Wolfgang K. Seiler
*Tel.* 2515

A5, C201

*5. November 2013*

# 8. Übungsblatt Elliptische Kurven

**Aufgabe 1:** *(8 Punkte)*

*a)* Bestimmen Sie alle Punkte der elliptischen Kurve $Y^2Z = X^3 + 3XZ^2 + 2Z^3$ über dem Körper mit fünf Elementen und stellen Sie die Gruppentafel auf!

*b)* Welche Ordnungen haben die einzelnen Punkte von $E$ ?

*c)* Wie viele Wendepunkte hat $E$?

**Aufgabe 2:** *(8 Punkte)*

*a)* Berechnen Sie für den Punkt $P = (1, 0)$ der elliptischen Kurve $Y^2Z = X^3 + XZ^2 + Z^3$ über $\mathbb{F}_{19}$ den Punkt $21P$ !

*b)* Zeigen Sie, daß die Punkte von $E$ eine zyklische Gruppe bilden!

**Aufgabe 3:** *(4 Punkte)*

Wie viele Additionen und wie viele Multiplikationen im Grundkörper $k$ werden benötigt, wenn wir nach dem Algorithmus von Montgomery die $x$-Koordinate des $N$-fachen eines Punktes einer elliptischen Kurve berechnen? Gehen Sie aus von der Annahme, daß keiner der betrachteten Zwischenpunkte gleich $O$ ist.

**Abgabe** bis zum Dienstag, dem 12. November 2013, um 15.25 Uhr