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

SS 2012
6. Juni 2012

Elliptische Kurven

Übungsblatt 3

Aufgabe 9

Sei E die elliptische Kurve mit affiner Gleichung $Y^2 = X^3 + aX + b$ über einem Körper K der Charakteristik $\neq 2, 3$.

Man zeige: Ein Punkt $P = (x, y) \in E(K)$ hat genau dann die Ordnung 3, falls

$$3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Aufgabe 10

Sei G eine multiplikativ geschriebene zyklische Gruppe der Ordnung N. Die Primfaktor-Zerlegung von N sei

$$N := \prod_{i=1}^{r} q_i^{k_i}.$$

a) Man zeige: $g \in G$ ist genau dann erzeugendes Element von G, falls

$$g^{N/q_i} \neq 1 \quad \text{für } i = 1, \ldots, r.$$

b) Wie groß ist die Wahrscheinlichkeit, dass ein zufällig gewähltes Element von G ein erzeugendes Element ist?

Aufgabe 11

Sei G wie in Aufgabe 10. Dann ist G bekanntlich isomorph zum Produkt $G_1 \times \ldots \times G_r$ von zyklischen Untergruppen $G_i \subset G$ der Ordnung $q_i^{k_i}$. Man gebe einen effizienten Algorithmus an, der erzeugende Elemente g_i von G_i konstruiert und implementiere das Verfahren im Fall $G = (\mathbb{Z}/p)^*$, (p ungerade Primzahl).

Aufgabe 12

Sei G eine abelsche Gruppe der Ordnung p^2, (p prim). Dann ist G bekanntlich isomorph zu einer der additiven Gruppen $\mathbb{Z}/p^2$ oder $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$. Wie kann man möglichst effizient entscheiden, welcher der beiden Fälle vorliegt?

Seien E_1 und E_2 die beiden elliptischen Kurven über dem Körper $\mathbb{F}_{31}$ mit den affinen Gleichungen

$$E_1: \quad Y^2 = X^3 + 11,$$
$$E_2: \quad Y^2 = X^3 + X + 17.$$

Die Kurven $E_i(\mathbb{F}_{31})$ haben beide die Ordnung 25. Man bestimme ihre Gruppen-Struktur.