Kryptographie **Blatt 10**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 8.1.2024, vor der Vorlesung

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

Aufgabe 1: Mehrfache Nullstellen bei einem Polynom vom Grad 3

Sei k ein Körper mit $\operatorname{char} k \neq 2, 3$.
Zeigen Sie: Das Polynom $f(x) = x^3 + ax + b \in k[x]$ hat genau dann mehrfache Nullstellen, wenn $4a^3 + 27b^2 = 0$ ist. (Tipp: $x^3 + ax + b = (x - u)^2(x - v)$ und Koeffizientenvergleich).
Inwiefern wird im Beweis benötigt, dass $\operatorname{char} k \neq 2, 3$ gilt?

Aufgabe 2: Elliptische Kurven über endlichen Körpern und Punkteaddition

Gegeben sei die über dem endlichen Körper $\mathbb{F}_p$ durch die Gleichung $y^2 = x^3 + x + 9$ definierte Lösungsmenge $E \subseteq \mathbb{F}_p^2$.

(a) Für welche $p \in \{2, 3, 5, 7, 19\}$ ist E eine elliptische Kurve?

(b) Welche der Punkte von E über $\mathbb{F}_{19}$ sind Schnittpunkte mit der Geraden $y = x + 6$?

(c) Sei $p = 19$ und sei $P := (12, 18)$, $Q := (7, 13)$, $R := (9, 14) \in E$. Berechnen Sie den Schnittpunkt $P * Q$ der Geraden durch P und Q mit E, sowie den Schnittpunkt $Q * R$ der Geraden durch Q und R mit E.

(d) Sei $P+Q$ der an der x-Achse gespiegelte Punkt $P*Q$ aus (c), und analog sei $Q+R$ gegeben. Rechnen Sie nach, dass $(P + Q) + R = P + (Q + R)$ gilt.

Aufgabe 3: Kurven dritten Grades und Tangenten

Skizzieren Sie folgende elliptische Kurven über $k = \mathbb{R}$:

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

Skizzieren Sie auch die Kurven $E_3 : y^2 = x^3 + x^2$, $E_4 : y^2 = x^3$, die nicht elliptisch sind.
Bestimmen Sie die Tangente im Punkt $P = [0 : 0 : 1]$ von E_1, und die Tangenten in den Punkten $Q_\pm = [0 : \pm 1 : 1]$ von E_2.

**** Frohe Weihnachten und einen guten Start ins neue Jahr 2024 ****