 \times 15$$

$$= 11 \times 16 - 35 \times 5 \quad (③ \text{ を代入})$$

$$= (81 - 35 \times 2) \times 16 - 35 \times 5$$

$$= 81 \times 16 - 35 \times 32 - 35 \times 5$$

$$= 81 \times 16 - 35 \times 37$$

$$= 81 \times 16 + 35 \times (-37)$$

1 = $81 \times 16 + 35 \times (-37)$ が得られたので、特殊解 $(16, -37)$ が求まった。

§3. 合同式とその計算

定義

a, b を整数, m を自然数とする.

$$a \equiv b \pmod{m} \iff a-b \text{ が } m \text{ の倍数}$$

(a 合同 b モド m)

例 mod 3 で考える

$$26 \equiv \square \pmod{3}$$

$$\iff 26 - \square = 3 \text{ の倍数}$$

$$\iff 26 - \square = 3k \quad (k \text{ は整数})$$

$$26 \pm 3k = \square$$

↑ 26 に 3 で足りたにリ引いたにリ
 じはものたにリは合同

$$\begin{array}{l} \text{(3k+27) 上第73} \\ \text{(3k+1)} \end{array} \quad \begin{array}{l} +3 \\ -3 \end{array} \quad \begin{array}{l} 29 \equiv 26 \equiv 23 \equiv 20 \equiv 17 \equiv 14 \equiv 11 \equiv 8 \equiv 5 \equiv \textcircled{2} \equiv -1 \\ 28 \equiv 25 \equiv 22 \equiv 19 \equiv 16 \equiv 13 \equiv 10 \equiv 7 \equiv 4 \equiv \textcircled{1} \equiv -2 \\ \text{(3k)} \quad 27 \equiv 24 \equiv 21 \equiv 18 \equiv 15 \equiv 12 \equiv 9 \equiv 6 \equiv 3 \equiv \textcircled{0} \equiv -3 \end{array}$$

このように、合同なものたにリは7"ル-7°を作る。

上から「3で割って2余る」「3で割って1余る」「3の倍数、

この例からわかるように、

a を m で割った余りが r のとき、

すなわち $a = m \cdot q + r$ のとき

$$a = r \pmod{m} \quad \text{商}$$

(a は、a を m で割った余りと合同)

301

$$(1) 7 \equiv 4 \pmod{3}$$

$$\iff 7 - 4 = 3 \text{ の倍数}$$

正しい

$$(2) 8 \equiv 3 \pmod{3}$$

$$8 - 3 = 5$$

正しいではない

$$(3) 14 \equiv 23 \pmod{3}$$

$$23 - 14 = 9$$

正しい

$$(4) 8 \equiv -11 \pmod{3}$$

$$8 - (-11) = 19$$

正しいではない

$$(5) 35 \equiv 35 \pmod{3}$$

$$35 - 35 = 0 \leftarrow 3 \text{ の倍数}$$

正しい

302

$$(1) 5 \equiv 2 \pmod{3}$$

$$(2) 25 \equiv 1 \pmod{3}$$

$$(3) -4 \equiv 2 \pmod{3}$$

$$\begin{array}{l} 4 \\ -6+2 \end{array}$$

303, 304

例えば、mod 3 であれば、

整数を $3k, 3k+1, 3k+2$ (k は整数)

の7"ル-7°に分けられる。

これらの7"ル-7°に対し、足したにリかけたにリした結果は、

また同じ7"ル-7°に決まる。

$$\text{例: } (3k+1) + (3l+2) = 3(k+l) + 3$$

整数

$$(3k+1)(3l+2) = 9kl + 6k + 3l + 2$$

3の倍数

3で割って
2余る

これらのことが、合同式に"とちょっと単純化できる。

304

[仮定]

$$\begin{cases} a \equiv b \pmod{m} & \dots (1) \\ p \equiv q \pmod{m} & \dots (2) \end{cases}$$

