佛教大学

代数学演習

問題と解答

Kazuma MATSUDA

2017 年 12 月 23 日

p.15

1　次の集合は環になるか論ぜよ.

(1)　自然数の集合 $\mathbb{N}$　　(2)　偶数の集合 $2\mathbb{Z}$

(1)

自然数の集合 N は環にならない．なぜなら，$a \in \mathbb{N}$ に対して加法についての単位元 b

$$a + b = b + a = a$$

となる $0_{\mathbb{N}} = b$ が存在しないからである.

(2)

偶数の集合 $2\mathbb{Z}$ は環にならない．なぜなら，$c \in 2\mathbb{Z}$ に対して乗法についての単位元 d

$$c \cdot d = d \cdot c = c$$

となる $1_{2\mathbb{Z}} = d$ が存在しないからである.

2　次の集合は環になるか論ぜよ.

(1)　$\left\{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\right\}$　　(2)　$\left\{a + \sqrt[3]{2}b \mid a,\ b \in \mathbb{Z}\right\}$

(1)

$\mathbb{Z}[\sqrt{2}] = \left\{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\right\}$ は環になる.

演算について

加法 : $\left(a+\sqrt{2}b\right)+\left(c+\sqrt{2}d\right)=(a+c)+\sqrt{2}(b+c) \quad \in \mathbb{Z}[\sqrt{2}]$

乗法 : $\left(a+\sqrt{2}b\right)\cdot\left(c+\sqrt{2}d\right)=(ac+2bd)+\sqrt{2}(ad+bc) \quad \in \mathbb{Z}[\sqrt{2}]$

よって演算について閉じている.

加法の交換則，結合則を満たすことは明らか.

零元について，零元を $0+\sqrt{2}0=0\in\mathbb{Z}[\sqrt{2}]$ とすれば

$$\left(a+\sqrt{2}b\right)+\left(0+\sqrt{2}0\right)=(a+0)+\sqrt{2}(b+0)=a+\sqrt{2}b$$

よって零元が存在する.

加法についての逆元について，$a+\sqrt{2}b$ に対し $-a+\sqrt{2}(-b)\in\mathbb{Z}[\sqrt{2}]$ とすれば

$$a+\sqrt{2}b+\left\{-a+\sqrt{2}(-b)\right\}=(a-a)+\sqrt{2}(b-b)=0+\sqrt{2}0=0$$

より逆元が存在する.

乗法についての結合則を満たすことは明らか.

乗法についての単位元を $1+\sqrt{2}0=1\in\mathbb{Z}[\sqrt{2}]$ とすれば

$$\left(a+\sqrt{2}b\right)\cdot\left(1+\sqrt{2}0\right)=a+\sqrt{2}b$$

よって単位元が存在する.

分配則を満たすことは明らか. □

(2)

$\mathbb{Z}[\sqrt[3]{2}]=\left\{a+\sqrt[3]{2}b \mid a,b\in\mathbb{Z}\right\}$ は環ではない.

乗法について，$c+\sqrt[3]{2}d\in\mathbb{Z}[\sqrt[3]{2}]$ とすると

$$\left(a+\sqrt[3]{2}b\right)\cdot\left(c+\sqrt[3]{2}d\right)=ac+\sqrt[3]{2}(ad+bc)+\sqrt[3]{4} \quad \notin\mathbb{Z}[\sqrt[3]{2}]$$

よって乗法について閉じていない.

3　整数の集合 $\mathbb{Z}$ を次のようにグループ分け (6 で割った余りの値でグループ分け) する：

$$[0]=\left\{\cdots,-6,0,6,12,18,\cdots\right\},$$
$$[1]=\left\{\cdots,-5,1,7,13,19,\cdots\right\},$$
$$[2]=\left\{\cdots,-4,2,8,14,20,\cdots\right\},$$
$$[3]=\left\{\cdots,-3,3,9,15,21,\cdots\right\},$$
$$[4]=\left\{\cdots,-2,4,10,16,22,\cdots\right\},$$
$$[5]=\left\{\cdots,-1,5,11,17,23,\cdots\right\}.$$

ここで，それぞれのグループ [0], [1], [2], [3], [4], [5] を元とする集合 R を考える.

(1)　次の計算を行え：

(i)　[2] + [3]　　(ii)　[4] + [5]　　(iii)　[0] · [3]　　(iv)　[2] · [5]

(i)

[2] + [3] = [5]

(ii)

[4] + [5] = [9] = [6]

(iiii)

[0] · [3] = [0]

(iv)

[2] · [5] = [10] = [4]

(2)　集合 R が上で与えた加法と乗法の下で環になることを実感し，零元と単位元を見出せ.

[0] + [0] = [0] , [0] + [1] = [1] , [0] + [2] = [2] , [0] + [3] = [3] , [0] + [4] = [4] , [0] + [5] = [5]
[1] + [1] = [2] , [1] + [3] = [4] , [1] + [4] = [5] , [1] + [5] = [6] = [0]
[2] + [2] = [4] , [2] + [3] = [5] , [2] + [4] = [6] = [0] , [2] + [5] = [7] = [1]
[3] + [3] = [6] = [0] , [3] + [4] = [7] = [1] , [3] + [5] = [8] = [2]
[4] + [4] = [8] = [2] , [4] + [5] = [9] = [3]
[5] + [5] = [10] = [4]

[0] · [0] = [0] , [0] · [1] = [0] , [0] · [2] = [0] , [0] · [3] = [0] , [0] · [4] = [0] , [0] · [5] = [0]
[1] · [1] = [1] , [1] · [2] = [2] , [1] · [3] = [3] , [1] · [4] = [4] , [1] · [5] = [5]
[2] · [2] = [4] , [2] · [3] = [6] = [0] , [2] · [4] = [8] − [2] , [2] · [5] = [10] = [4]
[3] · [3] = [9] = [3] , [3] · [4] = [12] = [0] , [3] · [5] = [15] = [3]
[4] · [4] = [16] = [4] , [4] · [5] = [20] = [2]
[5] · [5] = [1]

和	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

積	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

零元は [0]，単位元は [1].

(3)　命題 1.4 が成り立たない，つまり次の関係を満たす $[a]$, $[b]$ を見出せ：

$$[a]\cdot[b]=[0]\quad (a,\ b\neq 0)$$

▌例えば $a=2,\ b=3$ とすると $[2]\cdot[3]=[0]$.

(4)　上でみた集合は，通常は $\mathbb{Z}/(6\mathbb{Z})$ と表記される．
集合 $\mathbb{Z}/(6\mathbb{Z})$ の「親戚」で命題 1.4 が成り立つような集合はどのようなものか論ぜよ．

$\mathbb{Z}/(7\mathbb{Z})$

積	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

p.30-31

1　$2=1$ を導く次の論理の穴を正せ．

$$\begin{aligned}
x=y &\Leftrightarrow x^2=xy && (\because x\text{ を両辺に掛けた})\\
&\Leftrightarrow x^2-y^2=xy-y^2 && (\because -y^2\text{を両辺に加えた})\\
&\Leftrightarrow (x+y)(x-y)=y(x-y) && (\because \text{両辺を因数分解した})\\
&\Leftrightarrow x+y=y && (\because \text{両辺を } x-y \text{ で割った}) \quad \leftarrow \underline{x-y=0 \text{ で割っている}}\\
&\Leftrightarrow x+x=x && (\because y=x\text{ を代入した})\\
&\Leftrightarrow \underline{2=1}
\end{aligned}$$

2　$\boldsymbol{a}=\begin{pmatrix}1\\2\end{pmatrix}$, $\boldsymbol{x}=\begin{pmatrix}x\\y\end{pmatrix}$ とする．このとき，ベクトルの内積を用いた関係式 $\boldsymbol{a}\cdot\boldsymbol{x}=1$ を考えると，$\boldsymbol{x}$ は $\boldsymbol{a}$ の”逆元”とみなすことができそうである．しかし，通常はそういわない理由を考えよ．

$\boldsymbol{a}\cdot\boldsymbol{x}=1 \quad\Leftrightarrow\quad x+2y=1$ となり，これは直線の方程式を与える．即ち，$\boldsymbol{a}\cdot\boldsymbol{x}=1$ を満たす (x,y) は無数に存在し，一意に定まらない．

3　割り算記号「÷」と，分数表記が混在している小学校での算数を考える．

(1)　(2.12) $\dfrac{a}{b}\div\dfrac{c}{d}=\dfrac{a\div c}{b\div d}$ を確認せよ．

$$(\text{左辺})=\frac{a}{b}\times\frac{d}{c}=\frac{ad}{bc}$$

$$(\text{右辺})=\frac{\frac{a}{c}}{\frac{b}{d}}=\frac{ad}{cb}=\frac{ad}{bc}$$

(2)　(2.12）の計算手法の実践である次の計算について説明し，思うところを述べよ．

$$\frac{3}{5}\div\frac{2}{7}=\frac{3\times14\div2}{5\times14\div7}=\frac{3\times7}{5\times2}=\frac{21}{10}$$

$\div\dfrac{2}{7}$ の 7 と 2 の最小公倍数である 14 を分母・分子にかけることで，分数の分母・分子中での割り算の記号を消去している．
分数と割り算の記号が混在するのを避けることで計算の見通しがよくなる．

(3)　僕が学生に教えてもらった次の計算手法について説明し，思うところを述べよ．

$$\frac{1}{6}\div\frac{3}{4}=\frac{2}{12}\div\frac{9}{12}=\frac{2}{9}$$

分数の割り算を行う前に分母を揃えることで，分子だけの計算に帰着させている．
$\dfrac{2}{12}\div\dfrac{9}{12}=\left(\dfrac{2}{12}\times12\right)\div\left(\dfrac{9}{12}\times12\right)=2\div9.$
納得できれば，分数の割り算は結局整数の割り算に帰着させられる．

4 命題 2.1 を証明せよ.

証明

$\Rightarrow$

有限小数の定義 2.2 から，有理数 $\frac{n}{m}$ が有限小数であるとき $k \in \mathbb{N}$ が存在して

$$\frac{n}{m} \times 10^k \qquad \text{(a)}$$

を整数とすることができる．10^k の素因数は 2 と 5 なので，(a) が整数になるためには m の素因数が 2 と 5 のみ (2 だけ，5 だけを含む) でなければならない.

$\Leftarrow$

$\frac{n}{m}$ の分母の素因数が 2, 5 のみ，即ち

$$\frac{n}{m} = \frac{n}{2^s 5^t} \qquad s,\ t \in \mathbb{Z}$$

と書けるなら，$\frac{n}{m}$ に $10^k = \max(s, t)$ をかけることで整数にすることができるので，このとき $\frac{n}{m}$ は有限小数である.

5 有理数は小数表示し，循環小数は有理数表示せよ.

