Technische Universität Braunschweig
Institut für Analysis und Algebra

Prof. Dr. Harald Löwe
Prof. Dr. Thomas Sonar

Bachelorarbeit

Kryptographie auf elliptischen Kurven

Christian Hoffmeister
Maienstraße 23
38118 Braunschweig
c.hoffmeister@tu-bs.de

1-Fach-Bsc. Mathematik
Matr.-Nr. 2944344
Sommersemester 2010
Fachsemester 6

Inhaltsverzeichnis

1 Vorbereitungen **3**
1.1 Polynome . . . 3
1.2 Affine Kurven . . . 4
1.3 Projektive Kurven . . . 5
1.4 Projektive Geraden . . . 8

2 Elliptische Kurven **11**
2.1 Einführung . . . 11
2.2 Spezielle elliptische Kurven . . . 12
2.3 Diskriminante elliptischer Kurven . . . 14

3 Gruppenstruktur auf elliptischen Kurven **16**
3.1 Summe aller Vielfachheiten . . . 16
3.2 Gruppenstruktur . . . 20
3.3 Beweis der Gruppenstruktur mit Divisoren . . . 27

4 Kryptographie auf elliptischen Kurven **32**
4.1 Verschlüsselungsverfahren . . . 32
4.2 Diffie-Hellmann-Schlüsselaustausch . . . 33
4.3 Komplexität . . . 35

5 Fazit **38**

Abbildungsverzeichnis

1 $E_f(\mathbb{R})$ für $f(x,y) = y^2 - x^3 - 1$ bzw. $f(x,y) = y^2 - x^3 + 2x$ . . . 19
2 Darstellung des Punktes $[0:1:0]$ im affinen Raum . . . 20
3 Addition zweier verschiedener Punkte auf elliptischen Kurven . . . 21
4 Assoziativitätsraster . . . 22
5 Elliptische Kurve über $\mathbb{Z}_7$ . . . 26

Einleitung

Diese Arbeit gibt eine Einführung in die Mathematik der elliptischen Kurven. In Kapitel 2 werden der affine und der projektive Raum sowie affine und projektive ebene Kurven eingeführt. Mit deren Hilfe werden elliptische Kurven definiert und untersucht.

Das Kapitel 3 wird dann den größten Teil dieser Arbeit einnehmen. In diesem Kapitel wird eine Gruppenstruktur auf elliptischen Kurven definiert und bewiesen, dass es sich in der Tat um eine Gruppe handelt. Den Abschluss der theoretischen Vorarbeit bildet Kapitel 4. Hier soll auch anhand von konkreten Beispielen gezeigt werden, wie sich elliptische Kurven nun in der Kryptographie einsetzen lassen.

Zum Verständnis dieser Arbeit werden nur grundlegende Kenntnisse in linearer Algebra vorausgesetzt.

1 Vorbereitungen

In diesem Abschnitt werden wir alle nötigen Definitionen und Sätze kennenlernen, die für die Einführung von elliptischen Kurven notwendig sind. Es werden affine und projektive ebene Kurven eingeführt. Elliptische Kurven sind spezielle projektive ebene Kurven, deren affine Teile einen leichteren Zugang zur Untersuchung bieten.

1.1 Polynome

1.1.1 Definition (Polynome)**.** *Sei F ein Körper. Dann heißt ein Ausdruck der Form*

$$f(x_1, \ldots, x_n) = \sum_{\nu_1, \ldots, \nu_n \geq 0} \alpha_{\nu_1, \ldots, \nu_n} x_1^{\nu^1} \ldots x_n^{\nu^n}$$

mit Koeffizienten $\alpha_{\nu_1, \ldots, \nu_n} \in F$, von denen fast alle verschwinden, Polynom über F in $x_1, \ldots, x_n$. Die Menge aller Polynome über F in $x_1, \ldots, x_n$ wird mit

$$F[x_1, \ldots, x_n]$$

bezeichnet.

1.1.2 Definition (Ableitungen)**.** *Sei ein Polynom $f \in F[x_1, \ldots, x_n]$. Dann heißt für alle $i \in \{1, \ldots, n\}$*

$$\frac{\partial f}{\partial x_i}(x_1, \ldots, x_n) = \sum_{\nu_1, \ldots, \nu_n \geq 0, \nu_i > 0} \alpha_{\nu_1, \ldots, \nu_n} \nu_i x_1^{\nu_1} \ldots x_i^{\nu_i - 1} \ldots x_n^{\nu_n}$$

partielle Ableitung von f nach x_i. Weiter heißt

$$\nabla g(x_1, \ldots, x_n) = \left(\frac{\partial f}{\partial x_1}(x_1, \ldots, x_n), \ldots, \frac{\partial f}{\partial x_n}(x_1, \ldots, x_n) \right)$$

Gradient von f.

Falls $F = \mathbb{R}$ ist, so ergibt diese Definition der Ableitung dasselbe Ergebnis wie die analytische Definition der Ableitung über die Grenzwertbildung.

1.1.3 Satz (Ableitungsregeln)**.** *Mit der vorangegangenen Definition lassen sich folgende Regeln leicht nachvollziehen:*

- *Summenregel:* $\dfrac{\partial(f+g)}{\partial x_i} = \dfrac{\partial f}{\partial x_i} + \dfrac{\partial g}{\partial x_i}$
- *Produktregel:* $\dfrac{\partial(f \cdot g)}{\partial x_i} = f\dfrac{\partial g}{\partial x_i} + g\dfrac{\partial f}{\partial x_i}$

Seien $g_1, \ldots, g_n \in F[x_1, \ldots, x_n]$ *und* $f(g_1, \ldots, g_n)$ *das Polynom, welches man durch Einsetzen der Polynome* $g_1, \ldots, g_n$ *in* f *anstelle von Variablen* $x_1, \ldots, x_n$ *erhält.*

- *Kettenregel:* $\dfrac{\partial f(g_1, \ldots, g_n)}{\partial x_i} = \displaystyle\sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(g_j, \ldots, g_n)\frac{\partial g_j}{\partial x_i}(x_1, \ldots, x_n)$

1.1.4 Definition (Diskriminante)**.** *Sei* $f \in F[x]$ *ein Polynom vom Grad* n *in einer Variablen mit Nullstellen* $x_1, \ldots, x_n$ *der Form* $f(x) = a_n x^n + \ldots + a_1 x + a_0$*. Der Ausdruck*

$$D_n = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

heißt Diskriminante des Polynoms f*.*

Offensichtlich verschwindet der Ausdruck

$$\prod_{i<j} (x_i - x_j)$$

genau dann, wenn es mindestens eine doppelte Nullstelle gibt. Dieser Ausdruck ist jedoch nicht symmetrisch, wodurch sich sein Wert bei Umnummerierung der Nullstellen ändern kann. Durch quadrieren des Ausdrucks kann das verhindert werden. Der Faktor a_n^{2n-2} dient hierbei dazu, dass bei der Anwendung des Satz von Vieta keine Brüche auftauchen.

1.1.5 Satz (Diskriminante quadratischer und kubischer Polynome)**.** *Seien ein quadratischens Polynom der Form* $p_2(x) = ax^2+bx+c$ *und ein kubisches Polynom der Form* $p_3(x) = ax^3 + bx^2 + cx + d$ *gegeben. Mit dem Satz von Vieta lassen sich* D_2 *und* D_3 *berechnen als*

$$\begin{aligned} D_2 &= b^2 - ac \\ D_3 &= b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2. \end{aligned}$$

1.2 Affine Kurven

Ab nun sei F stets ein Körper wie etwa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{F}_q$.

1.2.1 Definition (Zweidimensionaler affiner Raum)**.** *Wir nennen*

$$\mathbb{A}^2 = F \times F = \{(a, b) : a, b \in F\}$$

den zweidimensionalen affinen Raum oder auch einfach affine Ebene.

1.2.2 Definition (Affine ebene Kurve)**.** *Gegeben sei ein Polynom $f \in F[x,y]$ mit*

$$f(x,y) = \sum_{i,j \geq 0} \alpha_{i,j}\ x^i y^j$$

von endlichem Grad mit $f \neq 0$. Dann heißt die Menge

$$C_f(F) := \{(a,b) \in \mathbb{A}^2 : f(a,b) = 0\}$$

affine ebene Kurve oder auch einfach affine Kurve.

Wenn wir affine Kurven nun über einen größeren Körper E mit $F \subset E$ betrachten, dann gilt offensichtlich auch $C_f(F) \subset C_f(E)$. Diese Aussage gilt insbesondere für den algebraischen Abschluss $\overline{F}$ von F.