$$(1) \ a + p \equiv b + q \pmod{m} \quad \dots (A)$$

$$(2) \ a - p \equiv b - q \pmod{m} \quad \dots (B)$$

$$(3) \ ap \equiv bq \pmod{m} \quad \dots (C)$$

①より

$$a - b = mk \quad (k \text{ は整数}) \quad \dots (1')$$

②より

$$p - q = ml \quad (l \text{ は整数}) \quad \dots (2')$$

[(1) の証明]

$$(A) \Leftrightarrow (a+p) - (b+q) = m \text{ の倍数} \quad \dots (A')$$

より (A') を示す

$$\begin{aligned} (a+p) - (b+q) &= a - b + p - q \\ &= mk + ml \quad (1', 2' \text{ より}) \\ &= m(k+l) \\ &\quad \text{整数} \end{aligned}$$

(A') が示せた。

(B') もほぼ同様 (= できる) (略)

[(3) の証明]

 $a-b$ or $p-q$

が整数

$$(C) \Leftrightarrow ap - bq = m \text{ の倍数} \quad \dots (C')$$

③ を示せば良い

$$\begin{aligned} ap - bq &= ap - aq + aq - bq \\ &= a(p-q) + (a-b)q \\ &= aml + mkq \quad (1', 2' \text{ より}) \\ &= m(al+kq) \\ &\quad \text{整数} \end{aligned}$$

よって (C') が示せた。

4日目

304

[仮定]

$$\begin{cases} a \equiv b \pmod{m} & \dots (1) \\ p \equiv q \pmod{m} & \dots (2) \end{cases}$$

$$\begin{cases} a \equiv b \pmod{m} & \dots (1) \\ p \equiv q \pmod{m} & \dots (2) \end{cases}$$

$$(1) a + p \equiv b + q \pmod{m} \dots (A)$$

$$(2) a - p \equiv b - q \pmod{m} \dots (B)$$

$$(3) ap \equiv bq \pmod{m} \dots (C)$$

①より

$$a - b = mk \quad (k \text{ は整数}) \dots (1')$$

②より

$$p - q = ml \quad (l \text{ は整数}) \dots (2')$$

[(1)の証明]

$$(A) \Leftrightarrow (a+p) - (b+q) = m \text{ の倍数} \dots (A')$$

より(A')を示す

$$\begin{aligned} (a+p) - (b+q) &= a - b + p - q \\ &= mk + ml \quad (1', 2' \text{ より}) \\ &= m(k+l) \\ &\quad \text{整数} \end{aligned}$$

(A')が示された。

(B')もほぼ同様にできる (略)

[(3)の証明]

$$(C) \Leftrightarrow ap - bq = m \text{ の倍数} \dots (C')$$

(C')を示せば良い。

$$\begin{aligned} ap - bq &= ap - aq + aq - bq \\ &= a(p-q) + (a-b)q \\ &= aml + mkq \quad (1', 2' \text{ より}) \\ &= m(al+kq) \\ &\quad \text{整数} \end{aligned}$$

よって(C')が示された。

定理

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

$$p \equiv q \pmod{m} \quad \text{のとき}$$

$$(1) a + p \equiv b + q \pmod{m}$$

$$(2) a - p \equiv b - q \pmod{m}$$

$$(3) ap \equiv bq \pmod{m}$$

$$(4) a^n \equiv b^n \pmod{m} \quad (n \text{ は整数})$$

使い方

303

ここでは mod 7 で考える。

以下では、ある計算結果について、

7 で割った余りを考える。

その際、「7 ルー7」が同じものであれば、

「計算結果を7で割った余りは一致する」ということ。

より「小さい」値で
計算した方が楽ということ。

$$(1) 37 \equiv \boxed{2} \pmod{7}$$

35+2

$$(2) 61 \equiv \boxed{5} \pmod{7}$$

56+5

$$(3) 37 + 61 \equiv \boxed{} \pmod{7}$$

定理(1)を使うと

実際の計算は

$$37 \equiv 2 \pmod{7}$$

$$+ \quad 61 \equiv 5 \pmod{7}$$

$$37 + 61 \equiv 2 + 5 \pmod{7}$$

$$\equiv 7 \pmod{7}$$

$$\equiv 0 \pmod{7}$$

$$37 + 61 \equiv 2 + 5 \pmod{7}$$

$$\equiv 7 \pmod{7}$$

$$\equiv 0 \pmod{7}$$

以下 mod 7 で計算する.

