Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

WS 2002/3

Übungen zur Kryptologie II

7. Übung

Aufgabe 1 (4 Punkte)

Betrachten Sie die über den reellen Zahlen mittels

$$y^2 = x^3 - 3x - 2$$

definierte elliptische Kurve.

a) Skizieren Sie zeichnerisch den Verlauf der Kurve.

b) Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.

c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.

Aufgabe 2

Sei E die über $\mathbb{Z}_{71}$ durch

$$y^2 = x^3 + x + 28$$

definierte elliptische Kurve E.

a) Bestimmen Sie die Anzahl der Punkte von E.

b) Zeigen Sie, dass E nicht zyklisch ist.

c) Bestimmen Sie einen Punkt maximaler Ordnung in E.

Aufgabe 3

Zeigen Sie, dass eine über

$$y^2 = x^3 + ax + b$$

definierte elliptische Kurve nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in $\mathbb{Z}_p$ hat.