暗号の数理試験

2012–2–13　　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：2 年生以上は 10 桁の在籍番号を書く事。1 年生は出席番号 (多くは 2 桁) でよい。

1 G が群であるとは G に演算「$\cdot$」が定義されていて次を満たすことをいう。

(1) 結合法則をみたす：$\forall x, y, z \in G\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$
(2) 単位元が存在する：$\exists e \in G \forall x \in G\ e \cdot x = x \cdot e = x$
(3) 逆元が存在する：$\forall x \in G \exists\, x^{-1}\ x \cdot x^{-1} = x^{-1} \cdot x = e$

ここで演算は「$\cdot$」という記号で書いたが，加法的な記号「$+$」で書かれていても同様である。
n を 2 以上の自然数とする。$\mathbb{Z}_n = \{\, [m] \mid m \in \mathbb{Z} \,\}$ とする。ただし整数 p, q に対し $[p] = [q]$ が成立するのは $p - q$ が n で割り切れるときであり，かつそのときに限るとする。$\mathbb{Z}_n$ の和を $[p] + [q] = [p + q]$ で定義する。このとき $\mathbb{Z}_n$ がこの和に関して群をなすことを証明せよ。ただし，整数の和が結合法則を満たすことは既知としてよい。

2 n，$\mathbb{Z}_n$ は問題 1 と同じとする。$\mathbb{Z}_n^* = \{\, [p] \in \mathbb{Z}_n \mid p \text{ と } n \text{ は互いに素} \,\}$ とする。積を $[x] \cdot [y] = [xy]$ で定義するとき，$\mathbb{Z}_n^*$ が積に関して群をなすことを示せ。ただし整数 p と q が互いに素であるとき，$k_1 p + k_2 q = 1$ となる整数 k_1, k_2 が存在するという事実および整数の積が結合法則を満たすことは既知としてよい。

別紙にも問題あり

学科		在番籍号		氏名	

3 $F_7 = \mathbb{Z}_7$ を 7 元体とする。ただし問題 1，2 では元を $[p]$ と書いたが，ここでは p と書くことにする。すなわち $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ である。F_7 では $0 = 7$ なので和・積については $4 + 6 = 10 = 7 + 3 = 0 + 3 = 3$ であり，$4 \cdot 5 = 20 = 14 + 6 = 7 \cdot 2 + 6 = 6$ 等が成立している。また $2 \cdot 4 = 1$ なので $\frac{1}{2} = 4$ 等が成立している。$E(F_7) = \left\{ (x, y) \in F_7 \,\middle|\, y^2 = x^3 + x + 1 \right\} \cup \{\mathcal{O}\}$ とし，$E(F_7)$ における和を次のように定義する。任意の $P \in E(F_7)$ に対し $\mathcal{O} + P = P + \mathcal{O} = P$ とする。$P = (x_1, y_1), Q = (x_2, y_2)$ に対し $x_1 \neq x_2$ のとき $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ とおき，$x_3 = \lambda^2 - x_1 - x_2$，$y_3 = \lambda(x_1 - x_3) - y_1$ とする。$P = Q$ のとき，即ち $x_1 = x_2$ かつ $y_1 = y_2$ のとき $\lambda = \dfrac{3x_1^2 + 1}{2y_1}$ とおき $x_3 = \lambda^2 - 2x_1$，$y_3 = \lambda(x_1 - x_3) - y_1$ とする。これらのとき $R = (x_3, y_3) = P + Q$ と定義する。また $P \neq Q$ かつ $x_1 = x_2$ のときは $P + Q = \mathcal{O}$ と定義する。この和に関して $E(F_7)$ は群になることが知られている。$P = (0, 1)$ とする。このとき $2P, 3P, 4P$ を求めよ。

4 最大公約数を求めるアルゴリズムであるユークリッドアルゴリズムとはどのようなアルゴリズムかを説明せよ。また $m = 2300, n = 1679$ にこのユークリッドアルゴリズムを適用して最大公約数を求めよ。この計算過程も記述すること。

別紙にも問題あり

学科		在番籍号		氏名	

5 次に答えよ。ただし前問までの問題文で述べられていることをは既知としてよい。

(1) 公開鍵暗号とはどのような暗号なのかを説明せよ。

(2) RSA 暗号とはどのような暗号なのかを説明せよ。

(3) RSA 暗号が実装可能であることを説明せよ。

別紙にも問題あり

学科		在番籍号		氏名	

(4) RSA 暗号の安全性の根拠について述べよ。

(5) 楕円曲線暗号とはどのような暗号なのか説明せよ。

(6) 楕円暗号の安全性の根拠について述べよ。

別紙にも問題あり

学科		在番籍号		氏名	