$$(4) 37 - 61 \equiv 2 - 5$$

$$\equiv -3$$

$$\equiv -3 + 7 \equiv \boxed{4}$$

$$-3 \equiv -3$$

$$+1) 0 \equiv 7$$

$$-3 \equiv -3 + 7$$

$$(5) 37 \times 61 \equiv \boxed{} \pmod{7}$$

$$37 \equiv 2$$

$$\times) 61 \equiv 5$$

$$37 \times 61 \equiv 2 \times 5$$

つまり、

$$37 \times 61 \equiv 2 \times 5$$

$$\equiv 10$$

$$\equiv \boxed{3}$$

$$(6) 37^2 \equiv \boxed{} \pmod{7}$$

$$37 \equiv 2$$

$$\times) 37 \equiv 2$$

$$37^2 \equiv 2^2$$

$$\equiv \boxed{4}$$

同様の考え方で、

定理 (4)

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

$$\Rightarrow a^n \equiv b^n \pmod{m}$$

が証明できる。

補充問題

空らんには 0, 1, 2, 3, 4, 5, 6 をうめよ。

$$(1) 82 \equiv \boxed{} \pmod{7}$$

$$(2) 67 \equiv \boxed{} \pmod{7}$$

$$(3) 82 + 67 \equiv \boxed{} \pmod{7}$$

$$(4) 82 \times 67 \equiv \boxed{} \pmod{7}$$

$$(5) 82 \times 8 + 67 \times 11 \equiv \boxed{} \pmod{7}$$

$$(6) 82 \times 53 - 67 \times 37 \equiv \boxed{} \pmod{7}$$

$$(7) 82^2 \equiv \boxed{} \pmod{7}$$

$$(8) 67^3 \equiv \boxed{} \pmod{7}$$

$$(9) 62^{100} \equiv \boxed{} \pmod{7}$$

$$(10) 68^{99} + 86^{99} \equiv \boxed{} \pmod{7}$$

解答

$$(1) 82 \equiv 5 \pmod{7}$$

$$(2) 67 \equiv 4 \pmod{7}$$

$$(3) 82 + 67 \equiv 5 + 4 \\ \equiv 9 \\ \equiv 2 \pmod{7}$$

$$(4) 82 \times 67 \equiv 5 \times 4 \\ \equiv 20 \\ \equiv 6 \pmod{7}$$

$$(5) 82 \times 8 + 67 \times 11 \equiv 5 \times 1 + 4 \times 4 \\ \equiv 5 + 16 \\ \equiv 21 \\ \equiv 0 \pmod{7}$$

$$\begin{aligned}
 (6) 82 \times 53 - 67 \times 37 &\equiv 5 \times 4 - 4 \times 2 \\
 &\equiv 20 - 8 \\
 &\equiv 12 \\
 &\equiv 5 \pmod{7}
 \end{aligned}$$

$$\begin{aligned}
 (7) 82^2 &\equiv 5^2 \\
 &\equiv 25 \\
 &\equiv 4 \pmod{7}
 \end{aligned}$$

$$\begin{aligned}
 (8) 67^3 &\equiv 4^3 \\
 &\equiv 16 \times 4 \\
 &\equiv 2 \times 4 \\
 &\equiv 8 \\
 &\equiv 1 \pmod{7}
 \end{aligned}$$

$$\begin{aligned}
 (9) 62^{100} &\equiv (-1)^{100} \\
 &\equiv 1
 \end{aligned}$$

$$\begin{aligned}
 (10) 68^{99} + 86^{99} &\equiv (-2)^{99} + 2^{99} \\
 &\equiv 0
 \end{aligned}$$

