Elliptic Curves and Modular Forms (Master)
Wintersemester 2017/18

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

Sheet 4

Problem 1 (2 Points)
Determine the rational points of finite order for $x^2 - Dy^2 = 1$ depending on squarefree $D \in \mathbb{Q}\backslash\{0\}$

Problem 2 (2 Points)
Calculate the local zeta-function $Z(T)$ for the d-dimensional affine space $\mathbb{K}^d$ and projective space $\mathbb{KP}^d$

Problem 3 (1+1+2 Points)
We study the reduction modulo p of our curve $y^2 - Dx^2 = 1$ of genus 0
for any squarefree $0 \neq D$.

a) For which primes p is this equation smooth over $\mathbb{F}_p$?

b) Determine the points of the projective completion for $D = -1$ over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$.

c) For all primes calculate the local zeta-function for any $0 \neq D$.

Hint: Do not forget the infinite point(s). In this exercise, let us count non-smooth points in characteristic $\neq 2$ *with multiplicity* 2.

Problem 4 (1+1+1+2+3+2+2 Points)
We want to calculate the local zeta-function of the Fermat curve $x^3 + y^3 = 1$
(which is an elliptic curve) as implicitly done by Gauss using Gauss sums.
Hint: The problem is given in a way that proving the $\star$*-parts can be skipped.*

a) Determine which primes are good reductions.
Assume in what follows p is such a prime.

b) Determine the number of solutions for any $\mathbb{F}_{p^k}$ with $3 \nmid p^k - 1$.
Assume in what follows that $3 \mid p^k - 1$.

c) Determine the infinite solution(s) and the solutions where x or y is zero.
Assume in what follows that $x, y \neq 0$ are finite.

d) $\star$ Let $\chi : \mathbb{F}_{p^k}^\times \to \mathbb{C}^\times$ a group homomorphism / character, denote the trivial character by $\chi_{triv}(a) = 1$. Prove for $a \in \mathbb{F}_{p^k}^\times$ that

$$|\{x^n = a\}| = \sum_{\chi^n = \chi_{triv}} \chi(a)$$

Hint: You may for simplicity assume n prime, but this is not necessary.
This formula easily implies an expression counting solutions of $x^3 + y^3 = 1$ in terms of so-called Jacobi sums $J(\chi_1, \chi_2) := \sum_{a \neq 0,1} \chi_1(a)\chi_2(1-a)$, namely:

$$|X(\mathbb{F}_{p^k})| - 9 = \sum_{a+b=1,\ a,b\neq 0} |\{x^3 = a\}| \cdot |\{y^3 = b\}| = \sum_{\substack{\chi_1,\chi_2 \\ \chi_1^3=\chi_1^3=\chi_{triv}}} J(\chi_1, \chi_2)$$

e) $\star$ Calculate some trivial Jacobi sums to arrive at

$$|X(\mathbb{F}_{p^k})| - 9 = p^k - 8 + J(\chi, \chi) + \overline{J(\chi, \chi)}$$

for $\chi, \overline{\chi}$ the nontrivial characters of order 3.

f) The Hasse-Daveport relation (Koblitz II 2 Problems 10-17) relates Jacobi sums over field extensions (for trivially extended characters) as follows

$$-J_{\mathbb{F}_{p^k}}(\chi_1, \chi_2) = (-J_{\mathbb{F}_p}(\chi_1, \chi_2))^k$$

Use this fact to give a formula for $|X(\mathbb{F}_{p^k})|$ for $3 \mid p^k - 1$, depending only on the unknown complex number $\alpha := -J_{\mathbb{F}_p}(\chi, \chi)$, and explicitly calculate the overall zeta-function for primes $3 \mid p - 1$.

Combine with your earlier findings to also give an explicit formula for the zeta-function for primes $3 \nmid p - 1$.
$\star\star$ Can you prove that the numerator is in fact rational, to be precise $1 + pT^2$?

g) For $p = 7$ determine explicitly the solutions of $x^3 + y^3 = 1$. Also, calculate explicitly the Jacobi sum α (and its absolute value) and compare your formula above for $|X(\mathbb{F}_p)|$ to your count. What is the prediction for $|X(\mathbb{F}_{p^2})|$? Write down the explicit zeta-function for $p = 7$.