

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

2019 年 1 月 24 日配布

提出締め切り：2019 年 2 月 7 日（木）

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．

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. $E: y^2 = x^3 + x^2 - 2x + 1$ を \mathbb{Q} 上定義された楕円曲線として， $P = (1, 1)$ ， $Q = (0, -1)$ とする．このとき， $2P$ ， $P + Q$ ， $2P + Q$ ， $3Q$ を求めよ．
2. $E: y^2 = x^3 + 1$ を \mathbb{F}_7 上定義された楕円曲線とする． $E(\mathbb{F}_7)$ で位数 2, 3 の点をすべて求めよ．
3. p を素数として， $p \neq 2$ ， $p \equiv 2 \pmod{3}$ を満たすとする． $k \in \mathbb{F}_p^\times$ として， $E: y^2 = x^3 + k$ を \mathbb{F}_p 上定義された楕円曲線とする．以下の問いに答えよ．
 - (a) 写像 $\varphi: \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$ を $\varphi(x) = x^3$ で定義する． φ は全単射であることを示せ．
 - (b) 写像 $\psi: \mathbb{F}_p \rightarrow \mathbb{F}_p$ を $\psi(x) = x^3 + k$ で定義する． ψ は全単射であることを示せ．
 - (c) $\#E(\mathbb{F}_p) = p + 1$ を示せ．

以下の問題では、次の定義を用いる。 K を標数が 2 でない完全体、 \overline{K} を K の代数閉包とする。 $C: y^2 = f(x)$ を K 上の種数 g 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、 \overline{K} で重根を持たないとする。 C 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 of 定義とは異なるので注意すること。)

4. $R \in \overline{K}(C)^\times$ は ∞ にのみ極を持つとする。このとき、 $R \in \overline{K}[C]$ であることを示せ。
5. $C: y^2 = x^5 - 3$ を \mathbb{F}_7 上定義された超楕円曲線とする。

$$D_1 = \text{div}(x^2 + 2x + 6, 3x + 2), \quad D_2 = \text{div}(x^2 + 5x + 5, 4x + 5)$$

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 $P_1, P_2 \in C(\overline{\mathbb{F}_7})$ を求めよ。
 - (b) $D_3 \sim D_1 + D_2$ となる被約因子 D_3 を求め、 $D_3 = \text{div}(U(x), V(x))$ の形で表せ。
6. $C: y^2 = x^5 - x$ を \mathbb{F}_3 上定義された超楕円曲線として、 J を C のヤコビアンとする。このとき、 $\#C(\mathbb{F}_3)$, $\#J(\mathbb{F}_3)$ を求めよ。