305

(1) 679 の自然数 N を

$$N = a \times 10^5 + b \times 10^4 + c \times 10^3 + d \times 10^2 + e \times 10^1 + f$$

と書く。以下を示す。

$$(i) N \equiv a + b + c + d + e + f \pmod{9}$$

$$(ii) N \equiv -a + b - c + d - e + f \pmod{11}$$

解答

(1) (i) 以下 $\text{mod } 9$ で考える。

$$N \equiv 10^5 a + 10^4 b + 10^3 c + 10^2 d + 10 e + f$$

$$\text{mod } 9 \text{ において, } 10^n \equiv 1^n \equiv 1 \quad (n \text{ は自然数})$$

$$\text{よって } N \equiv a + b + c + d + e + f$$

(ii) 以下 $\text{mod } 11$ で考える。

$$10^n \equiv (-1)^n \equiv \begin{cases} -1 & (n \text{ は奇数}) \\ 1 & (n \text{ は偶数}) \end{cases}$$

よって,

$$N \equiv -a + b - c + d - e + f$$

(2) 345678 を 9 で割り、 r は、 $(\text{mod } 9 \text{ で考えて})$

$$3+4+5+6+7+8 \equiv 7+8$$

$$\equiv 6$$

11 で割り、 r は、 $(\text{mod } 11 \text{ で考えて})$

$$-3+4-5+6-7+8 \equiv 1+1+1$$

$$\equiv 3$$

306

[累乗数を割った余り]

 2^{100} を 7 で割った余り

求める余りは 0~6 の 7 通り (0 はないから)

 $\Rightarrow 2^1, 2^2, 2^3, \dots$ と計算すると、どこかで 7 で割った余りは一致するだろう

以下 mod 7 で計算する

$$2^1 \equiv 2$$

$$2^2 \equiv 4$$

$$2^3 \equiv 8 \equiv 1$$

$$2^4 \equiv 8 \times 2 \equiv 1 \times 2 \equiv 2$$

となり、 2^n (n は自然数) を 7 で割った余りは

2, 4, 1 をくり返すことがわかる。

(長さ 3 の周期で循環する)

以下結論を計算で書くと

$$2^{100} \equiv 2^{3 \times 33 + 1} \equiv (2^3)^{33} \times 2$$

$$2^{100} \equiv (2^3)^{33} \times 2^1$$

$$\equiv 1^{33} \times 2$$

$$\equiv 2$$

307

(1) 2^{99} を 3 で割った余り

$$2^{99} \equiv (-1)^{99} \pmod{3}$$

$$\equiv -1 \pmod{3}$$

$$\equiv 2 \pmod{3}$$

フェルマの小定理

 p : 素数で a と p が互いに素のとき

$$a^{p-1} \equiv 1 \pmod{p}$$

(2) 3^{100} を 7 で割った余り

以下 mod 7 で考える。

まず 3^n のくり返しを見つける

$$3^1 \equiv 3$$

$$3^2 \equiv 9 \equiv 2$$

$$3^3 \equiv 9 \times 3 \equiv 2 \times 3 \equiv 6$$

$$3^4 \equiv 3^3 \times 3 \equiv 6 \times 3 \equiv 18 \equiv 4$$

$$3^5 \equiv 3^4 \times 3 \equiv 4 \times 3 \equiv 12 \equiv 5$$

$$3^6 \equiv 3^5 \times 3 \equiv 5 \times 3 \equiv 15 \equiv 1$$

よって、 3^n は長さ 6 の周期で循環する。

(3, 2, 6, 4, 5, 1, 3...)

