Fachbereich Mathematik
Wintersemester 2010/11

Mohamed Barakat
Simon Hampe

Cryptography
Homework assignment 12

Due date: Wednesday 02/02 at 13:45

Exercise 1. (1) Determine (as subsets) all lines in $\mathbb{P}^2(\mathbb{F}_2)$. Sketch all lines in a graph with vertices being the points of $\mathbb{P}^2(\mathbb{F}_2)$: If two vertices are connected by an edge then the corresponding points lie on a line.

(2) Derive a formula for the number of points in $\mathbb{P}^2(\mathbb{F}_q)$.

(3) Derive a formula for the number of lines in $\mathbb{P}^2(\mathbb{F}_q)$.

(4) Explain the relation between the two numbers.

Exercise 2. Let E be a WEIERSTRASS equation of the form $y^2 = f(x)$ over a field K with $f(x) = x^3 + a_2x^2 + a_4x + a_6$. A point $(x_0, y_0) \in E(K)$ is called **singular** if $\frac{\partial F}{\partial y}(x_0, y_0) = \frac{\partial F}{\partial x}(x_0, y_0) = 0$, where $F = y^2 - f(x)$.

(1) Show in the case $\operatorname{char} K \neq 2$:
  (a) Prove: E is singular $\iff$ $\operatorname{disc} f = 0$.
  The discriminant of a degree n polynomial $f \in K[x]$ is defined as $\operatorname{disc} f := \prod_{i \neq j}(\alpha_i - \alpha_j)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f in the splitting field. In particular, $\operatorname{disc} f = 0$ iff f has a multiple root (in the splitting field).
  (b) E has at most one singular point.

(2) Let $K = \mathbb{F}_{2^n}$ for $n \in \mathbb{N}$:
  (a) Each element of K is a square.
  (b) E is singular.

Exercise 3. Let $K = \mathbb{F}_{2^n}$ for $n \in \mathbb{N}$:

(1) Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a WEIERSTRASS equation over K. A linear transformation in the variables x, y is the substitution

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \cdot \begin{pmatrix} x \\ y \end{pmatrix} + b$$

with $A \in \mathrm{GL}_2(K)$ and $b \in K^2$. Show
  (a) If $a_1 \neq 0$ then E can be changed by a linear transformation to $a_4 = 0$ without altering a_1 and a_3.
  (b) If $a_1 = 0, a_3 \neq 0$ then E can be changed by a linear transformation to $a_2 = 0$ without altering a_1 and a_3.

(2) Describe a simple condition for the non-smoothness of E in the cases
  (a) $a_1 \neq 0$, $a_3 = 0$.
  (b) $a_1 = 0$, $a_3 \neq 0$.
  Hint: Assume the simple form of E achieved in (1).

(3) Classify all elliptic curves over $\mathbb{F}_2$ satisfying the simple form achieved in (1).