

EXAMINATION PAPER

Examination Session: May

2018

Year:

Exam Code:

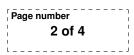
MATH4151-WE01

Title:

Topics in Algebra and Geometry

Time Allowed:	3 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	No	Models Permitted: Use of electronic calculators is forbidden.
Visiting Students may use diction	onaries: No	

Revision:



SECTION A

1. Locate all singular points, and find their tangent lines together with their multiplicities for the projective curve $C \subset \mathbb{P}^2_{\mathbb{C}}$ defined by

$$(X^2 + Y^2 - 4Z^2)^2 - 2Y^3Z = 0.$$

- 2. (a) State Bezout's Theorem. (You do not need to provide the definition of intersection multiplicity here).
 - (b) Let C, D be irreducible curves in $\mathbb{P}^2_{\mathbb{C}}$ of degrees d_1 and d_2 respectively with $d_1 \neq d_2$. Show that

$$\sharp((\operatorname{Sing}(C) \cup \operatorname{Sing}(D)) \cap C \cap D) \le \left\lceil \frac{d_1 d_2 + 1}{2} \right\rceil,$$

where for an $x \in \mathbb{R}$, [x] denotes the smallest integer larger or equal to x.

- 3. (a) Let $F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ be a homogeneous polynomial of degree d. State Euler's relation for F.
 - (b) Assume now that $d \ge 3$. Show that

$$Z\mathcal{H}_F = (d-1) \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_X & F_Y & F_Z \end{vmatrix},$$

where \mathcal{H}_F denotes the Hessian of F.

4. Let E be the cubic in $\mathbb{P}^2_{\mathbb{C}}$ defined by the equation

$$X^3 + Y^3 = Z^3.$$

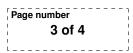
- (a) Show that E is non-singular.
- (b) Show that the point $\mathcal{O} = [1, -1, 0] \in E$ is a flex.
- (c) Considering the group law on E with \mathcal{O} as the neutral element show that for any point $P = [a, b, c] \in E$ we have

$$-P = [b, a, c].$$

- 5. Consider the elliptic curve E defined over \mathbb{F}_5 by the equation $Y^2Z = X^3 + 4XZ^2 + Z$, with $\mathcal{O} = [0, 1, 0]$ its neutral element.
 - (a) Find all points in $E(\mathbb{F}_5)$
 - (b) Show that $E(\mathbb{F}_5) \cong \mathbb{Z}/8\mathbb{Z}$ as abelian groups.
- 6. (a) Let $\rho = e^{2\pi i/3}$, and define the lattice $\Lambda_{\rho} := \mathbb{Z}\rho + \mathbb{Z} \subset \mathbb{C}$. Show that $\rho \Lambda_{\rho} = \Lambda_{\rho}$. (b) For a lattice Λ we define

$$G_4(\Lambda) = \sum_{0 \neq w \in \Lambda} w^{-4}.$$

Show that $G_4(\Lambda_{\rho}) = 0$, where Λ_{ρ} is as in (a) above.





SECTION B

- 7. (a) Let C and D be algebraic curves in $\mathbb{P}^2_{\mathbb{C}}$, and $P \in \mathbb{P}^2_{\mathbb{C}}$. Give necessary and sufficient conditions such that $I_P(C, D) = 1$.
 - (b) Find the points of intersection together with their intersection multiplicities of the pairs of projective curves C_F and C_G in $\mathbb{P}^2_{\mathbb{C}}$ defined by the polynomials

$$F(X, Y, Z) = X^3 - Y^3 + 4XZ^2$$

and

$$G(X, Y, Z) = X^2 + Y^2 + 4Z^2.$$

- (c) Let C_F and C_G be algebraic curves in $\mathbb{P}^2_{\mathbb{C}}$ both of degree n, defined by homogeneous polynomials $F, G \in \mathbb{C}[X, Y, Z]$, and assume $\sharp(C_F \cap C_G) = n^2$. We assume that there exists an irreducible curve C_H of degree m, defined by a homogeneous polynomial $H \in \mathbb{C}[X, Y, Z]$ such that $\sharp(C_H \cap C_F \cap C_G) = nm$ with $1 \leq m < n$.
 - i. Let $P = [a, b, c] \in C_H$ and assume that $P \notin C_F \cap C_G$. Define the polynomial

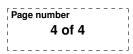
$$W(X, Y, Z) = F(a, b, c)G(X, Y, Z) - G(a, b, c)F(X, Y, Z).$$

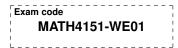
Show that H(X, Y, Z) divides W(X, Y, Z).

- ii. Show that there exists an algebraic curve E in $\mathbb{P}^2_{\mathbb{C}}$ of degree at most n-m that contains all the points in $(C_F \cap C_G) \setminus (C_H \cap C_F \cap C_G)$, that is the points in $C_F \cap C_G$, which are not points of C_H .
- iii. Show that the curve E above has degree exactly n m.
- 8. Let E be an elliptic curve in $\mathbb{P}^2_{\mathbb{C}}$ with neutral element \mathcal{O} being one of its flexes.
 - (a) Show that for any $P, Q, R \in E$ we have that
 - i. $P + Q = \mathcal{O}$ if and only if $L_{P,Q} \cap E = \{P, Q, \mathcal{O}\}.$
 - ii. $P + Q + R = \mathcal{O}$ if and only if $L_{P,Q} \cap E = \{P, Q, R\}$.