よって

$$3^{100} \equiv 3^{6 \times 16 + 4}$$

$$\equiv (3^6)^{16} \times 3^4$$

$$\equiv 1^{16} \times 3^4$$

$$\equiv 4$$

(3) 2^{998} を 11 で割った余り

以下 mod 11 で考える

$$2^1 \equiv 2$$

$$2^2 \equiv 4$$

$$2^3 \equiv 8$$

$$2^4 \equiv 8 \times 2 \equiv 16 \equiv 5$$

$$2^5 \equiv 5 \times 2 \equiv 10$$

$$2^6 \equiv 10 \times 2 \equiv 20 \equiv 9$$

$$2^7 \equiv 9 \times 2 \equiv 18 \equiv 7$$

$$2^8 \equiv 7 \times 2 \equiv 14 \equiv 3$$

$$2^9 \equiv 3 \times 2 \equiv 6$$

$$2^{10} \equiv 6 \times 2 \equiv 12 \equiv 1$$

よって、余りは長さ10の周期で循環する。

$$(1978 = 197 \times 10 + 8)$$

$$\begin{aligned} 2^{1978} &\equiv 2^{10 \times 197 + 8} \\ &\equiv (2^{10})^{197} \times 2^8 \\ &\equiv 1^{197} \times 2^8 \\ &\equiv 3 \end{aligned}$$

(4) 19^{159} を17で割った余り

以下 mod 17 で考える ($\Rightarrow 19 \equiv 2$ とできる)

$$2^1 \equiv 2$$

$$2^2 \equiv 4$$

$$2^3 \equiv 8$$

$$2^4 \equiv 16$$

$$2^5 \equiv 16 \times 2 \equiv 32 \equiv 15$$

$$2^6 \equiv 15 \times 2 \equiv 30 \equiv 13$$

$$2^7 \equiv 13 \times 2 \equiv 26 \equiv 9$$

$$2^8 \equiv 9 \times 2 \equiv 18 \equiv 1$$

よって、長さ8の周期で循環する。

$$\begin{aligned} 19^{159} &\equiv 2^{159} \\ &\equiv 2^{19 \times 8 + 7} \\ &\equiv (2^8)^{19} \times 2^7 \\ &\equiv 1 \times 2^7 \\ &\equiv 9 \end{aligned}$$

308

(1) 2^{369} を11で割った余り

$$A = 2^{369} = 2^{10 \times 36 + 9} \rightarrow a \text{ とおく}$$

まず、mod 11 で考える

$$2^1 \equiv 2$$

$$2^2 \equiv 4$$

$$2^3 \equiv 8$$

$$2^4 \equiv 5$$

$$2^5 \equiv 10$$

$$2^6 \equiv 9$$

$$2^7 \equiv 7$$

$$2^8 \equiv 3$$

$$2^9 \equiv 6$$

$$2^{10} \equiv 1$$

長さ10の周期で循環する

よって、 2^a を11で割った余りは
指数 a の mod 10 の値で決定される
(a の下4桁の値がわかれば良い)

以下、mod 10 で考える

$$a = 34^{569} \equiv 4^{569}$$

$4^1, 4^2, 4^3, 4^4, \dots$ を10で割った余りを考えると

$$4^1 \equiv 4, 4^2 \equiv 6, 4^3 \equiv 4, 4^4 \equiv 6$$

(指数の偶奇で値が決まる)

つまり、 $\begin{cases} 4 \text{ の奇数乗} \equiv 4 \\ 4 \text{ の偶数乗} \equiv 6 \end{cases}$ であり、

$$a \equiv 4^{569} \equiv 4$$

よって $a = 10k + 4$ (k は整数) と書ける。

再び mod 11 で計算して

$$\begin{aligned} A &= 2^{34^{569}} \equiv 2^{10k+4} \\ &\equiv (2^{10})^k \times 2^4 \\ &\equiv 1 \times 2^4 \equiv 5 \end{aligned}$$

