Elliptische Kurven in der Kryptographie, Teil II

Vortrag zum Seminar zur Funktionentheorie, 26.11.2007

Stefan Bodden

Im vorigen Vortrag haben wir gesehen, was eine elliptische Kurve ist. Ziel dieses Vortrags ist es nun weitere Eigenschaften dieser elliptischen Kurven zu betrachten. Dazu untersuchen wir im ersten Teil die Gruppenstruktur, die auf einer solchen Kurve gegeben ist. Im zweiten Teil versuchen wir dann die Anzahl der Punkte einer elliptischen Kurve zu bestimmen. Dazu stellen wir den sogenannten Schoof-Algorithmus, einen effektiven Algorithmus zur Bestimmung dieser Zahl, vor.

§1 Elliptische Kurven als Gruppen

In diesem Kapitel sei F ein beliebiger Körper.

(1.1) Definition (Projektive Gerade)
Sei $g \in F[X,Y,Z]$ ein homogenes Polynom vom Grad 1, also

$$g(X,Y,Z) = \alpha X + \beta Y + \gamma Z$$

mit $\alpha, \beta, \gamma \in F$, die nicht alle gleichzeitig Null sind. Dann nennen wir die Kurve $C_g(F) = \{[a:b:c] \in \mathbb{P}(F); g(a,b,c) = 0\}$ *projektive Gerade*. Anstatt $C_g(F)$ schreiben wir auch $L(\alpha,\beta,\gamma)$. ◇

Man sieht leicht, dass dann folgender Satz gilt:

(1.2) Satz
Eine projektive Gerade ist nicht-singulär. ◇

Beweis
Sei $C_g(F)$ eine projektive Gerade mit $g(X,Y,Z) = \alpha X + \beta Y + \gamma Z$ für alle $P \in C_g(F)$. Dann gilt:

$$\frac{\partial g}{\partial X}(P) = \alpha \quad \frac{\partial g}{\partial Y}(P) = \beta, \quad \frac{\partial g}{\partial Z}(P) = \gamma$$

Da α, β und γ nie gleichzeitig Null sind, folgt die Behauptung. □

Dass Geraden im projektiven Raum in mancher Hinsicht einfacher zu handhaben sind als gewöhnliche Geraden in der Ebene, zeigt folgendes

(1.3) Lemma

a) Durch je zwei verschiedene Punkte aus $\mathbb{P}^2(F)$ führt genau eine projektive Gerade.

b) Zwei verschiedene projektive Geraden schneiden sich in genau einem Punkt in $\mathbb{P}^2(F)$. ◇

Beweis

a) Seien $P_1 = [a_1 : b_1 : c_1]$ und $P_2 = [a_2 : b_2 : c_2]$ zwei verschiedene Punkte in $\mathbb{P}^2(F)$. Gesucht ist also ein Element $(0,0,0) \neq (\alpha, \beta, \gamma) \in F^3$ mit

$$\alpha a_1 + \beta b_1 + \gamma c_1 = 0 \text{ und}$$
$$\alpha a_2 + \beta b_2 + \gamma c_2 = 0$$

Das ist ein lineares Gleichungssystem mit der Koeffizientenmatrix $\left(\begin{smallmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{smallmatrix}\right)$. Da P_1 und P_2 verschieden sind, sind die Zeilen der Matrix linear unabhängig, so dass sie den Rang 2 hat. Aus der linearen Algebra ist bekannt, dass damit der Lösungsraum in F^3 eindimensional ist, das heißt: Falls (α, β, γ) und $(\alpha', \beta', \gamma')$ zwei verschiedene, nicht triviale Lösungen des Gleichungssystems sind, dann ist (α, β, γ) ein Vielfaches von $(\alpha', \beta', \gamma')$. Aus (1.1) folgt, dass $L(\alpha, \beta, \gamma) = L(\alpha', \beta', \gamma')$ ist. Daraus folgt wiederum, dass nur eine projektive Gerade existiert, die P_1 und P_2 schneidet.

b) Seien $L(\alpha_1, \beta_1, \gamma_1)$ und $L(\alpha_2, \beta_2, \gamma_2)$ zwei verschiedene projektive Geraden. Gesucht ist ein Element $(x, y, z) \in F^3$ mit:

$$\alpha_1 x + \beta_1 y + \gamma_1 z = 0 \text{ und}$$
$$\alpha_2 x + \beta_2 y + \gamma_2 z = 0$$

Analog zu Teil a) folgt, dass die Lösungsmenge ein eindimensionaler Teilraum von F^3 ist. Ist $(a, b, c) \neq 0$ ein Vektor aus der Lösungsmenge, dann schneiden sich offensichtlich die beiden Geraden in dem Punkt $P = [a : b : c]$. Ist $(a', b', c') \neq 0$ ein weiterer Vektor aus der Lösungsmenge, dann ist auch $P' = [a' : b' : c']$ ein Schnittpunkt der Geraden. Da die Lösungsmenge eindimensional ist, ist (a, b, c) ein Vielfaches von (a', b', c'). Somit folgt mit der Definition vom projektiven Raum, dass $P' = P$ ist. □

Man sieht also, dass sich zwei Geraden im projektiven Raum entweder in einem Punkt schneiden oder identisch sind. Demnach existieren dort also keine echt parallelen Geraden.

(1.4) Definition (Tangente in P an $C_g(F)$)
Sei $C_g(F)$ eine projektive ebene Kurve und $P = [a : b : c]$ ein nicht-singulärer Punkt auf $C_g(F)$. Die projektive Gerade

$$L\Big(\frac{\partial g}{\partial X}(a,b,c), \frac{\partial g}{\partial Y}(a,b,c), \frac{\partial g}{\partial Z}(a,b,c)\Big)$$

heißt dann *Tangente in P an $C_g(F)$*. ◇

Aus der Annahme, dass P ein nicht-singulärer Punkt ist, folgt, dass nicht alle drei Ableitungen gleichzeitig Null sind, also ist eine Tangente in der Tat eine projektive Gerade.

Man kann leicht sehen, dass P auch auf $L\big(\frac{\partial g}{\partial X}(a,b,c), \frac{\partial g}{\partial Y}(a,b,c), \frac{\partial g}{\partial Z}(a,b,c)\big)$ liegt: Sei

$$g(X,Y,Z) = \sum_{i=1}^{n} k_i X^{u_i} Y^{v_i} Z^{w_i}, \quad \forall i = 1,\dots,n: \quad u_i + v_i + w_i = d,\ k_i \in F;\ \ d, n \in \mathbb{N}$$

das zugrundeliegende homogene Polynom mit Grad d. Dann ist

$$\frac{\partial g}{\partial X}(X,Y,Z) = \sum_{i=1}^{n} u_i k_i X^{u_i - 1} Y^{v_i} Z^{w_i},$$

$$\frac{\partial g}{\partial Y}(X,Y,Z) = \sum_{i=1}^{n} v_i k_i X^{u_i} Y^{v_i - 1} Z^{w_i},$$

$$\frac{\partial g}{\partial Z}(X,Y,Z) = \sum_{i=1}^{n} w_i k_i X^{u_i} Y^{v_i} Z^{w_i - 1}$$

Daraus folgt, dass

$$\frac{\partial g}{\partial X}(a,b,c)a + \frac{\partial g}{\partial Y}(a,b,c)b + \frac{\partial g}{\partial Z}(a,b,c)c = \sum_{i=1}^{n} (u_i + v_i + w_i) k_i a^{u_i} b^{v_i} c^{w_i}$$

$$= d \sum_{i=1}^{n} k_i a^{u_i} b^{v_i} c^{w_i} = d \cdot \underbrace{g(a,b,c)}_{=0} = 0$$

gilt, also ist $P \in C_g(F)$.