1.2.3 Definition (Singularität von affinen Kurven)**.** *Sei $C_f(F)$ eine affine ebene Kurve.*

1. *$C_f(F)$ heißt singulär im Punkt $(a,b) \in C_f(F)$, falls $\nabla f(a,b) = (0,0)$ ist.*
2. *Umgekehrt heißt $C_f(F)$ nicht-singulär, falls beim Übergang zum algebraischen Abschluss für die affine Kurve $C_f(\overline{F})$ alle Punkte nicht singulär sind.*

1.3 Projektive Kurven

1.3.1 Definition (Homogene Polynome)**.** *Gegeben sei ein Polynom $g \in F[X,Y,Z]$ mit*

$$g(X,Y,Z) = \sum_{i,j,k \geq 0} \alpha_{i,j,k}\ X^i Y^j Z^k$$

von endlichem Grad. Dann heißt g homogen vom Grad d, falls es ein d gibt, so dass in allen Summanden, in denen $\alpha_{i,j,k}$ nicht verschwindet, die Summe der Exponenten $i+j+k = d$ ist.

1.3.2 Lemma. *Sei $g \in F[X,Y,Z]$ ein homogenes Polynom vom Grad d. Dann gilt für alle $a,b,c \in F$ und $t \in F \setminus \{0\}$*

$$g(a,b,c) = 0 \Leftrightarrow g(ta,tb,tc) = 0.$$

Beweis.

$$g(ta,tb,tc) = \sum_{i,j,k \geq 0} \alpha_{i,j,k}\ (ta)^i (tb)^j (tc)^k = \sum_{i,j,k \geq 0} \alpha_{i,j,k}\ t^{i+j+k} a^i b^j c^k = t^d g(a,b,c)\ \square$$

1.3.3 Definition (Zweidimensionaler projektiver Raum)**.** *Sei der F^3 gegeben.*

1. *Wir betrachten zwei Punkte $(a,b,c),(a',b',c') \in F^3$ als äquivalent, falls ein $t \in F \setminus \{0\}$ existiert mit*

$$a = ta' \quad b = tb' \quad c = tc'.$$

In diesem Fall schreiben wir einfach $(a,b,c) \sim (a',b',c')$.

2. *Den Raum, in dem alle Punkte des F^3, die im selben 1-dimensionalen Untervektorraum liegen, identifiziert werden, nennen wir den zweidimensionalen projektiven Raum oder auch einfach projektive Ebene. Er wird konkret mit*
$$\mathbb{P}^2(F) := (F^3 \setminus \{0\})/\sim$$
beschrieben.

3. *Punkte im $\mathbb{P}^2(F)$ werden mit $[a : b : c]$ bezeichnet. Jeder Punkt $(a, b, c) \neq 0$ liefert uns einen Punkt $[a : b : c] \in \mathbb{P}^2$ (seine Äquivalenzklasse).*

Ein Punkt $[a : b : c] \in \mathbb{P}^2(F)$ entspricht demnach dem 1-dimensionalen Untervektorraum $\langle (a, b, c) \rangle$ des F^3.

Da für homogene Polynome $g \in F[X, Y, Z]$ mit jeder Nullstelle alle Vielfachen ebenfalls Nullstellen sind, eignet sich der projektive zweidimensionale Raum – in dem Vielfache miteinander identifiziert werden – hervorragend um Nullstellenmengen solcher Polynome zu untersuchen. Dass der $\mathbb{P}^2(F)$ keinen Nullpunkt hat, stört dabei nicht, da homogene Polynome vom Grad $d \geq 1$ im Nullpunkt immer verschwinden.

1.3.4 Lemma (Zerlegung des zweidiemensionalen projektiven Raums)**.** *Sei der $\mathbb{P}^2(F)$ gegeben. Dann gilt*
$$\begin{aligned} \mathbb{P}^2(F) &= \{[a : b : 1] \in \mathbb{P}^2(F)\} \dot\cup \\ &= \{[a : 1 : 0] \in \mathbb{P}^2(F)\} \dot\cup \\ &= \{[1 : 0 : 0] \in \mathbb{P}^2(F)\}. \end{aligned}$$

Es sind auch andere Zerlegungen möglich. Dann sind die nachfolgenden Resultate analog zu führen. Im Rahmen dieser Arbeit werden wir nur diese Zerlegung betrachten.

1.3.5 Satz (Darstellung des zweidimensionalen projektiven Raums)**.** *Durch eine Einbettung der affinen Ebene und F in die projektive Ebene, lässt diese sich als disjunkte Vereinigung der affinen Ebene, F und einem weiteren Punkt darstellen.*

1. *Die Abbildung $i : A^2(F) \to \mathbb{P}^2(F) : i(a, b) = [a : b : 1]$ ist eine Einbettung.*

2. *Die Abbildung $j : F \to \mathbb{P}^2(F) : j(a) = [a : 1 : 0]$ ist eine Einbettung.*

3. *Es gilt $\mathbb{P}^2(F) = i(\mathbb{A}^2(F)) \dot\cup j(F) \dot\cup \{[1 : 0 : 0]\}$.* □

1.3.6 Definition (Affine Punkte, Fernpunkte)**.** *Seien die affine Ebene und die projektive Ebene gegeben. Alle Punkte der projektiven Ebene, die wie im vorangegangem Satz gesehen eine Entsprechung in der affinen Ebene haben, nennen wir affine Punkte. Alle anderen nennen wir Fernpunkte.*

1.3.7 Definition (Projektive ebene Kurve)**.** *Gegeben sei ein homogenes Polynom $g \in F[X, Y, Z]$ mit*
$$g(x, y, z) = \sum_{i,j \geq 0} \alpha_{i,j}\ x^i y^j z^{d-i-j}$$
von endlichem Grad d mit $g \neq 0$. Dann heißt die Menge
$$C_g(F) := \{[a : b : c] \in \mathbb{P}^2(F) : g(a, b, c) = 0\}$$
projektive ebene Kurve oder auch einfach projektive Kurve.

1.3.8 Satz (Übergang von affinen zu projektiven Koordinaten)**.** *Sei $f \in F[x,y]$ ein beliebiges Polynom außer das Nullpolynom vom Grad d. Dann können wir diesem Polynom in zwei Variablen ein Polynom in drei Variablen zuordnen auf folgende Weise:*

$$f(x,y) = \sum_{i,j \geq 0} \alpha_{i,j}\ x^i y^j$$

wird das Polynom

$$g(X,Y,Z) = \sum_{i,j \geq 0} \alpha_{i,j}\ X^i Y^j Z^{d-i-j}$$

zugeordnet. Es gilt dann:

1. *Das Polynom g ist homogen vom Grad d.*
2. *Für alle $(a,b) \in \mathbb{A}^2(F)$ ist $g(a,b,1) = f(a,b)$.*
3. *Die Abbildung $i : \mathbb{A}^2(F) \to \mathbb{P}^2(F)$ bettet $C_f(F)$ in $C_g(F)$ ein.*
4. *Aus $i(a,b) = [a:b:1] \in C_g(F)$ folgt $(a,b) \in C_f(F)$.*

Beweis. 1. Offensichtlich gilt für alle Summanden, in denen $\alpha_{i,j}$ nicht verschwindet, $i + j + (d - i - j) = d$.

2. Es gilt $g(a,b,1) = \sum_{i,j \geq 0} \alpha_{i,j}\ a^i b^j 1^{d-i-j} = \sum_{i,j \geq 0} \alpha_{i,j}\ a^i b^j = f(a,b)$.

3. Sei $(a,b) \in C_f(F)$. Dann gilt $0 = f(a,b) = g(a,b,1) = 0$. Also ist

   $$i(a,b) = [a:b:1] \in C_g(F)$$

   und zusammen mit der schon gezeigten Injektivität von i folgt die Behauptung.

4. Sei $i(a,b) = [a:b:1] \in C_g(F)$. Dann folgt $0 = g(a,b,1) = f(a,b) = 0$. Also ist auch $(a,b) \in C_f(F)$. □

1.3.9 Lemma. *Für ein Polynom f und sein zugeordnetes homogenes Polynom g gilt*

$$C_g(F) \cap i(\mathbb{A}^2(F)) = i(C_f(F)).$$

1.3.10 Definition (Singularität von projektiven Kurven)**.** *Sei $C_g(F)$ eine projektive ebene Kurve.*

1. *$C_g(F)$ heißt singulär im Punkt $[a:b:c] \in C_g(F)$, falls $\nabla g(a,b,c) = (0,0,0)$ ist.*
2. *Umgekehrt heißt $C_f(G)$ nicht-singulär, falls beim Übergang zum algebraischen Abschluss für die projektive Kurve $C_f(\overline{F})$ alle Punkte nicht singulär sind.*

Dies ist wohldefiniert, da das Verschwinden einer partiellen Ableitung aufgrund der Homogenität von g nicht von der Wahl der Darstellung des Punktes $[a : b : c]$ abhängt. Für den Fall, dass in jedem Summanden die Potenz von X größer gleich 1 ist, gilt

$$\begin{aligned}\frac{\partial g}{\partial X}(ta, tb, tc) &= \sum_{i,j,k\geq 0} \alpha_{i,j,k} i\ (ta)^{i-1}(tb)^j(tc)^k = \sum_{i,j,k\geq 0} \alpha_{i,j,k} i\ t^{d-1}a^{i-1}b^jc^k \\ &= t^{d-1}\frac{\partial g}{\partial X}(a, b, c).\end{aligned}$$

Falls es Summanden mit $X^0Y^jZ^k$ gibt, fallen diese auf beiden Seiten weg, so dass weiterhin gilt

$$\frac{\partial g}{\partial X}(ta, tb, tc) = 0 \ \Leftrightarrow\ \frac{\partial g}{\partial X}(a, b, c) = 0.$$

Analog gilt dies für die beiden anderen partiellen Ableitungen $\dfrac{\partial g}{\partial Y}$ und $\dfrac{\partial g}{\partial Z}$.