[合同方程式]

$$4x \equiv 3 \pmod{5} \text{ を解け.}$$

簡単な解法

表をかく.

x	0	1	2	3	4
$4x$	0	4	3	2	1

表より、 $x \equiv 2 \pmod{5}$

答えが1つにならない例

$$4x \equiv 2 \pmod{6}$$

x	0	1	2	3	4	5
$4x$	0	4	2	0	4	2

表より、 $x \equiv 2, 5 \pmod{6}$

例 $4x \equiv 1 \pmod{6}$ は解なし

代数的に解くとどうなるか?

$$4x \equiv 3 \pmod{5}$$

係数4に割りたい.

実は、 $4x \equiv 4 \times \text{整数}$ の形にすると、

実質的に「割り算」が可能

解答

以下 $\pmod{5}$ で計算する.

$$4x \equiv 3$$

← 5に割りたいので、
4を5に割って、
4×整数の形を作る

$$4x \equiv 3 + 5$$

$$\therefore 4x \equiv 8$$

5の倍数

$$\Leftrightarrow 4x - 8 = 5k \quad (k \text{ は整数})$$

$$\Leftrightarrow 4(x - 2) = 5k \quad \leftarrow \text{整数}$$

4と5は互いに素なので、 $x - 2$ は5で割り切れる

つまり、 $x - 2 = 5$ の倍数

$$\Leftrightarrow x \equiv 2 \pmod{5}$$

5日目

[合同方程式]

$$4x \equiv 3 \pmod{5} \text{ を解け.}$$

簡単な解法

表をかく。

x	0	1	2	3	4
$4x$	0	4	3	2	1

表より、 $x \equiv 2 \pmod{5}$

答えが1つにならない例

$$4x \equiv 2 \pmod{6}$$

x	0	1	2	3	4	5
$4x$	0	4	2	0	4	2

表より、 $x \equiv 2, 5 \pmod{6}$ 例 $4x \equiv 1 \pmod{6}$ は解なし。

代数的に解くとどうなるか?

$$4x \equiv 3 \pmod{5}$$

係数4を割りに1。

実は、 $4x \equiv 4 \times \text{整数}$ の形にすると、

実質的に割計算が可能

解答

以下 $\text{mod } 5$ で計算する。

$$4x \equiv 3$$

5を足して割り引いたりして
4×整数の形を作る

$$4x \equiv 3 + 5$$

$$\therefore 4x \equiv 8$$

5の倍数

$$\Leftrightarrow 4x - 8 = 5k \quad (k \text{ は整数})$$

$$\Leftrightarrow 4(x - 2) = 5k \quad \leftarrow \text{整数}$$

4と5は互いに素なので、 $x-2$ は5で割り切れるつまり、 $x-2 = 5$ の倍数

$$\Leftrightarrow x \equiv 2 \pmod{5}$$

309

右辺を3の倍数にする

$$(1) \quad 3x \equiv 1 \pmod{5}$$

$$3x \equiv 1 + 5 \pmod{5}$$

+0を足す

$$3x \equiv 6 \pmod{5}$$

$$\Leftrightarrow 3x - 6 = 5k \quad (k: \text{整数})$$

$$\Leftrightarrow 3(x - 2) = 5k$$

$$\Leftrightarrow x - 2 = (5 \text{ の倍数}) \quad (3 \text{ と } 5 \text{ は互いに素だから})$$

$$\Leftrightarrow x \equiv 2 \pmod{5}$$

2の倍数にする

$$(2) \quad 2x \equiv 4 \pmod{8}$$

$$\Leftrightarrow 2(x - 2) = 8k \quad (k: \text{整数})$$

等式なので割って良い

$$\Leftrightarrow x - 2 = 4k$$

(4の倍数)

$$\Leftrightarrow x \equiv 2 \pmod{4} \quad \dots \textcircled{1}$$

<補足>

表を描くと

x	0	1	2	3	4	5	6	7
$2x$	0	2	4	6	0	2	4	6

上図より、 $x \equiv 2, 5 \pmod{8}$

(①と同じこと)

