2023 年度　情報数学　期末試験　問題用紙

- 大問 7 以外はミニマム・リクワイアメントの問題である．中間試験と合わせて到達目標ごとに 6 割以上正解出来なければ単位認定されない．
- 問題数は変更の可能性がある．
- 「*****」は具体的な数値等は未確定（非公開）という意味である．試験のときはもちろん具体的な数値が入る．

1 （到達目標 a1）学習支援サイト「中間試験を踏まえた確認問題」の [1] と同様の問題を出題予定．

2 （到達目標 a1）学習支援サイト「中間試験を踏まえた確認問題」の [2] と同様の問題を出題予定．

3 （到達目標 a1）論述領域を -3 以上 3 以下の整数とする．命題 $Q(x,y)$ を「***」とする．

(1) $Q(*,*)$ の真偽を答えよ．
(2) $Q(*,*)$ の真偽を答えよ．
(3) $\forall x, \forall y, Q(x,y)$ の真偽を答えよ．
(4) $\exists x, \exists y, Q(x,y)$ の真偽を答えよ．
(5) $\forall x, \exists y, Q(x,y)$ の真偽を答えよ．
(6) $\exists x, \forall y, Q(x,y)$ の真偽を答えよ．

類題は学習支援サイト「全称命題と存在命題」の [2]．

4 （到達目標 b1）写像 $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を次で定める．

$$g(m,n) = \begin{cases} ******* \\ ******* \end{cases}$$

以下の問に答えよ．

(1) $g(1,1)$ を求めよ．
(2) $g(1,5)$ を求めよ．
(3) $g(2,1)$ を求めよ．
(4) $g(2,3)$ を求めよ．
(5) $g(3,1)$ を求めよ．
(6) $g(3,2)$ を求めよ．

学習支援サイト「関数の再帰的定義」の [2] と同様の問題を出題予定．ミニマム・リクワイアメントの問題でもあるので計算を間違えないように．

5 （到達目標 c1）次の合同方程式を解け．

(1) $*x \equiv * \pmod{*}$
(2) $*x \equiv * \pmod{*}$
(3) $*x \equiv * \pmod{*}$
(4) $*x \equiv * \pmod{*}$
(5) $*x \equiv * \pmod{*}$
(6) $*x \equiv * \pmod{*}$
(7) $*x \equiv * \pmod{*}$
(8) $*x \equiv * \pmod{*}$
(9) $*x \equiv * \pmod{*}$
(10) $*x \equiv * \pmod{*}$
(11) $*x \equiv * \pmod{*}$
(12) $*x \equiv * \pmod{*}$

学習支援サイト「合同方程式 (1)」「合同方程式 (2)」と同様の問題を出題予定．解答は「$x \equiv 5 \pmod{13}$」のように答えること．

6 （到達目標 c1）次の連立合同方程式を解け．

(1) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$
(2) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$
(3) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$
(4) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$
(5) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$
(6) $\begin{cases} *x \equiv * \pmod{*} \\ *x \equiv * \pmod{*} \end{cases}$

学習支援サイト「連立合同方程式」と同様の問題を出題予定．

7 （到達目標 c2）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 $x \in \mathbb{N}$ 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，元の文章（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 $x = **$ 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 $n = **, e = **$ 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 $p = **, q = **$ を選び $(p-1)(q-1) = **$ と互いに素な数として $e = **$ 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 $y = **$ 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 $n = **, e = **$ と送信者が送った暗号文 $y = **$ を盗んだ．このとき，受信者の秘密鍵は（　(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．

学習支援サイト「RSA 暗号 (***)」と同様の問題を出題予定．問い方は「暗号文 y は…」ではなく単に「暗号文は…」とする可能性もあるので RSA 暗号方式をしっかりと把握しておくこと．