MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Dr. Otto Forster

WS 2000/2001

Elliptische Funktionen und Elliptische Kurven, Übungen

Blatt 12

Es sei k stets ein algebraisch abgeschlossener Körper mit $\mathrm{char}(k) \neq 2, 3$ und p eine Primzahl > 3.

Aufgabe 45

Es seien zwei elliptische Kurven $E_1 : Y^2 = X^3 + aX + b$, $E_2 : Y^2 = X^3 + cX + d$ in $\mathbb{P}_2(k)$, die über dem Unterkörper $k_0 \subset k$ definiert sind, gegeben.
Ein *Isomorphismus* von E_1 nach E_2 über k_0 wird durch eine Zuordnung

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} \alpha X \\ \beta Y \end{pmatrix} \quad \text{mit } \alpha^3 = \beta^2 \quad \text{für } \alpha, \beta \in k_0^*$$

definiert, welche die Kurve E_1 in die Kurve E_2 überführt. Zeigen Sie:

Ist $a \neq 0$ ein Quadrat im Körper k_0, so ist $E_1 : Y^2 = X^3 + aX + b$ isomorph zu einer elliptischen Kurve

$$Y^2 = X^3 + X + b' \quad \text{mit geeignetem } b' \in k_0$$

Aufgabe 46

Man zeige für die zwei elliptischen Kurven über $k_0 \subset k$, $b, b' \in k_0$:
$Y^2 = X^3 + X + b$ ist genau dann isomorph zu $Y^2 = X^3 + X + b'$, wenn $b = \pm b'$.

Aufgabe 47

Man betrachte die elliptische Kurven $E_b : Y^2 = X^3 + b$ mit $b \neq 0$ über dem Körper $\mathbb{F}_p$.
Man zeige: Genau dann ist jede Kurve E_b, $b \in \mathbb{F}_p^*$, über $\mathbb{F}_p$ isomorph zu $Y^2 = X^3 + 1$, wenn 3 nicht $(p-1)$ teilt.

Aufgabe 48

Sei $E : Y^2 = X^3 + aX + b$ eine elliptische Kurve mit $a, b \in \mathbb{F}_p$, und

$$\mathrm{Card}(E(\mathbb{F}_p)) = (p+1) + t.$$

(Nach dem Satz von Hasse ist $|t| \leq 2\sqrt{p}$.) Man konstruiere, ausgehend von der Gleichung $Y^2 = X^3 + aX + b$, eine Kurve E' mit

$$\mathrm{Card}(E'(\mathbb{F}_p)) = (p+1) - t.$$

Abgabetermin: Montag, 29.01.2001, 9:10 Uhr, Übungskasten vor HS 138.
Bitte werfen Sie auch einen ausgefüllten **Übungsschein** in den Übungskasten ein.