Zur Illustration dient folgendes

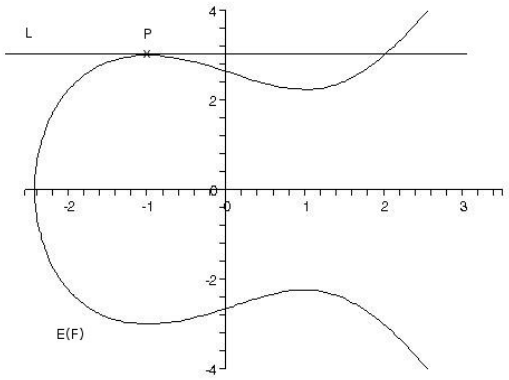
(1.5) Beispiel
Sei $F = \mathbb{R}$ und $E(F)$ die elliptische Kurve mit der Weierstraßgleichung

$$g(X, Y, Z) = Y^2Z - X^3 + 3XZ^2 - 7Z^3 = 0$$

Zu dem Punkt $P = [-1 : 3 : 1] \in E(F)$ betrachten wir die Tangente L in P an $E(F)$, wobei

$$L = L\Big(\frac{\partial g}{\partial X}(-1,3,1), \frac{\partial g}{\partial Y}(-1,3,1), \frac{\partial g}{\partial Z}(-1,3,1)\Big) = L(0,6,-18)$$

ist. Wenn wir jetzt in einer Zeichnung zu affinen Koordinaten übergehen, sieht man, dass L wirklich die Tangente an P ist:



◇

Als nächstes definieren wir die Vielfachheit, mit der sich eine Kurve und eine Gerade in einem Punkt schneiden.

(1.6) Definition
Seien $L(\alpha, \beta, \gamma)$ eine projektive Gerade, $C_g(F)$ eine projektive Kurve sowie der Punkt $P = [a : b : c] \in L(\alpha, \beta, \gamma)$ gegeben. Sei weiter $P' = [a' : b' : c'] \in L(\alpha, \beta, \gamma)$ ein beliebiger von P verschiedener Punkt. Dann ist die *Vielfachheit*, mit der sich $L(\alpha, \beta, \gamma)$ und $C_g(F)$ in P schneiden, definiert als die Nullstellenordnung des Polynoms

$$\psi(t) = g(a + ta', b + tb', c + tc')$$

in 0. Wir bezeichnen sie mit $m(P, L(\alpha, \beta, \gamma), C_g(F))$. ◇

Das Polynom ψ können wir auch in der Form

$$\psi(t) = w_0 + w_1 t + \cdots + w_l t^l,$$

mit geeignet gewählten $w_i \in F$ für alle $i = 0, \ldots, l$ und $l \in \mathbb{N}$ schreiben. Man sieht leicht, dass die Nullstellenordnung in 0 genau dann $j \in \{0, \ldots, l\}$ beträgt, falls $w_0 = w_1 = \ldots = w_{j-1} = 0$ und $w_j \neq 0$.

Dazu betrachten wir zwei

(1.7) Beispiele

a) Sei $L(\alpha, \beta, \gamma)$ eine projektive Gerade, $P = [a : b : c] \in L(\alpha, \beta, \gamma)$ und $C_g(F)$ eine projektive Kurve mit $P \notin C_g(F)$. Dann ist

$$\psi(0) = g(a, b, c) \neq 0,$$

also ist

$$m(P, L(\alpha, \beta, \gamma), C_g(F)) = 0.$$

b) Sei $L = L(\alpha, \beta, \gamma)$ die Tangente von $C_g(F)$ in $P = [a : b : c] \in C_g(F)$. Dann gilt

$$\psi(0) = g(a, b, c) = 0 (= w_0).$$

Sei weiter $P' = [a' : b' : c']$ ein beliebiger, von P verschiedener Punkt auf der projektiven Geraden. Dann ist

$$\psi'(0) = \frac{d}{dt}(g(a + ta', b + tb', c + tc'))|_{t=0} \overset{\text{Kettenregel}}{=} \underbrace{\frac{\partial g}{\partial X}(a, b, c)}_{=\alpha} \cdot a' + \underbrace{\frac{\partial g}{\partial Y}(a, b, c)}_{=\beta} \cdot b' +$$

$$\underbrace{\frac{\partial g}{\partial Z}(a, b, c)}_{=\gamma} \cdot c' \overset{P' \in L(\alpha, \beta, \gamma)}{=} 0 (= w_1),$$

also ist

$$m(P, L, C_g(F)) \geq 2.$$

Der Vollständigkeit halber definieren wir noch

$$m(P, L, C_g(F)) = 0 \quad \forall P \notin L.$$

Es gilt nun folgender wichtiger

(1.8) Satz

Für eine projektive Gerade L und eine elliptische Kurve $E(F)$ gilt: Die Summe aller Vielfachheiten

$$\sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F))$$

ist entweder 0, 1 oder 3. ◇

Beweis
Sei $L = L(\alpha, \beta, \gamma)$ eine projektive Gerade und $E(F)$ die elliptische Kurve zur Weierstraßgleichung

$$g(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

mit $a_1, a_2, a_3, a_4, a_6 \in F$. Nach (1.7) ist $m(P, L, E(F)) = 0$ für alle $P \in L$ mit $P \notin E(F)$. Deshalb müssen wir nur Punkte in der Schnittmenge $L \cap E(F)$ betrachten. Wir unterscheiden drei Fälle:

1. Fall: $\alpha = \beta = 0$ (also $\gamma \neq 0$)

Daraus folgt, dass jeder Punkt auf L die Form $[a : b : 0]$, $a, b \in F$, hat. Da wir die Menge $E(F) \cap L$ betrachten, kommt in diesem Fall nur $O = [0 : 1 : 0]$ in Frage.

Um $m(O, L, E(F))$ zu berechnen wählen wir als Hilfspunkt $[1 : 0 : 0] \in L$. Dann gilt:

$$\psi(t) = g(t, 1, 0) = -t^3,$$

also ist

$$\sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F)) = 3.$$

2. Fall: $\alpha \neq 0,\ \beta = 0$

Es sei $P = [x : y : z] \in L$. Dann gilt $\alpha x + \beta y + \gamma z = 0$, also $\alpha x = -\gamma z$. Das heißt: Für $z = 0$ ist $P = O = [0 : 1 : 0]$ und für $z \neq 0$ ist $P = [-\frac{\gamma}{\alpha} : y_0 : 1]$ mit $y_0 \in F$. Wir berechnen zuerst $m(O, L, E(F))$:

Als Hilfspunkt wählen wir $P' = [-\gamma : 0 : \alpha] \in L$, so dass

$$\psi(t) = g(-\gamma t, 1, \alpha t) = (\gamma^3 - a_2\gamma^2\alpha + a_4\gamma\alpha^2 - a_6\alpha^3)t^3 + (a_3\alpha^2 - a_1\gamma\alpha)t^2 + \alpha t.$$

Damit ist $\psi(0) = 0$ und $\psi'(0) = \alpha \neq 0$, also ist $m(O, L, E(F)) = 1$.

Für $P = [-\frac{\gamma}{\alpha} : y_0 : 1]$ gilt:

Der Punkt P liegt genau dann in $E(F)$, wenn y_0 eine Nullstelle des Polynoms

$$h(y) := g\Big(-\frac{\gamma}{\alpha}, y, 1\Big)$$

ist. Wir nehmen als Hilfspunkt $P' = O = [0 : 1 : 0] \in L$. Demnach folgt, dass

$$\psi(t) = g\Big(-\frac{\gamma}{\alpha}, y_0 + t, 1\Big) = h(y_0 + t)$$

ist. Wir betrachten nochmal das Polynom:

$$h(y) = (y - y_0)^k h^*(y),$$

wobei k die Ordnung der Nullstelle y_0 von h und h^* ein Polynom mit $h^*(y_0) \neq 0$ ist. Da

$$\psi(t) = h(y_0 + t) = t^k h^*(y_0 + t)$$

ist, ist k auch die Nullstellenordnung von ψ in Null. Weiter gilt:

$$h(y) = y^2 + \Big(a_3 - \frac{a_1\gamma}{\alpha}\Big)y + \frac{\gamma^3}{\alpha^3} - \frac{a_2\gamma^2}{\alpha^2} + \frac{a_4\gamma}{\alpha} - a_6,$$

also hat das Polynom $h(y)$ den Grad 2. Aus der Algebra folgt, dass h entweder keine Nullstelle in F, eine Nullstelle der Ordnung zwei oder zwei Nullstellen der Ordnung 1 in F hat. Im letzteren Fall hat h die Form $h(y) = (y - y_1)(y - y_2)$ mit $y_1 \neq y_2$. Demnach wären $P_1 = [-\frac{\gamma}{\alpha} : y_1 : 1]$ und $P_2 = [-\frac{\gamma}{\alpha} : y_2 : 1]$ zwei Schnittpunkte mit der Vielfachheit 1. Wenn dagegen $y_1 = y_2$ ist, ist $P = [-\frac{\gamma}{\alpha} : y_1 : 1]$ der einzige weitere Schnittpunkt. Dieser hat die Vielfachheit 2. Betrachten wir jetzt noch zusätzlich den Punkt O, folgt mit Obigem, dass

$$\sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F)) = 1 \text{ oder } \sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F)) = 3$$

ist.

