応用数理概論 (2)・広域数理科学概論 (4)・応用数理特別講義 II
レポート課題
2021 年 1 月 14 日配布
提出期限：2021 年 2 月 4 日 23:59

注意

- 以下の 6 問のうち，2 問以上解答すること．
- kibaco の「課題」機能を使い，**PDF ファイル**で提出すること．（PDF ファイル以外のファイル形式では提出しないこと．）
- レポートの最初に学修番号と名前を記入すること．
- 答えだけでなく，どのような計算・議論をしたか分かるように詳しく書くこと．

問題

以下の問題では，体 K の代数閉包を $\overline{K}$ で表す．また，以下の 3 問では，楕円曲線の無限遠点（単位元）を O で表す．

1. $E\colon y^2 = x^3 - x^2 - 2x - 5$ を $\mathbb{F}_{11}$ 上定義された楕円曲線として，$P = (1, 2)$, $Q = (6, 8)$ とする．このとき，$P + Q$, $2P$, $5P$, $5Q$ を求めよ．
2. a を $\mathbb{Q}$ 上の不定元として，$K = \mathbb{Q}(a)$ とする．K 上定義された楕円曲線
$$E\colon y^2 = x^3 + (-3a^2 - 6a + 1)x^2 + 8a(a - 1)(a + 1)x + 16a^2(a + 1)^2$$
を考える．$P = (0, 4a(a + 1))$ とする．以下の問いに答えよ．
   (a) $2P$, $3P$ を求めよ．
   (b) P の位数が有限であることを示せ．また，P の位数を求めよ．
3. E を $\mathbb{Q}$ 上定義された楕円曲線とする．正の整数 n に対して，
$$E[n] = \{P \in E(\overline{\mathbb{Q}}) \mid nP = O\}, \quad E(\mathbb{Q})[n] = \{P \in E(\mathbb{Q}) \mid nP = O\}, \quad \mu_n = \{x \in \overline{\mathbb{Q}}^{\times} \mid x^n = 1\}$$
と定義する．$\mu_n\colon E[n] \times E[n] \to \mu_n$ を Weil ペアリングとする．次の性質が知られている．
   - 任意の $P, Q \in E[n]$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ に対して，$\sigma(\mu_n(P, Q)) = \mu_n(\sigma(P), \sigma(Q))$ が成り立つ．

   この性質と講義で述べた Weil ペアリングの性質を用いて，以下の問いに答えよ．
   (a) $P, Q \in E(\mathbb{Q})[n]$ ならば $\mu_n(P, Q) \in \mathbb{Q}$ であることを示せ．
   (b) p が奇素数のとき，$E(\mathbb{Q})[p] = \{O\}$ または $E(\mathbb{Q})[p] \cong \mathbb{Z}/p\mathbb{Z}$ であることを示せ．

以下の 3 問では，超楕円曲線の無限遠点を ∞ で表す．その他，講義で述べた定義を用いるものとする．（特に，被約因子の定義は代数幾何学における通常の定義とは異なるので注意すること．）

4. $C\colon y^2 = x^5 + 6x^3 + x^2 + 3x + 1$ を $\mathbb{F}_{13}$ 上定義された超楕円曲線とする．C 上の有理関数 $F(x, y) = y - x^2 - 5x + 1$ の因子 $\mathrm{div}(F)$ を求めよ．

5. $C\colon y^2 = x^5 + x + 1$ を $\mathbb{F}_5$ 上定義された超楕円曲線とする．

$$D_1 = \mathrm{div}(x^2 + 4x + 1, 3x + 1), \quad D_2 = \mathrm{div}(x^2 + x, 2x + 4)$$

とする．$D_3 \sim D_1 + D_2$ となる被約因子 D_3 を求め，$D_3 = \mathrm{div}(U(x), V(x))$ の形で表せ．

6. K を標数が 2 でない体として，$C\colon y^2 = f(x)$ を K 上定義された種数 2 の超楕円曲線とする．ただし，$f(x)$ は K 係数モニック 5 次多項式であり，$\overline{K}$ で重根を持たないとする．$f(x)$ の根を $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \overline{K}$ とする．このとき，

$$[(\alpha_1, 0)] + [(\alpha_2, 0)] + [(\alpha_3, 0)] - 3[\infty] \sim [(\alpha_4, 0)] + [(\alpha_5, 0)] - 2[\infty]$$

が成り立つことを示せ．