1.3.11 Lemma. *Seien Polynome $f \in F[x, y]$ und $g \in F[X, Y, Z]$ gegeben, wobei g das f zugeordnete homogene Polynom ist. Sei $P \in \mathbb{P}^2(F)$ ein affiner Punkt und sei $Q \in \mathbb{A}^2(F)$ mit $i(Q) = P$. Dann ist $C_g(F)$ singulär in P genau dann, wenn $C_f(F)$ singulär ist in Q.*

Beweis. Sei $[a' : b' : c'] \in C_g(F)$ mit $i(a, b) = [a' : b' : c']$. Dann folgt nach Satz 1.3.8 schon, dass $(a, b) \in C_f(F)$ liegt und es gilt

$$\begin{aligned}\frac{\partial g}{\partial X}(a, b, 1) &= \sum_{i>0,j,k\geq 0} \alpha_{i,j} i\ a^{i-1}b^j1^k = \sum_{i>0,j\geq 0} \alpha_{i,j} i\ a^{i-1}b^j = \frac{\partial f}{\partial x}(a, b) \\ \frac{\partial g}{\partial Y}(a, b, 1) &= \sum_{i\geq 0,j>0,k\geq 0} \alpha_{i,j} j\ a^ib^{j-1}1^k = \sum_{i>0,j\geq 0} \alpha_{i,j} j\ a^ib^{j-1} = \frac{\partial f}{\partial y}(a, b) \\ \frac{\partial g}{\partial Z}(a, b, 1) &= \sum_{i,j,k\geq 0} \alpha_{i,j} k\ a^ib^j = \sum_{i,j,k\geq 0} \alpha_{i,j}(d - i - j)\ a^ib^j \\ &= d \cdot f(a, b) - a \cdot \frac{\partial f}{\partial x}(a, b) - b \cdot \frac{\partial f}{\partial y}(a, b).\end{aligned}$$

Da nun $f(a, b) = 0$ für $(a, b) \in C_f(F)$ gilt, folgt die Behauptung. □

1.4 Projektive Geraden

1.4.1 Definition (Projektive Geraden)**.** *Sei $g \in F[x, y, z]$ ein homogenes Polynom vom Grad 1 der Form*

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

mit $(\alpha, \beta, \gamma) \neq (0, 0, 0)$. Dann nennen wir $L(\alpha, \beta, \gamma) := C_g(F)$ projektive Gerade.

Offensichtlich sind projektive Geraden immer nicht-singulär, da für jeden Punkt $P \in C_g(\overline{F})$ gilt $\nabla g(P) = (\alpha, \beta, \gamma) \neq (0, 0, 0)$. Betrachten wir die zugeordnete affine Kurve $C_f(F) = C_g(F) \cap i(\mathbb{A}^2(F))$ mit

$$f(x, y) = \alpha x + \beta y + \gamma,$$

so gibt es drei Möglichkeiten:

Fall 1: $\alpha = \beta = 0$: In diesem Fall ist $\gamma \neq 0$ und $C_f(F) = \emptyset$.
Fall 2: $\beta \neq 0$: In diesem Fall ist $C_f(F) = \{(x, y) \in F \times \mathbb{F} : y = -\frac{\alpha}{\beta}x - \frac{\gamma}{\beta}\}$.
Fall 3: $\alpha \neq 0$: In diesem Fall ist $C_f(F) = \{(x, y) \in F \times \mathbb{F} : y = -\frac{\gamma}{\alpha}\}$.
Die zugeordnete affine Kurve ist also entweder leer oder eine Gerade im $\mathbb{A}^2(F)$.

Das Polynom, dessen Nullstellenmenge eine projektive Gerade definiert, entspricht der Darstellung einer gewöhnlichen Ebene durch den Ursprung im F^3. Eine projektive Gerade L entspricht demnach einem 2-dimensionalen Untervektorraum des F^3.

1.4.2 Lemma. *Für projektive Geraden gilt:*

1. *Zu je zwei verschiedenen Punkten der projektiven Ebene gibt es genau eine projektive Gerade, die diese verbindet.*
2. *Zu je zwei verschiedenen projektiven Geraden gibt es genau einen Punkt in der projektiven Ebene, in dem sich diese schneiden.*

Beweis. Zu zwei verschiedenen 1-dimensionalen Untervektorräumen des F^3 existiert genau ein 2-dimensionaler Untervektorraum, der beide enthält. Zu zwei verschiedenen 2-dimensionalen Untervektorräumen des F^3 existiert genau ein 1-dimensionaler Untervektorraum, der in beiden enthalten ist. □

1.4.3 Definition (Ferngerade)**.** *Die projektive Gerade, die genau alle Fernpunkte enthält und gegeben ist durch*

$$L(0, 0, 1) = \{[a : b : c] \in \mathbb{P}^2(F) : c = 0\},$$

heißt Ferngerade.

1.4.4 Definition (Tangenten)**.** *Sei $C_g(F)$ eine projektive Kurve. Weiterhin sei $P = [a : b : c] \in C_g(F)$ ein nicht-singulärer Punkt. Dann nennen wir die projektive Gerade*

$$L(\alpha, \beta, \gamma) := L\left(\nabla g(a, b, c)\right)$$

Tangente in P an $C_g(F)$.

Aus der Nicht-Singularität von P folgt sofort $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ und somit ist L wirklich eine projektive Gerade. Weiterhin hängt L nicht von der Wahl des Repräsentanten (a, b, c) ab. Auch liegt der Punkt P wirklich auf der Tangente,

wie man mit

$$\begin{aligned}
& a \cdot \frac{\partial g}{\partial X}(a,b,c) + b \cdot \frac{\partial g}{\partial Y}(a,b,c) + c \cdot \frac{\partial g}{\partial Z}(a,b,c) \\
= \; & a \cdot \sum_{i>0, j\geq 0} i \; \alpha_{i,j} \; a^{i-1} b^j c^{d-i-j} + b \cdot \sum_{i\geq 0, j>0} j \; \alpha_{i,j} \; a^i b^{j-1} c^{d-i-j} + \\
& c \cdot \sum_{i,j\geq 0, \; i+j<d} (d-i-j) \; \alpha_{i,j} \; a^i b^j c^{d-i-j-1} \\
= \; & i \cdot \sum_{i,j\geq 0} \alpha_{i,j} \; a^i b^j c^{d-i-j} + j \cdot \sum_{i,j\geq 0} \alpha_{i,j} \; a^i b^j c^{d-i-j} + \\
& (d-i-j) \cdot \sum_{i,j\geq 0} \alpha_{i,j} \; a^i b^j c^{d-i-j} \\
= \; & (i+j+(d-i-j)) \cdot g(a,b,c) \\
= \; & 0
\end{aligned}$$

sieht.

1.4.5 Definition (Vielfachheit)**.** *Sei $L(\alpha,\beta,\gamma)$ eine projektive Gerade, $C_g(F)$ eine projektive ebene Kurve und $P = [a : b : c] \in L(\alpha,\beta,\gamma)$. Sei weiterhin $P' = [a' : b' : c']$ ein weiterer beliebiger Punkt auf der Geraden. Dann ist*

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

ein Polynom in t und wir definieren die Vielfacheit, mit der sich die Gerade und die projektive Kurve in P schneiden mit

$$m(P, L(\alpha,\beta,\gamma), C_g(F)) := \text{ Nullstellenordnung von } \psi \text{ in } 0 \; .$$

Falls P nicht auf der Geraden liegt, so definieren wir die Vielfachheit als 0.

Es gilt

$$\psi(0) \neq 0 \;\Leftrightarrow\; g(a+0a', b+0b', c+0c') = g(a,b,c) \neq 0 \;\Leftrightarrow\; [a:b:c] \notin C_g(F).$$

Da die Nullstellenordnung einer Nicht-Nullstelle als 0 definiert ist, gilt also insgesamt, dass die Vielfachheit genau dann nicht Null ist, wenn der Punkt P sowohl auf der Gerade als auch auf der projektiven ebenen Kurve liegt. Es gilt noch zu bemerken, dass die Nullstellenordnung von ψ in 0 nicht von der Wahl des Punktes P' abhängt. Dies lässt sich einsehen, wenn man mit der Kettenregel die Ableitungen von ψ bestimmt. Ob diese Ableitungen in 0 verschwinden oder nicht, hängt weder von dem konkreten Punkt $[a' : b' : c']$ noch von der Wahl seines Repräsentanten ab. Die Nullstellenordnung eines Polynoms p in 0 ist gleich k genau dann, wenn

$$p(0) = 0, p'(0) = 0, \ldots, p^{(k)}(0) = 0, p^{(k+1)}(0) \neq 0$$

gilt.