3. Fall: $\beta \neq 0$

Da $\beta \neq 0$ ist, ist $O \notin L$. Deshalb hat ein möglicher Punkt $P \in L \cap E(F)$ die Form $P = [x_0 : y_0 : 1]$. Dieser liegt genau dann in $L \cap E(F)$, wenn

$$y_0 = -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x_0$$

und x_0 eine Nullstelle des Polynoms

$$h(x) := g\Big(x, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x, 1\Big)$$

ist. Zur Berechnung der Summe der Vielfachheiten nehmen wir als Hilfspunkt $P' = [-\beta : \alpha : 0] \in L$. Dann ist

$$\psi(t) = g(x_0 - t\beta, y_0 + t\alpha, 1) = g\Big(x_0 - t\beta, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}(x_0 - t\beta), 1\Big) = h(x_0 - t\beta).$$

Wie im zweiten Fall folgt daraus, dass $m(P, L, E(F))$ gleich der Ordnung der Nullstelle x_0 in h ist. Somit ist also $\sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F))$ gleich der Summe der Ordnungen aller Nullstellen von h, die in F liegen. Weiter gilt

$$g\Big(x, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x, 1\Big) = -x^3 + \Big(\frac{\alpha^2}{\beta^2} - \frac{a_1\alpha}{\beta} - a_2\Big)x^2 + \Big(\frac{2\gamma\alpha}{\beta^2} - \frac{a_1\gamma + a_3\alpha}{\beta} - a_4\Big)x$$

$$+\frac{\gamma^2}{\beta^2} - \frac{a_3\gamma}{\beta} - a_6 = -(x - x_1)(x - x_2)(x - x_3)$$

mit geeignet gewählten $x_1, x_2, x_3 \in \overline{F}$.

Aus der Algebra können wir folgern, dass entweder keine, eine oder drei – aber niemals zwei – Nullstellen inklusive Vielfachheiten in F liegen (falls wir eine Nullstelle x_1 in F gefunden haben, können wir $(x - x_1)$ vom Polynom abspalten. Das sich ergebene Polynom zweiten Grades hat dann entweder zwei oder keine Nullstellen in F.), also folgt auch in diesem Fall die Behauptung. □

(1.9) Korollar
Für eine elliptische Kurve $E(F)$ gilt:

a) Sind P und Q zwei verschiedene Punkte auf $E(F)$ und L die projektive Gerade, die beide verbindet, dann hat L (mit Vielfachheiten gezählt) noch einen dritten Schnittpunkt mit $E(F)$.

b) Ist L die Tangente an $E(F)$ im Punkt $P \in E(F)$, dann hat L (mit Vielfachheiten gezählt) noch einen dritten Schnittpunkt mit $E(F)$, wenn wir P doppelt zählen. ⋄

Beweis

a) Durch Satz (1.8) wissen wir, dass $\sum_{P \in \mathbb{P}^2(F)} m(P, L, E(F)) = 3$ ist. Entweder gibt es also einen Punkt $R \in L \cap E(F)$, der von P und Q verschieden ist, wobei dann alle drei Punkte die Vielfachheit 1 haben, oder aber einer der Punkte P und Q hat die Vielfachheit 2, der andere die Vielfachheit 1. Im ersten Fall ist R unser zusätzlicher Schnittpunkt, im zweiten Fall derjenige Punkt, der die Vielfachheit 2 hat.

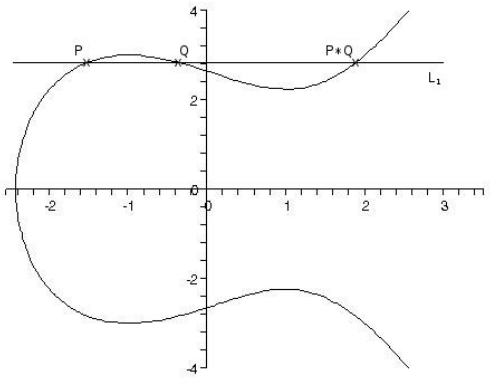
b) Nach (1.7) hat P eine Vielfachheit größer oder gleich 2, also folgt mit (1.8), dass entweder ein Punkt $Q \in L \cap E(F)$, der verschieden von P ist, existiert oder P die Vielfachheit 3 hat. Im ersten Fall ist Q, im zweiten P unser zusätzlicher Schnittpunkt. □

Jetzt können wir auf einer elliptischen Kurve $E(F)$ ein Gruppengesetz definieren:

(1.10) Definition
Es sei $E(F)$ eine elliptische Kurve. Für zwei verschiedene Punkte $P, Q \in E(F)$ definieren wir einen Punkt $P \oplus Q$ in $E(F)$ wie folgt: Wir legen eine projektive Gerade L_1 durch P und Q. Nach (1.9) schneidet L_1 die Kurve $E(F)$ in einem weiteren Punkt, den wir $P * Q$ nennen. Nun legen wir eine projektive Gerade L_2 durch $P * Q$ und den Punkt $O = [0 : 1 : 0]$, der in $E(F)$ liegt. (Wenn zufällig schon $P * Q = O$ sein sollte, so nehmen wir die Tangente an $E(F)$ in O und nennen sie L_2.) Die Gerade L_2 schneidet $E(F)$ nun ebenfalls in einem dritten Punkt. Dies sei der gesuchte Punkt $P \oplus Q$. Auf ähnliche Weise definieren wir einen Punkt $P \oplus P$ auf $E(F)$. Hier sei L_1 die Tangente an $E(F)$ in P und $P * P$ der dritte Schnittpunkt von L_1 mit $E(F)$. Nun verbinden wir wie oben $P * P$ und O durch eine projektive Gerade L_2, deren dritter Schnittpunkt mit $E(F)$ der Punkt $P \oplus P$ sei. ◇

Um uns das besser vorstellen zu können betrachten wir folgende

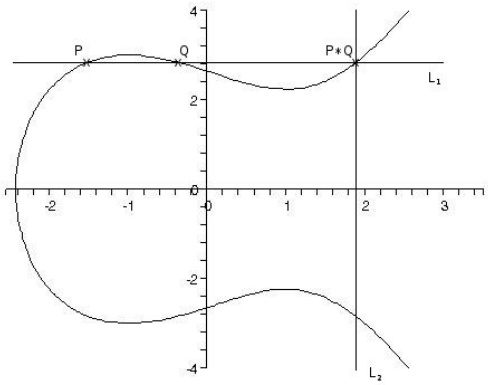
(1.11) Beispiele
a) Sei $F = \mathbb{R}$. Wir benutzen wieder die elliptische Kurve $E(F)$ aus dem Beispiel (1.5) und wählen zwei beliebige Punkte P und Q aus $E(F)$. Wie in der Definition legen wir eine Gerade L_1 durch P und Q, die $E(F)$ in dem Punkt $P * Q$ schneidet:



In der Zeichnung ist $P * Q$ ein Punkt $(x_0, y_0) \in \mathbb{A}^2(F)$, der dem Punkt $[x_0 : y_0 : 1]$ in $E(F)$ entspricht. Die Gerade L_2 soll diesen Punkt mit $O = [0 : 1 : 0]$ verbinden. Analog zum Beweis von (1.3) errechnet man L_2. Dabei ergibt sich

$$L_2 = L(1, 0, -x_0),$$

d. h. L_2 ist die Lösungsmenge der Gleichung $X - x_0 Z = 0$. Daher besteht L_2 aus dem Punkt $O = [0 : 1 : 0]$ und allen Punkten der Form $[x_0 : t : 1]$ für beliebiges $t \in F$, also ist L_2 in der affinen Ebene die Gerade $\{(x_0, y) : y \in F\}$. Diese ist parallel zur y-Achse:



