Problem sheet on canonical heights on Jacobians of hyperelliptic curves

PIMS Summer School on Explicit methods for Abelian Varieties

Problem 1. (Descent lemma and generators)

(a) Prove the descent lemma as stated in the lecture.

(b) Suppose that K is a number field, A/K is an abelian variety and $n \geq 2$ such that ${}^{A(K)}/_{nA(K)}$ is finite. Find an algorithm that computes generators of $A(K)$ given representatives $Q_1, \dots, Q_s \in A(K)$ of ${}^{A(K)}/_{nA(K)}$.

Problem 2. (Local decomposition of the height difference on elliptic curves)
Let $E/\mathbb{Q} : y^2 = x^3 + \alpha x + \beta$ be an elliptic curve, where $\alpha, \beta \in \mathbb{Z}$. If $P = (x_P, y_P) \in E(\mathbb{Q})$ is not 2-torsion, then $2P$ is an affine point with x-coordinate $g(P)/f(P)$, where

$$g(P) = x_P^4 - 2\alpha x_P^2 - 8\beta x_P(P) + \alpha^2\,,$$
$$f(P) = 4x_P^3 + 4\alpha x_P + 4\beta\,.$$

For a place v of $\mathbb{Q}$ (i.e. v is a prime number or $v = \infty$) and $P \in E(\mathbb{Q}_v) \setminus \{O\}$, define

$$\rho_v(P) := \frac{\max\{|f(P)|_v,\, |g(P)|_v\}}{\max\{|x_P|_v^4,\, 1\}} \in \mathbb{R}\,,$$

where the absolute values $|\cdot|_v$ are normalized to satisfy the product formula. We also define $\rho_v(O) := 1$. Show that the following functions are v-adically continuous and bounded on $E(\mathbb{Q}_v)$,

(a) the function ρ_v,

(b) the function $\varphi_v := \frac{1}{2}\log \rho_v$,

(c) the function Ψ_v defined by $\Psi_v(Q) := -\sum_{n=0}^{\infty} 4^{-n-1}\varphi_v(2^n Q)$.

Now let $P \in E(\mathbb{Q})$. Show that we have

(d) $\varphi_v(P) \neq 0$ only for finitely many v;

(e) $h(2P) - 4h(P) = \sum_v \varphi_v(P)$;

(f) $h(P) - \hat{h}(P) = \sum_v \Psi_v(P)\,.$

Note that one can also *define* the canonical height by $h - \sum_v \Psi_v$. Its properties are then simple consequences of the properties of h and Ψ_v.

In Problems 3 and 4 we denote by R be a discrete valuation ring with discrete valuation v, fraction field K of characteristic 0 and perfect residue field.

Let $\mathcal{C} \to \operatorname{Spec} R$ be a regular model of a nice curve C/K.

Problem 3. (Intersection matrix)

Show that the intersection matrix $M = (m_{ij})_{i,j} \in \mathbb{Q}^{n\times n}$ of $\mathcal{C}_v$ has the following properties:

(a) $m_{ij} = m_{ji} \geq 0$ for all $i \neq j$.

(b) $\sum_{j=1}^n m_{ij} = 0$ for all $i \in \{1,\ldots,n\}$.

(c) M is negative semidefinite.

(d) ${}^t(1 \ \ldots \ 1)$ generates $\ker(M)$.

Problem 4. (Correction divisor on an n-gon)

Suppose that the special fiber $\mathcal{C}_v$ is of the form $\mathcal{C}_v = \sum_{i=1}^n \Gamma_i$ and has the configurations of an n-gon (with transversal intersections). Let $i, j \in \{1,\ldots,n\}$ and let $D \in \operatorname{Div}^0(C/K)$ be a divisor such that

- $(D_{\mathcal{C}} \cdot \Gamma_i) = 1$,
- $(D_{\mathcal{C}} \cdot \Gamma_j) = -1$,
- $(D_{\mathcal{C}} \cdot \Gamma_k) = 0$ for $k \notin \{i,j\}$.

Compute $\Phi(D) \in \mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)/\mathbb{Q}\,\mathcal{C}_v$ and $\Phi(D)^2 \in \mathbb{Q}$.

Problem 5. (Automorphy factor of the Riemann theta function)

Let $\tau \in \mathbb{H}_g$ be a complex $g\times g$ matrix with positive definite imaginary part. Consider $\theta = \theta_{0,0}$, the Riemann theta function (with trivial characteristic) associated to τ:

$$\theta(z) = \theta_{0,0}(z) = \sum_{m\in\mathbb{Z}^g} \exp\left(\pi i {}^t m\tau m + 2\pi i {}^t m z\right) .$$

Show that θ satisfies the following functional equation with respect to the lattice $\mathbb{Z}^g + \tau\mathbb{Z}^g$:

$$\theta(z+\ell+\tau n) = \exp(-2\pi i {}^t n z - \pi i {}^t n\tau n)\,\theta(z)$$

for all $z \in \mathbb{C}^g$ and $\ell, n \in \mathbb{Z}^g$.

In Problems 6 and 7, let p be an odd prime and let

$$C/\mathbb{Q}_p \,:\, Y^2 \;=\; F(X,Z)$$

be a hyperelliptic curve, where $F \in \mathbb{Z}_p[X,Y]$ is a binary form of degree $2g+2 \geq 4$ such that $\operatorname{disc}(F) \neq 0$ and such that $f(x) := F(x,1)$ has degree $2g+1$ and is monic.
Let $\bar{C}$ be the Zariski closure of C in the weighted projective plane $\mathbb{P}_{\mathbb{Z}_p}(1,g+1,1)$.

Problem 6. (The valuation of the discriminant)

(a) Show that $\bar{C}$ is smooth if $\operatorname{ord}_p(\operatorname{disc}(F)) = 0$.

(b) Show that $\bar{C}$ is regular if $\operatorname{ord}_p(\operatorname{disc}(F)) \leq 1$.

Problem 7. (Computing a regular model)
Suppose that $F(X,Z)$ factors as $F(X,Z) = G(X,Z)\,(X^2+p^nZ^2)$, where $n \geq 1$ and $G \in \mathbb{Z}_p[X,Z]$ satisfies $\operatorname{ord}_p(\operatorname{disc}(G)) = 0$.

(a) Show that there is a unique singular point on $\bar{C}_p$.

(b) Using explicit blow-ups, show that there is a regular model $\mathcal{C}$ of C over $\mathbb{Z}_p$ such that the special fiber $\mathcal{C}_p$ is an n-gon.

Problem 8. (Intersection of sections)
Suppose that $\bar{C}$ is regular and let $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$ be distinct points in $C(\mathbb{Q}_p)$ such that $x_P, y_P, x_Q, y_Q \in \mathbb{Z}_p$. Show that

$$(P_{\bar{C}}, Q_{\bar{C}}) \;=\; \min\{\operatorname{ord}_p(x_P - x_Q),\, \operatorname{ord}_p(y_P - y_Q)\}\,.$$