1.4.6 Lemma. *Seien eine projektive Kurve $C_g(F)$, ein Punkt $P \in C_g(F)$ und die Tangente $L(\alpha,\beta,\gamma)$ in P an $C_g(F)$ gegeben. Dann ist*

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

Eine Tangente schneidet sich mit der zugehörigen projektiven Kurve im Berührungspunkt also immer mit einer Vielfachheit von mindestens 2.

Beweis. Da $P \in L \cap C_g(F)$ liegt, ist auf jeden Fall $\psi(0) = 0$. Mit der Kettenregel lässt sich berechnen, dass

$$\psi'(0) = \frac{\partial g}{\partial X}(a,b,c) \cdot a' + \frac{\partial g}{\partial Y}(a,b,c) \cdot b' + \frac{\partial g}{\partial Z}(a,b,c) \cdot c' = \alpha a' + \beta b' + \gamma c' = 0$$

ist, denn P' liegt auf der Tangente L. Da die nullte und erste Ableitung von ψ in 0 verschwinden, wissen wir, dass die Nullstellenordnung von ψ in 0 echt größer als 1 sein muss.

□

2 Elliptische Kurven

Nun haben wir alle nötigen Kenntisse die zur Einführung von elliptischen Kurven nötig sind. Im Wesentlichen handelt es sich bei elliptischen Kurven um eine spezielle Klasse von projektiven ebenen Kurven.

2.1 Einführung

2.1.1 Definition (Elliptische Kurven)**.** *Eine elliptische Kurve ist eine nichtsinguläre projektive ebene Kurve $C_g(F)$, wobei g ein Polynom der Form*

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

ist.

Also ist g homogen vom Grad 3 und enthält nur ganz bestimmte Summanden. Wir werden elliptische Kurven meistens auch einfach $E_g(F)$ nennen. Die Punkte der elliptischen Kurve sind gerade die Lösungen von $g(X,Y,Z) = 0$ oder anders geschrieben von der Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1}$$

welche auch (projektive) Weierstraßgleichung genannt wird. Die zugehörige affine Weierstraßgleichung hat die Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

Einer elliptischen Kurve wird also immer ein Polynom der Form

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

zugrunde liegen. Falls wir die elliptische Kurve über der affinen Ebene betrachten, so ist das zugehörige Polynom von der Form

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6. \tag{4}$$

Die Nummerierung der a_i hat historische Gründe. Nun stellt sich die Frage: Welche Punkte von $E_g(F)$ sind affin und welche nicht?

2.1.2 Lemma. *Seien f, g wie in den Gleichungen 3 und 4. Dann gilt*

$$C_g(F) = i(C_f(F)) \cup [0:1:0].$$

Beweis. Nach Lemma 1.3.9 wissen wir schon, dass die affinen Punkte in $C_g(F)$ den Punkten in $C_f(F)$ entsprechen. Sei nun ein Fernpunkt $P = [a : b : 0] \in C_g(F)$ gegeben. Dann folgt nach einsetzen in die Weierstraßgleichung, dass $a = 0$ ist und b beliebig sein kann. Also ist $P = [0 : 1 : 0]$. □

Diesen einzigen Fernpunkt nennen wir O und sagen von ihm, dass er im Unendlichen liegt.

2.1.3 Lemma (Singularität von projektiven ebenen Kurven über der Weierstraßgleichung)**.** *Seien f, g wie in den Gleichungen 3 und 4. Dann ist g singulär genau dann, wenn f singulär ist.*

Beweis. Wir wissen schon, dass $C_g(F) = i(C_f(F)) \cup O$ ist. Das bleibt auch so beim Übergang zum algebraischen Abschluss. Im Fernpunkt O ist $C_g(F)$ nie singulär, denn es gilt

$$\frac{\partial g}{\partial Z}(0, 1, 0) = 1$$

für jedes beliebige Weierstraßpolynom g. Die affinen Punkte sind nach Lemma 1.3.11 genau dann singulär, wenn die affine ebene Kurve $C_f(F)$ im zugehörigen Punkt in der affinen Ebene singulär ist. □

2.2 Spezielle elliptische Kurven

Die unhandliche Form der Weierstraßgleichung lässt sich in einigen Fällen vereinfachen. Wichtig ist hier vor allem die Charakteristik des Grundkörpers F. Im Rahmen dieser Arbeit werden wir nur den Fall $\mathrm{char}(F) > 3$ betrachten.

2.2.1 Satz (Transformation projektiver ebener Kurven)**.** *Seien g ein homogenes Polynom vom Grad n, $C_g(F)$ eine projektive ebene Kurve, $A \in F^{n \times n}$ eine invertierbare Matrix und $\vec{x} \in F^n$ ein Vektor. Mit der Definition*

$$g_A(\vec{x}) := g(\vec{x} \cdot A)$$

gilt dann:

1. $C_g(F) \cdot A^{-1} = C_{g_A}(F)$
2. *$C_g(F)$ ist singulär genau dann, wenn $C_{g_A}(F)$ singulär ist.*

Beweis.

1. Es gilt $\vec{x} \in C_g(F) \Leftrightarrow g(\vec{x}) = 0 \Leftrightarrow g(\vec{x}A^{-1}A) = 0 \Leftrightarrow g_A(\vec{x}A^{-1}) = 0 \Leftrightarrow \vec{x}A^{-1} \in C_{g_A}(F)$.

2. Wir zeigen zuerst mit komponentenweisem Vergleichen, dass

$$\nabla(g_A)(\vec{x}) = (\nabla g)(\vec{x}A) \cdot A$$

gilt. Seien mit a_{ij} die Einträge von A und mit A_j die Spalten von A bezeichnet. Dann gilt für die jeweils j-te Koordinate der linken bzw. rechten Seite mit Kettenregel

$$\frac{\partial g(\vec{x}A)}{\partial x_j}(\vec{x}) = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}(\vec{x}A) \cdot \frac{\partial \vec{x}A_i}{\partial x_j}(\vec{x}) = \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}(\vec{x}A) \cdot a_{ji}.$$

Damit ist ein Punkt $\vec{x_0} \in \mathbb{P}^2(F)$ singulär in $C_g(\overline{F})$ genau dann, wenn $\vec{x_0}A^{-1}$ singulär ist in $C_{g_A}(\overline{F})$. □

2.2.2 Satz (Vereinfachung der Weierstraßgleichung I)**.** *Sei also $C_g(F)$ eine elliptische Kurve und* $\mathrm{char}(F) \neq 2$*. Dann ist die Abbildung*

$$\Phi : \mathbb{P}^2(F) \to \mathbb{P}^2(F) : [r : s : t] \mapsto [r : s + \frac{a_1}{2}r + \frac{a_3}{2}t : t]$$

bijektiv und

$$\Phi(C_g(F)) := C_{h_1}(F)$$

mit

$$h_1(X, Y, Z) = Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3,$$

wobei

$$b_2 = a_1^2 + 4a_2 \quad b_4 = 2a_4 + a_1a_3 \quad b_6 = a_3^2 + 4a_6$$

ist. In diesem Fall ist auch $C_{h_1}(F)$ eine elliptische Kurve.

Beweis. Die Abbildung Φ ist sinnvoll, da wir $\mathrm{char}(F) \neq 2$ vorausgesetzt haben. Φ ist auch bijektiv, da die zugehörige Abbildungsmatrix

$$A = \begin{pmatrix} 1 & a_1/2 & 0 \\ 0 & 1 & 0 \\ 0 & a_3/2 & 1 \end{pmatrix}$$

invertierbar ist. Weiterhin gilt

$$\begin{aligned}
& g(X, Y - \frac{a_1}{2}X - \frac{a_3}{2}Z, Z) \\
= \; & \left(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z\right)^2 Z + a_1X(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z)Z \\
& + a_3\left(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z\right)Z^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\
= \; & \left[Y^2 - 2Y\left(\frac{a_1}{2}X + \frac{a_3}{2}Z\right) + \left(\frac{a_1^2}{4}X^2 + 2\frac{a_1a_3}{4}XZ + \frac{a_3^2}{4}Z^2\right)\right]Z \\
& + a_1XYZ - \frac{a_1^2}{2}X^2Z - \frac{a_1a_3}{2}XZ^2 + a_3YZ^2 - \frac{a_1a_3}{2}XZ^2 - \frac{a_3^2}{2}Z^3 \\
& - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\
= \; & Y^2Z - X^3 + \left(-\frac{a_1^2}{4} - a_2\right)X^2Z + \left(-\frac{a_1a_3}{2} - a_4\right)XZ^2 + \left(-\frac{a_3^2}{4} - a_6\right)Z^3 \\
= \; & Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3 \\
= \; & h_1(X, Y, Z).
\end{aligned}$$

Es gilt also (falls man mit Φ auch die Abbildung bezeichnet, die analog von F^3 nach F^3 abbildet)

$$h_1(r, s, t) = g(\Phi^{-1}(r, s, t)),$$

woraus folgt, dass g verschwindet genau dann, wenn $h_1 \circ \Phi$ verschwindet. Also ist

$$\Phi(C_g(F)) = C_{g_{A^{-1}}}(F) = C_{h_1}(F).$$

Die Nicht-Singularität folgt sofort mit Satz 2.2.1 und somit ist $C_h(F)$ eine elliptische Kurve. □

2.2.3 Satz (Vereinfachung der Weierstraßgleichung II)**.** *Sei also $C_{h_1}(F)$ eine elliptische Kurve mit Darstellung entsprechend dem vorangegangenen Satz und* $\operatorname{char}(F) > 3$*. Dann ist die Abbildung*

$$\varphi : \mathbb{P}^2(F) \to \mathbb{P}^2(F) : [r : s : t] \mapsto [36r + 3b_2t : 216s : t]$$

bijektiv und

$$\varphi(C_{h_1}(F)) := C_{h_2}(F)$$

mit

$$h_2(X, Y, Z) = Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3,$$

wobei

$$c_4 = b_2^2 - 24b_4 \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

ist. In diesem Fall ist auch $C_{h_2}(F)$ eine elliptische Kurve.

