Kryptosysteme, Keymanagment (KSK3) für CMS
11. Übungsblatt für den 9. Jänner 2007

40. Bestimme alle Punkte der elliptischen Kurve EC über $\mathbb{Z}_{11}$

$$EC: \quad y^2 = x^3 + 7x + 5.$$

Welche Ordnung hat diese elliptische Kurve?

41. Gegeben seien die Punkte $P_1 = \begin{pmatrix} 2 \\ 7 \end{pmatrix}, P_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix}, Q_1 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, Q_2 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ der elliptischen Kurve aus Bsp. 40. Berechne $P_1 + Q_1$, $P_1 + Q_2$ und $2P_2$.

42. Gegeben sei der Punkt $P = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ der elliptischen Kurve aus Bsp. 40. Berechne $9P$ mittels „Square & Multiply“.

43. Sei $\mathbf{F}$ der endliche Körper $\mathbb{Z}_5[t]/(2 + 3t + t^3)$, und sei $\alpha = [t]_{2+3t+t^3}$. Überprüfe, dass

$$P = \begin{pmatrix} \alpha + \alpha^2 \\ 2 + 3\alpha + \alpha^2 \end{pmatrix} \text{ und } Q = \begin{pmatrix} 4 + 4\alpha + 3\alpha^2 \\ 4 + \alpha + 2\alpha^2 \end{pmatrix}$$

Punkte der elliptischen Kurve EC über $\mathbf{F}$ sind, die wie folgt definiert ist:

$$EC: \quad y^2 = x^3 + (3 + 2\alpha^2)x + (1 + 4\alpha + 4\alpha^2).$$

Berechne $P + Q$ sowie $2P$.

44. (*Recherche*) Wie sind elliptische Kurven über einem Körper der Charakteristik 2 oder 3 definiert. Wie lauten die Additions- und Verdopplungsformeln?