佛教大学

代数学演習

問題

Kazuma MATSUDA

2017 年 12 月 20 日

p.15

$\boxed{1}$ 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 $2\mathbb{Z}$

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

$\boxed{3}$ 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：

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

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) $[0] \cdot [3]$ (iv) $[2] \cdot [5]$

(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.

(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：

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

(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.

p.30-31

$\boxed{1}$ $2 = 1$ を導く次の論理の穴を正せ.

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

$\boxed{2}$ $\boldsymbol{a} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $\boldsymbol{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ 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.

$\boxed{3}$ 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.

(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.

$$\frac{3}{5} \div \frac{2}{7} = \frac{3 \times 14 \div 2}{5 \times 14 \div 7} = \frac{3 \times 7}{5 \times 2} = \frac{21}{10}$$

(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.

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

$\boxed{4}$ 命題 2.1 を証明せよ.

$\boxed{5}$ 有理数は小数表示し，循環小数は有理数表示せよ.

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

$\boxed{6}$ 次の数の連分数表示を求めよ.

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

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

$\boxed{8}$ 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.

p46-47

$\boxed{1}$　次の集合 R を考える：

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

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 : $(a_1, b_1) \cdot (a_2, b_2) = (a_1b_1, a_2b_2)$.

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

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

が成り立つことを示せ.

$\boxed{3}$　体の公理から

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

を示せ.

$\boxed{4}$　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)　$\dfrac{9 + 7\sqrt{5}}{p + q\sqrt{5}} = 3 - \sqrt{5}$

$\boxed{5}$　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.

$\boxed{6}$　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)　$\dfrac{4 + 5\sqrt[3]{2}}{1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}}$

$\boxed{7}$　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.

$\boxed{8}$　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.

p.59

$\boxed{1}$　次を示せ.

(1)　$7 \mid 343$　　(2)　$2017 \mid 0$

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

$\boxed{3}$　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.

$\boxed{4}$　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.

$\boxed{5}$　数学的帰納法を用いて次を示せ.

$$9 \mid (4^n + 15n - 1)\ .$$

$\boxed{6}$　次の数を 2 進数表示せよ.

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

$\boxed{7}$　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)　$(10111)_{(2)} \div (11)_{(2)}$

$\boxed{8}$　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)

$\boxed{9}$　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)　$(65102)_{(7)} \div (24)_{(7)}$

p.71

$\boxed{1}$ 次の最大公約数を求めよ

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

$\boxed{2}$ (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.

$\boxed{3}$ 次の最大公約数を求めよ.

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

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

$\boxed{4}$ 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) $3313772x + 1587894y = 1078$

$\boxed{5}$ 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

$\boxed{1}$ 1 を素数と呼べないことを説明せよ.

$\boxed{2}$ 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.

$\boxed{3}$ 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.

$\boxed{4}$ 503 が素数であることを示せ.

$\boxed{5}$　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

$\boxed{6}$　次の最小公倍数を求めよ.

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

$\boxed{7}$　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.

$\boxed{8}$　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.

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

$\boxed{10}$　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

$\boxed{1}$　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)　$11 \equiv 98 \mod 8$

$\boxed{2}$　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)　$-321 \mod 101$

$\boxed{3}$　例 5.1 に倣って、整数の集合を法 7 の下で類別せよ.

$\boxed{4}$　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.

$\boxed{5}$　命題 5.1 を示せ.

$\boxed{6}$　命題 5.2 を示せ.

$\boxed{7}$　次の関係を実感せよ：

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

$\boxed{8}$　p を素数、a, b を整数とするとき、次を示せ.

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

$\boxed{9}$　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

$\boxed{10}$　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 $(138 \times 10^8$ 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)　$987x \equiv 610 \mod 1597$

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)　$123x \equiv 456 \mod 789$

$\boxed{3}$　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)　$258x + 147y = 369$

$\boxed{4}$　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．

$\boxed{5}$　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

$\boxed{1}$　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？

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

$\boxed{3}$ 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．

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

$\boxed{5}$　命題 7.1 を示せ．

$\boxed{6}$　次の合同式を与えられた法の下で解け．

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

$\boxed{7}$　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

$\boxed{1}$　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

$\boxed{2}$　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：

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

上式から，ウィルソンの定理を示せ．

$\boxed{3}$　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．

$\boxed{4}$　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．

p.116

$\boxed{1}$　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．

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

$\boxed{2}$　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．

$\boxed{3}$　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.

$\boxed{4}$　素数 p を分母とする単位分数 $\dfrac{1}{p}$ を考える．p が 2, 5 の場合は，$\dfrac{1}{p}$ は有限小数となるが，それ以外の素数 p のとき循環小数 $\dfrac{1}{p}$ 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

$\boxed{1}$　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.

$\boxed{2}$　次のオイラー関数を求めよ

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

$\boxed{3}$　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.

$\boxed{4}$　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.

$\boxed{5}$　合成数 N を分母とする単位分数 $\dfrac{1}{N}$ 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

$\boxed{1}$　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)　$7^{327} \mod 853$

$\boxed{2}$　命題 11.1 を示せ.

$\boxed{3}$　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)　$4x \equiv 7 \mod 15$

$\boxed{4}$　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)　$x^{131} \equiv 758 \mod 1073$ $(1073 = 29 \cdot 37)$

p.133