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。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。

(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：$\forall x \in G \exists\, x^{-1}\ x \cdot x^{-1} = x^{-1} \cdot x = e$

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。

$[p], [q], [r]$ を $\mathbb{Z}_n$ の任意の元とする。

$$([p] + [q]) + [r] = [p + q] + [r] = [(p + q) + r] = [p + (q + r)] = [p] + [q + r] = [p] + ([q] + [r])$$

となり結合法則が成立する。
$[0] \in \mathbb{Z}_n$ は任意の元 $[p] \in \mathbb{Z}_n$ に対し

$$[0] + [p] = [0 + p] = [p] = [p + 0] = [p] + [0]$$

となるので単位元である。
任意の元 $[p] \in \mathbb{Z}_n$ に対し $[-p] \in \mathbb{Z}_n$ が存在して

$$[p] + [-p] = [p + (-p)] = [0]$$

となるので $[-p]$ は $[p]$ の逆元である。以上により $\mathbb{Z}_n$ は群をなす。

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は既知としてよい。

$[x], [y], [z]$ を $\mathbb{Z}_n^*$ の任意の元とする。

$$([x] \cdot [y]) \cdot [z] = [xy] \cdot [z] = [(xy)z] = [x(yz)] = [x] \cdot [yz] = [x] \cdot ([y] \cdot [z])$$

となり結合法則が成立する。
$[1] \in \mathbb{Z}_n^*$ は任意の元 $[x] \in \mathbb{Z}_n^*$ に対し

$$[1] \cdot [x] = [1x] = [x] = [x1] = [x] \cdot [1]$$

となるので単位元である。
任意の元 $[x] \in \mathbb{Z}_n^*$ に対し n と x は互いに素なので

$$k_1 x + k_2 n = 1$$

となる整数 k_1, k_2 が存在する。k_1 が n と互いに素でなければ $k_1 x + k_2 n$ も n と互いに素ではなく，1 と n が互いに素でないことになる。よって k_1 は n と互いに素である。このとき

$$[1] = [k_1 x + k_2 n] = [k_1][x] + [k_2][n] = [k_1][x]$$

となり，$[x]$ の逆元 $[k_1]$ が存在する。以上により $\mathbb{Z}_n^*$ は群である。

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 $\dfrac{1}{2} = 4$ 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。

$2P$ を計算する。$P = (0, 1)$ なので $x_1 = 0, y_1 = 1$ として計算する。

$$\lambda = \frac{3x_1^2 + 1}{2y_1} = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = \frac{1}{2} = 4$$
$$x_3 = \lambda^2 - 2x_1 = 4^2 - 2 \cdot 0 = 16 = 2$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 4(0 - 2) - 1 = -9 = 5$$

より $2P = (2, 5)$ である。

$3P = P + 2P$ なので $(x_1, y_1) = (0, 1), (x_2, y_2) = (2, 5)$ とする。

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - 1}{2 - 0} = \frac{4}{2} = 2$$
$$x_3 = \lambda^2 - x_1 - x_2 = 2^2 - 0 - 2 = 2$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 2(0 - 2) - 1 = -5 = 2$$

なので $3P = (2, 2)$ となる。同様に計算すると $4P = (0, 6)$ となる。

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。

m, n を自然数で $m \geqq n$ とする。このとき自然数 p, r が存在して

$$m = pn + r \qquad (0 \leqq r < n)$$

となる。m と n の最大公約数を (m, n) とすると，$r = 0$ のときは $(m, n) = n$ となり，$r \neq 0$ のときは $(m, n) = (n, r)$ となる。

よって m, n が与えられたとき r を求め，$r = 0$ のときは n を返し，$r \neq 0$ のときは m に n を n に r を代入し，この操作を繰り返す。r は次第に小さくなるので，この操作はいつかは停止する。これをユークリッドアルゴリズムと呼ぶ。

$m = 2300, n = 1679$ とすると $r = 621$ なので $(2300, 1679) = (1679, 621)$ である。
$m = 1679, n = 621$ とすると $r = 437$ なので $(1679, 621) = (621, 437)$ である。
$m = 621, n = 437$ とすると $r = 184$ なので $(621, 437) = (437, 184)$ である。
$m = 437, n = 184$ とすると $r = 69$ なので $(437, 184) = (184, 69)$ である。
$m = 184, n = 69$ とすると $r = 46$ なので $(184, 69) = (69, 46)$ である。
$m = 69, n = 46$ とすると $r = 23$ なので $(69, 46) = (46, 23)$ である。
$m = 46, n = 23$ とすると $r = 0$ なので $(46, 23) = 23$ である。
以上により $(2300, 1679) = 23$ が得られる。

