Kryptography Sheet 10

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 8.1.2024, before the lecture starts

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

Exercise 1: Multiple zeros of a polynomial of degree 3

Let k be a field with $\operatorname{char} k \neq 2, 3$.
Show: The polynomial $f(x) = x^3 + ax + b \in k[x]$ has multiple zeros if and only if $4a^3 + 27b^2 = 0$.
(Hint: $x^3 + ax + b = (x-u)^2(x-v)$ and comparison of coefficients).
Explain why the condition $\operatorname{char} k \neq 2, 3$ is needed in the proof.

Exercise 2: Elliptic curves over finite fields and addition of points

Consider over the finite field $\mathbb{F}_p$ the equation $y^2 = x^3 + x + 9$ and its solution set $E \subseteq \mathbb{F}_p^2$.

(a) For which $p \in \{2, 3, 5, 7, 19\}$ is E an elliptic curve?

(b) Which of the points of E over $\mathbb{F}_{19}$ are intersection points with the line $y = x + 6$?

(c) Let $p = 19$ and let $P := (12, 18)$, $Q := (7, 13)$, $R := (9, 14) \in E$. Compute the intersection point $P * Q$ of the line through P and Q with E, and also the intersection point $Q * R$ of the line through Q and R with E.

(d) Let $P + Q$ the point which is given as the reflection of $P * Q$ from (c) at the x-axis, and analogously let $Q + R$ be given. Compute that $(P + Q) + R = P + (Q + R)$ holds.

Exercise 3: Curves of degree 3 and tangents

Sketch the following elliptic curves over $k = \mathbb{R}$:

$$E_1 : y^2 = x^3 - x$$
$$E_2 : y^2 = x^3 + 1$$

Sketch also the curves $E_3 : y^2 = x^3 + x^2$, $E_4 : y^2 = x^3$, which are not elliptic.
Determine the tangent in the point $P = [0 : 0 : 1]$ of E_1, and the tangents in the points $Q_\pm = [0 : \pm 1 : 1]$ of E_2.

**** Merry Christmas and a good start for the new year 2024 ****