**18.782 Introduction to Arithmetic Geometry** **Fall 2020**
**Problem Set #12** **Due: 12/9/2020**

---

These problems are related to the material covered in Lectures 33-35. I have made every effort to proof-read them, but some errors may remain. The first person to spot each error will receive 1-5 points of extra credit.

The problem set is due by 10:00pm on 12/9/2020 and should be submitted electronically as a pdf-file e-mailed to zzyzhang@mit.edu and roed@mit.edu (please include "18.782" in the subject of the email). Due to MIT end-of-term regulations and to give Zhiyu enough time to grade the homework, **no extensions will be given**: if you have not submitted the assignment by 10pm it will count as your dropped problem set for the term. As usual, you can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions and to identify collaborators and any sources not listed in the syllabus.

## Problem 1. Jacobians of hyperelliptic curves (60 points)

Suppose $k$ is a perfect field with $\mathrm{char}(k) \neq 2$ and $C/k$ is a hyperelliptic curve of the form $y^2 = f(x)$ with $f(x)$ monic and squarefree of degree $2g+1$. Recall that the Jacobian of $C$ is defined as the quotient $J_C = \mathrm{Div}^0(C)/\,\mathrm{Princ}(C)$ of divisors of degree 0 by the subgroup of principal divisors. In this problem we will describe a method due to David Cantor for computing in this group explicitly. We remark that there are similar algorithms available for other models of hyperelliptic curves (e.g. if $f(x)$ has degree $2g+2$), as well as a completely different approach using Riemann-Roch spaces due to Khuri-Makdisi.

**(a)** Let $P_\infty$ be the unique point at infinity on $C$. Show that any divisor of degree 0 is equivalent to a divisor of the form $\sum_{i=1}^r P_i - r \cdot P_\infty$, where $P_i \neq P_\infty$.

**(b)** We say that such a divisor is *semi-reduced* if there is no pair $P_i = (x, y)$ and $P_j = (x, -y)$ with $i \neq j$ (in particular, this implies that the multiplicity of any point with $y = 0$ must be 1). A semi-reduced divisor is *reduced* if $r \leq g$. Prove that every divisor is equivalent to a unique reduced divisor.

**(c)** (Mumford coordinates) Given a semi-reduced divisor $D = \sum_{i=1}^r \cdot P_i - r \cdot P_\infty$ with $P_i = (x_i, y_i)$, let $a = \prod_i (u - x_i) \in \bar{k}[u]$ and let $m_i$ be the multiplicity of $P_i$. Show that there is a unique polynomial $b \in \bar{k}[u]$ so that

(i) $b(u) - y_i$ is divisible by $(u - x_i)^{m_i}$,

(ii) $\deg(b) < r$.

Conversely, $a$ and $b$ determine $D$ since $a$ determines the $x_i$ and then $b$ determines the $y_i$. We write $D = \mathrm{div}(a, b)$.

**(d)** Show that $D$ is defined over $k$ if and only if $a, b \in k[u]$.

**(e)** Given two semi-reduced divisors $D_1 = \mathrm{div}(a_1, b_1)$ and $D_2 = \mathrm{div}(a_2, b_2)$, we'd like to describe the Mumford coordinates of $D_1 + D_2$ in terms of $a_1, b_1, a_2$ and $b_2$. We make the simplifying assumptions that $\gcd(a_1, a_2) = 1$ (all of the points in the summands have distinct $x$-coordinates) and that no $y$-coordinate is 0 for any point in the support of either divisor. Define $h_1$ and $h_2$ by

$$1 = a_1 h_1 + a_2 h_2,$$

and $a, b$ by

$$\begin{aligned} a &= a_1 a_2 \\ b &\equiv h_1 a_1 b_2 + h_2 a_2 b_1 \pmod{a}. \end{aligned}$$

Show that $D_1 + D_2 = \operatorname{div}(a, b)$.

**(f)** (optional due to tedious casework) In general, let $d = \gcd(a_1, a_2, b_1 + b_2)$ and define $h_1, h_2, h_3$ by

$$d = a_1 h_1 + a_2 h_2 + (b_1 + b_2) h_3,$$

and $a, b$ by

$$\begin{aligned} a &= a_1 a_2 / d^2 \\ b &\equiv (h_1 a_1 b_2 + h_2 a_2 b_1 + h_3(b_1 b_2 + f))/d \pmod{a}. \end{aligned}$$

Show that the numerator in the definition of $b$ is divisible by $d$ and that $D_1 + D_2 = \operatorname{div}(a, b)$. *Remark:* If $D_1 = D_2$ then $b \equiv b_1 + h_3(f - b_1^2)/d \pmod{a}$.

**(g)** The algorithm in **(e)** and **(f)** expresses $D_1 + D_2$ as a semi-reduced divisor, but in order to test for equality in the Jacobian we also need a reduction process. Suppose that $D = \operatorname{div}(a, b)$ is semi-reduced; we'd like to find an equivalent reduced divisor. Set

$$\begin{aligned} a' &= (f - b^2)/a, \\ b' &\equiv -b \pmod{a'}, \end{aligned}$$

and $E = \operatorname{div}(a', b')$. Show that the numerator in the definition of $a'$ is divisible by $a$, and that $E - D$ is the principal divisor associated to the function $b(x) - y$. Moreover, show that if $\deg(a) = m \geq g + 2$ then $\deg(a') \leq m - 2$, while if $\deg(a) = g + 1$ then $\deg(a') \leq g$. So repeating this process produces a reduced divisor equivalent to $D$.