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。

暗号化鍵と復号化鍵が異なる暗号であり，暗号化鍵から復号化鍵，復号化鍵から暗号化鍵を導出することが困難な暗号のこと。

通常使われているこのタイプの暗号は鍵が暗号化にも復号化にも使え，一方を公開し，他方を秘匿する。この場合，公開する鍵を公開鍵と呼び，秘匿する鍵を秘密鍵と呼ぶ。

(2) RSA 暗号とはどのような暗号なのかを説明せよ。

2 つの素数 p, q をとり $n = pq$ とする。$\varphi(n)$ を 1 から $n-1$ までの自然数の中で n と互いに素であるものの個数とする。$\varphi(n)$ と互いに素であって $1 < e < \varphi(n)$ となる自然数 e を選ぶ。また $ed \equiv 1 \mod \varphi(n)$ となる自然数 d を求める。そして (n, e) を公開鍵として公開し，d を秘密鍵として秘匿する。

平文が $[x] \in \mathbb{Z}_n$ の元として実現されているとする。$[x]$ を $[x]^e$ に変換することが公開鍵による暗号化 (復号化) である。$[x]$ を $[x]^d$ に変換することが秘密鍵による復号化 (暗号化) である。

(3) RSA 暗号が実装可能であることを説明せよ。

RSA 暗号を実装するためには，(1) 大きな (知られていない) 素数を選ぶことができる，(2) 指数計算が高速でできる，ことが必要である。

(1) は確率的には可能である。即ち素数である確率が 99.99…9%であるような数は素数とみなす。例えばミラー・ラビン法が知られている。もともと公開鍵暗号の安全性は確率的なものなので (偶然に解読される可能性は 0 ではない)，実際上問題は発生しない。

(2) は高速指数計算法により可能である。これは x の巾乗を計算するのに，$x^2, \left(x^2\right)^2, \left(\left(x^2\right)^2\right)^2, \ldots$ を計算していくことで求める方法である。x^a を計算するのに a を 2 進展開して $a = a_0 + a_1 2 + a_2 2^2 + \cdots + a_k 2^k$ $(0 \leqq a_i < 2)$ としたとき

$$x^a = x^{a_0} \left(x^2\right)^{a_1} \left(x^{2^2}\right)^{a_2} \cdots \left(x^{2^k}\right)^{a_k}$$

となる。よって $x^2, \ldots, x^{2^k}$ を計算することにより x^a を計算することができる。

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。

$\varphi(n)$ を知っている人間は e から d を簡単に計算できる。$\varphi(n)$ を知るためには，今の所 n を因数分解するしか方法がないと思われる。因数分解は困難であると思われているので，RSA 暗号も安全だと思われている。

(5) 楕円曲線暗号とはどのような暗号なのか説明せよ。

p を素数とし，n を自然数とし $q = p^n$ とする。有限体 F_q 上の楕円曲線

$$E(F_q) = \left\{ (x, y) \in F_q^2 \,\middle|\, y^2 = x^3 + ax + b \right\} \qquad (4a^3 + 27b^2 \neq 0)$$

には和が定義されて群をなすことが知られている。楕円曲線上の点 P を自然数 k に対し $Q = kP$ とする。このとき $E(F_q)$ と P, Q を公開し，k を秘密鍵として秘匿する。

平文が $X \in E(F_q)$ として表現されているとする。公開鍵で暗号化する場合，乱数で適当な自然数 r を発生させる。

$$A = rP \qquad B = X + rQ$$

を計算し (A, B) を送信する。

秘密鍵を知っているものは $B - kA$ を計算することで X を得ることができる。

(6) 楕円暗号の安全性の根拠について述べよ。

P と kP から k を求める問題は楕円曲線上の離散対数問題と呼ばれている。楕円曲線上の離散対数問題は困難だと考えられており，これが楕円曲線暗号の安全性の根拠である。

別紙にも問題あり

学科		在番籍号		氏名	