CS688 - COMPUTATIONAL ARITHMETIC-GEOMETRY & APPLICATIONS
NITIN SAXENA

ASSIGNMENT 4

POINTS: 70

DATE GIVEN: 03-APR-2023 DUE: 21-APR-2023 (6PM)

Rules:

- You are strongly encouraged to work *independently*. That is the best way to understand the subject.
- Write the solutions on your own and honorably *acknowledge* the sources if any. `cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Clearly express the fundamental *idea* of your proof/ algorithm before going into the other proof details. The distribution of partial marks is according to the proof steps.
- There will be a penalty if you write unnecessary or unrelated details in your solution. Also, do not repeat the proofs done in the class.
- Submit your solutions, before time, to your TA. Preferably, submit a printed/pdf copy of your LaTeXed or Word processed solution sheet.
  TA: Diptajit Roy `diptajit@cse.iitk.ac.in`
- Problems marked '0 points' are for practice.

Assume the field k to be $\overline{\mathbb{F}}_p$, let C be a smooth projective curve of genus g, and fix a point $P_0 \in C$.

Question 1: *[10 points]* Let D be a degree zero divisor. Show that there exists a degree $g-1$ divisor E such that $\ell(D + (2g-1)P_0 - E) = 1$.

Question 2: *[5 points]* Let D, E be as above. Show that $D + (g-1)P_0 - E$ is equal to a divisor D', s.t.:

(1) $D' =: \sum_{1 \le i \le g} P_i - g \cdot P_0$, and
(2) $P_1, \ldots, P_g$ are points on the curve C (i.e. $\deg(P_i) = 1$).

Question 3: *[15 points]* Let E be a degree $g-1$ divisor. Show that $\mathcal{D}_E := \{D \in \mathrm{Cl}_0(C) \,|\, \ell(D + (2g-1)P_0 - E) = 1\}$ is a quasi-projective variety.

Is it *smooth*?

Question 4: *[20 points]* Show that $\mathrm{Cl}_0(C)$ can be realized exactly as the set $J(C) := \{\sum_{1\le i\le g} P_i - g\cdot P_0 \,|\, P_i \in C\}$, satisfying:

(1) $J(C)$ is isomorphic to the projective variety $C^{(g)}/\mathrm{Symm}_g$, where $C^{(g)}$ is the g-fold Segre product of C; and identify tuple $(P_1 : P_2 : \cdots : P_g)$ as equal to all its permutations.
(2) $J(C)$ is a smooth projective variety of dimension g.
(3) For any divisor E of degree $g-1$, the quasi-PV $\mathcal{D}_E$ is an open set of $J(C)$. Thus, Qns.1-3 give a recipe to find an *open neighborhood* of any degree zero divisor D.

[$J(C)$ is called the *Jacobian* variety of the curve. It is both a PV and an *infinite* abelian group!]

Definition. What are the points P in the group $J(C)$ that have *finite* order? If $\ell \cdot P = 0$ then P is called an *ℓ-torsion* point of the Jacobian. The set of all such points is denoted $J(C)[\ell]$.

Question 5: *[10 points]* Let C be a *hyperelliptic* curve, given as $y^2 = f(x)$. Give a fast algorithm to compute $J(C)[2]$.

Question 6: *[10 points]* Compute the zeta function $Z(T)$ for the function field K of the curve $C : y^2 = x^3$, over $k = \mathbb{F}_q$.

Question 7: *[0 points]* Compute the *genus* of the three curves: $y^2 = x^2 + x$, $y^2 = x^3 + x$, and $y^2 = x^4 + x$.

Question 8: *[0 points]* Given a planar (smooth projective) curve C, give a fast algorithm to compute the genus g and a canonical class divisor W.

Question 9: *[0 points]* Given an explicit hyperelliptic curve as $y^2 = f(x)$, could the polynomial ideal system for its Jacobian $J(C)$ be *efficiently* presentable?

Question 10: *[0 points]* Is the ℓ-torsion finite? What is the structure of the ℓ-torsion group $J(C)[\ell]$?

Question 11: *[0 points]* What is the action of the Frobenius map on $J(C)[\ell]$, and what is its characteristic polynomial?

□□□