7. Übungsblatt

Abgabe: Mittwoch, 24.06.09

Aufgabe 1 Gegeben sei die Edwardskurve $Ed : x^2 + y^2 = 1 + dx^2y^2$ über einem endlichen Körper K von ungerader Charakteristik. Ferner sei d ein Nichtquadrat in K. Zeige:

(a) $(0, 1)$ ist das neutrale Element in $Ed(K)$.

(b) Es gilt $-(x, y) = (-x, y)$ für alle $(x, y) \in Ed(K)$.

(c) $Ed(K)$ enthält genau ein Element der Ordnung 2.

(d) $Ed(K)$ enthält stets ein Element der Ordnung 4.

Aufgabe 2 Sei $Ed : x^2 + y^2 = 1 + 2x^2y^2$ eine Edwardskurve über $K = \mathbb{Z}_5$.

(a) Bestimme die K-rationalen Punkte auf Ed.

(b) Zeige, dass $Ed(K)$ zyklisch ist.

Aufgabe 3 Verwenden Sie den Pohlig-Hellman-Algorithmus, um den diskreten Logarithmus von 2 zur Basis 3 mod 65537 zu berechnen.

Aufgabe 4 Berechnen Sie mit dem Index-Calculus-Algorithmus unter Verwendung der Faktorbasis $\{2, 3, 5, 7, 11, \}$ die Lösung von $7^x \equiv 13 \bmod 2039$.