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

SS 2012
16. Mai 2012

Elliptische Kurven

Übungsblatt 2

Aufgabe 5 Sei E die elliptische Kurve mit affiner Gleichung $Y^2 = X^3 + aX + b$ über dem endlichen Körper $k := \mathbb{F}_q$, (q ungerade). Für $u \in k^*$ sei E_u die Kurve mit der affinen Gleichung

$$uY^2 = X^3 + aX + b.$$

Man zeige:

a) Die Kurve E_u ist über k isomorph zur elliptischen Kurve mit der affinen Gleichung

$$Y^2 = X^3 + au^2X + bu^3.$$

b) Ist u ein Quadrat in k, so ist E_u über k isomorph zu E.

c) Ist u kein Quadrat in k, so gilt

$$\#E(k) + \#E_u(k) = 2q + 2.$$

Aufgabe 6 Für jedes $m \in \{3, 4, \ldots, 12, 13\}$ gebe man ein Beispiel einer elliptischen Kurven E_{ab} mit affiner Gleichung $Y^2 = X^3 + aX + b$ über dem Körper $\mathbb{F}_7$, so dass

$$\#E_{ab}(\mathbb{F}_q) = m.$$

Aufgabe 7 Sei E eine elliptische Kurve über einem endlichen Körper k der Charakteristik $\neq 2$ mit affiner Gleichung $Y^2 = f(X) := X^3 + aX + b$. Man beweise:

a) Genau dann hat das Polynom $f(X)$ (mindestens) eine Nullstelle in k, wenn die Gruppenordnung $\#E(k)$ gerade ist.

b) Genau dann hat $f(X)$ drei Nullstellen im Körper k, wenn die Gruppe $E(k)$ eine zur Kleinschen Vierergruppe $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$ isomorphe Untergruppe hat.

Aufgabe 8

Man konstuiere elliptische Kurven E, E' über dem Körper $\mathbb{F}_3$, so dass $E(\mathbb{F}_3)$ isomorph zur zyklischen Gruppe $\mathbb{Z}/4$ und $E'(\mathbb{F}_3)$ isomorph zur Kleinschen Vierergruppe ist.