Demnach ist $P \oplus Q$ also der Punkt, der entsteht, wenn man $P * Q$ an der horizontalen Symmetrieachse spiegelt.

b) Sei $E(F)$ eine elliptische Kurve und P ein Punkt in $E(F)$. Wir wollen nun den Punkt $P \oplus O$ bestimmen. Wenn $P = O$ ist, so ist L_1 die Tangente an $E(F)$ im Punkt O. Sei

$$g(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

die Weierstraßgleichung zu $E(F)$. Dann ist

$$\frac{\partial g}{\partial X}(0,1,0) = 0, \quad \frac{\partial g}{\partial Y}(0,1,0) = 0, \quad \frac{\partial g}{\partial Z}(0,1,0) = 1.$$

Also ist L_1 die Gerade $L(0,0,1)$ gegeben durch die Gleichung $Z = 0$. Da nur O aus $E(F)$ diese Gleichung erfüllt, ist der dritte Schnittpunkt wieder O. Also ist der Punkt $O * O$ gleich O. Die Gerade L_2 ist daher die Tangente in O an $E(F)$ und somit ist $L_2 = L_1$. Daraus folgt, dass

$$O \oplus O = O$$

ist. Sei nun $P \neq O$. Wir legen wieder eine Gerade L_1 durch P und O und erhalten den Punkt $P * O$. Da also L_1 die Gerade durch $P * O$ und O ist, muss $L_1 = L_2$ sein. Also ist der dritte Schnittpunkt von L_2 mit $E(F)$ gleich P, d. h.

$$P \oplus O = P.$$

Wir sehen also, dass O die Eigenschaft eines neutralen Elementes hat. ◇

(1.12) Lemma
Wenn P, Q und R drei verschiedene Punkte in $E(F)$ sind, die auf der projektiven Geraden L liegen, so ist

$$(P \oplus Q) \oplus R = O.$$

Dasselbe gilt wenn P, Q und R nicht notwendigerweise verschieden sind, aber nur gerade so oft unter P, Q, R auftreten, wie es ihrer Vielfachheit $m(\cdot, L, E(F))$ entspricht.

Beweis
Wir berechnen zunächst $P \oplus Q$. Dabei gilt, dass $L_1 = L$ ist. Weiter folgt mit (1.8), dass der dritte Schnittpunkt von L mit $E(F)$ gleich R ist, also ist $P \oplus Q$ der dritte Schnittpunkt der Geraden L_2 durch R und O mit $E(F)$. Hierzu wollen wir nun R addieren, also legen wir eine wir eine Gerade L_1' durch R und $P \oplus Q$. Demnach ist $L_1' = L_2$. Der dritte Schnittpunkt ist deshalb O. Da der dritte Schnittpunkt mit $E(F)$ der Tangenten L_2' in O wieder O ist, folgt

$$(P \oplus Q) \oplus R = O. \qquad \square$$

Wir wollen nun zeigen, dass eine elliptische Kurve in der Tat eine Gruppe ist. Dazu betrachten wir folgenden wichtigen

(1.13) Satz
Es sei $E(F)$ eine elliptische Kurve. Die in (1.10) definierte Verknüpfung

$$\oplus : (P, Q) \mapsto P \oplus Q$$

macht $E(F)$ zu einer abelschen Gruppe mit neutralem Element O, d. h. es gilt:

a) $P \oplus O = P$ für alle $P \in E(F)$.

b) Für alle $P \in E(F)$ gibt es einen Punkt $\ominus P \in E(F)$ mit $P \oplus (\ominus P) = O$.

c) $P \oplus Q = Q \oplus P$ für alle $P, Q \in E(F)$.

d) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ für alle $P, Q, R \in E(F)$. $\diamond$

Beweis

a) Haben wir in (1.11) gezeigt.

b) Sei $\ominus P$ definiert als der dritte Schnittpunkt der Geraden durch O und P mit $E(F)$. Nach (1.12) gilt also

$$O = (P \oplus O) \oplus (\ominus P).$$

c) folgt aus der Definition (1.10): Die Gerade L_1, mit der wir starten, hängt nicht von der Reihenfolge von P und Q ab und damit auch nicht das Ergebnis $P \oplus Q$ unserer Konstruktion.

d) ohne Beweis □

Da also die Verknüpfung $\oplus$ ein Gruppengesetz definiert, schreiben wir ab sofort $P + Q$ anstatt $P \oplus Q$ und $-P$ anstatt $\ominus P$. Außerdem definieren wir:

$$mP = \underbrace{P + \ldots + P}_{m} \text{ für } m > 0,$$

$$(-m)P = -(mP) \text{ für } m > 0 \text{ und}$$

$$0P = O.$$

Als nächstes wollen wir den Punkt $P + Q$ in Koordinaten angeben. Da wir schon wissen, wie sich das neutrale Element O unter Addition eines beliebigen $P \in E(F)$ verhält, müssen wir nur Summen $P + Q$ für $P, Q \neq O$ beschreiben. Wenn $E(F)$ durch ein Polynom

$$g(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

gegeben ist, brauchen wir also nur Punkte aus $E(F) \cap i(\mathbb{A}^2(F)) = i(C_f(F))$ für

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

zu betrachten. Der folgende Satz zeigt, wie man die Summe zweier solcher Punkte explizit berechnet. Wir lassen hier der Einfachheit halber die Abbildung i weg, d. h. wir schreiben einfach (x, y) statt $[x : y : 1]$.

(1.14) Satz

i) Für $P_1 = (x_1, y_1) \in C_f(F)$ ist $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

ii) Seien $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ zwei Punkte in $C_f(F)$.

a) Falls $x_1 = x_2$ und $y_1 + y_2 + a_1x_1 + a_3 = 0$, so ist $P_1 + P_2 = O$.

b) Falls diese Bedingungen nicht gelten, liegt $P_3 = P_1 + P_2$ in $C_f(F)$ und hat die affinen Koordinaten (x_3, y_3), wobei gilt:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ und}$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

◇

mit $\lambda, \nu \in F$, die folgendermaßen definiert sind:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, \quad \text{falls } x_1 \neq x_2 \text{ und}$$

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \text{falls } x_1 = x_2.$$

Beweis

i) Der Punkt $-P_1$ ist der dritte Schnittpunkt der Geraden L durch P_1 und O mit $E(F)$. Nach (1.11) ist diese Gerade L gleich $L(1, 0, -x_1)$, d. h. jeder Punkt $P = (x, y)$, der auf L liegt, genügt der Gleichung $x - x_1 = 0$, also $x = x_1$. Jeder Punkt der außerdem noch in $E(F)$ liegt, erfüllt zusätzlich die Weierstraßgleichung $f(x, y) = 0$. Hier setzen wir $x = x_1$ ein und erhalten

$$y^2 + (a_1 x_1 + a_3)y - x_1^3 - a_2 x_1^2 - a_4 x_1 - a_6 = 0$$

Da das eine quadratische Gleichung ist, hat sie entweder zwei oder keine Lösungen mit Vielfachheiten in F. Weil $P_1 = (x_1, y_1)$ ein Punkt aus $E(F) \cap L$ ist, ist $y_1 \in F$ eine Lösung der Gleichung, das heißt, dass eine zweite Lösung $y_1' \in F$ existiert. Demnach ist

$$y^2 + (a_1 x_1 + a_3)y - x_1^3 - a_2 x_1^2 - a_4 x_1 - a_6 = (y - y_1)(y - y_1').$$

Multipliziert man die rechte Seite aus und vergleicht die Koeffizienten, so gilt $-y_1 - y_1' = a_1 x_1 + a_3$, also

$$y_1' = -y_1 - a_1 x_1 - a_3.$$

Daraus folgt, dass $E(F) \cap L$ aus den Punkten O, P_1 und (x_1, y_1') besteht. Wenn $(x_1, y_1') = P_1$, dann hat P_1 die Vielfachheit 2 und O die Vielfachheit 1 – da es maximal drei Schnittpunkte von $E(F)$ mit L gibt –, denn angenommen O hätte die Vielfachheit 2, dann wäre nach (1.12) $O + P_1 = O$, also $P_1 = O$, was ein Widerspruch zur Voraussetzung wäre, also hat O die Vielfachheit 1.

ii) Falls für zwei Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ in $E(F)$ gilt

$$x_2 = x_1 \text{ und } y_2 = -y_1 - a_1 x_1 - a_3,$$

so folgt aus i), dass $P_2 = -P_1$, also $P_1 + P_2 = O$ ist. Wir nehmen also ab jetzt an, dass dies nicht der Fall ist und untersuchen zunächst den Fall $P_1 \neq P_2$. In diesem Fall muss $x_1 \neq x_2$ sein. Wäre nämlich $x_1 = x_2$, so läge P_2 auf der

Gerade $L(1, 0, -x_1)$ durch O und P_1. Da P_2 von O und P_1 verschieden ist, würde $P_2 = -P_1$ folgen, also nach i) auch $y_2 = -y_1 - a_1x_1 - a_3$, und diesen Fall haben wir gerade ausgeschlossen.