Beweis. Wieder ist die zugehörige Abbildungsmatrix

$$A = \begin{pmatrix} 36 & 0 & 0 \\ 0 & 216 & 0 \\ 3b_2 & 0 & 1 \end{pmatrix}$$

invertierbar. Da $12 = 2^2 3$, $36 = 2^2 3^3$ und $216 = 2^3 3^3$ ist, sorgt die Voraussetzung $\operatorname{char}(F) > 3$ dafür, dass hier keine Probleme entstehen. Durch Nachrechnen erhalten wir

$$h_2(X, Y, Z) = 2^6 3^6 h_1\left(\frac{1}{36}X - \frac{b_2}{12}Z, \frac{1}{216}Y, Z\right),$$

woraus wieder direkt folgt, dass h_1 verschwindet genau dann, wenn $h_2 \circ \varphi$ verschwindet. Also ist

$$\varphi(C_{h_1}(F)) = C_{h_{1_{A^{-1}}}}(F) = C_{h_2}(F)$$

und die Nicht-Singularität folgt wieder mit Satz 2.2.1. □

Bemerkung. Von nun an wollen wir immer annehmen, dass $\operatorname{char}(F) > 3$ ist. Dann können wir jede beliebige elliptische Kurve $E_g(F)$ durch Anwenden der Abbildung $\Phi \circ \varphi$ vereinfachen. Wir können also immer annehmen, dass einer elliptische Kurve $E_g(F)$ die vereinfachte Weierstraßgleichung

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

zugrunde liegt, die eindeutig durch die beiden Parameter a und b bestimmt ist.

2.3 Diskriminante elliptischer Kurven

2.3.1 Definition (Diskriminante von projektiven ebenen Kurven über einem Weierstraßpolynom)**.** *Für das allgemeine Weierstraßpolynom*

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

nennen wir die Zahl

$$\Delta = -b_2^2b_8 - 8b - 4^3 - 27b_6^2 + 9b_2b_4b_6$$

mit Koeffizienten

$$b_2 = a_1^2 + 4a_2 \qquad b_4 = 2a_4 + a_1a_3 \qquad b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

Diskriminante von $C_g(F)$.

Da wir $\text{char}(F) > 3$ annehmen, können wir auch annehmen, dass g von der Form

$$g(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$$

ist. Somit ist die Diskriminante gleich

$$\Delta = 4a^3 + 27b^2.$$

2.3.2 Satz (Kriterium für Singularität von elliptischen Kurven)**.** *Sei* $\text{char}(F) > 3$ *und* $E_g(F)$ *eine elliptische Kurve mit*

$$g(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3.$$

Dann ist $E_g(F)$ *singulär genau dann, wenn die Diskriminante verschwindet.*

Beweis. Nach Lemma 2.1.3 wissen wir schon, dass $E_g(F)$ nicht-singulär ist genau dann, wenn die zugeordnete affine ebene Kurve $C_f(F)$ mit

$$f(x, y) = y^2 - x^3 - ax - b$$

nicht-singulär ist. Per Definition ist $C_f(F)$ singulär, falls ein Punkt $(r, s) \in \overline{F}$ existiert mit

$$\begin{aligned} f(r, s) &= s^2 - r^3 - ar - b = 0 \\ \frac{\partial f}{\partial x}(r, s) &= -3r^2 - a = 0 \\ \frac{\partial f}{\partial y}(r, s) &= 2s = 0. \end{aligned}$$

Sei nun σ definiert als ein Polynom mit

$$\sigma(x) := f(x, 0).$$

Dann ist $C_f(F)$ singulär genau dann, wenn ein $r \in \overline{F}$ existiert mit

$$\sigma(r) = \frac{d\sigma}{dx}(r) = 0.$$

Das Polynom σ zerfällt definitionsgemäß über dem algebraischen Abschluss $\overline{F}$ in Linearfaktoren

$$\sigma(x) = (x - n_1)(x - n_2)(x - n_3)$$

mit Nullstellen $n_i \in \overline{F}$. Für die drei Fälle, in denen σ verschwindet, nimmt die Ableitung von σ folgende Werte an:

$$\begin{aligned}\frac{d\sigma}{dx}(n_1) &= -(n_1-n_2)(n_1-n_3)\\ \frac{d\sigma}{dx}(n_2) &= -(n_2-n_1)(n_2-n_3)\\ \frac{d\sigma}{dx}(n_3) &= -(n_3-n_1)(n_3-n_2)\end{aligned}$$

Die Ableitung von f verschwindet also genau dann gleichzeitig mit f, falls σ über $\overline{F}$ eine doppelte Nullstelle besitzt. Nach Satz 1.1.4 ist dies genau dann der Fall, falls die Diskriminante verschwindet. Mit Satz 1.1.5 lässt sich die Diskriminante von σ bestimmen als

$$D(\sigma) = 4a^3 + 27b^2 = \Delta.$$

Damit ist die Behauptung gezeigt. □

3 Gruppenstruktur auf elliptischen Kurven

3.1 Summe aller Vielfachheiten

3.1.1 Satz (Summe aller Vielfachheiten)**.** *Sei L eine projektive Gerade und $E_g(F)$ eine elliptische Kurve. Dann gilt*

$$\sum_{P\in\mathbb{P}^2(F)} m(P, L, E_g(F)) \in \{0,1,3\}.$$

Beweis. Wir haben schon gesehen, dass die Vielfachheit gleich Null ist, falls P nicht in $L \cap E_g(F)$ liegt. Zu betrachten sind also nur die Fälle, die in diesem Schnitt liegen.

Fall 1: $L = L(0,0,1)$: Dann gilt

$$L = \{[a:b:c] \in \mathbb{P}^2(F) : c = 0\} = \mathbb{P}^2(F) \setminus i(\mathbb{A}^2(F)).$$

Aus Lemma 2.1.2 wissen wir, dass der Schnitt nur aus dem Punkt $[0:1:0]$ besteht. Nehmen wir uns als Hilfspunkt $P' = [1:1:0]$, so gilt

$$\psi(t) = g(0+t1, 1+t1, 0+t0) = g(t, 1+t, 0) = -t^3,$$

womit die Nullstellenordnung in 0 und somit auch die Summe aller Vielfachheiten 3 ist.

Fall 2: $L = L(1,0,\gamma)$: Sei $P = [a:b:c] \in L$. Dann gilt $a = -\gamma c$.

Fall $c = 0$: Dann muss $P = [0:1:0]$ sein und P liegt auch in der elliptischen Kurve $E_g(F)$. Die Vielfachheit lässt sich mit dem Hilfspunkt $P' = [-\gamma:0:1]$ berechnen als die Nullstellenordnung in 0 von

$$\begin{aligned}\psi(t) &= g(0-t\gamma, 1+t0, 0+t) = g(-\gamma t, 1, t)\\ &= t - a_1\gamma t^2 + a_3 t^2 - \gamma^3 t^3 - a_2\gamma^2 t^3 + a_4\gamma t^3 - a_6 t^3\\ &= \left[1 + (-a_1\gamma + a_3)t + (\gamma^3 + a_2\gamma^2 + a_4\gamma - a_6)t^2\right] t.\end{aligned}$$

Damit ist die Nullstellenordnung von ψ in 0 gleich 1 und somit auch die Summe aller Vielfachheiten.

Fall $c \neq 0$: Dann muss $P = [-\frac{\gamma}{\alpha} : b_0 : 1]$ sein und dieser liegt offensichtlich genau dann in der elliptischen Kurve, falls b_0 Nullstelle des Polynoms

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

ist. Nehmen wir den Punkt $P' = [0 : 1 : 0]$ zur Hilfe, so ergibt sich, dass die Vielfachheit gerade der Nullstellenordnung der Nullstelle 0 des Polynoms

$$\psi(t) := g(-\frac{\gamma}{\alpha} + t0, b_0 + t1, 1 + t0) = g(-\frac{\gamma}{\alpha}, b_0 + t, 1) = h(b_0 + t)$$

entspricht. Sei nun k die Ordnung der Nullstelle b_0 von h. Dann können wir h schreiben als

$$h(b) = (b - b_0)^k \cdot h^*(b),$$

wobei h^* nicht mehr b_0 als Nullstelle besitzt. Dies gibt uns eine Darstellung von ψ folgender Form

$$\psi(t) = h(b_0 + t) = (b_0 + t - b_0)^k \cdot h^*(b_0 + t) = t^k \cdot h^*(b_0 + t).$$

Mit dieser Darstellung können wir die Nullstellenordnung von ψ in 0 direkt bestimmen als k. Insbesondere ist die Nullstellenordnung ψ in 0 gleich der Nullstellenordnung von h in b_0.

