TOPICS IN NUMBER THEORY 2013
FINAL ASSIGNMENT
DUE DATE: JULY 21, 2013

Instructions:
You may not consult with anyone except myself.
To be handed in by July 21, 2013 either in person, in my mailbox or by email. Please keep a copy for yourself!

1. Let N_n be a sequence of numbers, with $|N_n| \leq r^n$ for some $r > 0$. Define the generating function

$$Z(u) := \exp \sum_{n=1}^{\infty} N_n \frac{u^n}{n}, \quad |u| < 1/r$$

Suppose that we know that $Z(u)$ is a rational function of the form

$$Z(u) = \frac{\prod_{j=1}^{J}(1-\alpha_j u)}{\prod_{k=1}^{K}(1-\beta_k u)}$$

Show that

$$N_n = \sum_{k=1}^{K} \beta_k^n - \sum_{j=1}^{J} \alpha_j^n$$

2. Let $s > 1$, $\epsilon_1, \dots, \epsilon_s \in \{\pm 1\}$ be a choice of signs, and $0 \leq a_1 < \dots < a_s$ distinct integers. For an odd prime p, let $N(p)$ be the number of residues $x \in \mathbb{Z}/p\mathbb{Z}$ for which

$$(\frac{x+a_1}{p}) = \epsilon_1, \dots, (\frac{x+a_s}{p}) = \epsilon_s$$

where $(\frac{x}{p})$ is the Legendre symbol. Show that

$$N(p) \sim \frac{p}{2^s}$$

as $p \to \infty$.

3. Let q be a prime power, $r > 2$, $r \mid q-1$ and assume that -1 is an r-th power in the finite field $\mathbb{F}_q$.

a. Show that the number N_1^{aff} of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the equation $x^r + y^r = 1$ is given by

$$N_1^{\text{aff}} = q + 1 - r + \sum^{*} J(\chi_1, \chi_2)$$

the sum $\sum^*$ taken over all pairs (χ_1, χ_2) of characters of $\mathbb{F}_q^\times$ with $\chi_1^r = \chi_2^r = \mathbf{1}$ such that $\chi_1, \chi_2, \chi_1 \cdot \chi_2 \neq \mathbf{1}$, and where

$$J(\chi_1, \chi_2) = \sum_{\substack{u \in \mathbb{F}_q \\ u \neq 0,1}} \chi_1(u)\chi_2(1-u)$$

is the Jacobi sum.

b. Find the number N_n^{proj} of points $(X : Y : Z) \in \mathbb{P}^2$ on the projective curve

$$C_r = \{X^r + Y^r = Z^r\} \subset \mathbb{P}^2$$

with coordinates in the degree n extension $\mathbb{F}_{q^n}$ (including points at infinity, if any exist).

c. Show that the zeta function of $C_r/\mathbb{F}_q$, defined as

$$Z(C_r/\mathbb{F}_q, T) := \exp(\sum_{n \geq 1} N_n^{\text{proj}} \frac{T^n}{n}), \quad |T| < 1/q \ ,$$

is given by

$$Z(C_r/\mathbb{F}_q, T) = \frac{\prod(1 + J(\chi_1, \chi_2)T)}{(1-T)(1-qT)}$$

the product over all pairs (χ_1, χ_2) of characters as in part **3.a**.

d. Prove the functional equation for $Z(T) = Z(C_r/\mathbb{F}_q, T)$:

$$Z(\frac{1}{qT}) = (qT^2)^{1-g} Z(T)$$

where $g = (r-1)(r-2)/2$.