Sei nun $L = L(\lambda', \mu', \nu')$ die Gerade, die P_1 und P_2 verbindet, mit $\lambda', \mu', \nu' \in F$. Das heißt, dass die Punkte P mit der Form $P = (x, y)$ in L der Gleichung

$$\lambda'x + \mu'y + \nu' = 0, \quad \text{also} \quad -\mu'y = \lambda'x + \nu'$$

genügen. Wir nehmen an, dass $\mu' = 0$ ist. Dann würden die beiden Punkte P_1 und P_2, die auf L liegen, die Gleichung

$$\lambda'x_1 + \nu' = 0 = \lambda'x_2 + \nu'$$

erfüllen. Da $x_1 \neq x_2$ ist, muss dann $\lambda' = 0$ sein, und damit auch $\nu' = 0$. Dann wären alle drei Werte gleich Null, was nach der Definition einer projektiven Geraden nicht möglich ist. Daher ist $\mu' \neq 0$ und wir können die Geradengleichung umformen zu einer Gleichung der Form

$$y = \lambda x + \nu$$

mit Koeffizienten $\lambda = -\frac{\lambda'}{\mu'}$ und $\nu = -\frac{\nu'}{\mu'}$ aus F. Da $P_1, P_2 \in L$ sind, gilt

$$y_1 = \lambda x_1 + \nu \quad \text{und} \quad y_2 = \lambda x_2 + \nu,$$

also $\lambda(x_2 - x_1) = y_2 - y_1$. Wir wissen, dass $x_1 \neq x_2$ gilt. Deshalb folgt

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Demnach gilt weiter, dass

$$\nu = y_1 - \lambda x_1 = y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1 = \frac{y_1(x_2 - x_1) - x_1(y_2 - y_1)}{x_2 - x_1} = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

ist. Wir setzen nun unsere Ergebnisse in die affine Weierstraßgleichung $f(x, y) = 0$ ein, und schließen, dass jeder Punkt $P = (x, y)$, der auf $E(F)$ und L liegt, der Gleichung

$$(\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3x(\lambda x + \nu) - x^3 - a_2x^2 - a_4x - a_6 = 0$$

genügt. Nach Ausmultiplizieren und Umsortieren ergibt das die Gleichung

$$-x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\nu + a_1\nu + a_3\lambda - a_4)x + (\nu^2 + a_3\nu - a_6) = 0.$$

Hier haben wir wieder ein Polynom dritten Grades, wobei x_1 und x_2 die Gleichung lösen. Aus der Algebra können wir deshalb folgern, dass noch ein $x' \in F$ existiert, das die Gleichung löst. Deshalb können wir die linke Seite auch schreiben als

$$-(x - x_1)(x - x_2)(x - x').$$

Wenn wir nun die Koeffizienten der beiden Polynome vergleichen, folgt, dass

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x', \text{ also } x' = \lambda^2 + a_1\lambda - x_1 - x_2.$$

Somit wissen wir, dass P_1, P_2 und $P' = (x', \lambda x' + \nu)$ die Punkte sind, die auf $L \cap E(F)$ liegen. Wenn P' von P_1 und P_2 verschieden ist, ist P' der gesuchte dritte Schnittpunkt von $E(F) \cap L$, wobei $P' = -(P_1 + P_2)$ ist. Falls aber $P' = P_1$ oder $P' = P_2$ ist, müssen wir die Vielfachheiten ausrechnen, um den weiteren Schnittpunkt zu berechnen. Wir nehmen an, dass $P' = P_1$ ist, der andere Fall geht analog. Genau wie im Beweis zu (1.8) 3. Fall kann man zeigen, dass die Vielfachheit von P_1 gleich der Ordnung der Nullstelle x_1 in dem oben stehendem Polynom ist. (Bei genauer Betrachtung des 3. Falls sieht man, dass dem dort definierten Polynom h unser oben genanntes entspricht.) Da die Ordnung der Nullstelle 2 beträgt, ist somit die Vielfachheit von P_1 gleich 2. Daher gilt auch in diesem Fall $P' = -(P_1 + P_2)$.

Mit Teil i) folgt also, dass

$$P_1 + P_2 = P_3 = (x_3, y_3) \text{ mit } P_3 = -P' \text{ also}$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ und}$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

wobei λ und ν die oben berechneten Werte entsprechen.

Als letztes müssen wir noch den Fall $P_1 = P_2$ betrachten: Sei $L = L(\lambda', \mu', \nu')$ die Tangente an $E(F)$ in $P_1 = [x_1 : y_1 : 1]$. Dann ist

$$\lambda' = \frac{\partial g}{\partial X}(x_1, y_1, 1) = a_1y_1 - 2x_1^2 - 2a_2x_1 - a_4,$$

$$\mu' = \frac{\partial g}{\partial Y}(x_1, y_1, 1) = 2y_1 + a_1x_1 + a_3,$$

$$\nu' = \frac{\partial g}{\partial Z}(x_1, y_1, 1) = y_1^2 + a_1x_1y_1 + 2a_3y_1 - a_2x_1^2 - 2a_4x_1 - 3a_6.$$

Auch hier nehmen wir an, dass $\mu' = 0$ ist. Dann würde der Punkt $O = [0 : 1 : 0]$ auch auf L liegen, woraus folgen würde, dass $P_1 + P_1 = O$, also $P_1 = -P_1$,

ist. Dieseen Fall haben wir vorher ausgeschlossen. Demnach ist $\mu' \neq 0$. Daher genügt $P_1 = (x_1, y_1)$ der Gleichung

$$y_1 = \lambda x_1 + \nu$$

mit

$$\begin{aligned}
\lambda &= -\frac{\lambda'}{\mu'} = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \\
\nu &= -\frac{\nu'}{\mu'} = \frac{-y_1^2 - a_1x_1y_1 - 2a_3y_1 + a_2x_1^2 + 2a_4x_1 + 3a_6}{2y_1 + a_1x_1 + a_3} \\
&= \frac{-\overbrace{(y_1^2 - x_1^3 - a_4x_1 - a_6)}^{=f(x_1,y_1)=0} - x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \\
&= \frac{-x^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.
\end{aligned}$$

Wir setzen wieder $y = \lambda x + \nu$ in die affine Weierstraßgleichung $f(x, y) = 0$ und erhalten, analog zum vorigen Fall, eine Gleichung der Form

$$-(x - x_1)(x - x_2')(x - x_3') = 0.$$

für entsprechend gewählte $x_2', x_3' \in \overline{F}$, wobei nach Koeffizientenvergleich folgt, dass

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2' + x_3'$$

ist. Da L die Tangente in P_1 an $E(F)$ ist, ist die Vielfachheit von P_1 in $E(F) \cap L$ größer oder gleich 2. Wir gehen wieder analog wie in (1.8) 3. Fall vor und erhalten dann, dass die Vielfachheit gleich der Ordnung der Nullstelle x_1 in $-(x - x_1)(x - x_2')(x - x_3')$ ist. Wir nehmen also o. B. d. A. an, dass $x_1 = x_2'$ ist. Dann folgt

$$x_3' = \lambda^2 + a_1\lambda - a_2 - 2x_1,$$

so dass x_3' ebenfalls in F liegt. Die Gerade L schneidet $E(F)$ also noch im Punkt $P_3' = (x_3', y_3')$ mit

$$y_3' = \lambda x_3' + \nu.$$

Wenn $P_3' \neq P_1$ ist, so muss $-(P_1 + P_2) = P_3'$ sein. Wenn aber $P_3' = P_1$ ist, so hat das Polynom $-(x - x_1)(x - x_2')(x - x_3')$ eine Nullstelle dritter Ordnung in x_1, der Punkt P_1 hat also die Vielfachheit 3. Auch hier ist also $P_3' = P_1$ der gesuchte dritte Schnittpunkt, d. h. $-(P_1 + P_2) = P_3'$.