Für h lässt sich nun leicht ausrechnen

$$h(b) = g(-\frac{\gamma}{\alpha}, b, 1) = b^2 + r(b),$$

wobei r vom Grad eins ist. Demnach ist h ein quadratisches Polynom womit die Summe aller Nullstellenordnungen von h gleich 0 oder 2 ist. Damit ist die Summe aller Vielfachheiten 1 oder 3, womit auch in diesem Fall die Behauptung erfüllt wäre.

Fall 3: $L = L(\alpha, 1, \gamma)$: Der Punkt $[0 : 1 : 0]$ kann hier nicht auf der Gerade liegen, womit $L \cap E_g(F) \subset i(\mathbb{A}^2(F))$ gilt. Sei $P = [a_0 : b_0 : 1]$. Dann liegt $P \in L$ genau dann, wenn

$$[a_0 : b_0 : 1] \in L \;\Leftrightarrow\; \alpha a_0 + \beta b_0 + \gamma = 0 \;\Leftrightarrow\; b_0 = -\frac{\gamma}{\beta} - \frac{\alpha}{\beta} a_0.$$

Damit P auch noch in $E_g(F)$ liegt, muss zusätzlich gelten, dass a_0 Nullstelle des Polynoms

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

ist. Nehmen wir $P' = [-\beta : \alpha : 0] \in L$ als Hilfspunkt, so lässt sich die Vielfachheit berechnen als die Nullstellenordnung in 0 von

$$\begin{aligned} \psi(t) &:= g(a_0 - t\beta, b_0 + t\alpha, 1 + t0) \\ &= g(a_0 - t\beta, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}(a_0 - t\beta), 1) \\ &= h(a_0 - t\beta). \end{aligned}$$

Analog zum vorangegangenen Fall folgt wieder, dass die Summe aller Vielfachheiten der Anzahl der Nullstellen mit Vielfachheit von h in F entspricht. Für h lässt sich berechnen

$$\begin{aligned} & g(a, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x, 1) \\ = & \left(-\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x\right)^2 + a_1 x\left(-\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x\right) + a_3\left(-\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x\right) - x^3 - a_2x^2 - a_4x - a_6 \\ = & -x^3 + r(x), \end{aligned}$$

wobei r vom Grad 2 ist. Also ist h eine Polynom vom Grad 3 mit Leitkoeffizient -1. Daher zerfällt h über dem algebraischen Abschluss $\overline{F}$ zu

$$\begin{aligned} h(a) &= -(a-a_1)(a-a_2)(a-a_3) \\ &= -(a^3 - a_1a^2 - a_2a^2 + a_1a_2a + a_3a^2 + a_1a_3a + a_2a_3a - a_1a_2a_3) \\ &= -a^3 + (a_1+a_2+a_3)a^2 - (a_1a_2 + a_2a_3 + a_3a_1)a + a_1a_2a_3 \end{aligned}$$

für gewisse $a_i \in \overline{F}$, die nicht notwendigerweise verschieden sein müssen. Die Summe aller Nullstellenordnungen von h ist also die Anzahl der a_i, die in F liegen. Diese muss also kleiner oder gleich 3 sein. Weiterhin muss $a_1 + a_2 + a_3$ in F liegen, da h ein Polynom über F ist. Also sind auch insbesondere seine Koeffizienten aus F. Daher kann die Summe aller Nullstellenordnungen nicht 2 sein, denn mit je zwei $a_i \in F$ würde auch das dritte a_i in F liegen. □

3.1.2 Korollar. *Sei $E_g(F)$ eine elliptische Kurve. Dann gilt:*

1. *Seien $P, Q \in E_g(F)$ zwei verschiedene Punkte und sei L die projektive Gerade, die beide verbindet. Dann liegt auf L noch ein dritter (mit Vielfachheiten gezählt) Punkt aus $E_g(F)$.*

2. *Sei $P \in E_g(F)$ und L die Tangente in P an $E_g(F)$. Dann liegt auf L noch ein dritter (mit Vielfachheiten gezählt) Punkt aus $E_g(F)$.*

Beweis. In beiden Fällen ist die Summe aller Vielfachheiten nach Voraussetzung schon größer gleich 2. Im ersten Fall haben wir zwei verschiedene Punkte P und Q mit Vielfachheit größer oder gleich 1 und im zweiten Fall haben wir einen Punkt P mit Vielfachheit größer oder gleich 2. Da nach Satz 3.1.1 die Summe aller Vielfachheiten nur 0, 1 oder 3 sein kann, muss sie also gleich 3 sein und somit gibt es auch einen dritten Punkt in $L \cap E_g(F)$, der jedoch nicht unbedingt verschieden von P, Q bzw. P sein muss. □

Betrachtung (Elliptische Kurven über $\mathbb{R}$)**.** Betrachten wir nun elliptische Kurven $E(\mathbb{R})$ über dem Grundkörper $\mathbb{R}$ und schneiden diese mit dem affinen Raum. D.h. wir ignorieren den Punkt $O = [0:1:0]$ und betrachten nur die Lösungsmenge der zugeordneten affinen Weierstraßgleichung

$$y^2 = x^3 + ax + b.$$

Dann zeigt uns Abbildung 1, welche typischen Formen $E_g(F)$ annehmen kann. Natürlich können wir in eine Abbildung über dem affinen Raum den Punkt O nicht einzeichnen. Es lässt sich jedoch Folgendes leicht einsehen:

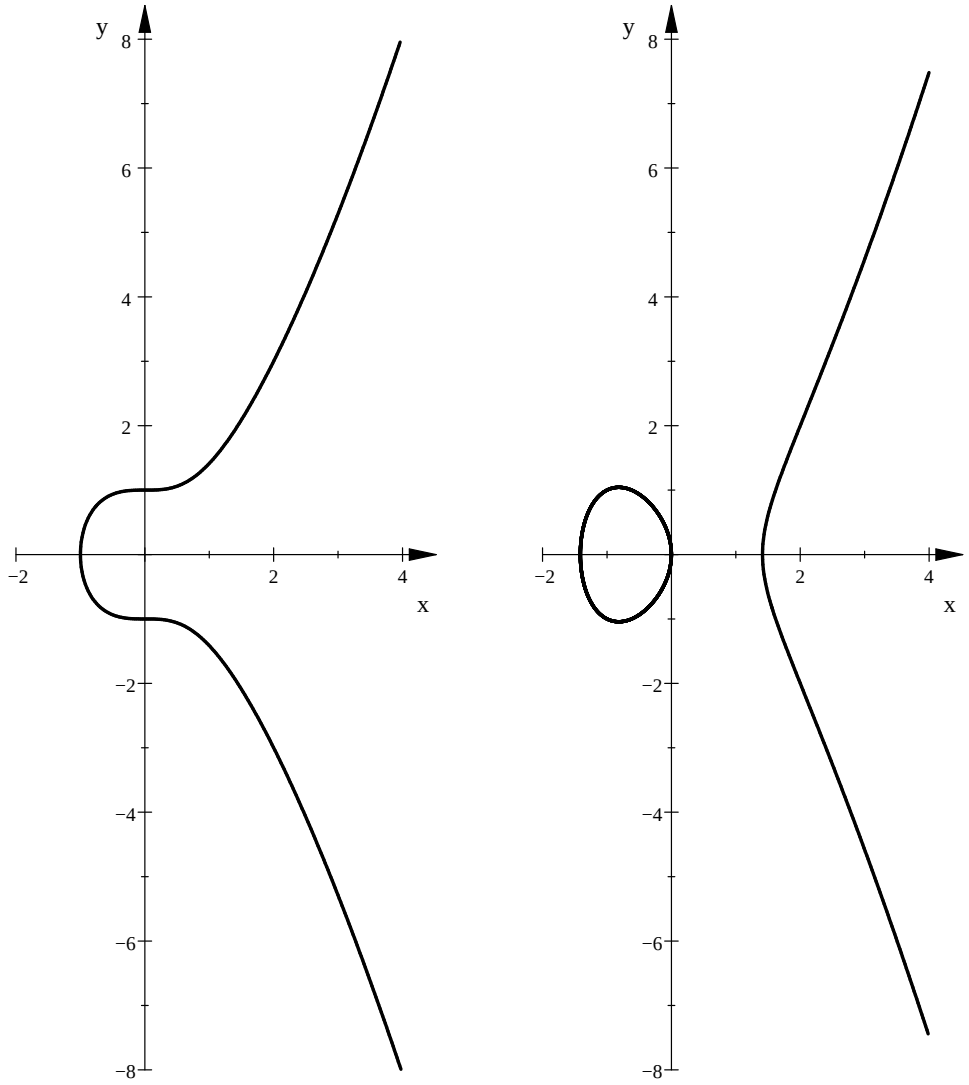

Abbildung 1: $E_f(\mathbb{R})$ für $f(x,y) = y^2 - x^3 - 1$ bzw. $f(x,y) = y^2 - x^3 + 2x$

