2024年度　科学リテラシー　期末試験　問題用紙（両面1枚）

1 次の文章の空欄を埋めよ．ただし，解答の選択肢を $\forall$, $\exists$, $\subset$, $\in$, $\cap$, $\cup$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ のいずれかとする．

「任意の…」を表す記号は（　(1)　）であり，「…が存在する」を表す記号は（　(2)　）である．あるものが集合に「属する」ときに用いられる記号は（　(3)　）であり，ふたつの集合間に「部分集合である」という関係があるときに用いられる記号は（　(4)　）である．ふたつの集合の共通部分を表す記号は（　(5)　）であり，和集合を表す記号は（　(6)　）である．整数全体の集合を表す記号は（　(7)　）であり，有理数全体の集合を表す記号は（　(8)　）である．

2 $U = \{0, 1, 2, \ldots, 9\}$ を全体集合とし，$A = \{0, 2, 4, 6, 8\}$, $B = \{x \in U \mid x \text{ は素数 }\}$ とする．以下の問に答えよ．

(1) B を外延的記法（要素を列挙する記法）で表せ．
(2) $A \cap B$ を外延的記法で表せ．
(3) $A \cup B$ を外延的記法で表せ．
(4) $A \setminus B$ を外延的記法で表せ．
(5) $\overline{A} \cap \overline{B}$ を外延的記法で表せ．
(6) $A \cup \overline{B}$ を外延的記法で表せ．

3 $\mathbb{R}$ 上の二項関係 $\sim_1$ を $a \sim_1 b \overset{\text{def}}{\iff} a^2 = b^2$ と定める．
$\mathbb{R}$ 上の二項関係 $\sim_2$ を $a \sim_2 b \overset{\text{def}}{\iff} |a - b| < 1$ と定める．
$\mathbb{Z}$ 上の二項関係 $\sim_3$ を $a \sim_3 b \overset{\text{def}}{\iff} \exists n \in \mathbb{N}$ s.t. $a - b = 3n$ と定める．

これらの二項関係 $\sim_1, \sim_2, \sim_3$ がそれぞれ反射的か，対称的か，推移的かについて，表中の (1)〜(9) が「○」か「×」か答えよ．

	反射的	対称的	推移的
$\sim_1$	(1)	(2)	(3)
$\sim_2$	(4)	(5)	(6)
$\sim_3$	(7)	(8)	(9)

4 次の合同方程式を解け．ただし，解は mod k に対して $0, 1, \ldots, k-1$ の範囲で答えること．

(1) $8x \equiv 11 \pmod{13}$
(2) $10x \equiv 2 \pmod{17}$
(3) $5x \equiv 9 \pmod{23}$
(4) $11x \equiv 10 \pmod{20}$
(5) $9x \equiv 2 \pmod{18}$
(6) $12x \equiv 8 \pmod{16}$

5 次の連立合同方程式を解け．

(1) $\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$

(2) $\begin{cases} 2x \equiv 3 \pmod{5} \\ 6x \equiv 8 \pmod{11} \end{cases}$

6 次の合同方程式を解け．ただし，解は mod k に対して $0, 1, \ldots, k-1$ の範囲で答えること．

(1) $x^2 \equiv 25 \pmod{29}$
(2) $x^2 \equiv 2 \pmod{23}$
(3) $x^2 + 11x + 7 \equiv 0 \pmod{17}$

7 次のルジャンドル記号の値を求めよ．

(1) $\left(\dfrac{5}{7}\right)$
(2) $\left(\dfrac{46}{7}\right)$
(3) $\left(\dfrac{24}{29}\right)$
(4) $\left(\dfrac{24}{31}\right)$

（裏面に続く）

8 A を送信者，B を受信者とするときの RSA 暗号方式は以下の通りである．

Step 1. B は自身の公開鍵と秘密鍵を作る．
- 素数 p, q を用意し，$n = pq$ とする．
- $e \in \mathbb{N}$ を $(p-1)(q-1)$ と互いに素な数とする．
- $d \in \mathbb{N}$ を $ed \equiv 1 \pmod{(p-1)(q-1)}$ を満たすようにとる．

Step 2. B は公開鍵 (n と e) を A に送る．

Step 3. A は受け取った公開鍵を使って文章（平文）を暗号化．
- 送りたいメッセージを $x \in N$ とする（ただし $x < n$）．
- x^e を n で割った余りを y とする，つまり $y \equiv x^e \pmod{n}$ とする．

Step 4. A は暗号文 y を B に送る．

Step 5. B は自身の秘密鍵を使って復号化，もとの文章（平文）を得る．
- y^d を n でわった余りを求める．これが平文 x となる．

次の空欄を埋めよ．

- あなたは送信者である．平文 $x = 32$ を受信者から受け取った公開鍵を使って暗号化したい．いま，受信者から公開鍵として $n = 35, e = 5$ を受け取った．このとき暗号文 y は（　(1)　）である．
- あなたは受信者である．あなたはふたつの素数として $p = 3, q = 7$ を選び $(p-1)(q-1) = 12$ と互いに素な数として $e = 5$ を選んだ．このとき，あなたの秘密鍵 d は（　(2)　）である，ただし d は秘密鍵として使える数のうち最小の自然数とする．送信者から暗号文 $y = 4$ が送られてきた．送信者の平文 x は（　(3)　）である．
- あなたは盗聴者である．あなたは受信者が送る公開鍵 $n = 35, e = 5$ と送信者が送った暗号文 $y = 18$ を盗んだ．このとき，受信者の秘密鍵 d は（　(4)　）である，ただし d は秘密鍵として使える数のうち最小の自然数とする．また，送信者の平文 x は（　(5)　）である．

（問題は以上）

2024年度　科学リテラシー　期末試験　解答用紙（片面1枚）

学籍番号 _____　　名前 _____

1	(1)		(2)		(3)		(4)		(5)		(6)		(7)		(8)	

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

3	(1)		(2)		(3)	
	(4)		(5)		(6)	
	(7)		(8)		(9)	

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

5	(1)		(2)	

6	(1)		(2)		(3)	

7	(1)		(2)		(3)		(4)	

8	(1)		(2)		(3)	
	(4)		(5)			