Nun wenden wir wieder i) an und erhalten $P_1 + P_2 = P_3 = (x_3, y_3)$ mit

$$x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1 \text{ und}$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

wobei λ und ν den obigen Formeln genügen. □

Im letzten Vortrag haben wir gesehen, dass, wenn die Charakteristik unseres Grundkörpers nicht 2 oder 3 ist, wir annehmen können, dass die Weierstraßgleichung für $E(F)$ die einfache Form

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

hat. Hier ist also $E(F) \cap i(\mathbb{A}^2(F)) = i(C_f(F))$ für

$$f(x, y) = y^2 - x^3 - a_4x - a_6.$$

In diesem Fall lassen sich unsere Formeln aus Satz (1.14) folgendermassen vereinfachen:

(1.15) Satz

In der obigen Situation gilt:

a) Für $P_1 = (x_1, y_1) \in C_f(F)$ ist $-P_1 = (x_1, -y_1)$.

b) Für $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ aus $C_f(F)$ mit $P_1 \neq -P_2$ ist $P_1 + P_2 = P_3 = (x_3, y_3)$, wobei

$$x_3 = \lambda^2 - x_1 - x_2 \text{ und } y_3 = \lambda(x_1 - x_3) - y_1 \text{ ist mit}$$
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{falls } P_1 \neq P_2 \\ \frac{3x_1^2 + a_4}{2y_1}, & \text{falls } P_1 = P_2 \end{cases}$$

Beweis

a) Die Behauptung folgt mit (1.14) i), da $a_1 = a_3 = 0$ gilt.

b) Da $a_1 = a_2 = a_3 = 0$ gilt, folgt mit Hilfe von (1.14), dass

$$x_3 = \lambda^2 - x_1 - x_2 \text{ und } y_3 = -\lambda x_3 - \nu$$

gilt, wobei λ genau wie in der Behauptung definiert ist. Im Beweis von (1.14) haben wir gesehen, dass $y_1 = \lambda x_1 + \nu$, also ist $\nu = y_1 - \lambda x_1$. Nach Einsetzen erhält man dann, dass

$$y_3 = -\lambda x_3 + \lambda x_1 - y_1 = \lambda(x_1 - x_3) - y_1$$

gilt. □

§ 2 Elliptische Kurven über endlichen Körpern

In dem ersten Teil dieses Abschnitts wird die Frobeniusabbildung für elliptische Kurven über endlichen Körpern vorgestellt. Im zweiten und dritten Abschnitt gehen wir kurz auf verschiedene Verfahren ein um die Gruppenordnung von $E(F)$ zu bestimmen.

In diesem Abschnitt ist F immer ein endlicher Körper, d. h. es ist $F = \mathbb{F}_q$ für ein $q = p^r$, wobei p eine Primzahl und r in $\mathbb{N}$ ist. Die Charakteristik von F ist also gleich p. Mit $\overline{F}$ bezeichnen wir den algebraischen Abschluss von F. Dabei können wir eine elliptische Kurve $E(F)$ auch über $\overline{F}$ betrachten, indem wir die Weierstraßgleichung einfach als Gleichung über dem algebraischen Abschluss auffassen. Offensichtlich gilt dann $E(F) \subset E(\overline{F})$.

— *Der Frobenius* —

(2.1) Lemma
Es sei $E(F)$ eine elliptische Kurve über dem endlichen Körper $F = \mathbb{F}_q$. Dann ist die Abbildung $\phi : E(\overline{F}) \to E(\overline{F})$, $[x : y : z] \mapsto [x^q : y^q : z^q]$ wohldefiniert und ein Gruppenhomomorphismus. Dieser wird *Frobeniusendomorphismus* (oder kurz *Frobenius*) genannt.

Beweis
Wohldefiniertheit: ϕ ist offensichtlich eine Abbildung von $\mathbb{P}^2(\overline{F})$ nach $\mathbb{P}^2(\overline{F})$, denn es gilt:

a) $[x^q : y^q : z^q] = [0 : 0 : 0]$ genau dann, wenn $[x : y : z] = [0 : 0 : 0]$. Da $[0 : 0 : 0] \notin \mathbb{P}^2(\overline{F})$ ist, existiert kein Element $[a : b : c]$ in $\mathbb{P}^2(\overline{F})$ mit $\phi([a : b : c]) = [0 : 0 : 0]$.

b) Die Abbildung ϕ erhält die Äquivalenzrelation, mit der $\mathbb{P}^2(\overline{F})$ definiert ist.

Im weiteren Vorgehen benutzen wir den Satz „Schülers Traum“ aus der linearen Algebra, der folgendes besagt: Für einen endlichen Körper $\mathbb{F}_q$ und beliebigen Elementen $a, b \in \overline{\mathbb{F}_q}$ gilt

$$(a + b)^q = a^q + b^q.$$

Sei nun $E(F)$ eine elliptische Kurve mit dem Weierstraßpolynom

$$g(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

Für $[x : y : z] \in E(\overline{F})$ gilt dann

$$g(x^q, y^q, z^q) = (y^q)^2 z^q + a_1 x^q y^q z^q + a_3 y^q (z^q)^2 - (x^q)^3 - a_2 (x^q)^2 z^q - a_4 x^q (z^q)^2 - a_6 (z^q)^3$$

$$\underset{a=a^q \ \forall a \in F}{=} (y^2 z)^q + (a_1 xyz)^q + (a_3 yz^2)^q - (x^3)^q - (a_2 x^2 z)^q - (a_4 xz^2)^q - (a_6 z^3)^q$$

$$\underset{\text{Schülers Traum}}{=} (y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3)^q = (\underbrace{g(x, y, z)}_{=0})^q = 0,$$

also ist $[x^q : y^q : z^q] \in E(\overline{F})$.

Gruppenhomomorphismus: Hierfür müssen wir zeigen, dass

a) $\phi(O) = O$ und

b) $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$ für alle $P_1, P_2 \in E(\overline{F})$.

zu a) Es gilt $\phi([0 : 1 : 0]) = [0^q : 1^q : 0^q] = [0 : 1 : 0]$, also ist $\phi(O) = O$.

zu b) Für alle $P \in E(\overline{F})$ ist

$$\phi(P + O) = \phi(P) = \phi(P) + O = \phi(P) + \phi(O).$$

Seien nun $P_1, P_2 \in E(\overline{F}) \setminus \{O\}$. Wir wenden (1.14) an und schreiben $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$. Falls $P_1 + P_2 \neq O$ ist, so gilt $P_1 + P_2 = (x_3, y_3)$ mit

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 \ \text{ und } \ y_3 = -(\lambda + a_1) x_3 - \nu - a_3$$

und gewissen $\lambda, \nu \in \overline{F}$. Daraus folgt, dass

$$\phi(P_1 + P_2) = (x_3^q, y_3^q)$$

ist, wobei

$$x_3^q = (\lambda^2 + a_1 \lambda - a_2 - x_1 - x_2)^q = (\lambda^q)^2 + a_1 \lambda^q - a_2 - x_1^q - x_2^q \ \text{ und}$$

$$y_3^q = (-(\lambda + a_1) x_3 - \nu - a_3)^q = -(\lambda^q + a_1) x_3^q - \nu^q - a_3$$

ist. Dabei haben wir wieder aus der linearen Algebra den Satz „Schülers Traum“ verwendet und benutzt, dass $a = a^q \ \forall a \in F$ gilt. Damit sieht man auch, dass die Werte λ^q und ν^q gerade den durch die Addition von $\phi(P_1) = (x_1^q, y_1^q)$ und $\phi(P_2) = (x_2^q, y_2^q)$ definierten Konstanten λ und ν aus (1.14) entsprechen, also folgt

$$(x_3^q, y_3^q) = \phi(P_1) + \phi(P_2)$$

und damit

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2).$$

Als letztes müssen wir noch den Fall $P_1 + P_2 = O$ untersuchen:

Mit (1.14) folgt dann, dass $P_2 = -P_1$, d. h. $P_2 = (x_1, -y_1 - a_1x_1 - a_3)$, ist. Analog zu oben folgt, dass

$$\phi(P_1) = (x_1^q, y_1^q) \text{ und } \phi(P_2) = (x_1^q, -y_1^q - a_1x_1^q - a_3)$$

ist. Demnach ist

$$\phi(P_2) = -\phi(P_1), \text{ also } \phi(P_1) + \phi(P_2) = O = \phi(P_1 + P_2).$$

Insgesamt folgt also

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \text{ für alle } P_1, P_2 \in E(\overline{F}). \qquad \square$$

— Punkte zählen —

Als nächstes möchten wir die Anzahl der Punkte in einer beliebigen elliptischen Kurve $E(F)$ bestimmen. Dazu geben wir im folgenden Satz eine Obergrenze.