(Here we follow the convention from the lectures that $L_{P,Q}$ denotes the unique line that contains P and Q if $P \neq Q$, otherwise $L_{P,Q} = T_P(E)$, the tangent line of E at P.)

- (b) Show that any line through two distinct flexes of E meets E again at a different flex.
- (c) Consider two lines L_1 and L_2 in $\mathbb{P}^2_{\mathbb{C}}$ and assume that $L_1 \cap E = \{A_1, A_2, A_3\}$ and $L_2 \cap E = \{B_1, B_2, B_3\}$. Define points $C_1, C_2, C_3 \in E$ by $L_{A_i, B_i} \cap E = \{A_i, B_i, C_i\}$. Show that C_1, C_2, C_3 are collinear.
- (d) Assume now that E is given by $Y^2Z = X^3 + AXZ^2 + BZ^3$ with $4A^3 + 27B^2 \neq 0$ and $\mathcal{O} = [0, 1, 0]$. Let P and Q be any two flexes of E. Show that if we write [a, b, c] for the coordinates of the point P + 2Q with respect to the addition on E then $b \neq 0$.





- 9. Let $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$ be a lattice in \mathbb{C} and write $\wp(z) = \frac{1}{z^2} + \sum_{0 \neq w \in \Lambda} \left(\frac{1}{(z-w)^2} \frac{1}{w^2} \right)$ for the Weierstrass \wp -function associated to Λ .
 - (a) Show that $\wp'(z+w) = \wp'(z)$ for all $w \in \Lambda$ and that $\wp'(\frac{w_i}{2}) = 0$ for i = 1, 2, 3, where $w_3 := w_1 + w_2$.
 - (b) Let $1 < n \in \mathbb{N}$, and let $u \in \mathbb{C}$ with $nu \in \Lambda$. Then show that

$$u \equiv -u \mod \Lambda$$
, if and only if, $u \equiv \begin{cases} 0 \mod \Lambda, \text{ if } n \text{ odd} \\ 0, \frac{w_1}{2}, \frac{w_2}{2}, \frac{w_3}{2} \mod \Lambda, \text{ if } n \text{ is even} \end{cases}$

(c) Show that for all $1 < n \in \mathbb{N}$ there exist polynomials $P_n(X) \in \mathbb{C}[X]$ such that

$$(P_n(\wp(z)))^2 = n^2 \prod_{0 \neq u \in (\mathbb{C}/\Lambda)[n]} (\wp(z) - \wp(u))$$
 if *n* is odd,

and

$$\wp'(z)^2 \left(P_n(\wp(z)) \right)^2 = n^2 \prod_{0 \neq u \in (\mathbb{C}/\Lambda)[n]} \left(\wp(z) - \wp(u) \right) \quad \text{if } n \text{ is even},$$

(d) For each fixed choice of $P_n(X)$ as above, we define

$$f_n(z) = \begin{cases} P_n(\wp(z)) & \text{if } n \text{ is odd} \\ \wp'(z)P_n(\wp(z)) & \text{if } n \text{ is even} \end{cases}$$

Show that $\operatorname{ord}_0(f_n) = -(n^2 - 1)$. Further show that $f_n(z) = 0$ if and only if $z \in \mathbb{C} \setminus \Lambda$ and $nz \in \Lambda$.

(e) Let n > 2. Find the zeros and poles and their orders of the function

$$\frac{f_{n-1}(z)f_{n+1}(z)}{(f_n(z))^2}$$

10. Let *E* be an elliptic curve defined over the finite field \mathbb{F}_q , with $q = p^m$ for some prime *p*, and $m \in \mathbb{N}$. Define $a \in \mathbb{Z}$ by $\sharp E(\mathbb{F}_q) = q + 1 - a$, and $\alpha, \beta \in \mathbb{C}$ by

$$x^{2} - ax + q = (x - \alpha)(x - \beta).$$

- (a) Set $s_n = \alpha^n + \beta^n$, for $n \in \mathbb{N}$. Show that $s_0 = 2$, $s_1 = a$ and $s_{n+1} = as_n qs_{n-1}$ for $n \ge 1$.
- (b) Show that $a \equiv 0 \pmod{p}$ implies that $\sharp E(\mathbb{F}_{q^n})[p] = 1$ for all $n \in \mathbb{N}$.
- (c) Show that $a \not\equiv 0 \pmod{p}$ implies that $\sharp E(\mathbb{F}_{q^{p-1}})[p] \neq 1$
- (d) Assume $p \ge 5$ and m = 1. Show that $\sharp E(\mathbb{F}_p) = p+1$ if and only if $\sharp E(\mathbb{F}_{p^n})[p] = 1$ for all $n \in \mathbb{N}$.
- (e) Let p = 5 and consider the elliptic curve E over \mathbb{F}_5 defined by $Y^2 Z = X^3 + Z^3$ with $\mathcal{O} = [0, 1, 0]$. Determine $\sharp E(\mathbb{F}_{125})$ and $\sharp E(\mathbb{F}_{25})[5]$.