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

SS 2012
27. Juni 2012

Elliptische Kurven

Übungsblatt 4

Aufgabe 13

Seien E_1 und E_2 elliptische Kurven über dem Körper $\mathbb{F}_p$ (p ungerade Primzahl) mit den affinen Gleichungen

$$\begin{aligned} E_1 &: \quad Y^2 = X^3 + aX + b, \\ E_2 &: \quad Y^2 = X^3 + aX - b. \end{aligned}$$

Man zeige: (1) Gilt $p \equiv 1 \bmod 4$, so sind E_1 und E_2 über dem Körper $\mathbb{F}_p$ isomorph.
(2) Gilt $p \equiv 3 \bmod 4$, so folgt

$$\#E_1(\mathbb{F}_p) + \#E_2(\mathbb{F}_p) = 2p + 2.$$

Aufgabe 14

Sei $p \equiv 3 \bmod 4$ prim und a_0 ein fester quadratischer Nichtrest modulo p. Man zeige: Jede elliptische Kurve über $\mathbb{F}_p$ ist isomorph zu einer Kurve der folgenden Typen:

$$\begin{aligned} Y^2 &= X^3 + b, \\ Y^2 &= X^3 + X + b, \\ Y^2 &= X^3 + a_0X + b. \end{aligned}$$

Aufgabe 15

Sei $p \equiv 3 \bmod 4$ prim und E eine elliptische Kurve über $\mathbb{F}_p$ mit affiner Gleichung

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

Man zeige: Für jede ganze Zahl $0 < x < p/2$ ist entweder x oder $p - x$ die X-Koordinate eines Punktes von $E(\mathbb{F}_p)$.

Aufgabe 16

Sei G eine zyklische Gruppe der Ordnung m mit erzeugendem Element g. Beim Pollardschen Rho-Verfahren zur Berechnung des diskreten Logarithmus eines Elementes $x \in G$ werden pseudo-zufällige Potenz-Produkte $x^k g^\ell$ erzeugt, bis eine Kollision

$$x^k g^\ell = x^{k'} g^{\ell'}$$

entdeckt wird.

a) Man zeige: Ist $\gcd(k - k', m) = 1$, so kann man damit $\log_g(x)$ berechnen.

b) Wie kann man $\log_g(x)$ berechnen, falls $\gcd(k - k', m) = d > 1$, aber klein ist?