(1) $\frac{1}{13}$ (2) $\frac{1}{81}$ (3) $5.\dot{2}8\dot{6}$

(1)

$$\frac{1}{13} = 0.\dot{0}76923\dot{}$$

(2)

$$\frac{1}{81} = 0.\dot{0}12345679\dot{}$$

(3)

$$\begin{array}{rrcl} & a & = & 5.286286\cdots \\ -) & 1000a & = & 5286.286286\cdots \\ \hline & -999a & = & -5281 \end{array}$$

$$\therefore a = \frac{5281}{999}$$

6 次の数の連分数表示を求めよ.

(1) $\frac{67}{29}$ (2) $\sqrt{5}$ (3) $\frac{24-\sqrt{15}}{17}$

(1)

$$\frac{67}{29} = 2 + \frac{9}{29} = 2 + \frac{1}{\frac{29}{9}} = 2 + \frac{1}{3 + \frac{2}{9}} = 2 + \frac{1}{3 + \frac{1}{\frac{9}{2}}} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

(2)

$$\sqrt{5} = 2 + \left(\sqrt{5} - 2\right) = 2 + \frac{1}{\frac{1}{\sqrt{5}-2}} = 2 + \frac{1}{\sqrt{5}+2} = 2 + \frac{1}{4 + \left(\sqrt{5} - 2\right)} = 2 + \frac{1}{4 + \frac{1}{\sqrt{5}+2}}$$

$$= 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}$$

(3)

$$\frac{24 - \sqrt{15}}{17} = 1 + \frac{7 - \sqrt{15}}{17} = 1 + \frac{1}{\frac{17}{7 - \sqrt{15}}} = 1 + \frac{1}{\frac{17(7 + \sqrt{15})}{34}} = 1 + \frac{1}{\frac{7 + \sqrt{15}}{2}} = 1 + \frac{1}{5 + \frac{\sqrt{15} - 3}{2}}$$

$$= 1 + \frac{1}{5 + \frac{1}{\frac{2}{\sqrt{15}-3}}} = 1 + \frac{1}{5 + \frac{1}{\frac{2(\sqrt{15}+3)}{6}}} = 1 + \frac{1}{5 + \frac{1}{\frac{\sqrt{15}+3}{3}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{\sqrt{15}-3}{3}}}$$

$$= 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{\frac{3}{\sqrt{15}-3}}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{\frac{3(\sqrt{15}+3)}{6}}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{3 + \frac{\sqrt{15}-3}{2}}}}$$

$$= 1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\frac{2}{\sqrt{15}-3}}}}} = 1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\frac{2}{\sqrt{15}-3}}}}} = 1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\ddots}}}}}}$$

7 無限に続く連分数表示 $[1; 1, 1, \cdots]$ を持つ無理数を求めよ.

$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}$ と置くと

$$x = 1 + \frac{1}{x}$$
$$x^2 = x + 1$$
$$x^2 - x - 1 = 0$$
$$\therefore x = \frac{1 + \sqrt{5}}{2} \quad (> 0)$$

8　π の連分数表示は (2.39) で与えられる．ここで，292 という大きな数が出てきたことに注目し，この手前で連分数を止めた場合の π の有理数近似を求めよ．

$$\pi \fallingdotseq 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} = 3 + \cfrac{1}{7 + \cfrac{1}{16}} = 3 + \frac{113}{16} = 3 + \frac{16}{113} = 3 + 0.14159292\cdots$$
$$= 3.14159292\cdots$$

p46-47

1　次の集合 R を考える：

$$R = \left\{(a, b) \mid a,\ b \in \mathbb{Q}\right\}.$$

この集合に対して，加法と乗法を以下のように定めたとき，R は環にはなるが，体にはならないことを示せ．

加法 : $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$,
乗法 : $(a_1, b_1) \cdot (a_2, b_2) = (a_1 b_1, a_2 b_2)$.

加法について，単位元 $0_R = (0, 0)$ とすれば

$$(a, b) + (0, 0) = (0, 0) + (a, b) = (a, b)$$

加法について，(a, b) の逆元を $(-a, -b)$ とすれば

$$(a, b) + (-a, -b) = (-a, -b) + (a, b) = (0, 0) = 0_R$$

乗法にてついて結合則を満たすのは明らか．
乗法についての単位元を $1R = (1, 1)$ とすれば

$$(a, b) \cdot (1, 1) = (1, 1) \cdot (a, b) = (a, b)$$

分配則

$$(a_1, b_1)\{(a_2, b_2) + (a_3 + b_3)\} = (a_1, b_1)(a_2 + a_3, b_2 + b_3) = (a_1 a_2 + a_1 a_3, b_1 b_2 + b_1 b_3)$$
$$= (a_1, b_1)(a_2, b_2) + (a_1 b_1)(a_3, b_3)$$

以上より R は環である．0_R でない R の元として $(1, 0)$ をとれば，$(1, 0) \in R$ に対する逆元を (a', b') として

$$(1, 0) \cdot (a', b') = (a', 0) = (1, 1) = 1_R$$

を満たす (a', b') は存在しないので R は体ではない．

2　体 $\mathbb{Q}(\sqrt{3})$ においても，実数体 $\mathbb{R}$ で成り立つ

$$ab = 0 \quad \Rightarrow \quad a = 0 \quad \text{または} \quad b = 0$$

が成り立つことを示せ.

集合 $\mathbb{Q}(\sqrt{3})$ の任意の元を

$$\alpha = a + b\sqrt{3} \qquad a,\ b \in \mathbb{Q}$$

とする．$\alpha = a + b\sqrt{3},\ \beta = c + d\sqrt{3}$ とすると

$$\alpha + \beta = (a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \qquad \in \mathbb{Q}(\sqrt{3})$$
$$\alpha\beta = (a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \qquad \in \mathbb{Q}(\sqrt{3})$$

$\alpha\beta = 0$ とすると

$$\begin{cases} ac + 3bd = 0 \\ ad + bc = 0 \end{cases} \qquad \text{(a)}$$

$a = b$ とすると

$$\begin{cases} 3bd = 0 \\ bc = 0 \end{cases} \qquad \text{(b)}$$

$b = 0$ は (a) を満たす．$b \neq 0$ とすると $d = c = 0$.
よって，$a = b = 0$ または $c = d = 0$.

(a) で $c = 0$ とすると

$$\begin{cases} 3bd = 0 \\ bc = 0 \end{cases} \qquad \text{(c)}$$

$d = 0$ は (c) を満たす．$d \neq 0$ とすると $b = a = 0$
よって $c = d = 0$ または $a = b = 0$.
以上より $\alpha\beta = 0$ ならば $a = b = 0$ または
$c = d = 0$.

3　体の公理から

$$ab = 0 \quad \Rightarrow \quad a = 0 \quad \text{または} \quad b = 0$$

を示せ.

4　次の方程式を満たす有理数 $p,\ q$ を求めよ.

(1)　$(1+2\sqrt{2})(p+4\sqrt{2}) = q+10\sqrt{2}$　　(2)　$\dfrac{9+7\sqrt{5}}{p+q\sqrt{5}} = 3-\sqrt{5}$

(1)

$$\begin{aligned}\left(1+2\sqrt{2}\right)\left(p+4\sqrt{2}\right) &= p+16+(2p+4)\sqrt{2}\\ &= q+10\sqrt{2}\end{aligned}$$

よって

$$\begin{cases} p+16=q \\ 2p+4=10 \end{cases} \quad \therefore \begin{cases} p=3 \\ q=19 \end{cases}$$

(2)

$$\frac{9+7\sqrt{5}}{p+q\sqrt{5}} = 3-\sqrt{5}$$

$$\frac{p+q\sqrt{5}}{9+7\sqrt{5}} = \frac{1}{3-\sqrt{5}}$$

$$p+q\sqrt{5} = \frac{9+7\sqrt{5}}{3-\sqrt{5}} = \frac{\left(9+7\sqrt{5}\right)\left(3+\sqrt{5}\right)}{9-5} = \frac{27+35+(9+21)\sqrt{5}}{4} = \frac{62+30\sqrt{5}}{4} = \frac{31}{2}+\frac{15}{2}\sqrt{5}$$

よって

$$\begin{cases} p=\dfrac{31}{2} \\ q=\dfrac{15}{2} \end{cases}$$

5　体 $\mathbb{Q}(\sqrt{5})$ について考える.

(1)　$\mathbb{Q}(\sqrt{5})$ の 2 元 $5,\ 2\sqrt{5}$ は $\mathbb{Q}$ 上で線型独立であることを示せ.

(2)　$\mathbb{Q}(\sqrt{5})$ の 2 元 $\sqrt{5},\ -\dfrac{2}{3\sqrt{5}}$ は $\mathbb{Q}$ 上で線型従属であることを示せ.

(3)　$\mathbb{Q}(\sqrt{5})$ の 2 元 $a+b\sqrt{5},\ c+d\sqrt{5}$ が $\mathbb{Q}$ 上で線型独立である必要十分条件は $ad-bc\neq 0$ であることを示せ.

(1)

$\alpha = 5a+b2\sqrt{5}$,　$a,\ b\in\mathbb{Q}$ において,　$b\neq 0$ とすると

$$\sqrt{5} = -\frac{5a}{2b}$$

となり,　上式の左辺は無理数で右辺は有理数なので不合理.　よって $b=0$.　このとき

$$\alpha = 5a + 0 \cdot \sqrt{5} = 0$$
$$\therefore a = 0$$

即ち $5 + b2\sqrt{5} = 0 \quad \Leftrightarrow \quad a = b = 0$. よって $\mathbb{Q}(\sqrt{5})$ の元 $5,\ 2\sqrt{5}$ は線型独立である.

(2)
$a\sqrt{5} + b\left(-\dfrac{2}{3\sqrt{5}}\right) = 0$, $a,\ b \in \mathbb{Q}$ ……(a) において, $b \neq 0$ とすると

$$a\sqrt{5} = b\frac{2}{3\sqrt{5}}$$
$$a = b \cdot \frac{2}{15}$$

よって $b = 1,\ a = \dfrac{2}{15}$ は (a) を満たすので $\mathrm{Q}(\sqrt{5})$ の元 $\sqrt{5},\ -\dfrac{2}{3\sqrt{5}}$ は線型従属である.

(3) $\mathrm{Q}(\sqrt{5})$ の元 $a + b\sqrt{5}$ と $c + d\sqrt{5}$ が Q 上で線型独立ならば

$$p(a + b\sqrt{5}) + q(c + d\sqrt{5}) = 0 \tag{1}$$

となるのが $p = q = 0$ のときのみである.
(1) は

$$\begin{pmatrix} p \\ q \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{5} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

と書けるので, 上式が $p = q = 0$ のときのみ成立するためには $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の行列式が

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$$

でなければならない. よって

$$ad - bc = 0$$

またこのとき, (1) を満足するのは $p = q = 0$ のときに限る. □

6　体 $\mathbb{Q}(\sqrt[3]{2})$ において次を計算し，$a+b\sqrt[3]{2}+c\sqrt[3]{4}$ の形に表せ.