(2.2) Satz
Sei $E(F)$ eine elliptische Kurve. Dann ist

$$\#E(F) \leq 2q + 1. \qquad \diamond$$

Beweis
Sei $E(F)$ eine elliptische Kurve mit der Weierstraßgleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Wir wissen, dass genau ein Punkt aus $E(F)$, nämlich $O = [0 : 1 : 0]$, nicht im affinen Raum liegt. Also besteht $E(F)$ aus O und den Lösungen der affinen Weierstraßgleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

in $\mathbb{A}^2(F)$. Wenn wir jetzt ein beliebiges x aus F in die Gleichung einsetzen, erhalten wir eine quadratische Gleichung für y. Also gibt es zu jedem festen x höchstens zwei Werte y aus F, so dass (x, y) eine gesuchte Lösung ist. Da wir für x genau q Möglichkeiten haben, ist die Anzahl der Punkte von $E(F)$ somit kleiner oder gleich $2q + 1$. $\square$

Wenn wir annehmen, dass die Charakteristik von F nicht 2 ist, dann können wir, wie wir im vorigen Vortrag gesehen haben, ebenfalls annehmen, dass die affine Weierstraßgleichung die Form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 =: h(x)$$

hat. Falls $h(x) = 0$ ist, so ist $y = 0$ die einzige Lösung. Falls $h(x) \neq 0$ ein Quadrat in $\mathbb{F}_q$ ist, so finden wir zwei Lösungen (x, y) und $(x, -y)$ dieser Gleichung, und falls $h(x)$ kein Quadrat in $\mathbb{F}_q$ ist, so hat $y^2 = h(x)$ gar keine Lösung. Aufgrunddessen definieren wir folgende Funktion:

$$\chi : \mathbb{F}_q^* \to \{-1, 1\},$$

wobei $\chi(x) = 1$, falls x ein Quadrat in $\mathbb{F}_q$ ist und $\chi(x) = -1$, falls x kein Quadrat in $\mathbb{F}_q$ ist. Sei nun ζ ein beliebiger Erzeuger der zyklischen Gruppe $\mathbb{F}_q^*$. Dann gilt offensichtlich

$$\chi(\zeta^k) = \begin{cases} 1, & \text{falls } k \text{ gerade, und} \\ -1, & \text{falls } k \text{ ungerade ist.} \end{cases}$$

Mit dieser Beschreibung sieht man leicht, dass

$$\chi(x_1x_2) = \chi(x_1)\chi(x_2)$$

für alle $x_1, x_2 \in \mathbb{F}_q^*$ ist. Wir können χ zu einer Abbildung

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\}$$

ergänzen, indem wir $\chi(0) = 0$ setzen. Dann hat für jedes x in $\mathbb{F}_q$ die Gleichung $y^2 = h(x)$ genau $\chi(h(x)) + 1$ Lösungen y in $\mathbb{F}_q$. Wir können also alle Lösungen der affinen Weierstraßgleichung durch

$$\sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1)$$

zählen. Daher folgt, wenn wir noch den Punkt O berücksichtigen,

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(h(x)).$$

In manchen Fällen kann man damit die Anzahl der Punkte einer elliptischen Kurve $E(\mathbb{F}_q)$ berechnen:

(2.3) Beispiel
Sei $E(\mathbb{F}_{31})$ durch die affine Weierstraßgleichung

$$y^2 = x^3 - x$$

über $\mathbb{F}_{31}$ gegeben, wobei hier -1 kein Quadrat in diesem Körper ist. Daher gilt $\chi(-1) = -1$, woraus für alle x in $\mathbb{F}_{31}$ mit $x^3 - x \neq 0$ folgt, dass

$$\chi((-x)^3 - (-x)) = \chi(-(x^3 - x)) = \chi(-1)\chi(x^3 - x) = -\chi(x^3 - x)$$

ist. Die Gleichung $x^3 - x = 0$ gilt genau dann, wenn $x = 0$, $x = 1$ oder $x = -1$ ist, wobei in diesen Fällen $\chi(x^3 - x) = 0$ ist, also ist

$$\chi(x^3 - x) + \chi((-x)^3 - (-x)) = 0.$$

Daraus folgt, dass

$$\#E(\mathbb{F}_{31}) = 1 + 31 + \sum_{x \in \mathbb{F}_{31}^* \setminus \{\pm 1\}} \chi(x^3 - x) = 32$$

ist, da sich die Beiträge für x in $\mathbb{F}_{31}^*$ paarweise wegheben. ◇

Wir haben oben gesehen, dass

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(h(x)), \quad \text{also}$$

$$\sum_{x \in \mathbb{F}_q} \chi(h(x)) = \#E(\mathbb{F}_q) - q - 1$$

ist. Nach (2.2) gilt weiter

$$\#E(\mathbb{F}_q) - q - 1 \leq q.$$

Durch den sogenannten Satz von Hasse können wir diese Schranke noch verbessern, wobei wir sogar die Voraussetzung, dass $a_1 = a_3 = 0$ ist, fallenlassen können.

(2.4) Satz (Hasse)
Es sei $E(F)$ eine beliebige elliptische Kurve über dem endlichen Körper $F = \mathbb{F}_q$. Dann gilt

$$|\#E(F) - q - 1| \leq 2\sqrt{q}.$$

Beweis
Dafür wird mehr Theorie über elliptische Kurven benötigt, weshalb hier kein Beweis angegeben wird. □

Mit dem Satz von Hasse können wir also $E(F)$, wobei F ein Körper mit q Elementen ist, folgendermaßen abschätzen:

$$-2\sqrt{q}+q+1 \leq \#E(F) \leq 2\sqrt{q}+q+1.$$

Wir wollen kurz darauf eingehen, warum die Zahl $q+1-\#E(F)$ auch *Spur des Frobenius* genannt wird.

Den Ring

$$\mathbb{Z}_p = \{(x_n)_{n\geq 1} : x_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ und } x_{n+1} \equiv x_n \bmod p^n \text{ für alle } n \geq 1\}$$

bezeichnen wir als *Ring der p-adischen ganzen Zahlen* für eine Primzahl p. Jede ganze Zahl m definiert dabei eine Folge $m + p^n\mathbb{Z}$ und kann daher als Element von $\mathbb{Z}_p$ aufgefasst werden (Der Quotientenkörper $\mathbb{Q}_p$ des Ringes ist dann der Körper der p-adischen Zahlen). Für jede Primzahl $l \neq p = \text{char}\,(F)$ und alle $n \geq 1$ sei weiter

$$E[l^n] := \{P \in E(\overline{F}) : l^n P = 0\}.$$

Als nächstes definieren wir den Tatemodul

$$T_l(E) = \{(P_n)_{n\geq 1} : P_n \in E[l^n] \text{ und } lP_{n+1} = P_n \forall n \geq 1\}$$

Der Tatemodul $T_l(E)$ ist nun ein freier $\mathbb{Z}_l$-Modul vom Rang 2, d. h. es gibt eine Basis $x, y \in T_l(E)$, so dass

$$T_l(E) = \mathbb{Z}_l x \oplus \mathbb{Z}_l y$$

ist. Der Frobeniusendomorphismus $\phi : E(\overline{F}) \to E(\overline{F})$ induziert eine $\mathbb{Z}_l$-lineare Abbildung

$$\phi_l : T_l(E) \to T_l(E),$$

gegeben durch

$$\phi_l(P_n)_{n\geq 1} = (\phi(P_n))_{n\geq 1}.$$

Wenn wir nun wie oben eine Basis x, y des $\mathbb{Z}_l$-Moduls $T_l(E)$ wählen, so lässt sich die lineare Abbildung ϕ_l darstellen durch eine (2×2) -Matrix $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ mit Einträgen in $\mathbb{Z}_l$.