$$0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \quad \leftarrow \text{mod } 8 \text{ で}$$

$$0 \ 1 \ 2 \ 3 \ 0 \ 1 \ 2 \ 3 \quad \leftarrow \text{mod } 4 \text{ で}$$

mod 4 で $x = 2$ はmod 8 で $x = 2, 6$ と同じこと

3/0

7で割ると6余り、11で割ると3余る整数 N を全て求めよ。

例: 2で割った余りと3で割った余りを考える。

n	0	1	2	3	4	5	6	7	8	9	10	11	12	...
2で割った余り	0	1	0	1	0	1	0	1	0	1	0	1	0	...
3で割った余り	0	1	2	0	1	2	0	1	2	0	1	2	0	...

余りの組は、

長さ6の周期で循環

一般に、0以上の整数を自然数 p, q で割った余りは

p, q の最小公倍数の長さの周期を繰り返す。

本問では、7, 11は互いに素なので、

割った余りの組は 7×11 の長さの周期で繰り返す。

ここでは、合同方程式を解いて求める。

解答

$$N = 7x + 6 = 11y + 3 \dots \textcircled{1} \quad (x, y \text{ は整数})$$

とおける。

①を $\text{mod } 7$ か $\text{mod } 11$ で解く

x の係数 y の係数

以下 $\text{mod } 7$ で計算する。

$$\textcircled{1} \text{ は } 7x + 6 \equiv 11y + 3$$

$$\begin{aligned} \text{より、} \quad 6 &\equiv 4y + 3 \\ 6 - 3 &\equiv 4y \end{aligned} \quad \begin{array}{l} \text{合同式は} \\ \text{移項できる} \end{array}$$

$$\therefore 4y \equiv 3 \quad \leftarrow 4 \text{ の倍数にする (+7して)} \equiv$$

$$4y \equiv 3 + 7 + 7 + 7$$

$\underbrace{\hspace{1.5cm}}_{10}$
 $\underbrace{\hspace{1.5cm}}_{17}$
 $\underbrace{\hspace{1.5cm}}_{24}$

$$\therefore 4y \equiv 24$$

$$\therefore 4y \equiv 24$$

$$\Leftrightarrow 4(y-6) = 7k \quad (k: \text{整数})$$

↑
7の倍数

4と7は互いに素なので

$$y-6 = 7 \text{ の倍数}$$

$$\Leftrightarrow y \equiv 6 \pmod{7}$$

$$\text{つまり } y = 7l + 6 \quad (l: \text{整数})$$

①に代入して

$$N = 11(7l + 6) + 3$$

$$= 77l + 69 \quad (l: \text{整数})$$

§4. 合同式を用いた論証

401

(1) 以下 $\text{mod } 13$ で計算する.

$$\begin{aligned}
 & 4^{2n+1} + 3^{n+2} \\
 &= 4^{2n} \times 4 + 3^n \times 3^2 \\
 &= (4^2)^n \times 4 + 3^n \times 9 \\
 &= 4 \times 16^n + 9 \times 3^n & (6 \equiv 3 \pmod{13}) \\
 &= 4 \times 3^n + 9 \times 3^n & \text{よって } 16^n \equiv 3^n \pmod{13} \\
 &= 13 \times 3^n \\
 &\equiv 0
 \end{aligned}$$

(2) 以下 $\text{mod } 3$ で考える.すると、 $n \equiv 0, 1, 2$

$\begin{array}{ccc} \nearrow & \uparrow & \nwarrow \\ \text{3の倍数全て} & \text{3で割って} & \text{3で割って} \\ \text{表している} & \text{1余る数} & \text{2余る数} \\ \text{考えられる} & \text{表す} & \text{表す} \\ (3k) & (3k+1) & (3k+2) \quad (k: \text{整数}) \end{array}$

