ANALYTIC NUMBER THEORY IN FUNCTION FIELDS
TCC 2015
PROBLEM SHEET 4

JULIO ANDRADE

1-) Fill in the details of the proof of Proposition 3.4 in [1].

2-) Fill in the details of the proof of Theorem 3.5 in [1].

3-) Suppose $d \mid q-1$ and that $m \in A$ is a polynomial of positive degree. Show that the number of d-th powers in $(A/mA)^*$ is given by $\Phi(m)/d^{\lambda(m)}$, where $\lambda(m)$ is the number of distinct monic prime divisors of m.

4-) Let $P \in A$ be a prime and consider the congruence $X^2 \equiv -1 (\text{mod } P)$ Show this congruence is solvable except in the case where $q \equiv 3 (\text{mod } 4)$ and $\deg(P)$ is odd.

5-) Suppose $d^{'} \mid q-1$ and $\alpha \in \mathbb{F}_q^*$ is an element of order $d^{'}$. Let $P \in A$ be a prime of positive degree and suppose that d is a divisor of $|P|-1$. Show that $X^d \equiv \alpha (\text{mod } P)$ is solvable if and only if $dd^{'}$ divides $|P|-1$. Show how Exercise 4 is a special case of this result.

6-) Suppose that d is a positive integer and that $q \equiv 1 (\text{ mod } 4d)$. Let $P \in A$ be a monic prime. Show that $X^d \equiv T (\text{mod } P)$ if and only if the constant term of P, i.e. $P(0)$, is a d-th power in $\mathbb{F}_q$.

7-) Suppose d divides $q-1$ and that $P \in A$ is a prime. Show that the number of solutions to $X^d \equiv a (\text{mod} P)$ is given by

$$1 + \left(\frac{a}{P}\right)_d + \left(\frac{a}{P}\right)_d^2 + \cdots + \left(\frac{a}{P}\right)_d^{d-1}.$$

8-) Let $b \in A$ and suppose $b = \beta P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is the prime decomposition of b. Here, $\beta \in \mathbb{F}_q^*$ and the P_i are distinct monic primes. Consider $(a/b)_d$ as a homomorphism from $(A/bA)^*$ to the cyclic group $\langle \zeta_d \rangle$ generated by an element $\zeta_d \in \mathbb{F}_q^*$ of order d. Show that this map is onto if and only if the greatest common divisor of the set $\{e_1, e_2, \ldots, e_t\}$ is relatively prime to d.

Date: April 28, 2015.

9-) Suppose $d \mid q-1$ and $a, b_1, b_2 \in A$. Show that $(a/b_1)_d = (a/b_2)_d$ if the following conditions hold: $b_1 \equiv b_2 (\text{mod } a)$, $\deg(b_1) \equiv \deg(b_2) (\text{mod } d)$, and $\text{sgn}_d(b_1) = \text{sgn}_d(b_2)$.

10-) In this exercise we give an analogue of the classical Gauss criterion for the Legendre symbol. Let $P \in A$ be a prime. Show that every non-zero residue class modulo P has a unique representative of the form μm where $\mu \in \mathbb{F}_q^*$ and m is a monic polynomial of degree less than $\deg(P)$. Let $\mathcal{M}$ denote the set of monics of degree less than $\deg(P)$. Suppose $a \in A$ with $P \nmid a$. For each $m \in \mathcal{M}$ write $am \equiv \mu_m m^{'} (\text{mod } P)$ where $\mu_m \in \mathbb{F}_q^*$ and $m^{'} \in \mathcal{M}$. Show

$$\left(\frac{a}{P}\right)_{q-1} = \prod_{m \in \mathcal{M}} \mu_m.$$

References

[1] M. Rosen: Number Theory in Function Fields, Graduate Texts in Mathematics 210, Springer-Verlag, New York (2002).

University of Oxford - Mathematical Institute
E-mail address: j.c.andrade.math@gmail.com