(1)　$(1+2\sqrt[3]{2})(3+4\sqrt[3]{2}+5\sqrt[3]{4})$　　(2)　$\dfrac{4+5\sqrt[3]{2}}{1+2\sqrt[3]{2}+3\sqrt[3]{4}}$

(1)

$$\begin{aligned}\left(1+2\sqrt[3]{2}\right)\left(3+4\sqrt[3]{2}+5\sqrt[3]{4}\right) &= 3+4\sqrt[3]{2}+5\sqrt[3]{4}+6\sqrt[3]{2}+8\sqrt[3]{4}+10\sqrt[3]{8}\\ &= 3+(4+6)\sqrt[3]{2}+(5+8)\sqrt[3]{4}+10\cdot 2\\ &= 23+10\sqrt[3]{2}+13\sqrt[3]{4}\end{aligned}$$

(2)

$\dfrac{1}{a+b\sqrt[3]{2}+c\sqrt[3]{4}} = \dfrac{a^2-2bc+\left(2c^2-ab\right)\sqrt[3]{2}+\left(b^2-ca\right)\sqrt[3]{4}}{a^3+2b^3+4c^3-6abc}$ を用いると

$$\frac{1}{1+2\sqrt[3]{2}+3\sqrt[3]{4}} = \frac{1-12+(18-2)\sqrt[3]{2}+(4-3)\sqrt[3]{4}}{1+16+108-36} = \frac{-11+16\sqrt[3]{2}+\sqrt[3]{4}}{89}$$

よって与式は

$$\begin{aligned}\frac{\left(4+5\sqrt[3]{2}\right)\left(-11+16\sqrt[3]{2}+\sqrt[3]{4}\right)}{89} &= \frac{-44+64\sqrt[3]{2}+4\sqrt[3]{4}-55\sqrt[3]{2}+80\sqrt[3]{4}+10}{89} = \frac{-34+9\sqrt[3]{2}+84\sqrt[3]{4}}{89}\\ &= -\frac{34}{89}+\frac{9}{89}\sqrt[3]{2}+\frac{84}{89}\sqrt[3]{4}\end{aligned}$$

7　有理数の集合 $\mathbb{Q}$ に，1 の 3 乗根の 1 つである $\omega=\dfrac{-1+\sqrt{3}i}{2}$ を加えて，加減乗除した数全体を $\mathbb{Q}(\omega)$ とする.

(1)　$\mathbb{Q}(\omega)$ の元が $a+b\omega,\ a,\ b\in\mathbb{Q}$ と書けることを実感するために $a+b\omega$ の形の元が加法と乗法の下で閉じていることを確認せよ.

(2)　$\mathbb{Q}(\omega)$ の元 $a+b\omega\neq 0$ について，その逆元を求めよ.

(1)

$\omega=\dfrac{-1+\sqrt{3}i}{2}$，$\omega^2=\dfrac{-1-\sqrt{3}i}{2}$，$\omega^3=1$.

加法について

$$(a+b\omega)+(c+d\omega)=(a+c)+(b+d)\omega \qquad \in\mathbb{Q}(\omega)$$

乗法について

$$(a+b\omega)\cdot(c+d\omega) = ac + bd\omega^2 + (ad+bc)\omega = ac - \frac{bd}{2} - \frac{bd\sqrt{3}i}{2} - \frac{ad+bc}{2} + \frac{(ad+bc)\sqrt{3}i}{2}$$

$$= ac - bd + \frac{bd}{2} - \frac{ad+bc}{2} - \frac{bd\sqrt{3}i}{2} + \frac{(ad+bc)\sqrt{3}i}{2}$$

$$= ac - bd + \frac{-(ad+bc-bd) + (ad+bc-bd)\sqrt{3}i}{2}$$

$$= ac + bd + (ad+bc-bd)\omega \qquad \in \mathbb{Q}(\omega)$$

(2)

$a+b\omega = a + b\dfrac{-1+\sqrt{3}i}{2} = \dfrac{(2a-b)+b\sqrt{3}i}{2}$ より

$$\frac{2}{(2a-b)+b\sqrt{3}i} = \frac{2\left\{(2a-b)+b\sqrt{3}i\right\}}{(2a-b)^2+3b^2} = \frac{4a-2b-2b\sqrt{3}i}{4a^2-4ab+b^2+3b^2} = \frac{4a-4b+2b-2b\sqrt{3}i}{4a^2-4ab+4b^2}$$

$$= \frac{a-b-b\left(-1+\sqrt{3}i\right)}{a^2+ab+b^2} = \frac{1}{a^2+ab+b^2}\{(a-b)-b\omega\}$$

8 次の行列を考える：

$$E = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad I = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \qquad J = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \qquad K = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

但し，i は虚数単位で $i^2 = -1$ を満たす．このとき，次を示せ．

(1) $I^2 = J^2 = K^2 = -E$.

(2) $IJ = -JI = K,\ JK = -KJ = I,\ KI = -IK = J$.

(3) $A = aE + bI + cJ + dK,\ \ a,\ b,\ c,\ d \in \mathbb{R},\ A \neq 0$ のとき，

$$B = \frac{1}{a^2+b^2+c^2+d^2}(aE - bI - cJ - dK)$$

とすれば、$AB = E$ となり、B は A の逆元となる．

これは、ハミルトンの四元数体という、非可換体をなす．

(1)

$$I^2 = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E$$

$$J^2 = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E$$

$$K^2 = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E$$

(2)

$$IJ = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = K$$

$$JI = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -IJ$$

$$JK = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = I$$

$$KJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -JK$$

$$KI = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = J$$

$$IK = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -KI$$

(3)

$$\begin{aligned} AB &= (aE + bI + cJ + dK)\frac{1}{a^2 + b^2 + c^2 + d^2}(aE - bI - cJ - dK) \\ &= \frac{1}{a^2 + b^2 + c^2 + d^2}(aE + bI + cJ + dK)(aE - bI - cJ - dK) \\ &= \frac{1}{a^2 + b^2 + c^2 + d^2}\Big(a^2E^2 - abEI - acEJ - adEK + baIE - b^2I^2 - bcIJ - bdIK \\ &\qquad + caJE - cbJI - c^2J^2 - cdJK + daKE - dbKI - dcKJ - d^2K^2\Big) \\ &= \frac{1}{a^2 + b^2 + c^2 + d^2}\Big(a^2E + abI - acJ - adK + abI + b^2E - bcK + bdJ \\ &\qquad + acJ + bcK + c^2E - cdI + adK - bdJ + cdI + d^2E\Big) \\ &= \frac{1}{a^2 + b^2 + c^2 + d^2}\Big(a^2 + b^2 + c^2 + d^2\Big)E = E \end{aligned}$$

p.59

1 次を示せ.

(1) $7 \mid 343$ (2) $2017 \mid 0$

(1)

$343 \div 7 = 49$

(2)

$0 \div 2017 = 0$

2　$a, b, c, d \in \mathbb{Z}$ とする．$a \mid b,\ c \mid d$ であるとき、$ac \mid bd$ を示せ．

$a \mid b \quad \Rightarrow \quad b = ak \qquad (k \in \mathbb{Z})$
$c \mid d \quad \Rightarrow \quad d = cl \qquad (l \in \mathbb{Z})$

よって

$$bd = ac(kl)$$
$$\therefore\ ac \mid bd$$

3　a を整数とするとき、$a^3 - a$ が 3 で割り切れることを示せ．

$$a^3 - a = a\left(a^2 - a\right) = a(a+1)(a-1) = (a-1)a(a+1)$$

連続する 3 個の整数の積であるから，このうちの一つは 3 の倍数である．よって $a^3 - a$ は 3 で割りきれる．

4　奇数の 2 乗は、ある整数 m を用いて、$8m + 1$ と書けることを示せ．

奇数を $2n + 1$ と書くと

$$(2n+1)^2 = 4n^2 + 4n + 1$$
$$= 4n(n+1) + 1$$

ここで n と $n + 1$ は連続する 2 個の整数だからどちらかは偶数である．よって $4n(n + 1)$ は $4 \cdot 2m = 8m$ と書ける．然るに

$$(2n+1)^2 = 8m + 1 \qquad (2m = (n(n+1))$$

5　数学的帰納法を用いて次を示せ．

$9 \mid (4^n + 15n - 1)$ ．

6　次の数を 2 進数表示せよ.

(1)　$(127)_{(10)}$　　(2)　$(525)_{(10)}$

(1)

	2)	127	
	2)	63	1
	2)	31	1
	2)	15	1
	2)	7	1
	2)	3	1
		1	1

$127_{(10)} = (1111111)_{(2)}$

(2)

	2)	525	
	2)	262	1
	2)	131	0
	2)	65	1
	2)	32	1
	2)	16	0
	2)	8	0
	2)	4	0
	2)	2	0
		1	0

$(525)_{(10)} = (1000001101)_{(2)}$

7　2 進数表示で計算せよ.

(1)　$(1111)_{(2)} + (1011)_{(2)}$　　(2)　$(11010001)_{(2)} - (10010)_{(2)}$　　(3)　$(1010101)_{(2)} \times (1101)_{(2)}$

(4)　$(10111)_{(2)} \div (11)_{(2)}$

(1)

$$\begin{array}{rr} & 1111_{(2)} \\ +) & 1101_{(2)} \\ \hline & 11010_{(2)} \end{array}$$

(2)

$$\begin{array}{rr} & 1101001_{(2)} \\ -) & 10010_{(2)} \\ \hline & 1010111_{(2)} \end{array}$$

(3)

$$\begin{array}{rr} & 1010101_{(2)} \\ \times) & 1101_{(2)} \\ \hline & 1010101 \\ & 1010101 \\ & 1010101 \\ \hline & 10001010001_{(2)} \end{array}$$

(4)

$$\begin{array}{rr} & 111 \\ \hline 11 &) \ 10111 \\ & 11 \\ \hline & 101 \\ & 11 \\ \hline & 101 \\ & 11 \\ \hline & 10 \end{array}$$

$(111)_{(2)}$ 余り $(10)_{(2)}$

8　次の数を与えられた基数で表示せよ.

