Angewandte diskrete Mathematik *Wintersemester 2008/2009*
Barbara Baumeister
Jŕgen Schütz

13. Übungsblatt

Abgabe: Die, 3.2.2009

Aufgabe 1 Gegeben sei die elliptische Kurve $E : y^2 = x^3 - x$.

(a) Berechnen Sie $|E(\mathbb{Z}_5)|$.

(b) Bestimmen Sie die Struktur von $E(\mathbb{Z}_5)$.

Aufgabe 2 Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über dem Körper K. Wie viele Elemente der Ordnung 2 kann $E(K)$ höchstens haben?

Aufgabe 3 Berechnen Sie unter Verwendung eines Computer-Algebrasystems den diskreten Logarithmus $log_3 1996$ in $\mathbb{Z}^\star_{1999}$ mittels des Baby-Step-Giant-Step-Algorithmus.