暗号の数理試験

2010–2–8　　河野

注意: ・答案は日本語として理解可能なものである事。数式に対し説明が必要な場合に，数式のみで説明がないときには仮に数式が正しくても満点とならないことがある。
・採点は減点法を採用する。つまり間違いの内容によっては**白紙答案より低い点数になる**場合がある。careless miss でそのような事はないが,「分からなくても適当に何か書いておけ」という姿勢で回答するとそうなることがある。
・内容を理解せずに丸暗記していると判断されたものに対して大きく減点することがあるので注意すること。
・在籍番号欄について：再履修者は 10 桁の在籍番号を書く事。再履修者以外は出席番号 (多くは 2 桁) でよい。

1 R を集合 A 上の関係とする。即ち $R \subseteq A \times A$ とする。$(x,y) \in R$ のとき $x \sim y$ と書き，$(x,y) \notin R$ のとき $x \not\sim y$ と書く。次の 3 つが成立するとき関係 $\sim$ (関係 R) は同値関係であるという。
(a) $x \sim x$ が成立する。
(b) $x \sim y$ ならば $y \sim x$ が成立する。
(c) $x \sim y$ および $y \sim z$ が成立するならば $x \sim z$ が成立する。
整数 $\mathbb{Z}$ 上の同値関係 R を $R = \{\,(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m-n \text{ は } 5 \text{ で割り切れる}\,\}$ とする。R が同値関係になるときはそれを証明し，そうでないときは反例をあげよ。

裏にも問題あり。別紙にも問題あり

学科		在番籍号		氏名	

2 G を 2 項演算「$\cdot$」が定義されている集合とする。次の 3 つの条件が満たされる時，G を**群** (*group*) という。

(a) この演算は結合法則を満たす，すなわち 任意の $x, y, z \in G$ に対し $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ が成立する。

(b) 単位元が存在する，すなわちある元 $e \in G$ が存在して任意の $x \in G$ に対し $x \cdot e = e \cdot x = x$ が成立する。

(c) G の任意の元に対して，その逆元が存在する，すなわち任意の元 $x \in G$ に対し G の元 x^{-1} が存在して $x \cdot x^{-1} = x^{-1} \cdot x = e$ が成立する。

(1) $M(2) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$，$G = \mathrm{GL}(2, \mathbb{R}) = \{ A \in M(2) \,|\, A \text{ の逆行列 } A^{-1} \text{が存在する} \}$ とするとき G が行列の積という演算に関して群をなすことを示せ。ただし線型代数の知識で知っていることは使用してよい。

(2) G を群とし，H を G の空でない部分集合とする。H が部分群であるための必要十分条件は，次の (a), (b) が成り立つことである。

(a) 任意の $a, b \in H$ に対して $a \cdot b \in H$

(b) 任意の $a \in H$ に対して $a^{-1} \in H$

$H = \mathrm{SL}(2, \mathbb{R}) = \{ A \in \mathrm{GL}(2, \mathbb{R}) \,|\, \det A = 1 \}$ とする。ただし，$\det A$ は A の行列式である。このとき H が G の部分群であることを示せ。ただし線型代数の知識で知っていることは使用してよい。

3 $\mathbb{Z}$ を整数全体の作る集合とする。このとき $10\mathbb{Z}$ による剰余群 $\mathbb{Z}/10\mathbb{Z}$ を Z_{10} と書く。$\mathbb{Z}_{10} = \{\, 0+10\mathbb{Z}, 1+10\mathbb{Z}, 2+10\mathbb{Z}, \ldots, 9+10\mathbb{Z} \,\}$ であるが，代表元 $0, 1, \ldots, 9$ を選んで $\mathbb{Z}_{10} = \{\, 0, 1, 2, \ldots, 9 \,\}$ と表しておく。$\mathbb{Z}_{10}$ には $\mathbb{Z}$ の演算から決定される「足し算」と「掛け算」が定義されている。$\mathbb{Z}_{10}$ において次の演算結果は何になるか結果のみ記せ。