(1)　$(2017)_{(10)}$ (5 進数表示)　　(2)　$(3267)_{(10)}$ (7 進数表示)　　(3)　$(1023)_{(4)}$ (10 進数表示)

(1)

5)	2017	
5)	403	2
5)	80	3
5)	16	0
5)	3	1

$(2017)_{(10)} = (31032)_{(5)}$

(2)

7)	3267	
7)	466	5
7)	66	4
7)	9	3
7)	1	2

$(3267)_{10} = (12345)_{(7)}$

(3)

$$(1023)_{(4)} = 1 \times 4^3 + 0 \times 4^2 + 2 \times 4^1 + 3 \times 4^0$$
$$= 64 + 8 + 3 = 75_{(10)}$$

9　与えられた基数で計算せよ．割り算については、商とあまりを求めよ.

(1)　$(2345)_{(8)} + (567)_{(8)}$　　(2)　$(43010)_{(5)} - (4024)_{(5)}$　　(3)　$(5525)_{(6)} \times (25)_{(6)}$

(4)　$(65102)_{(7)} \div (24)_{(7)}$

(1)

$$\begin{array}{rr} & 2345_{(8)} \\ +) & 567_{(8)} \\ \hline & 3134_{(8)} \end{array}$$

(2)

$$\begin{array}{rr} & 43010_{(5)} \\ -) & 4024_{(5)} \\ \hline & 33431_{(5)} \end{array}$$

(3)

$$\begin{array}{rr} & 5525_{(6)} \\ -) & 25_{(6)} \\ \hline & 45321 \\ & 15454 \\ \hline & 244301_{(6)} \end{array}$$

(4)

$$\begin{array}{rr} & 2422 \\ \hline 24 &) \ 65402 \\ & 51 \\ \hline & 141 \\ & 132 \\ \hline & 60 \\ & 51 \\ \hline & 62 \\ & 51 \\ \hline & 11 \end{array}$$

$(2422)_{(7)}$　余り $(11)_{(7)}$

p.71

1　次の最大公約数を求めよ

(1)　$\gcd(187, 77)$　　(2)　$\gcd(54321, 9876)$

(1)

$$187 = 77 \cdot 2 + 23$$
$$77 = 33 \cdot 2 + 11$$
$$33 = 11 \cdot 3 + 0$$
$$\therefore \gcd(187, 77) = 11$$

(2)

$$54321 = 9876 \cdot +1461$$
$$9876 = 1461 \cdot 6 + 1110$$
$$1461 = 1110 \cdot 1 + 351$$
$$351 = 57 \cdot 6 + 9$$
$$57 = 9 \cdot 6 + 3$$
$$9 = 3 \cdot 3 + 0$$
$$\therefore \gcd(54321, 9876) = 3$$

2　(3.29) $\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_{N+1} & 1 \\ 1 & 0 \end{pmatrix}$ で定義された行列 Q について、その行列式が $|Q| = (-1)^{N+1}$ となることを示せ.

$$\begin{vmatrix} q_k & 1 \\ 0 & 1 \end{vmatrix} = -1 \qquad (1 \leq k \leq N+1)$$

より

$$|Q| = \left|\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_{N+1} & 1 \\ 1 & 0 \end{pmatrix}\right| = \begin{vmatrix} q_1 & 1 \\ 1 & 0 \end{vmatrix}\begin{vmatrix} q_2 & 1 \\ 1 & 0 \end{vmatrix}\cdots\begin{vmatrix} q_{N+1} & 1 \\ 1 & 0 \end{vmatrix}$$
$$= \underbrace{(-1)\cdot(-1)\cdots(-1)}_{N+1\text{ 個}} = (-1)^{N+1}$$

3 次の最大公約数を求めよ.

(1) $\gcd(222, 102)$ (2) $\gcd(198, 252)$ (3) $\gcd(44350, 20785)$

(4) $\gcd(3313772, 1587894)$

(1)

$$222 = 102 \cdot 2 + 18$$
$$102 = 18 \cdot 5 + 12$$
$$18 = 12 \cdot 1 + 6$$
$$12 = 6 \cdot 2 + 0$$
$$\therefore \gcd(222, .102) = 6$$

(2)

$$252 = 198 \cdot 1 + 54$$
$$198 = 54 \cdot 3 + 36$$
$$54 = 36 \cdot 1 + 18$$
$$36 = 18 \cdot 2 + 0$$
$$\therefore \gcd(198, 252) = 18$$

(3)

$$44350 = 20785 \cdot 2 + 2780$$
$$20785 = 2780 \cdot 7 + 1325$$
$$2780 = 1325 \cdot 2 + 130$$
$$1325 = 130 \cdot 10 + 25$$
$$25 = 5 \cdot 5 + 0$$
$$\therefore \gcd(44350, 2078) = 5$$

(4)

$$3313772 = 1578794 \cdot 2 + 137984$$
$$1578794 = 137984 \cdot 11 + 70070$$
$$137984 = 70070 \cdot 1 + 67914$$
$$70070 = 67914 \cdot 1 + 2156$$
$$67914 = 2456 \cdot 3 + 1078$$
$$2156 = 1078 \cdot 2 + 0$$
$$\therefore \gcd(3313772, 1587894) = 1078$$

4 次の 1 次方程式について、解が存在すれば、その一般解を求めよ.

(1) $8x + 4y = 19$ (2) $2x + 5y = 11$ (3) $18x + 14y = 2$

(4) $127x + 52y = 1$ (5) $21x + 14y = 147$ (6) $3313772x + 1587894y = 1078$

(1)

$\gcd(8, 4) = 4 \nmid 19$ より整数解なし.

(2)

$$\begin{pmatrix}2\\5\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}5\\2\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$$

よって

$$Q = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix} = \begin{pmatrix}2 & 1\\5 & 2\end{pmatrix}$$
$$Q^{-1} = \begin{pmatrix}-2 & 1\\5 & -2\end{pmatrix}$$

ゆえに

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} 11 & t \end{pmatrix}\begin{pmatrix} -2 & 1 \\ 5 & -2 \end{pmatrix}$$
$$= \begin{pmatrix} -22+5t & 11-2t \end{pmatrix}$$

(3)

$$\begin{pmatrix} 18 \\ 14 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 14 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

よって

$$Q = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 7 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$$
$$Q^{-1} = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}$$

ゆえに

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} 1 & t \end{pmatrix}\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \qquad = \begin{pmatrix} -3+7t & 4-9t \end{pmatrix}$$

(4)

$$\begin{pmatrix} 127 \\ 52 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 52 \\ 23 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 23 \\ 6 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix}$$
$$= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

よって

$$Q = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 127 & 22 \\ 52 & 9 \end{pmatrix}$$
$$Q^{-1} = \begin{pmatrix} -9 & 22 \\ 52 & -127 \end{pmatrix}$$

よって

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} 1 & t \end{pmatrix}\begin{pmatrix} -9 & 22 \\ 52 & -127 \end{pmatrix}$$
$$= \begin{pmatrix} -9+52t & 22-127t \end{pmatrix}$$

(5)

$$\begin{pmatrix} 21 \\ 14 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 7 \\ 0 \end{pmatrix}$$

よって

$$Q=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}=\begin{pmatrix}3&1\\1&1\end{pmatrix}$$
$$Q^{-1}=\begin{pmatrix}1&-1\\-2&3\end{pmatrix}$$

ゆえに

$$\begin{aligned}\begin{pmatrix}x&y\end{pmatrix}&=\begin{pmatrix}21&t\end{pmatrix}\begin{pmatrix}1&-1\\-2&3\end{pmatrix}\\&=\begin{pmatrix}21-2t&-21+3t\end{pmatrix}\end{aligned}$$

(6)

$$\begin{aligned}\begin{pmatrix}3313772\\1587894\end{pmatrix}&=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1587894\\137984\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}137984\\70070\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}70070\\67914\end{pmatrix}\\&=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}67914\\2156\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}31&1\\1&0\end{pmatrix}\begin{pmatrix}2156\\1078\end{pmatrix}\\&=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}31&1\\1&0\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1078\\0\end{pmatrix}\end{aligned}$$

よって

$$Q=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}31&1\\1&0\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}=\begin{pmatrix}3074&1513\\1473&725\end{pmatrix}$$
$$Q^{-1}=\begin{pmatrix}725&-1513\\-1473&3074\end{pmatrix}$$

ゆえに

$$\begin{pmatrix}x&y\end{pmatrix}=\begin{pmatrix}1&t\end{pmatrix}\begin{pmatrix}725&-1513\\-1473&3074\end{pmatrix}\begin{pmatrix}725+1473t&-1513-3074t\end{pmatrix}$$

5　果物屋さんのあなたは、810 円をちょうど使って、以下の仕入れ値の果物をそれぞれ 1 個以上仕入れたい．可能な個数をそれぞれ求めよ．

(1)　1 個あたりの仕入れ値 25 円のりんごと 18 円のみかん．

(2)　1 個あたりの仕入れ値 18 円のみかんと 33 円のグレープフルーツ．

p.77-79

1　1 を素数と呼べないことを説明せよ.

$n \geq 2$ である任意の自然数は，素数 p_i により

$$n = p_1 p_2 \cdots p_r$$

と一意に書ける．1 が素数とすると

$$n = p_1 p_2 \cdots p_n \times 1^k \qquad k \in \mathbb{Z}$$

と書け，一意性が失われる.

2　円 $x^2 + y^2 = 1$ と直線 $y = x$ の交点が有理数でないことを示せ.

$$\begin{cases} x^2 + y^2 = 1 \\ x = y \end{cases}$$

より

$$x^2 + x^2 = 1$$
$$2x^2 = 1$$
$$x = \pm\frac{1}{\sqrt{2}} = \pm\frac{\sqrt{2}}{2}$$

よって

$$(x, y) = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right),\ \left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right)$$

であり，$x^2 + y^2 = 1$ と $x = y$ の交点の座標は有理数ではない.

3 次の問いに答えよ.

(1) 素数 p について $\sqrt{p}$ が無理数であることを示せ.

(2) $\sqrt{6}$ が無理数であることを示せ.

(3) 「$\sqrt{m}$が有理数」 $\Leftrightarrow$ 「m が平方数」を示せ.

(4) $\log_{10} 2$ が無理数であることを示せ.

(1)

$\sqrt{p} = \dfrac{m}{n}$, $m,\ n \in \mathbb{Z}_{>0},\ \gcd(m,n) = 1$ とする.

$$p = \frac{m^2}{n^2}$$
$$m^2 = pn^2$$

となり m は n で割りきれるので $m = pl\ \ l \in \mathbb{Z}_{>0}$ が存在する. よって

$$p^2l^2 = pn^2$$
$$pl^2 = n^2$$

となり $p \mid n^2$ より $p \mid n$. ゆえに m と n は p で割り切れ, $\gcd(m,n) = 1$ に矛盾する. よって $\sqrt{p}$ は無理数である.

