JProf. Dr. Simon Lentner
Algebra and Number Theory
FB Mathematik, Universität Hamburg

Sheet 5

Problem 1 (3 Points)
For any prime q we consider the Fermat curve for power $q+1$ in characteristic q:

$$x^{q+1} + y^{q+1} = 1$$

Show that the number of projective points over $\mathbb{F}_q,\ \mathbb{F}_{q^2}$ are $q+1,\ q^2+1+q(q-1)q$.

The Fermat curve has genus $q(q-1)/2$. Show that the number of solutions over $\mathbb{F}_{q^2}$ are the maximal number of solutions for a curve of this genus allowed by the proven Weil conjectures. Then determine the local zeta function from this observation.
Hint: For counting $\mathbb{F}_{q^2}$-points, show first that always $x^{q+1} \in \mathbb{F}_q$

Problem 2 (1+1+1+2+1+3+3+2+1+2 Points)
For any prime q we consider the Drinfel'd curve in characteristic q:

$$Y:\ xy^q - x^q y = 1$$

a) Prove that the group $\mathrm{SL}_2(\mathbb{F}_q)$ of matrices with determinant one over $\mathbb{F}_q$ acts by linear transformations on the points $Y(\mathbb{K})$.

b) Which primes give good reductions?

c) Calculate the infinite points of the projective completions $\tilde{Y}(\mathbb{K})$.

d) Calculate the solutions $Y(\mathbb{F}_q), \tilde{Y}(\mathbb{F}_q)$ and $Y(\mathbb{F}_{q^2}), \tilde{Y}(\mathbb{F}_{q^2})$.

e) Consider the map from $\tilde{Y}$ to $X := \mathbb{KP}^1$ sending $(x,y,z) \mapsto (x,y)\mathbb{K}$. Over which points in X lay infinite points of $\tilde{Y}$? Show that the finite points of Y lay over $\mathbb{KP}^1 \backslash \mathbb{F}_q\mathbb{P}^1$ and the fibre (preimage) over $t \in \mathbb{K}\backslash\mathbb{F}_q$ are solutions to

$$t^q - t = z^{q+1}, \qquad z \neq 0$$

What is the fibre for the algebraic closure $\mathbb{K} = \bar{\mathbb{F}}_q$?

f) $\star$ Let us assume some odd prime $\ell \neq p$ such that q is a generator of $\mathbb{Z}_\ell^\times$. Convince yourself that $\mathbb{F}_q(\zeta), \zeta^\ell = 1$ is the unique field $\mathbb{F}_{q^k}$ of even degee $k = \ell - 1$. Then show that the number of solutions $(z,t), t \neq \mathbb{F}_q$ is q times the number of nonzero vectors $v \in (\mathbb{F}_q)^k$ with $v^T A v = 0$ for

$$A_{ij} = \begin{cases} -k/2, & \text{for } i-j\pm 1 = k/2 \text{ modulo } k \\ 1, & \text{else} \end{cases} \qquad \text{resp.} \begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix} \text{ for } k=2$$

Hint: Go into an explicit basis and characterize first all values $t^q - t$

g) Calculate the rank r and the determinant d of the nondegenerate part of A, depending on q^k. You may start with $k = 2, 4$.

h) Show that $d(-1)^{k/2}$ is always a nonsquare modulo p. You will need the famous quadratic reciprocity law by Gauß.

i) It is known that quadratic forms in n variables over $\mathbb{F}_q$ are classified by the rank and whether the determinant d is square or not. Some calculations show that the number of (finite) zeroes is for even n

$$|\{v|v^T Av = 0\}| = \begin{cases} q^{n-r}\left(q^{r-1} + (q-1)q^{r/2-1}\right), & \text{for } d(-1)^{k/2} \text{ a square} \\ q^{n-r}\left(q^{r-1} - (q-1)q^{r/2-1}\right), & \text{for } d(-1)^{k/2} \text{ a nonsquare} \end{cases}$$

Conclude for q, ℓ, k as above the overall number of projective points of $\tilde{Y}$ to be

$$|\tilde{Y}(\mathbb{F}_{q^k})| = \begin{cases} q^k + 1 - (q-1)q^{k/2}, & \text{for } k = 2\ (4) \\ q^k + 1 - q(q-1)q^{k/2}, & \text{for } k = 0\ (4) \end{cases}$$

j) By Riemann-Roch an irreducible smooth projective curve of degree d has genus $g = (d-1)(d-2)/2$. Use the proven Weil conjectures to determine the local zeta function of $\tilde{Y}$ over the prime q.

Hint: You may assume $q = 3\ (4)$ to use the formula above for $\ell = 5, k = 4$, but is this really necessary?