(1) $6 + 5 =$

(2) $4 \times 3 =$

4 問題 3 と同様に自然数 n に対して $n\mathbb{Z}$ による $\mathbb{Z}$ の剰余群 $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}_n$ と書く。$\mathbb{Z}_n = \{\, 0+10\mathbb{Z}, 1+10\mathbb{Z}, 2+10\mathbb{Z}, \ldots, (n-1)+10\mathbb{Z} \,\}$ であるが，代表元 $0, 1, \ldots, n-1$ を選んで $\mathbb{Z}_{10} = \{\, 0, 1, 2, \ldots, n-1 \,\}$ と表しておく。$\mathbb{Z}_n$ には $\mathbb{Z}$ の演算から決定される「足し算」と「掛け算」が定義されている。$\mathbb{Z}_n^* = \{\, k \in \mathbb{Z}_n \mid n \text{ と } k \text{ は互いに素} \,\}$ と置く。

(1) $n = 12$ のとき $|\mathbb{Z}_{12}^*|$ ($\mathbb{Z}_{12}^*$ の元の個数) はいくらか。

(1) $n = 13$ のとき $|\mathbb{Z}_{13}^*|$ ($\mathbb{Z}_{13}^*$ の元の個数) はいくらか。

(2) $\mathbb{Z}_{13}^*$ とし，演算は掛け算を考える。2^{-1} はいくらか。

5 次の問いに答えよ。ただし，アルゴリズムに基づいた計算過程もきちんと書くこと。

(1) ユークリッドアルゴリズムを用いて 79 と 89 の最大公約数を求めよ。

(2) 拡張ユークリッドアルゴリズムを用いて，$79k_1 + 89k_2 = 1$ を満たす整数 k_1, k_2 を 1 組見つけよ。

裏にも問題あり。別紙にも問題あり

学科		在番籍号		氏名	

6 A 国と B 国は長年紛争状態にあったが，C 国の秘密調停により和平交渉を行うことになった。A 国と B 国は，この交渉を行うにあたって，多くの秘密文書を通信経路を通してやり取りする必要があるが，これはあくまで秘密交渉の段階であり，A 国，B 国，C 国の交渉担当者以外の者に情報が漏れることを避けなければならない。

A 国から B 国へと秘密文書を送る場合，公開鍵暗号を利用して，下記の条件 (a)〜(c) が全て満たされるようにしたい。そこで以下のような方法で実行することにした。

A 国は B 国直接に文書を送るのではなく，C 国を経由して送ることにする。A 国は文書 T を自分の秘密鍵 S_A を用いて暗号化する。更に C 国の公開鍵 P_C を用いて，T および $S_A(T)$ を暗号化する。このとき $P_C(T)$ と $P_C(S_A(T))$ が得られる。この 2 つの文書をこの文書に表れない記号 (暗号は数字列と考えられるので例えば改行コードなど) で連結して 1 つの文書とする。これを $(P_C(T), P_C(S_A(T)))$ と書こう。この文書を C 国に送る。

C 国は秘密鍵 S_C を用いて $(T, S_A(T))$ を得ることができる。その後 C 国は B 国の公開鍵 P_B を用いて文書 $(P_B(T), P_B(S_A(T)))$ を作り B 国に送る。

この方法が下記の条件 (a)，(b)，(c) を満たしていることを説明 (証明) せよ。ただし次のことは仮定する。(1) 各国の公開鍵 P_A, P_B, P_C は公開されており，秘密鍵 S_A, S_B, S_C は各国の担当者のみが知っている。(2) 公開鍵暗号は公開鍵で暗号化した平文は秘密鍵で復号化でき，秘密鍵で暗号化した平文は公開鍵で復号化できるタイプ，すなわち RSA 暗号と同じタイプの暗号とする。(3) 公開鍵暗号は秘密鍵なしに元の平文を得ること (すなわち解読) は不可能である。

(a) B 国は，受け取ったメッセージが確実に A 国が作成したものであり，C 国を含めた第 3 者が途中で改ざんした可能性はないことを確認できる。

(b) C 国は，この交渉の過程を把握する必要がある。C 国は，A 国が B 国に送ったメッセージの内容を知る必要があり，さらに，その内容が確実に A 国が B 国に送ったものであることを確認できる。すなわち，A 国が実際に B 国へ送ったものと異なるものを C 国へ送ったり，B 国が実際に A 国から受け取ったものと異なるものを C 国へ送ったり，あるいは，第 3 者が A 国や B 国の名をかたって，A 国から B 国への文書であると偽って C 国へと文書を送ったりすることができないようにする。

(c) これらの文書のやり取りの中で，そのデータを盗聴した者がいたとしても，その内容を知ることはできない。

(1) (a) を満たしていること：

(2) (b) を満たしていること：

(3) (c) を満たしていること：