Sei $(a,b) \in \mathbb{A}^2(F)$ ein beliebiger Punkt des affinen Raums. Dann ist $P := i(a,b) = [a:b:1] \in \mathbb{P}^2(F)$ und wir können die projektive Gerade L bestimmen, die P und $O = [0:1:0]$ verbindet. Gesucht sind die Koeffizienten α, β, γ von L, so dass folgendes lineares Gleichungssystem

$$\begin{pmatrix} a & b & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

erfüllt ist. Es ist $\beta = 0$ und $\gamma = -\alpha a$. Wir erhalten damit die projektive Gerade

$$L_0 := L(\alpha, 0, -\alpha a) = L(1, 0, -a).$$

Auf dieser Gerade liegen alle Punkte, die die Gleichung $X - aZ = 0$ erfüllen. Das ist die Menge

$$\{[a:t:1] : t \in F\} \cup [0:1:0].$$

Im affinen Raum ist die Verbindungsgerade zwischen $(a,b) \in \mathbb{A}^2(F)$ und $O \in \mathbb{P}^2(F)$ die Senkrechte zur y-Achse, die durch (a,b) verläuft. Wollte man versuchen,

den Punkt im Unendlichen in den affinen Raum einzuzeichnen, so könnte man das Gitter so verzerren, dass alle Parallelen zur y-Achse sich im Unendlichen im Punkt O treffen, wie in Abbildung 2 zu sehen. Jedoch sollte nicht vergessen

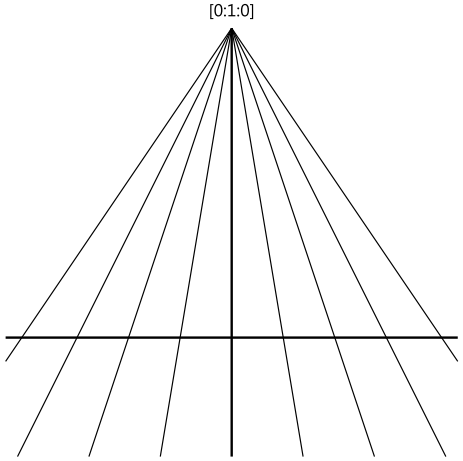

Abbildung 2: Darstellung des Punktes $[0 : 1 : 0]$ im affinen Raum

werden, dass $[0 : 1 : 0]$ nicht zum affinen Raum gehört.

3.2 Gruppenstruktur

3.2.1 Definition (Addition auf elliptischen Kurven)**.** *Sei $E_g(F)$ eine elliptische Kurve und $P, Q \in E_g(F)$ zwei verschiedene Punkte auf dieser Kurve. Sei L_1 die projektive Gerade, die P und Q verbindet. Dann definieren wir $P * Q$ als den dritten Punkt in $L_1 \cap E_g(F)$. Sei nun L_2 die projektive Gerade, die $P * Q$ und $O = [0 : 1 : 0]$ verbindet. Dann definieren wir $P \oplus Q$ als den dritten Punkt in $L_2 \cap E_g(F)$. In Abbildung 3 ist dieses konstruktive Verfahren beispielhaft (im affinen Raum und über dem Grundkörper $\mathbb{R}$) dargestellt.*

Sollte es der Fall sein, dass wir mit L_1 oder L_2 zweimal denselben Punkt verbinden müssen, falls also $P = Q$ oder $P * Q = O$ ist, so wählen wir als „Verbindungsgerade“ die Tangente.

Der zweite Konstruktionsschritt liefert uns auch direkt den Begriff eines Inversens. Daher definieren wir auch gleich $\ominus P$ als den dritten Punkt der Verbindungsgeraden von P und O. Somit lässt sich $P * Q$ auch schreiben als $\ominus(P \oplus Q)$. Der Beweis, dass $(\ominus P) \oplus P = O$ wirklich gilt, wird im nächsten Satz nachgeliefert. Falls P im affinen Raum liegt, gehen P und $\ominus P$ durch Spieglung an der x-Achse auseinander hervor.

Dass es immer einen dritten (mit Vielfachheiten gezählt) Schnittpunkt gibt, sichert uns das Korollar 3.1.2.

An diesem Punkt haben wir schlussendlich alle notwendigen Vorbereitungen getroffen, um einen Satz zu formulieren, der für die kryptographische Verwendung von elliptischen Kurven grundlegend ist. Wir können nun auf elliptischen Kurven eine Gruppenstruktur definieren. Der Satz dazu lautet wie folgt:

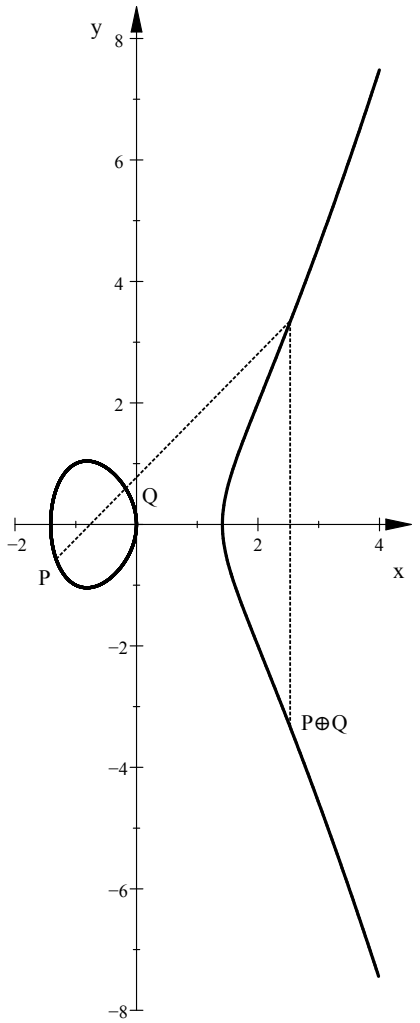

Abbildung 3: Addition zweier verschiedener Punkte auf elliptischen Kurven

3.2.2 Satz (Gruppenstruktur auf elliptischen Kurven)**.** *Sei F ein Körper und $E_g(F) = C_g(F)$ eine elliptische Kurve mit*

$$g(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3.$$

Dann macht die in Definition 3.2.1 definierte Verknüpfung

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

die Menge $E_g(F)$ zu einer Gruppe $(E_g(F), \oplus)$.

Beweis. Zu zeigen sind die Kommutativität, die Existenz eines neutralen Elements, die Existenz von inversen Elementen und die Assoziativität:

1. Dass $\oplus$ eine kommutative Verknüpfung ist, folgt direkt aus der Definition, denn die Gerade L_1 ist unabhängig von der Reihenfolge der Punkte, durch die sie läuft.

2. Sei $P \in E_g(F)$. Bei der Berechnung von $P \oplus O$ gibt es zwei Fälle:

Fall 1: $P = O$: In diesem Fall ist $O \oplus O$ gesucht. Wir wissen schon, dass die Vielfachheit von O bzgl. seiner Tangenten $L_1 = L(0, 0, 1)$ drei ist. Daher hat L_1 als dritten Schnittpunkt wieder O, so dass $O * O = O$ ist. Analog hat auch die Tangente L_2 im Punkt O als dritten Schnittpunkt O, so dass $O \oplus O = O$ gilt.

Fall 2: $P \neq O$: Nun ist L_1 die Gerade, die P und O verbindet und als dritten Punkt $P * O$ hat. L_2 ist die Gerade, die $P * O$ und O verbindet. Sie ist also nach Lemma 1.4.2 mit L_1 identisch und hat somit als dritten Punkt P. Damit gilt $P \oplus O = P$.

Da $\oplus$ kommutativ ist, gilt also auch $O \oplus P = P$ und somit haben wir das neutrale Element, nämlich $O = [0 : 1 : 0]$, gefunden.

3. Sei $P \in E_g(F)$. Wir haben $\ominus P$ als den dritten Schnittpunkt der Verbindungsgeraden L_0 von P und O definiert. Offensichtlich gilt $P \oplus (\ominus P) = O$, denn die Gerade L_1 hat als dritten Punkt $O = P * (\ominus P)$. Dann ist L_2 wieder die Tangente in O und hat somit als dritten Punkt auch wieder O.

4. Der Beweis der Assoziativität auf elementarem Weg bedarf der Unterscheidung vieler Spezialfälle. Wir nehmen daher an, dass $O, P, Q, R, P * Q, Q * R, P \oplus Q, Q \oplus R, P * (Q \oplus R), (P \oplus Q) * R$ paarweise verschieden sind und ignorieren im Rahmen dieser Arbeit die Sonderfälle. Dann lässt sich die Frage nach der Assoziativität wie in Abbildung 4 darstellen.