(2)

$\sqrt{6} = \dfrac{m}{n}$, $m,\ n \in \mathbb{Z}_{>0},\ \gcd(m,n) = 1$ とする. $6 = \dfrac{m^2}{n^2}$ より $6n^2 = m^2$. よって $6 \mid m^2 \ \ \therefore 6 \mid m$. ゆえに $m = 6l\ \ l \in \mathbb{Z}_{>0}$ と書ける. このとき

$$6n^2 = 6^2l^2$$
$$\therefore n^2 = 6l^2$$

よって $6 \mid n^2 \ \ \therefore 6 \mid n$. 従って $m,\ n$ は 6 で割り切れるので $\gcd(m,n) = 1$ に矛盾する. よって $\sqrt{6}$ は無理数である.

(3)

(4)

4 503 が素数であることを示せ.

$\sqrt{503} = 22.47\cdots$. 503 は $p < 22$ となる素数 2, 3, 5, 7, 11, 13, 17, 19 のいずれでも割り切れないので素数である.

5 エラトステネスのふるいにより、200 までの素数表を完成させよ.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

6 次の最小公倍数を求めよ.

(1) $\mathrm{lcm}(8, 20)$ (2) $\mathrm{lcm}(111, 303)$ (3) $\mathrm{lcm}(256, 5040)$

(1)

$8 = 2^3$

$12 = 2^2 \cdot 3$

$\therefore \mathrm{lcm}(8, 12) = 2^3 \cdot 3 = 24$

(2)

$111 = 3 \cdot 37$

$303 = 3 \cdot 101$

$\therefore \mathrm{lcm}(111, 303) = 3 \cdot 37 \cdot 101 = 11211$

(3)

$256 = 4^4$

$5040 = 7 \cdot 5 \cdot 3^2 \cdot 4^2$

$\therefore \mathrm{lcm}(256, 5040) = 4^4 \cdot 7 \cdot 5 \cdot 3^2 = 4^2 \cdot 5040$

$= 80640$

7　最大公約数が 48、最小公倍数が 1440 である 3 桁の自然数 m, n を求めよ.

$48 \mid m,\ 48 \mid n$ より $m = 48k,\ n = 48l\ \ (k, l \in \mathbb{Z})$.　$1440 = 5 \cdot 3 \cdot 2$ より

$$(m, n) = (48 \cdot 5, 48 \cdot 6) = (240, 288)$$
$$(m, n) = (48 \cdot 5 \cdot 2, 48 \cdot 3) = (480, 144)$$

8　互いに値の近い素数 p, q の積であるという合成数 $n = 3493157$ の素因数分解を考える.

(1)　等式 $n = pq$ うぃ与える次の等式を示せ.

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

(2)　上の等式で $p - q = 4$ とするとき,

$$3493157 = \left(\frac{p+q}{2}\right)^2 - 4 \qquad \therefore \left(\frac{p+q}{4}\right)^2 = 3493161$$

となる．ここで，3493161 が平方数になることを確認し，p, q を求めよ.

(3)　互いに近い素数 p, q の積である合成数 $n = 4553947$ の素因数分解を遂行せよ.

9　三つ子素数 $(p, p+2, p+4)$ は，$(3, 5, 7)$ のみであることを示せ.

10　次の連続する n 個の数は、全て合成数であることを示せ：

$$(n+1)! + 2\ ,\ (n+1)! + 3\ ,\ (n+1)! + 4\ ,\ \cdots\ ,\ (n+1)! + (n+1)$$

また、これを用いて、連続する 10 個の合成数を見出せ.

p.87-88

1　次の主張の真偽を判定せよ.

(1)　$24 \equiv 4 \mod 5$　　(2)　$52 \equiv 36 \mod 4$　　(3)　$26 \equiv -96 \mod 11$

(4)　$11 \equiv 98 \mod 8$

(1)

$24 - 4 = 20 = 5 \cdot 4$: 真 .

(2)

$52 - 36 = 16 = 4 \cdot 4$: 真 .

(3)

$26 - (-95) = 121 = 11 \cdot 11$: 真 .

(4)

$11 - 98 = -87$: 偽 .

2 次の数を与えられた法の下で簡単化せよ.

(1) $25 \mod 2$ (2) $134 \mod 7$ (3) $121 \mod 11$ (4) $-321 \mod 101$

(1)

$25 \equiv 1 \mod 2$

(2)

$134 \equiv 1 \mod 7$

(3)

$121 \equiv 0 \mod 11$

(4)

$-131 \equiv 83 \mod 101$

3 例 5.1 に倣って、整数の集合を法 7 の下で類別せよ.

7 は素数なので

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6]\}$$

4 8 で割ったら 5 余る数、つまり $x = 5 \mod 8$ を満たす 3 桁の数 x のうち、最大のものを求めよ.

$$x \equiv 5 \mod 8 \quad \Leftrightarrow \quad x - 5 = 8k \quad (k \in \mathbb{Z})$$

$1000 = 8 \cdot 125$. よって

$$x - 5 = 124 \cdot 8$$
$$x - 5 = 992$$
$$\therefore x = 997$$

5 命題 5.1 を示せ.

6 命題 5.2 を示せ.

7 次の関係を実感せよ：

$$6 \equiv 30 \mod 8 \begin{cases} \Leftrightarrow & 2 \equiv 10 \mod 8 \\ \Leftrightarrow & 3 \equiv 15 \mod 4 \\ \Leftrightarrow & 42 \equiv 120 \mod 56 \\ \Leftrightarrow & 18 \equiv 90 \mod 8 \\ \not\Leftrightarrow & 3 \equiv 15 \mod 8 \end{cases}$$

8　p を素数、a, b を整数とするとき、次を示せ.

$$ab \equiv 0 \mod p \quad \Rightarrow \quad a \equiv 0 \mod p \quad \text{または} \quad b \equiv 0 \mod p$$

9　整数 a, b について，a は 7 で割ると 3 余り，b は 7 で割ると 4 余るという．このとき，次の数を 7 で割ったときの余りを求めよ.

(1)　$a + 2b$　　(2)　a^4

10　ビッグバン宇宙論によると、我々の宇宙空間は、今から 138 億年前 (138×10^8 年前) に開闢した．1 念を 365 日として，今日からちょうど 138 億年前にあった宇宙の誕生日は何曜日だったかを答えよ.

11　10 進法で表された数の，奇数位の数字の和と，偶数位の数字の和，の差が 11 で割りきれるとき，もとの整数は 11 で割りきれることが知られている．これを，5 桁の整数について示せ.

12　次の等式の ◯ に入る数字を定めるために，両辺を 9 で評価する方法を用いよ

$$7653 \times 3975 = 304 \bigcirc 0675 .$$

13　次の等式の中の ◯ に入る数字を定める：

$$172195 \times 572167 = 985242 \bigcirc 6565 .$$

(1)　両辺を法 9 で評価せよ.

(2)　(1) では答えが 1 つに定まらなかった．しからば，法 11 で評価せよ.

14　次の合同式を示せ.

$$1^{30} + 2^{30} + \cdots + 10^{30} \equiv -1 \mod 11$$

15　ISBN のチェックディジットについて考える.

(1)　手元にある本の ISBN について，チェックディジットを確認せよ.

(2)　バーコードのある 1 つの数字を読み間違えたとする．この間違いのまま，チェックディジットを計算すると，その値は，必ず，本物と異なる値となることを示せ.

(3)　バーコードの読み取り機が，ある連続する 2 桁の数を反対に読み取ってしまった．この場合は，チェックディジットを用いた間違いの感知率は 100% ではない．その理由を答えよ.

p.93

1 次の重要な日の曜日を求めよ.

(1) グレゴリウス暦が実施された 1582 年 10 月 15 日.

(2) 今年 150 周年を迎える，大政奉還 1867 年 11 月 9 日.

(3) 日本がグレゴリウス暦を採用した 1873 年 1 月 1 日.

(4) 佛大の開学日 1910 年 10 月 23 日.

p.100

1 次の合同式を与えられた法の下で解け.

(1) $7x \equiv 4 \mod 12$ (2) $13x \equiv 5 \mod 8$ (3) $15x \equiv 1 \mod 101$

(4) $128x \equiv 833 \mod 1001$ (5) $987x \equiv 610 \mod 1597$

(1)

$$
\begin{aligned}
7x &\equiv 4 \mod 12 \\
35x &\equiv 20 \mod 12 \\
35x &\equiv 8 \mod 12 \\
36x &\equiv 0 \mod 12 \\
x &\equiv -8 \mod 12 \\
&\equiv 4 \mod 12
\end{aligned}
$$

(2)

$$
\begin{aligned}
13x &\equiv 5 \mod 8 \\
39 &\equiv 15 \mod 8 \\
39x &\equiv 7 \mod 8 \\
8x &\equiv 0 \mod 8 \\
40x &\equiv 0 \mod 8 \\
x &\equiv -7 \mod 8 \\
&\equiv 1 \mod 8
\end{aligned}
$$

(3)

$$
\begin{aligned}
15x &\equiv 1 \mod 101 \\
105x &\equiv 7 \mod 101 \\
101x &\equiv 0 \mod 101 \\
4x &\equiv 7 \mod 101 \\
16x &\equiv 28 \mod 101 \\
x &\equiv 27 \mod 101
\end{aligned}
$$

(4)

$$
\begin{aligned}
1287x &\equiv 833 \mod 1001 \\
1001x &\equiv 0 \mod 1001 \\
873 &\equiv -1833 \mod 1001 \\
&\equiv 168 \mod 1001 \\
869x &\equiv 5831 \mod 1001 \\
&\equiv 826 \mod 1001 \\
23x &\equiv 658 \mod 1001 \\
115x &\equiv 3290 \mod 1001 \\
&\equiv 287 \mod 1001 \\
13x &\equiv 546 \mod 1001 \\
10x &\equiv 112 \mod 1001 \\
1000x &\equiv 11200 \mod 1001 \\
x &\equiv -189 \mod 1001 \\
&\equiv 812 \mod 1001
\end{aligned}
$$

(5)

$$987x \equiv 610 \mod 1597$$

2　次の合同式を与えられた法の下で解け.

(1)　$12x \equiv 5 \mod 6$　　(2)　$3x \equiv 6 \mod 12$　　(3)　$123x \equiv 456 \mod 789$

(1)

$\gcd(12, 6) = 2,\ 2 \nmid 5$ より解なし.

