Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2012
13. Juli 2012

Elliptische Kurven

Klausur

Aufgabe 1

Sei K ein algebraisch abgeschlossener Körper mit $\mathrm{Char}(K) \neq 2$.
Sei $C \subset \mathbb{P}_2(K)$ die projektiv-algebraische Kurve mit affiner Geichung

$$X^4 + Y^4 = 1.$$

Man bestimme alle unendlich fernen Punkte und alle Singularitäten von C.

Aufgabe 2

Sei K ein endlicher Körper der Charakteristik > 3 und E die elliptische Kurve mit affiner Gleichung

$$Y^2 = f(X) := X^3 + aX + b, \qquad a, b \in K, \quad 4a^3 + 27b^2 \neq 0.$$

Man beweise: Genau dann ist $\#E(K)$ gerade, wenn das Polynom $f(X)$ eine Nullstelle in K besitzt.

Aufgabe 3

Sei E elliptische Kurve über dem Körper $\mathbb{F}_5$ mit affiner Gleichung

$$Y^2 = X^3 + X + 1.$$

a) Man bestimme die Anzahl der Punkte $\#E(\mathbb{F}_5)$.

b)* (Nur bearbeiten, wenn alle anderen Aufgaben gelöst sind!)
Man zeige, dass die Gruppe $E(\mathbb{F}_5)$ zyklisch ist.

Aufgabe 4

Sei p eine Primzahl und G eine zyklische Gruppe der Ordnung p^2 mit erzeugendem Element g. Sei $x \in G$ ein weiteres Element.

a) Man beweise, dass G genau eine zyklische Untergruppe G_1 der Ordnung p hat.

b) Man zeige, wie man das Problem der Berechnung des diskreten Logarithmus $\log_g(x)$ auf das DL-Problem in der Untergruppe G_1 zurückführen kann.