このとき、 $n^3 + 2n$ を計算すると

n	0	1	2
n^2	0	1	1
n^3	0	1	2
$2n$	0	2	1
$n^3 + 2n$	0	0	0

$(\text{mod } 3)$

よって、どの場合も $n^3 + 2n = 0$

<補足>

 $n = 0, 1, 2 \pmod{3}$ のときの $n^3 + 2n$ の値を計算すれば良い。(3) 以下 $\text{mod } 7$ で考える. n は 7 の倍数でないので

$$n \equiv \pm 1, \pm 2, \pm 3$$

について $n^6 - 1$ を計算すれば良い。(4 $\equiv$ -3, 5 $\equiv$ -2, 6 $\equiv$ -1 とすると計算が楽)

方法1

n	± 1	± 2	± 3
n^2	1	4	2
n^6	1	1	1
$n^6 - 1$	0	0	0

上表より、 $n^6 - 1 \equiv 0$

方法2 (計算を書くと)

以下 $\text{mod } 7$ で計算する. $n \equiv \pm 1$ のとき

$$n^6 - 1 \equiv (\pm 1)^6 - 1 \equiv 1 - 1 \equiv 0$$

 $n \equiv \pm 2$ のとき

$$n^6 - 1 \equiv (\pm 2)^6 - 1 \equiv 4^3 - 1 \equiv 0$$

 $n \equiv \pm 3$ のとき

$$\begin{aligned}
 n^6 - 1 &\equiv (\pm 3)^6 - 1 \equiv 9^3 - 1 \\
 &\equiv 2^3 - 1 \equiv 0
 \end{aligned}$$

403

[ピタゴラス数]

 $a^2 + b^2 = c^2 \dots ①$ を満たす (a, b, c) の組を

ピタゴラス数といい、

(3, 4, 5)

(5, 12, 13)

(8, 15, 17)

...

など無限にある

①を満たす整数 a, b, c において a, b の少なくとも一方は 3 の倍数であることを証明する。

背理法で考える

「そうでないとすると矛盾が起こる」ことを示して、

題意が正しいことの主張とする方法

「 a, b の少なくとも一方が 3 の倍数」を否定すると、

(1つ以上が)

「1つも 3 の倍数でない」つまり

「 a, b が両方とも 3 の倍数でない」

と仮定して (①を通して) 矛盾を導く。

以下 mod 3 で考える

一般に、自然数 n の平方数は

n	0	1, 2
n^2	0	1, 1

→ n が
3 の倍数で
ない場合より、 $a^2 \equiv 1, b^2 \equiv 1$ である。 a, b は ① を満たすので

$$a^2 + b^2 \equiv 1 + 1 \equiv 2$$

一方 ① より $c^2 \equiv 0, 1$ よって $a^2 + b^2 \neq c^2$ より $a^2 + b^2 \neq c^2$

つまり ① に矛盾する。

よって題意が証明された。

404

(1) 整数 a, b, c が $a^2 + b^2 = c^2 \dots ①$ を満たす。このとき、 a, b, c のうち少なくとも一つは 5 の倍数であることを証明せよ。

背理法で考える。

「 a, b, c は全て 5 の倍数でない」と仮定する。

以下 mod 5 で考える。

整数 n の平方数は

n	0	1	2	3	4
n^2	0	1	4	4	1

 a, b, c よって、 a^2, b^2 のとりうる値は 1 or 4 であるすると、 $a^2 + b^2$ の値は

$$1 + 1 = 2$$

$$1 + 4 = 0$$

$$4 + 1 = 0$$

$$4 + 4 = 3$$

$a^2 + b^2$	1	4
1	2	0
4	0	3

 $a^2 + b^2 \equiv n$ c も 0 より、 $c^2 \equiv 1, 4$ であるが $a^2 + b^2 \equiv 2, 3$ となり ① に反する。

よって題意が示された。