Wir definieren nun die Spur von ϕ_l als die Spur der Matrix A, also

$$\text{Spur}\,\phi_l = \text{Spur}\,A = a_{11} + a_{22}$$

und die Determinante von ϕ_l als die Determinante von A, also

$$\det\phi_l = \det A = a_{11}a_{22} - a_{12}a_{21}.$$

Diese Werte wollen wir nun bestimmen.

(2.5) Proposition
Es ist $\det \phi_l = q$ und $\text{Spur}\, \phi_l = q + 1 - \#E(F)$. ◇

Beweis
Dies geht über unsere Mittel hinaus. Der Beweis wird deshalb weggelassen. □

Für jede (2×2) -Matrix A gilt nun:

$$A^2 - (\text{Spur}\, A) \cdot A + \det A \cdot E = 0.$$

Es gilt also

$$\phi_l^2 - (1 + q - \#E(F)) \cdot \phi_l + q \cdot \text{id} = 0.$$

Man kann nun zeigen, dass der Übergang von einem Homomorphismus der elliptischen Kurve zu einer linearen Abbildung des Tatemoduls injektiv ist. Daraus folgt folgender

(2.6) Satz
Es gilt:

$$\phi^2 - (1 + q - \#E(F)) \cdot \phi + q \cdot \text{id} = 0,$$

d. h. für jedes $P \in E(\overline{F})$ ist

$$\phi^2(P) - (1 + q - \#E(F))\phi(P) + qP = O.$$ ◇

Ein effektiver Algorithmus zur Bestimmung von $\#E(F)$ ist der sogenannte *Schoof-Algorithmus*.

— *Der Schoof-Algorithmus* —

Wir nehmen an, dass die Charakteristik von F größer als 2 ist und dass $E(F)$ durch die affine Weierstraßgleichung

$$y^2 = x^3 + a_4 x + a_6$$

gegeben ist. Als nächstes wollen wir die Spur des Frobenius $t = q + 1 - \#E(F)$ modulo der ersten Primzahlen $l = 2, 3, 5, 7, 11, \ldots$ betrachten. Wieviele dieser Informationen t mod l braucht man, um t und damit $\#E(F)$ zu berechnen?

Es seien $l_1 = 2, l_2 = 3, l_3 = 5, \ldots, l_r$ die ersten r Primzahlen. Nach dem Chinesischen Restsatz vermittelt die Restklassenabbildung

$$\mathbb{Z} \to \mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_r\mathbb{Z}$$

eine Bijektion

$$\mathbb{Z}/(l_1 \cdot \ldots \cdot l_r)\mathbb{Z} \to \mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_r\mathbb{Z} \text{ mit } t \mapsto (t \bmod l_1, \ldots, t \bmod l_r).$$

Wenn also

$$-\frac{l_1 \cdot \ldots \cdot l_r}{2} < t < \frac{l_1 \cdot \ldots \cdot l_r}{2}$$

ist, so ist t durch seine Restklasse in $\mathbb{Z}/(l_1 \cdot \ldots \cdot l_r)$, und damit auch durch die r Restklassen

$$(t \bmod l_1, \ldots, t \bmod l_r)$$

eindeutig bestimmt. Durch den Satz von Hasse wissen wir, dass $-2\sqrt{q} \leq t \leq 2\sqrt{q}$ ist. Es genügt also, r so zu wählen, dass

$$l_1 \cdot \ldots \cdot l_r > 4\sqrt{q}$$

ist.

Wir bestimmen zunächst t mod 2. Da q ungerade ist, folgt, dass

$$t \equiv (q + 1 - \#E(F)) \bmod 2 \equiv \#E(F) \bmod 2.$$

ist. Es reicht also zu überprüfen, ob $\#E(F)$ gerade oder ungerade ist. Für ein festes x aus F mit $x^3 + a_4x + a_6 \neq 0$ hat die Gleichung $y^2 = x^3 + a_4x + a_6$ keine oder zwei Lösungen y. Demnach ist die Anzahl aller Lösungen (x, y) mit $y \neq 0$ gerade. Diese Punkte im affinen Raum können wir somit vernachlässigen, also reicht es, nur die affinen Punkte $(x, 0)$ und O zu betrachten. Falls die Gleichung $x^3 + a_4x + a_6 = 0$ eine Lösung $x_0 \in F$ hat, dann ist

$$x^3 + a_4x + a_6 = (x - x_0)(x - x_1)(x - x_2)$$

mit geeignet gewählten x_1, x_2 in $\overline{F}$. Man kann leicht nachrechnen, dass die Nullstellen x_0, x_1 und x_2 paarweise verschieden sind, da ansonsten die Kurve singulär wäre. Weiter haben wir schon vorher gesehen, dass entweder $x_1, x_2 \in F$ oder $x_1, x_2 \notin F$, d. h. es gibt entweder drei Punkte der Form $(x, 0)$ in $E(F)$ oder nur einen. Wenn wir also noch den Nullpunkt O berücksichtigen, so folgt insgesamt, dass $t \equiv 1 \bmod 2$ genau dann ist, wenn $x^3 + a_4x + a_6$ keine Lösung in F hat. In diesem Fall wird das Polynom $X^3 + a_4X + a_6$ also nicht von einem Faktor der Form $(X - b)$ für ein b in F geteilt. Da wir in der linearen Algebra gesehen haben, dass

$$X^q - X = \prod_{b \in F} (X - b)$$

ist, ist dies genau dann der Fall, wenn im Polynomring $F[X]$ gilt, dass

$$\mathrm{ggT}\,(X^3 + a_4X + a_6, X^q - X) = 1$$

ist. Dies lässt sich leicht mit dem euklidischen Algorithmus berechnen.

Für $l \geq 3$ ist die Bestimmung von t mod l etwas schwieriger. Wir werden hier auch nur kurz die grundlegende Idee skizzieren. In (2.6) haben wir gesehen, dass der Frobenius ϕ der Gleichung

$$\phi^2(P) - t\phi(P) + qP = O \text{ für alle } P \in E(\overline{F})$$

genügt. Wir suchen jetzt eine Zahl $\tau \in \{0, \ldots, l-1\}$, so dass die Gleichung

$$\phi^2(P) - \tau\phi(P) + qP = O$$

für jeden Punkt P aus der endlichen Untergruppe

$$E[l] := \{P \in E(\overline{F}) : lP = O\}$$

gilt. Wenn wir ein solches τ gefunden haben, muss für jedes $P \neq O$ in $E[l]$, wenn wir die beiden Gleichungen oben voneinander subtrahieren,

$$(t - \tau)\phi(P) = O$$

sein. Da der Frobenius ein Gruppenhomomorphismus ist, ist $\phi(P) \neq O$, und offenbar ist $\phi(P)$ auch in $E[l]$, d. h. $\phi(P)$ hat die Ordnung l in der Gruppe $E(\overline{F})$. Daher muss l ein Teiler von $t - \tau$ sein, also ist

$$t \equiv \tau \bmod l.$$

Wir wollen noch kurz darauf eingehen, wie man ein solches τ findet:

Wir schreiben die Gleichung

$$\phi^2(P) - t\phi(P) + qP = O \text{ für alle } P \in E(\overline{F})$$

in eine Polynomgleichung um, indem wir (1.14) benutzen, und wenden weiter die sogenannten Divisionspolynome, die wir hier nicht näher erläutern wollen, an, mit denen man testen kann, ob ein Punkt in $E[l]$ liegt.

Für $\tau = 0, 1, \ldots, l-1$ probiert man nun der Reihe nach, ob diese Polynomgleichung erfüllt ist. Sobald dies der Fall ist, hat man das richtige τ gefunden.