Übungen zur Vorlesung **Blatt 4**

Elliptische Kurven und Kryptographie 18.05.2015

PD Dr. K. Halupczok

Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 18. Mai 2015, bis 12:15 Uhr in die Briefkästen

---

Aufgabe 1:

Sei $k = \mathbb{F}_2$ und $f(x) = x^3 + x + 1$.

(a) Zeigen Sie, dass das Polynom f irreduzibel in $\mathbb{F}_2[x]$ ist.
(b) Bestimmen Sie das inverse Element der Restklasse x^2 in $\mathbb{F}_2[x]/(f)$.
(c) Ist das Polynom $g(x) = x^3 + x^2 + x + 1$ auch irreduzibel? Falls nein, geben Sie eine Faktorisierung an.

Aufgabe 2:

Sei k ein Körper mit p^r Elementen. Zeigen Sie auf zwei verschiedene Weisen, dass es $p^{2r}+p^r+1$ Punkte in $\mathbb{P}^2(k)$ gibt.

Aufgabe 3:

Sei $f(x,y) = y^2 - x^3 - ax - b$ mit $a, b \in \mathbb{R}$ und $\mathcal{C}_f(\mathbb{R}^2)$ die zugehörige affine Kurve. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

(a) Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle.
(b) $4a^3 = -27b^2$
(c) $\mathcal{C}_f(\mathbb{R}^2)$ hat einen singulären Punkt.

Aufgabe 4:

(a) Berechnen Sie alle unendlich fernen Punkte auf den Parabeln $y = x^2$ und $y = -x^2 + 1$.
(b) Wieviele projektive Schnittpunkte (gezählt mit Vielfachheiten) gibt es?
(c) Wie könnte eine Verallgemeinerung von b) auf die Kurven $f_1(x,y) = 0$ und $f_2(x,y) = 0$ aussehen, wobei $f_1, f_2 \in \mathbb{C}[x,y]$ mit $f_1 \neq f_2$? Denken Sie dabei auch an den Fall zweier Geraden.

Aufgabe 5 (4 Zusatzpunkte)

Unter dem Link `www.savoir-sans-frontieres.com/JPP/telechargeables/Deutch/DAS%20_TOPOLOGIKON.pdf` findet man auf S. 50 der pdf–Datei eine Bastelanleitung der Boyschen Fläche, die $\mathbb{P}^2(\mathbb{R})$ im $\mathbb{R}^3$ darstellt. Basteln Sie diese Fläche nach und bringen Sie ihr Modell in die Übungsgruppe mit.