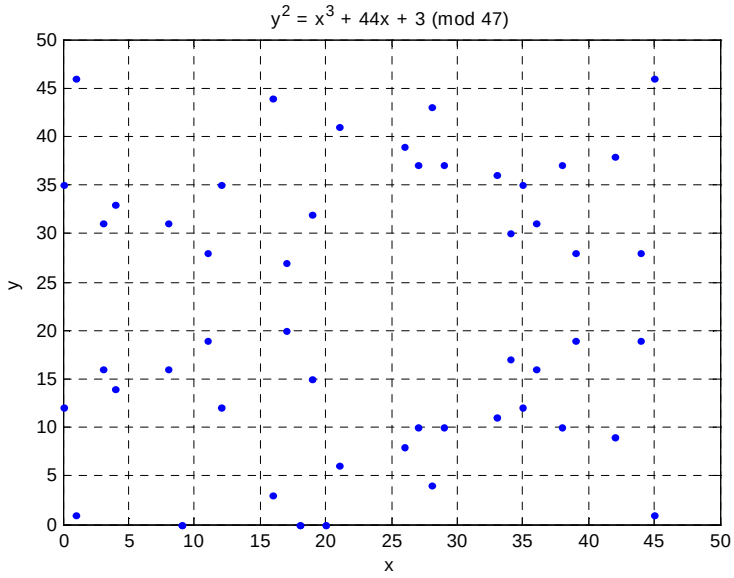

Figur 141: Elliptische Kurve im Restklassenkörper GF(47)

Die Addition von Punkten wird genau gleich wie beim Rechnen im reellen Körper definiert.

Addition von Punkten

Gegeben sind zwei Punkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ mit $y_P \neq -y_Q$. Die Summe $S = P + Q = (x_S, y_S)$ wird dann nach folgenden Regeln bestimmt:

$$x_S = m^2 - x_P - x_Q$$
$$y_S = m \cdot (x_P - x_R) - y_P$$

mit

$$m = \begin{cases} (y_Q - y_P) \cdot (x_Q - x_P)^{-1} & \text{falls } P \neq Q \\ (3x_P^2 + a_4) \cdot (2y_P)^{-1} & \text{falls } P = Q \end{cases}$$

Alle Berechnungen werden dabei im Restklassenkörper Z_p durchgeführt. Dies bedeutet insbesondere, dass bei allen Zwischenresultate nur der Rest bei Division durch p betrachtet werden muss.

Beispiel

Auf der elliptischen Kurve des vorherigen Beispiels befindet sich der Punkt (3, 16). Es soll P + P = 2P berechnet werden.

In diesem Fall gilt P = Q und daher