広域数理科学概論 (4) レポート課題（訂正版）
2017 年 1 月 19 日配布
提出締め切り：2017 年 2 月 8 日（水）

注意

- 以下の 6 問のうち，2 問以上解答すること．
- 8 号館 6 階東側エレベーターホールのレポート入れに提出すること．
- 1 枚目に科目名・学修番号・氏名を書くこと．
- レポートが複数枚にわたるときは，左上をホッチキス等で綴じること．
- A4 レポート用紙を使用すること．
- 第 3 問の下線部が誤っていたので訂正しました．

問題

以下の問題では，楕円曲線の無限遠点（単位元）を O で表す．

1. $E\colon y^2 = x^3 + x + 2$ を $\mathbb{F}_{23}$ 上の楕円曲線とする．以下の問いに答えよ．
   (a) 点 $(1,2), (3,3), (10,0) \in E(\mathbb{F}_{23})$ の位数をそれぞれ求めよ．
   (b) $E(\mathbb{F}_{23}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ であることを示せ．また，$E(\mathbb{F}_{23})$ の生成元を求めよ．
2. p を奇素数として，$E\colon y^2 = x^3 + ax^2 + bx + c$ を $\mathbb{F}_p$ 上の楕円曲線とする．$d \in \mathbb{F}_p$ は $\mathbb{F}_p$ の元の平方でないとして，楕円曲線 E' を $y^2 = x^3 + adx^2 + bd^2x + cd^3$ で定義する．以下の問いに答えよ．
   (a) 曲線 C を $dy^2 = x^3 + ax^2 + bx + c$ で定義し，
   $$C(\mathbb{F}_p) = \{(x,y) \mid dy^2 = x^3 + ax^2 + bx + c, x, y \in \mathbb{F}_p\} \cup \{O\}$$
   とおく．写像 $\varphi\colon E'(\mathbb{F}_p) \to C(\mathbb{F}_p)$ を $\varphi((x,y)) = (x/d, y/d^2)$, $\varphi(O) = O$ で定義する．このとき，φ が全単射であることを示せ．
   (b) $\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1)$ が成り立つことを示せ．
3. $E\colon y^2 = x^3 + 2x + 7$ を $\mathbb{F}_{97}$ 上の楕円曲線とする．$P = (11,14), Q = (76,93) \in E(\mathbb{F}_{97})$ に対して，$Q = nP$ を満たす整数 n を一つ求めよ．ただし，どのようなアルゴリズムを用いたか明らかにすること．また，必要なら $E(\mathbb{F}_{97}) = 105$ であることを用いてよい．

以下の問題では，次の定義を用いる．K を標数が 2 でない体，$\bar{K}$ を K の代数閉包とする．$C\colon Y^2 = f(X)$ を K 上の超楕円曲線とする．ただし，$f(X)$ は $2g+1$ 次の K 係数モニック多項式であり，重根を持たないとする．K の拡大体 L に対して，

$$C(L) = \{(x, y) \mid y^2 = f(x), x, y \in L\} \cup \{\infty\}$$

と定義する．ただし，∞ は無限遠点を表す．$C(\bar{K})$ を C と表す．$\bar{K}(C)$ を C の $\bar{K}$ 上の関数体とする．

4. $R, S \in \bar{K}(C)$ を C 上の有理関数として，$P \in C$ とする．P が R, S の極でないとする．以下の問いに答えよ．
   (a) R の P での値 $R(P)$ の定義を述べよ．（講義で与えた定義以外のものでもよい．）
   (b) (a) で述べた定義に基づいて，

   $$R(P) + S(P) = (R+S)(P), \quad R(P)S(P) = (RS)(P)$$

   が成り立つことを示せ．
5. $D = \sum_{i=1}^{r} P_i - r\infty$ を C 上の半被約因子とする．ただし，$P_1, P_2, \ldots, P_r \in C \backslash \{\infty\}$ は相異なるとする．$P_i = (x_i, y_i)$ として，

   $$a(X) = \prod_{i=1}^{r} (X - x_i), \quad b(X) = \sum_{i=1}^{r} y_i \prod_{\substack{1 \le j \le r \\ j \neq i}} \frac{(X - x_j)}{(x_i - x_j)}$$

   とおく．このとき，以下の条件が成り立つことを示せ．
   (1) $\deg_X b(X) < \deg_X a(X)$.
   (2) すべての $i = 1, 2, \ldots, r$ に対して，$b(x_i) = y_i$.
   (3) $b(X)^2 - f(X)$ は $a(X)$ で割り切れる．
6. $C\colon Y^2 = X^5 + X + 1$ を $\mathbb{F}_{11}$ 上定義された超楕円曲線とする．

   $$D_1 = \mathrm{div}(X^2 + X + 9, 9X + 7), \quad D_2 = \mathrm{div}(X^2 + 1, 6X + 2)$$

   とする．以下の問いに答えよ．
   (a) $D_1 = P_1 + P_2 - 2\infty$ を満たす $P_1, P_2 \in C$ を求めよ．
   (b) $D_3 \sim D_1 + D_2$ となる被約因子 D_3 を求め，$D_3 = \mathrm{div}(a(X), b(X))$ の形で表せ．