Kryptography Sheet 9

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 18.12.2023, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: Projective plane over a finite field

Let k be a field with p^r many elements.
Show in two different ways that there are $p^{2r} + p^r + 1$ many points in $\mathbb{P}^2(k)$.
Why are there just as many lines in $\mathbb{P}^2(k)$?

Exercise 2: Calculation of projective intersection points with multiplicities

Let k be an arbitrary field.

(a) Calculate all points at infinity that lie on the parabolas $y = x^2$ and $y = -x^2 + 1$.

(b) How many projective intersection points are there (counted with multiplicities)?

(c) How could be formulated a generalization of (b) for curves $f_1(x, y) = 0$ and $f_2(x, y) = 0$, where $f_1, f_2 \in \mathbb{C}[x, y]$ with $f_1 \neq f_2$? Think also of the case of two lines.

Exercise 3: Singular points on a projective curve

(a) Let k be a field of characteristic 0 and $F(X, Y, Z) \in k[X, Y, Z] \setminus k$ be homogeneous of degree d. Show that F solves Euler's Differential Equation

$$X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} + Z\frac{\partial F}{\partial Z} = dF.$$

(b) Bernoulli's Lemniscate is the curve $\mathcal{C}_f$ with $f(x, y) = (x^2 + y^2)^2 - 2(x^2 - y^2)$. Determine all singular points on $\mathcal{C}_{F_f} \subseteq \mathbb{P}^2(\mathbb{C})$. Which points lie on the line of infinity?

Exercise 4: A model of Boy's surface

Visit the link
`www.savoir-sans-frontieres.com/JPP/telechargeables/Deutch/DAS%20_TOPOLOGIKON.pdf`
where you find on p. 48 of the pdf-file an instruction for assembling Boy's surface which represents $\mathbb{P}^2(\mathbb{R})$ in $\mathbb{R}^3$. Fold this surface and bring your model to the exercise group.