RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Jun.-Prof. Roberto Avanzi
Enrico Thomae

Präsenzübungen zur Vorlesung

Diskrete Mathematik II

SoSe 2010

Blatt 6 / 29. Juni 2010

AUFGABE 41:
Seien E_1 und E_2 zwei über dem Körper $\mathbb{F}_q$ isomorphe Kurven in allgemeiner Weierstrass-Form. Zeigen sie E_1 ist genau dann singulär, wenn E_2 singulär ist, d.h. E_1 ist genau dann elliptisch, wenn E_2 elliptisch ist.

AUFGABE 42:
Für die vereinfachte Weierstrass-Form $y^2 = x^3 + ax + b$ wurde gezeigt, dass sie singulär ist genau dann, wenn $4a^3 + 27b^2 = 0$ ist. Zeigen Sie, dass diese vereinfachte Weierstrass-Form für Körper der Charakteristik 2 immer eine singuläre Kurve beschreibt. Was können Sie in Körpern der Charakteristik 3 aussagen?

AUFGABE 43:
Für Körper der Charakteristik 2 lautet die vereinfachte Weierstrass-Form

$$E : y^2 + xy = x^3 + a_2x^2 + a_6.$$

Zeigen Sie, dass sich diese Kurve durch admissible change of variables in allgemeine Weierstrass-Form bringen lässt, d.h. dass die vereinfachte Form isomorph zur allgemeinen Weierstrass-Form ist.

AUFGABE 44:
Sei $E : y^2 = x^3 + 2x + 3$ die in Aufgabe 36 über $\mathbb{F}_{17}$ definierte elliptische Kurve. Berechnen Sie

(a) $(9, 11) + (3, 11)$,

(b) $2 \cdot (9, 11)$,

(c) $377 \cdot (9, 11)$.