(2)

$$\begin{aligned} 3x &\equiv 6 \mod 12 \\ x &\equiv \mod 4 \\ x &= 2 + 4t \\ &= 2, 6, 10 \end{aligned}$$

(3)

$$\begin{aligned} 123x &\equiv 456 \mod 789 \\ 41x &\equiv 152 \mod 263 \\ 263x &\equiv 0 \mod 263 \\ 246 &\equiv 912 \mod 263 \\ &\equiv 123 \mod 263 \\ 17x &\equiv -123 \mod 263 \\ &\equiv 140 \mod 263 \\ 51x &\equiv 420 \mod 263 \\ &\equiv 157 \mod 263 \\ 10x &\equiv 5 \mod 263 \\ 40x &\equiv 20 \mod 263 \\ x &\equiv 132 \mod 263 \\ x &= 132 + 263t \\ &= 132,\ 395,\ 658 \end{aligned}$$

3　次の方程式の整数解について，その一般解を求めよ.

(1)　$13x + 14y = 9$　　(2)　$7x + 18y = 208$　　(3)　$258x + 147y = 369$

(1)

$13x + 14y = 9$

$$\begin{aligned} 13x &\equiv 9 \mod 14 \\ 14x &\equiv 0 \mod 14 \\ x &\equiv -9 \mod 14 \end{aligned}$$

よって

$$\begin{aligned} 14 \cdot 13t - 13 \cdot 9 + 14y &= 9 \\ 14 \cdot (13 - y) &= 14 \cdot 9 \\ 13t - y &= 9 \\ y &= 13t + 9 \end{aligned}$$

(2)

$7x + 18y = 208$

$$\begin{aligned} 7x &\equiv 208 \mod 18 \\ &\equiv 10 \mod 18 \\ 18x &\equiv 0 \mod 18 \\ 14x &\equiv 20 \mod 18 \\ 14x &\equiv 2 \mod 18 \\ 21x &\equiv 30 \mod 18 \\ &\equiv 12 \mod 18 \\ 3x &\equiv 12 \mod 18 \\ x &\equiv 4 \mod 18 \\ \therefore x &= 18t + 4 \end{aligned}$$

よって

$$\begin{aligned} 7 \cdot 18t + 7 \cdot 4 + 18y &= 208 \\ 7 \cdot 18t + 18y &= 180 \\ 7t + y &= 10 \\ y &= -7t + 10 \end{aligned}$$

(3)

$258x + 147y = 369 \quad \therefore 86x + 49y = 123$

$$\begin{aligned} 86x &\equiv 123 \mod 49 \\ &\equiv 25 \mod 49 \\ 49x &\equiv 0 \mod 49 \\ 98x &\equiv 0 \mod 49 \\ 12x &\equiv -25 \mod 49 \\ &\equiv 24 \mod 49 \\ 48x &\equiv 96 \mod 49 \\ &\equiv -2 \mod 49 \\ x &\equiv 2 \mod 49 \\ \therefore x &= 49t + 2 \end{aligned}$$

よって

$$\begin{aligned} 86(49t + 2) + 49y &= 123 \\ 86 \cdot 49t + 172 + 49y &= 123 \\ 86 \cdot 49t + 49y &= -49 \\ 86t + y &= -1 \\ y &= -86t - 1 \end{aligned}$$

4　50 人が登録している講義で計算用紙を一人に 30 枚ずつ配った．500 枚一組でまとめておいた計算用紙の束をいくつか持ってきたのだが，配り終わったら 10 枚ずつ余っていた．講義に参加していた学生は 50 人中何人だったのか．

$500x - 30y = 10 \quad \therefore 50x - 3y = 1$ より

$$\begin{aligned} 50x &\equiv 1 \mod 3 \\ 3x &\equiv 0 \mod 3 \\ 51x &\equiv 0 \mod 3 \\ x &\equiv -1 \mod 3 \\ &\equiv 2 \mod 3 \\ \therefore x &= 3t + 2 \end{aligned}$$

よって

$$\begin{aligned} 50(3t + 2) - 3y &= 1 \\ 150t + 100 - 3y &= 1 \\ -3y &= -150t - 99 \\ y &= 50t + 33 \end{aligned}$$

よって $t = 0$ のとき $y = 33$ で 33 人.

5　次の方程式の整数解について，その一般解を求めよ．

$$6x + 10y + 15z = 7$$

p.108

1　次の問題を解け．

今ここに物が有るが其の数を知らない
其の数を 3 ずつ数えれば 2 余り
其の数を 5 ずつ数えれば 3 余り
其の数を 7 ずつ数えれば 2 余る
ここに物は何個あるか？

$$(☆)\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$$

解くべき合同式は

$$\begin{cases} 35x \equiv 1 \mod 3 \\ 21x \equiv 1 \mod 5 \\ 15x \equiv 1 \mod 7 \end{cases}$$

よって

$$\begin{aligned} 35x &\equiv 1 \mod 3 \\ 36x &\equiv 0 \mod 3 \\ x &\equiv -1 \mod 3 \\ x &\equiv 2 \mod 3 \end{aligned} \qquad \begin{aligned} 21x &\equiv 1 \mod 5 \\ 20x &\equiv 0 \mod 5 \\ x &\equiv \mod 5 \end{aligned} \qquad \begin{aligned} 15x &\equiv 1 \mod 7 \\ 14x &\equiv 0 \mod 7 \\ x &\equiv 1 \mod 7 \end{aligned}$$

これより

$$(★)\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases}$$

(☆), (★) より

$$\begin{aligned} c &= 5 \cdot 7 \cdot 2 \cdot 2 + 3 \cdot 7 \cdot 1 \cdot 3 + 3 \cdot 5 \cdot 1 \cdot 2 \\ &\equiv 233 \mod 105 \\ &\equiv 23 \mod 105 \end{aligned}$$

2 次の連立合同式を解け.

(1) $\begin{cases} 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases}$ (2) $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 6 \mod 11 \end{cases}$

(1)

$$\begin{aligned} 2x &\equiv 1 \mod 5 \\ 4x &\equiv 2 \mod 5 \\ 5x &\equiv 0 \mod 5 \\ x &\equiv -2 \mod 5 \\ x &\equiv 3 \mod 5 \end{aligned} \qquad \begin{aligned} 3x &\equiv 4 \mod 7 \\ 6x &\equiv 8 \mod 7 \\ 6x &\equiv 1 \mod 7 \\ 7x &\equiv 0 \mod 7 \\ x &\equiv -1 \mod 7 \\ x &\equiv 6 \mod 7 \end{aligned}$$

よって

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}$$

$x = 5s + 3$ と書けるので

$$\begin{aligned} 5s + 3 &\equiv 6 \mod 7 \\ 5s &\equiv 3 \mod 7 \\ 20s &\equiv 12 \mod 7 \\ 20s &\equiv 5 \mod 7 \\ 21s &\equiv 0 \mod 7 \\ s &\equiv -5 \mod 7 \\ s &\equiv 2 \mod 7 \\ \therefore s &= 7t + 2 \end{aligned}$$

ゆえに

$$\begin{aligned} x &= 5(7t + 2) + 3 \\ &= 35t + 13 \\ \therefore x &\equiv 13 \mod 35 \end{aligned}$$

(2)

$$\begin{cases} x \equiv 1 \mod 3 & \cdots\cdots ① \\ x \equiv 2 \mod 5 & \cdots\cdots ② \\ x \equiv 6 \mod 11 & \cdots\cdots ③ \end{cases}$$

①より $x = 3x + 1$ を②へ代入して

$$
\begin{aligned}
3s + 1 &\equiv 2 \mod 5 \\
3x &\equiv 1 \mod 5 \\
21s &\equiv 7 \mod 5 \\
21s &\equiv 2 \mod 5 \\
20s &\equiv 0 \mod 5 \\
s &\equiv 2 \mod 5 \\
\therefore s &= 5t + 2
\end{aligned}
$$

よって

$$
\begin{aligned}
x &= 3(5t + 2) + 1 \\
&= 15t + 7 \\
\therefore x &\equiv 7 \mod 15
\end{aligned}
$$

$x = 15t + 7$ を③へ代入して

$$
\begin{aligned}
15t + 7 &\equiv 6 \mod 11 \\
15t &\equiv -1 \mod 11 \\
15t &\equiv 10 \mod 11 \\
11t &\equiv 0 \mod 11 \\
4t &\equiv 10 \mod 11 \\
12t &\equiv 30 \mod 11 \\
12t &\equiv 8 \mod 11 \\
3t &\equiv 2 \mod 11 \\
t &\equiv 8 \mod 11 \\
\therefore t &= 11u + 8
\end{aligned}
$$

よって

$$
\begin{aligned}
x &= 15(11u + 8) + 7 \\
&= 165u + 127 \\
\therefore x &\equiv 127 \mod 165
\end{aligned}
$$

3 中国の剰余定理を示せ：

$\gcd(m, n) = 1$ なる整数 m, n について，$x \equiv a \mod m$，$x \equiv b \mod n$ を同時に満たす解が法 mn の下で存在する．

4 次の連立合同式を解け.

(1) $\begin{cases} 2x \equiv 3 \mod 5 \\ 3x \equiv 4 \mod 8 \\ 4x \equiv 5 \mod 9 \end{cases}$

(2) $\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 2 \mod 7 \\ x \equiv 3 \mod 9 \\ x \equiv 4 \mod 11 \end{cases}$

(1)

$2x \equiv 3 \mod 5$
$4x \equiv 6 \mod 5$
$4x \equiv 1 \mod 5$
$5x \equiv 0 \mod 5$
$x \equiv -1 \mod 5$
$x \equiv 4 \mod 5$

$3x \equiv 4 \mod 8$
$9x \equiv 12 \mod 8$
$9x \equiv 4 \mod 8$
$8x \equiv 0 \mod 8$
$x \equiv 4 \mod 8$

$4x \equiv 5 \mod 9$
$8x \equiv 10 \mod 9$
$8x \equiv 1 \mod 9$
$9x \equiv 0 \mod 9$
$x \equiv -1 \mod 9$
$x \equiv 8 \mod 9$

より

$$(\text{☆}) \begin{cases} x \equiv 4 \mod 5 \\ x \equiv 4 \mod 8 \\ x \equiv 8 \mod 9 \end{cases}$$

よって解くべき連立合同式は

$$\begin{cases} 72x \equiv 1 \mod 5 \\ 45x \equiv 1 \mod 8 \\ 40x \equiv 1 \mod 9 \end{cases}$$

それぞれを解いて

$45x$

よって

$$(\bigstar) \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 8 \\ x \equiv 7 \mod 9 \end{cases}$$

(☆), (★) 以上より

$$\begin{aligned} c &= 72 \cdot 12 + 45 \cdot 20 + 40 \cdot 56 \\ &\equiv 4004 \mod 360 \\ &\equiv 44 \mod 360 \end{aligned}$$

(2)

$$(\text{☆})\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 2 \mod 7 \\ x \equiv 3 \mod 9 \\ x \equiv 4 \mod 11 \end{cases}$$

解くべき合同式は

$$\begin{cases} 693x \equiv 1 \mod 5 \\ 495x \equiv 1 \mod 7 \\ 385x \equiv 1 \mod 9 \\ 315 \equiv 1 \mod 11 \end{cases}$$

