応用数理概論 (2)・応用数理特別講義 II
レポート課題
2023 年 1 月 31 日配布
提出期限：2023 年 2 月 10 日（金）17:00

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．
- 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. $E\colon y^2 = x^3 + 2x^2 - x - 2$ を $\mathbb{F}_{23}$ 上定義された楕円曲線として，$P = (-4, -4)$, $Q = (6, -2)$ とする．このとき，$P + Q$, $2P$, $3Q$, $6Q$ を求めよ．
2. $n = 493$ とする．$\mathbb{Z}/n\mathbb{Z}$ 上の（擬）楕円曲線 $E\colon y^2 = x^3 - 5x - 8$ と点 $P = (3, 2) \in E(\mathbb{Z}/n\mathbb{Z})$ を考える．$3P$ を計算することにより，n を素因数分解せよ．
3. A, B を整数として，楕円曲線 $E\colon y^2 = x^3 + Ax + B$ を考える．整数 n に対して，等分多項式 ψ_n は以下で定義される．

$$
\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \quad (n \geq 2),\\
\psi_{2n} &= \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad (n \geq 3),\\
\psi_n &= -\psi_{-n} \quad (n < 0).
\end{aligned}
$$

このとき，以下が成り立つことを示せ．

(a) n が奇数ならば，$\psi_n \in \mathbb{Z}[x, y^2]$ であり，n が偶数ならば，$\psi_n \in 2y\mathbb{Z}[x, y^2]$ である．

(b) k が正の整数，n が 2^k の倍数ならば，$\psi_n \in 2^k y\mathbb{Z}[x, y^2]$ である．

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. $C\colon y^2 = x^5 - 2x + 3$ を $\mathbb{F}_{11}$ 上定義された超楕円曲線とする．

$$D_1 = \mathrm{div}(x^2 + 3x + 1, 5x + 4), \quad D_2 = \mathrm{div}(x^2 + 6x + 3, 2)$$

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．

5. $C\colon y^2 = x^5 - x^3 + 1$ 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．

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 g の超楕円曲線とする．ただし，$f(x)$ は K 係数モニック $2g + 1$ 次多項式であり，$\overline{K}$ で重根を持たないとする．$D \in \mathrm{Div}^0(C)$ を半被約因子として，$D = \mathrm{div}(U(x), V(x))$, $U(x), V(x) \in \overline{K}[x]$ とする．このとき，

$$-D \sim \mathrm{div}(U(x), -V(x))$$

が成り立つことを示せ．