Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 10
19. Dezember 2018

Übungen zur Kryptographie
Lösung

Aufgabe 39

Man beachte, dass es für $p \equiv 1 \bmod 4$ ein i mit $i^2 \equiv -1 \bmod p$ gibt. Wir erhalten

$$\begin{aligned}(x,y) \in E &\Leftrightarrow y^2 = x^3 + x + b \\ &\Leftrightarrow (iy)^2 = -y^2 = -x^3 - x - b = (-x)^3 + (-x) - b \Leftrightarrow (-x, iy) \in E'\end{aligned}$$

Sei nun $p \equiv 3 \bmod 4$. Für $b = 0$ gilt $E \simeq E'$. Sei $b \neq 0$. Dann ist -1 kein Quadrat modulo p, d.h. für $x^3 + x + b \neq 0 \bmod p$:

$$\left(\frac{x^3+x+b}{p}\right)\left(\frac{-x^3-x-b}{p}\right) = \left(\frac{-(x^3+x+b)^2}{p}\right) = \left(\frac{-1}{p}\right) = -1.$$

Somit ist für jedes x mit $x^3 + x + b \neq 0 \bmod p$ entweder $(x,y),(x,-y) \in E$ für ein y oder $(-x,y'),(-x,-y') \in E'$ für ein y'. Ist $x^3+x+b = 0 = -x^3-x-b$, so erhält man jeweils einen Punkt $(x,0) \in E$ und einen Punkt $(-x,0) \in E'$. D.h. es gibt genau $2p$ Punkte in $E_{\text{aff}} \cup E'_{\text{aff}}$ mit $\#E_{\text{aff}} + \#E'_{\text{aff}} = 2p$. Die beiden Kurven haben natürlich gleich viele Punkte, wenn $b = 0$. Das Beispiel $p = 31$ und $b = 6$ zeigt, dass dies auch für $b \neq 0$ möglich ist:

$(1,15),(1,16),(2,4),(2,27),(3,6),(3,25),(9,0),(12,14),(12,17),(14,6),(14,25),(17,10),$
$(17,21),(18,11),(18,20),(19,8),(19,23),(20,11),(20,20),(21,9),(21,22),(24,11),(24,20),$
$(25,1),(25,30),(26,0),(27,0),(28,10),(28,21),(30,2),(30,29) \in E$

und

$(0,5),(0,26),(2,2),(2,29),(4,0),(5,0),(8,7),(8,24),(9,9),(9,22),(15,6),(15,25),$
$(16,13),(16,18),(18,4),(18,27),(20,4),(20,27),(21,10),(21,21),(22,0),(23,1),(23,30),$
$(24,4),(24,27),(25,12),(25,19),(26,9),(26,22),(27,9),(27,22) \in E'.$

Aufgabe 40

a) Wir klammern aus und erhalten $x(a_3x^2 + a_2x + a_1)$. Der Term hat genau dann die mehrfache Nullstelle 0, wenn $a_1 = 0$. Eine andere mehrfache Nullstelle ergibt sich, wenn $a_2^2 - 4a_3a_1 = 0$. Zusammen erhalten wir die Bedingung $4a_1^2a_3 - a_2^2a_1 \neq 0$.[1]

b) Wir erkennen sofort, dass $(0,0) \in E$ liegt. Weiter hat $(0,0)$ die Ordnung 2 und diese muss die Gruppenordnung teilen. Man beachte, dass eine nicht-singuläre[2] Kurve $a_3x^3 + a_2x^2 + a_1x - y^3 = 0$ in $x_0 = y_0 = 0$ die Tangentialgleichung

$$(3a_3x_0^2 + 2a_2x_0 + a_1)(x - x_0) - 2y_0(y - y_0) = a_1x = 0,$$

und damit eine Tangente senkrecht zur x-Achse, hat.

[1] Ist zudem a_3 invertierbar, so kann man auch $4a_1^3a_3^2 - a_1a_2^2a_3 \neq 0$ schreiben.
[2] siehe Teil a)