それぞれ解くと

$693x \equiv 1 \mod 5$
$690x \equiv 0 \mod 5$
$3x \equiv 1 \mod 5$
$695x \equiv 0 \mod 5$
$2x \equiv -1 \mod 5$
$2x \equiv 4 \mod 5$
$x \equiv -3 \mod 5$
$x \equiv 2 \mod 5$

$495x \equiv \mod 7$
$490 \equiv 0 \mod 7$
$5x \equiv 1 \mod 7$
$497 \equiv 0 \mod 7$
$2x \equiv -1 \mod 7$
$2x \equiv 6 \mod 7$
$3x \equiv -5 \mod 7$
$3x \equiv 2 \mod 7$
$x \equiv -4 \mod 7$
$x \equiv 3 \mod 7$

$385x \equiv \mod 9$
$378x \equiv 0 \mod 9$
$7x \equiv 1 \mod 9$
$387x \equiv 0 \mod 9$
$2x \equiv -1 \equiv 8 \mod 9$
$5x \equiv -7 \mod 9$
$5x \equiv 2 \mod 9$
$4x \equiv 16 \mod 9$
$4x \equiv 7 \mod 9$
$x \equiv -5 \mod 9$
$x \equiv 4 \mod 9$

$315x \equiv 1 \mod 11$
$308x \equiv 0 \mod 11$
$7x \equiv 1 \mod 11$
$319x \equiv 0 \mod 11$
$4x \equiv -1 \mod 11$
$4x \equiv 10 \mod 11$
$3x \equiv -9 \mod 11$
$3x \equiv 2 \mod 11$
$6x \equiv 4 \mod 11$
$x \equiv -3 \mod 11$
$x \equiv 8 \mod 11$

よって

$$(\text{★})\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 4 \mod 9 \\ x \equiv 4 \mod 11 \end{cases}$$

(☆), (★) より

$$\begin{aligned} c &= 7 \cdot +9 \cdot 11 \cdot 1 \cdot 2 + 5 \cdot 9 \cdot 11 \cdot 2 \cdot 3 + 5 \cdot 7 \cdot 11 \cdot 3 \cdot 4 + 5 \cdot 7 \cdot 9 \cdot 4 \cdot 8 = 1386 + 2970 + 4620 + 10080 \\ &\equiv 19056 \mod 3465 \\ &\equiv 1731 \mod 3465 \end{aligned}$$

5 命題 7.1 を示せ.

6 次の合同式を与えられた法の下で解け.

(1) $5x \equiv 12 \mod 1512$ (2) $3x \equiv 8 \mod 1133$

(1)

$1512 = 2^3 \cdot 3^2 \cdot 7 = 56 \cdot 27$. よって

$$\begin{cases} 5x \equiv 12 \mod 56 \\ 5x \equiv 12 \mod 27 \end{cases}$$

それぞれ解いて

$$\begin{aligned} 5x &\equiv 12 \mod 56 \\ 55x &\equiv 132 \mod 56 \\ 55x &\equiv 20 \mod 56 \\ 56x &\equiv 0 \mod 56 \\ x &\equiv -20 \mod 56 \\ x &\equiv 36 \mod 56 \end{aligned}$$

$$\begin{aligned} 5x &\equiv 12 \mod 27 \\ 25x &\equiv 60 \mod 27 \\ 25x &\equiv 6 \mod 27 \\ 27x &\equiv 0 \mod 27 \\ 2x &\equiv -6 \mod 27 \\ 4x &\equiv -12 \mod 27 \\ x &\equiv 24 \mod 27 \end{aligned}$$

よって

$$\begin{cases} x \equiv 36 \mod 56 \\ x \equiv 24 \mod 27 \end{cases}$$

よって解くべき合同式は

$$\begin{cases} 27x \equiv 1 \mod 56 \\ 56x \equiv 1 \mod 27 \end{cases}$$

それぞれ解いて

$$\begin{aligned} 27x &\equiv 1 \mod 56 \\ 54x &\equiv 2 \mod 56 \\ 56x &\equiv 0 \mod 56 \\ 2x &\equiv -2 \mod 56 \\ 26x &\equiv -26 \mod 56 \\ x &\equiv 27 \mod 56 \end{aligned}$$

$$\begin{aligned} 56x &\equiv \mod 27 \\ 54x &\equiv 0 \mod 27 \\ 2x &\equiv 1 \mod 27 \\ 27x &\equiv 0 \mod 27 \\ 26x &\equiv 13 \mod 27 \\ x &\equiv -13 \mod 27 \\ x &\equiv 14 \mod 27 \end{aligned}$$

よって

$$\begin{cases} x \equiv 27 \mod 56 \\ x \equiv 14 \mod 27 \end{cases}$$

(☆), (★) より

$$\begin{aligned} c &= 27 \cdot 36 \cdot 27 + 56 \cdot 24 \cdot 14 = 26244 + 18816 \\ &\equiv 45060 \mod 1512 \\ &\equiv 1212 \mod 1512 \end{aligned}$$

(2)

$1133 = 11 \cdot 103$ より

$$\begin{cases} 3x \equiv 8 \mod 11 \\ 3x \equiv 8 \mod 103 \end{cases}$$

それぞれ解いて

$$\begin{aligned} 3x &\equiv 8 \mod 11 \\ 9x &\equiv 24 \mod 11 \\ 9x &\equiv 2 \mod 11 \\ 11x &\equiv 0 \mod 11 \\ 2x &\equiv -2 \mod 11 \\ x &\equiv 10 \mod 11 \end{aligned} \qquad \begin{aligned} 3x &\equiv 8 \mod 103 \\ 102x &\equiv 272 \mod 103 \\ 102x &\equiv 66 \mod 103 \\ 103x &\equiv 0 \mod 103 \\ x &\equiv -66 \mod 103 \\ x &\equiv 37 \mod 103 \end{aligned}$$

よって

$$(☆) \begin{cases} x \equiv 10 \mod 11 \\ x \equiv 37 \mod 103 \end{cases}$$

解くべき合同式は

$$\begin{cases} 103x \equiv 1 \mod 11 \\ 11x \equiv 1 \mod 103 \end{cases}$$

それぞれ解いて

$$\begin{aligned} 103x &\equiv 1 \mod 11 \\ 99x &\equiv 0 \mod 11 \\ 4x &\equiv 1 \mod 11 \\ 110x &\equiv 0 \mod 11 \\ 7x &\equiv -1 \mod 11 \\ 3x &\equiv -2 \mod 11 \\ x &\equiv 3 \mod 11 \end{aligned} \qquad \begin{aligned} 11x &\equiv 1 \mod 103 \\ 110x &\equiv 10 \mod 103 \\ 103x &\equiv 0 \mod 103 \\ 7x &\equiv 10 \mod 103 \\ 4x &\equiv -9 \mod 103 \\ 3x &\equiv 19 \mod 103 \\ x &\equiv -28 \mod 103 \\ x &\equiv 75 \mod 103 \end{aligned}$$

よって

$$(\bigstar)\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 75 \mod 103 \end{cases}$$

(☆), (★) より

$$\begin{aligned} c &= 103 \cdot 10 \cdot 3 + 11 \cdot 37 \cdot 75 = 3090 + 30525 \\ &\equiv 33615 \mod 1133 \\ &\equiv 758 \mod 1133 \end{aligned}$$

7 次の連立合同式を解け.

(1) $\begin{cases} x \equiv 3 \mod 3 \\ x \equiv 5 \mod 24 \end{cases}$ (2) $\begin{cases} x \equiv 5 \mod 6 \\ x \equiv 3 \mod 10 \\ x \equiv 8 \mod 15 \end{cases}$ (3) $\begin{cases} x \equiv 2 \mod 6 \\ x \equiv 4 \mod 8 \\ x \equiv 2 \mod 14 \\ x \equiv 14 \mod 15 \end{cases}$

p.113

1 次の数の法 11 の下での逆元を求めよ.

(1) 2 (2) 3 (3) 5 (4) 7 (5) 10

(1)

$$\begin{aligned} 2 \cdot 6 &\equiv 12 \mod 11 \\ &\equiv 1 \mod 11 \end{aligned}$$

よって 6.

(2)

$$\begin{aligned} 3 \cdot 4 &\equiv 12 \mod 12 \\ &\equiv 1 \mod 12 \end{aligned}$$

よって 4.

(3)

$$\begin{aligned} 5 \cdot 9 &\equiv 45 \mod 11 \\ &\equiv 1 \mod 11 \end{aligned}$$

よって 8.

(4)

$$\begin{aligned} 10 \cdot 10 &\equiv 100 \mod 11 \\ &\equiv 1 \mod 11 \end{aligned}$$

よって 10.

2　円周を p 等分する p 個の点を考える．ここで，p は素数とする．この p 個の点を結んで閉じた図形をつくる．

(1)　可能な形の総数を求めよ．($p = 5$ では 12 個．)

(2)　(1) で求めた図形のうち，円の中心を中心とした角度 $\dfrac{2\pi}{p}$ の回転の下で不変な図形は何個あるか．($p = 5$ では 2 個，$p = 7$ では 3 個．)

(3)　次の等式を $p = 5$ のときの図を見ながら実感せよ：

$$\text{((1) で得られた数)} - \text{((2) で得られた数)} = \left(\frac{2\pi}{p}\text{回転で移り変わる } p \text{ 個}\right) \times (\text{「独立」な形の数 (種類)})$$

上式から，ウィルソンの定理を示せ．

3　ウィルソンの定理の逆，つまり，以下の命題を示せ：

自然数 n が $(n-1)! \equiv -1 \mod n$ を満たすとすると，n は素数である．

4　次の問いに答えよ．

(1)　49! を 53 で割った余りを求めよ．

(2)　$8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ を 7 で割った余りを求めよ．

(1)

53 は素数

$$52! \equiv -1 \mod 53$$

よって

$$52 \cdot 51 \cdot 50 \cdot 49! \equiv -1 \mod 53$$

$19! = x$ とすると

$$52 \cdot 51 \cdot 50x \equiv -1 \mod 53$$

$52 \equiv -1 \mod 53$, $51 \equiv -2 \mod 53$, $50 \equiv -3 \mod 53$ より

$$\begin{aligned}(-1)(-2)(-3)x &\equiv -1 \mod 53\\ -6x &\equiv -1 \mod 53\\ 6x &\equiv 1 \mod 53\\ 54x &\equiv 9 \mod 53\\ 23x &\equiv 0 \mod 53\\ x &\equiv 9 \mod 53\end{aligned}$$

(2)