**(h)** (optional due to trickiness: this was the main contribution of Cantor) Use the extended Euclidean algorithm to find polynomials $c, d$ so that setting $E = -(\operatorname{div}(c(x)b(x) - d(x)y) - D)$ yields a reduced divisor in one step (here div is the principal divisor associated to a function on $C$). The algorithm described in **(g)** requires $O(g^3)$ arithmetic operations (or $O(g^2 \log(g))$ if fast multiplication is used), while it is possible to save a factor of $g$ by computing $c$ and $d$ separately.

## Problem 2. Weil polynomials (40 points)

In this problem you will find an algorithm for producing all integer polynomials of degree $d$ all of whose roots have absolute value $\sqrt{q}$ for an integer $q$. You may find the following results useful:

**Theorem** (Rolle's theorem)**.** *Suppose $f : [a, b] \to \mathbb{R}$ is continuous on $[a, b]$, differentiable on $(a, b)$, and $f(a) = f(b)$. Then there exists $c \in [a, b]$ with $f'(c) = 0$.*

**Theorem** (Descartes' rule of signs). *Suppose $f(x) \in \mathbb{R}[x]$ is a polynomial, and let $m$ be the number of sign changes in the coefficients of $f$, ignoring zeros (e.g. if all coefficients are positive then $m = 0$). Then the number of positive roots of $f$ is at most $m$, and is congruent to $m$ modulo 2.*

**Theorem** (Newton identities). *Suppose $f(x) = \sum_{i=0}^{g} a_i x^i = a_g \prod_{i=1}^{g}(x - r_i)$. Define*

$$s_m = \sum_{i=1}^{g} r_i^m.$$

*Then*

$$m a_{g-m} + \sum_{j=0}^{m-1} a_{g-j} s_{m-j} = 0 \qquad (m = 1, \ldots, g).$$

**(a)** Let $S_{N,q} \subset \mathbb{Z}[x]$ be the set of polynomials of degree $N$ all of whose roots have absolute value $\sqrt{q}$, and let $T_{g,q} \subset \mathbb{Z}[x]$ be the set of polynomials of degree $g$ all of whose roots are real and within the interval $[-2\sqrt{q}, 2\sqrt{q}]$. Say that $f \in S_{2g,q}$ is *traceable* if the multiplicity of $\sqrt{q}$ as a root of $f$ is even. Prove that

$$\begin{aligned} S_{2g,q} &\leftrightarrow T_{g,q} \\ x^g f(x + q/x) &\leftarrow f \\ c\prod_{i=1}^{g}(x - \alpha_i)(x - \bar{\alpha}_i) &\mapsto c\prod_{i=1}^{g}(x - \alpha_i - \bar{\alpha}_i) \end{aligned}$$

define mutually inverse bijections between traceable elements of $S_{2g,q}$ and $T_{g,q}$.

**(b)** Show that every $f \in S_{2g+1,q}$ is divisible by either $x - \sqrt{q}$ or $x + \sqrt{q}$ (and, in particular, is empty if $q$ is not a square). It thus suffices to enumerate $T_{g,q}$ for each $g$ and $q$.

**(c)** Elements of $S_{2g,q}$ have $2g + 1$ coefficients, which seems like more degrees of freedom than the $g + 1$ coefficients needed to specify elements of $T_{g,q}$. We can resolve this discrepancy as follows. Show that, if $f = \sum_{i=0}^{2g} a_i x^i \in S_{2g,q}$ then either

(i) $a_i = q^{g-i} a_{2g-i}$ for $i = 0, \ldots, g$ if $f$ is traceable,

(ii) $a_i = -q^{g-i} a_{2g-i}$ for $i = 0, \ldots, g$ if $f$ is not traceable.

**(d)** Show that differentiation induces a map $D : T_{g,q} \to T_{g-1,q}$. Show that the fiber above any polynomial $f(x)$ is either empty or of the form $\{F(x) + d : d \in I \cap \mathbb{Z}\}$, where $f(x) = F'(x)$ and $I$ is a closed interval depending on $F$.

**(e)** Use **(c)** to describe an iterative algorithm for finding the monic elements of $T_{g,q}$ (and thus of $S_{2g,q}$ and $S_{2g+1,q}$).

**(f)** (optional) Execute the case $g = q = 2$. Either run your algorithm by hand, or implement and run it on a computer, and confirm that you find 35 traceable Weil polynomials.

**(g)** The basic algorithm described above can be improved by attempting to narrow the intervals early in order to avoid traversing down paths that eventually lead to no solutions (though you won't see this behavior in small cases such as $g = q = 2$). One can also modify it to allow for congruence conditions on the coefficients of the eventual element of $S_{2g,q}$ (this is useful when applying the Weil conjectures to $p$-adic methods for computing zeta functions, since working with a finite $p$-adic precision eventually yields congruences on the coefficients). Flesh out at least one improvement to the algorithm you gave in part **(d)**.

## Problem 3. Survey

Complete the following survey by rating each problem on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem.

| | Interest | Difficulty | Time Spent |
|---|---|---|---|
| Problem 1 | | | |
| Problem 2 | | | |

You should also make sure to fill out the MIT **course survey**; I'm also happy to hear suggestions personally (by Zulip or email) for improving the class if I teach something similar again in the future.