$9 \cdot 11 \equiv 99 \equiv 1 \mod 7$, $10 \cdot 12 = 120 \equiv 1 \mod 7$ より

$$\begin{aligned} & 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \mod 7 \\ & \equiv 8 \cdot (9 \cdot 11) \cdot (10 \cdot 12) \cdot 13 \mod 7 \\ & \equiv 8 \cdot 1 \cdot 1 \cdot 13 \equiv 8 \cdot 13 \mod 7 \\ & \equiv 104 \mod 7 \\ & \equiv 6 \mod 7 \end{aligned}$$

p.116

1　a, b を整数とし，p を素数とするとき，次が成り立つことを示せ.

$$(a_1 + a_2 + \cdots + a_n)^p \equiv {a_1}^p + {a_2}^p + \cdots + {a_n}^p \mod p$$

$a = 2$ のとき

$$(a_1 + a_2)^p \equiv {a_1}^p + {a_2}^p \mod p$$

が成り立つ．$n = k$ のとき

$$(a_1 + a_2 + \cdots + a_k)^p = {a_1}^p + {a_2}^p + \cdots + {a_k}^p$$

が成り立つとすると，$n = k + 1$ のとき

$$\begin{aligned} (a_1 + a_2 + \cdots + a_k + a_{k+1})^p &= \{(a_1 + a_2 + \cdots + a_k) + a_{k+1}\}^p \\ &= (a_1 + a_2 + \cdots + a_k)^p + {a_{k+1}}^p + \sum_{l=1}^{p-1} {}_pC_l (a_1 + \cdots + a_k)^{p-l} {a_{k+1}}^l \\ &= (a_1 + a_2 + \cdots + a_k)^p + {a_{k+1}}^p \\ &= {a_1}^p + {a_2}^p + \cdots + {a_k}^p + {a_{k+1}}^p \end{aligned}$$

□

2　次の問いに答えよ.

(1)　10^{222} を 23 で割った余りを求めよ.

(2)　$5^{7407} - 13$ が 7 で割りきれることを示せ.

(1)

$10^{22} \equiv 1 \mod 23$.

$$10^{222} = 10^{22\cdot10+2} = 10^{22\cdot10}\cdot10^2 \equiv 1\cdot10^2 \mod 23$$
$$\equiv 100 \mod 23$$
$$\equiv 8 \mod 23$$

(2)

$5^6 \equiv 1 \mod 7$.

$$5^{7407} = 5^{6\cdot1234+3} = 5^{6\cdot1234}\cdot5^3 \equiv 1\cdot5^3 \mod 7$$
$$\equiv 125 \mod 7$$
$$\equiv 6 \mod 7$$
$$\equiv 13 \mod 7$$

よって

$$5^{7407} - 13 \equiv 0 \mod 7$$

3 3 を除く素数に対して $p^2 \equiv 1 \mod 3$ となることを示し，異なる 3 個の素数の平方の和は素数になり得ないことを示せ.

4 素数 p を分母とする単位分数 $\frac{1}{p}$ を考える．p が 2, 5 の場合は，$\frac{1}{p}$ は有限小数となるが，それ以外の素数 p のとき循環小数 $\frac{1}{p}$ の循環節の長さ n は $p-1$ の約数となると主張する 定理 2.2 を示せ.

p.123

1 次の問いに答えよ.

(1) オイラー関数 $\varphi(22)$ を求めよ.

(2) 2017^{2017} を 22 で割った余りを求めよ.

(1)

$$\varphi(22) = \varphi(11)\varphi(2) \qquad (\gcd(11,2) = 1)$$
$$= 10\cdot1 = 10$$

(2)

$$2017^{\varphi(22)} \equiv 1 \mod 22$$
$$\therefore 2017^{10} \equiv 1 \mod 22$$

$2017^{2017} = 2017^{10\cdot201+7} = 2017^{10\cdot201}\cdot2017^7 \equiv 1\cdot2017^7 \mod 22$, $2017 \equiv 15 \mod 22$ より

$$
\begin{aligned}
2017 &\equiv -7 \mod 22 \\
2017^2 &\equiv 49 \mod 22 \\
&\equiv 5 \mod 22 \\
2017^3 &\equiv -35 \mod 22 \\
&\equiv -13 \mod 22 \\
2017^4 &\equiv 91 \mod 22 \\
&\equiv 3 \mod 22 \\
2017^5 &\equiv -21 \mod 22 \\
&\equiv 1 \mod 22 \\
2017^6 &\equiv -7 \mod 22 \\
2017^7 &\equiv 49 \mod 22 \\
&\equiv 5 \mod 22
\end{aligned}
$$

よって 5.

2 次のオイラー関数を求めよ

(1) $\varphi(100)$ (2) $\varphi(720)$ (3) $\varphi(20!)$

(1)

$100 = 2^2 \cdot 5^2$

$$
\begin{aligned}
\varphi(100) &= 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} \\
&= 40
\end{aligned}
$$

(2)

$720 = 2^4 \cdot 3^2 \cdot 5$

$$
\begin{aligned}
\varphi(720) &= 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) \\
&= 720 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 24 \cdot 8 \\
&= 192
\end{aligned}
$$

(3)

$20! = 2^{18} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

$$\begin{aligned}\varphi(20!) &= 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \\ &\quad \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{17}\right)\left(1-\frac{1}{19}\right) \\ &= 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} \\ &= 2^{18} \cdot 3^8 \cdot 5^3 \cdot 7 \cdot 2 \cdot 2^2 \cdot 2 \cdot 2^2 \cdot 3 \cdot 2^4 \cdot 2 \cdot 3^2 \\ &= 2^{29} \cdot 3^{11} \cdot 5^4 \cdot 7\end{aligned}$$

3 次の分数

$$\frac{1}{4536},\ \frac{2}{4536},\ \frac{3}{4536},\ \cdots,\ \frac{4535}{4536},\ \frac{4536}{4536}$$

の中に既約分数はいくつあるか.

4 次の問いに答えよ.

(1) 123^{123} の下 2 桁を求めよ.

(2) 3^{100} を 7 進数展開したときの 1 桁目，2 桁目の数を求めよ.

5 合成数 N を分母とする単位分数 $\frac{1}{N}$ を考える．これを小数表示したとき，その循環節の長さがオイラー関数 $\varphi(N)$ の約数となることを示せ.

p.129

1 繰り返し自乗法を用いて以下の数を評価せよ.

(1) $5^{13} \mod 23$　　(2) $7^{327} \mod 853$

2 命題 11.1 を示せ.

3　オイラーの定理やフェルマーの小定理を用いて次の合同式を与えられた法の下で解け.

(1)　$7x \equiv 12 \mod 17$　　(2)　$4x \equiv 7 \mod 15$

(1)

$$7x \equiv 12 \mod 17$$
$$x \equiv 7^{\varphi(17)-1} \cdot 12 \equiv 7^{15} \cdot 12 \mod 17$$

より

$$7 \cdot 12 \equiv 84 \mod 17$$
$$\equiv -1 \mod 17$$
$$7^3 \cdot 12 \equiv -49 \equiv 2 \mod 17$$
$$7^4 \cdot 12 \equiv 14 \equiv 3 \mod 17$$
$$7^5 \cdot 12 \equiv 21 \equiv 4 \mod 17$$
$$7^6 \cdot 12 \equiv 28 \equiv 6 \mod 17$$
$$7^7 \cdot 12 \equiv 42 \equiv 8 \mod 17$$
$$7^8 \cdot 12 \equiv 56 \equiv 5 \mod 17$$
$$7^9 \cdot 12 \equiv 35 \equiv 1 \mod 17$$
$$7^{10} \cdot 12 \equiv 7 \mod 17$$
$$7^{11} \cdot 12 \equiv 49 \mod 17$$
$$7^{12} \cdot 12 \equiv -2 \mod 17$$
$$7^{13} \cdot 12 \equiv -14 \equiv 3 \mod 17$$
$$7^{14} \cdot 12 \equiv 21 \equiv 4 \mod 17$$
$$7^{15} \cdot 12 \equiv 28 \mod 17$$
$$\equiv 9 \mod 17$$

(2)

$$4x \equiv 7 \mod 15$$
$$x \equiv 4^{\varphi(15)} \cdot 7 \mod 15$$
$$\equiv 4^7 \cdot 7 \mod 15$$

より

$$4 \cdot 7 \equiv -2 \mod 15$$
$$4^2 \cdot 7 \equiv -8 \mod 15$$
$$4^3 \cdot 7 \equiv -32 \equiv -2 \mod 15$$
$$4^4 \cdot 7 \equiv -8 \mod 15$$
$$4^5 \cdot 7 \equiv -2 \mod 15$$
$$4^6 \cdot 7 \equiv -8 \equiv 7 \mod 15$$
$$4^7 \cdot 7 \equiv 28 \mod 15$$
$$\equiv 13 \mod 15$$

4 次の合同式を与えられた法の下で解け.

(1) $x^{11} \equiv 13 \mod 35$　　(2) $x^{7} \equiv 11 \mod 63$　　(3) $x^{131} \equiv 758 \mod 1073$ $(1073 = 29 \cdot 37)$

(1)

$\varphi(35) = \varphi(7)\varphi(5) = 6 \cdot 4 = 24$

$$
\begin{aligned}
11\bar{k} &\equiv 1 \mod 24 \\
22\bar{k} &\equiv 2 \mod 24 \\
24\bar{k} &\equiv 0 \mod 24 \\
2\bar{k} &\equiv -2 \mod 24 \\
10\bar{k} &\equiv -10 \mod 24 \\
\bar{k} &\equiv 11 \mod 24
\end{aligned}
$$

よって $x \equiv 13^{11} \mod 35$. $11 = 2^3 + 2^1 + 2^0$ より

$$
\begin{aligned}
13 &\equiv 13 \mod 35 \\
13^2 &\equiv 169 \equiv -6 \mod 35 \\
13^4 &\equiv 36 \equiv 1 \mod 35 \\
13^4 &\equiv 36 \equiv 1 \mod 35
\end{aligned}
$$

従って

$$
\begin{aligned}
x \equiv 13^{11} &\equiv 13 \cdot 29 \cdot 11 \mod 35 \\
&\equiv 377 \mod 35 \\
&\equiv 27 \mod 35
\end{aligned}
$$

(2)

$\varphi(7) = 6$

$$
\begin{aligned}
7\bar{k} &\equiv 1 \mod 6 \\
6\bar{k} &\equiv 0 \mod 6 \\
\bar{k} &\equiv 11 \mod 6
\end{aligned}
$$

よって

$$
\begin{aligned}
x &\equiv 11^{1} \mod 63 \\
&\equiv 11 \mod 63
\end{aligned}
$$

(3)

p.133

1	6	6	8	5	4	2	4	7	8
A	L	L	T	H	E	B	E	S	T

ALL THE BEST