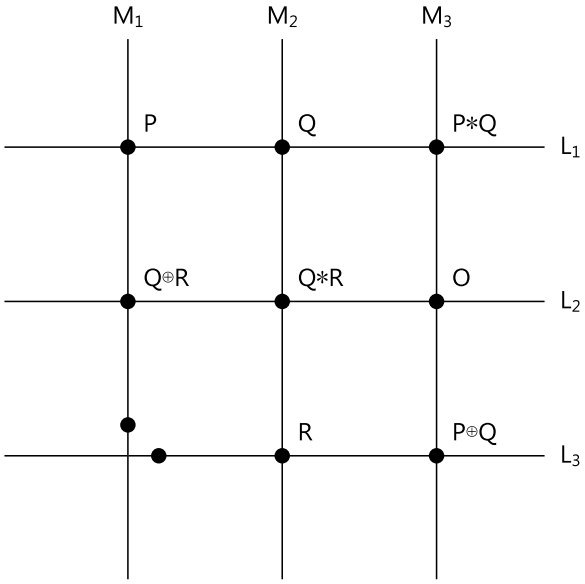

Abbildung 4: Assoziativitätsraster

Es seien $l_1, l_2, l_3, m_1, m_2, m_3$ die homogenen Polynome vom Grad 1, die die projektiven Geraden $L_1, L_2, L_3, M_1, M_2, M_3$ erzeugen. Die beiden Punkte unten links entsprechen $P * (Q \oplus R)$ und $(P \oplus Q) * R$. Es genügt offensichtlich zu zeigen, dass diese beiden Punkte identisch sind. Dafür reicht es zu zeigen, dass der Schnittpunkt T von M_1 und L_3 in $E_g(F)$ liegt, denn nach Satz 3.1.1 gilt für die Summe der Vielfachheiten

$$m(P \oplus Q, L_3, E_g(F)) + m(R, L_3, E_g(F)) + m((P \oplus Q) * R, L_3, E_g(F)) = 3,$$

$$m(P, M_1, E_g(F)) + m(Q \oplus R, M_1, E_g(F)) + m(P * (Q \oplus R), M_1, E_g(F)) = 3.$$

Da aus $T \in E_g(F)$ folgt, dass $m(T, M_1, E_g(F)) > 0$ und $m(T, L_3, E_g(F)) > 0$ ist, muss in diesem Fall T einer von den jeweils drei Punkten sein, woraus direkt

$$(P \oplus Q) * R = T = P * (Q \oplus R)$$

folgt. Sei nun also T der Schittpunkt von M_1 und L_3 und V der F-Vektorraum der homogenen Polynome $p \in F[X, Y, Z]$ vom Grad 3. Dieser hat die Dimension 10 über F, da die Monome

$$X^3, X^2Y, X^2Z, XY^2, XYZ, XZ^2, Y^3, Y^2Z, YZ^2, Z^3$$

eine Basis bilden. Wir definieren V' als den Untervektorraum von V, der nur die Polynome enthält, die in allen acht Punkten $O, P, Q, R, P \oplus Q, Q \oplus R, (P \oplus Q) * R, P * (Q \oplus R)$ verschwinden. Damit liegt insbesondere das Polynom g, das unsere elliptische Kurve erzeugt, in V'. Weiter definieren wir für jeden Punkt $S \in \mathbb{P}^2(F)$ den Untervektorraum V_S, der nur die Polynome enthält, die in S verschwinden.

Für einen Punkt $S \in \mathbb{P}^2(F)$ definieren wir nun eine lineare Abbildung ψ_S wie folgt

$$\psi_S : V \to F : p \mapsto p(S).$$

Mit dieser Abbildung ist $p(S) = 0$ äquivalent dazu, dass p im Kern der linearen Abbildung ψ_S liegt. Nach Dimensionsformel hat damit $V_S = \ker(\psi_S)$ die Dimension 9, woraus auch folgt, dass

$$V' = V_O \cap V_P \cap V_Q \cap V_R \cap V_{P \oplus Q} \cap V_{Q \oplus R} \cap (P \oplus Q) * R \cap V_{P * (Q \oplus R)}$$

die Dimension 2 oder größer hat.

Sei nun S der Schnittpunkt von L_1 und L_2. Dieser existiert nach Lemma 1.4.2 und ist nach unseren Annahmen verschieden von allen in Abbildung 4 eingezeichneten Punkten. Sei p ein beliebiges Polynom aus $V' \cap V_S$. Dieses erzeugt eine projektive ebene Kurve $C_p(F)$, welche mit den projektiven Geraden L_1 und L_2 jeweils vier gemeinsame Punkte (je die drei aus der Abbildung und S) hat. Daher muss p ein Vielfaches vom Polynom l_1 und l_2 sein. Dieses kann man mit einem Spezielfall des Lemmas von Bézout zeigen:

Seien g, h homogene Polynome vom Grad n bzw. m. Falls kein homogenes, nicht-konstantes Polynom existiert, dass g und h teilt, so haben $C_g(F)$ und $C_h(F)$ höchstens nm gemeinsame Punkte. In unserem Fall wählen wir $g = p$ und $h = l_1$, wobei l_1 vom Grad 1 ist und p höchstens vom Grad 3. Da wir schon gesehen haben, dass $C_p(F)$ und L_1 vier gemeinsame Punkte haben, muss es ein gemeinsames homogenes Polynom vom Grad > 0 geben, das p und l_1 teilt. Da l_1 selber homogen vom Grad 1 ist, muss das teilende Polynom bis auf einen konstanten Faktor gleich l_1 sein. Analog zeigt man, dass p von l_2 geteilt wird.

Es ist also

$$p = l_1 l_2 l,$$

wobei l ein homogenes Polynom vom Grad 1 sein muss. Daher definiert l eine projektive Gerade. Da $p \in V'$ liegt, sind auch R und $P \oplus Q$ Nullstellen von p. Laut Voraussetzung sind sie aber weder Nullstelle von l_1 noch von l_2. Also sind sie Nullstellen von l. Da es nach Lemma 1.4.2 nur eine projektive Gerade gibt, die R und $P \oplus Q$ verbindet, muss also $C_l(F) = L_3$ und damit p ein Vielfaches von $l_1 l_2 l_3$ sein. Somit ist $V' \cap V_S = \langle l_1 l_2 l_3 \rangle$ eindimensional. Nach Dimensionsformel gilt daher

$$\begin{aligned} 2 = 1 + 1 &= \dim(V' \cap V_s) + 1 = \dim V' + \dim V_s - \dim(V' + V_s) + 1 \\ &\geq \dim V' + 9 - 10 + 1 = \dim V', \end{aligned}$$

wodurch $\dim V' = 2$ sein muss. Wir definieren die beiden Polynome

$$p_1 = l_1 l_2 l_3 \qquad p_2 = m_1 m_2 m_3.$$

Sei ein beliebiger Punkt gegeben, der Nullstelle von einem der Polynome l_i aber keine Nullstelle von einem der Polynome m_i ist. Dann ist dieser Punkt Nullstelle von p_1 aber nicht von p_2. Es existiert also keine nicht-triviale Linearkombination von p_1 und p_2, die das Nullpolynom ergibt. Daher sind p_1 und p_2 linear unabhängig und bilden aus Dimensionsgründen eine Basis von V'. Damit hat g eine Darstellung

$$g = \alpha p_1 + \beta p_2$$

für gewisse $\alpha, \beta \in F$. Da der Schnittpunkt $T \in M_1 \cap L_3$ offensichtlich Nullstelle der beiden Polynome m_1 und l_3 ist, so ist er auch Nullstelle von p_1 und p_2 und damit auch von g. Daher liegt T tatsächlich in $E_g(F)$. □

Nun haben wir den Beweis erbracht, dass die in 3.2.1 definierte Verknüpfung auf einer elliptischen Kurve wirklich eine Gruppenstruktur hat. Daher schreiben wir ab jetzt $P + Q$ und $-P$ anstatt $P \oplus Q$ bzw. $\ominus P$. Einen anderen, eleganteren Beweis werden wir später in Abschnitt 3.3 kennenlernen.

3.2.3 Definition (Elliptische Kurven als $\mathbb{Z}$-Modul)**.** *Wir können jetzt auch die Multiplikation von Elementen aus $\mathbb{Z}$ mit Elementen aus $E_g(F)$ definieren, da $E_g(F)$ wie jede andere abelsche Gruppe ein $\mathbb{Z}$-Modul ist mit*

$$\begin{aligned} nP &= \underbrace{P + \ldots + P}_{n} \qquad \text{für } n \in \mathbb{N} \\ (-n)P &= -(nP) \\ 0P &= O. \end{aligned}$$

3.2.4 Satz (Algebraische Berechnung der Addition auf elliptischen Kurven)**.** *Sei F ein Körper mit Charakteristik größer als 3 und sei $E_g(F)$ eine elliptische Kurve. Sei $C_f(F)$ die affine Kurve mit $i(C_f(F)) \cup O = E_g(F)$, wobei*

$$f(x, y) = y^2 - x^3 - ax - b.$$

Seien $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in C_f(F)$, wobei $P_1 \neq -P_2$ ist. Dann lässt sich die Addition der Gruppe $(E_g(F), +)$ algebraisch berechnen nach folgender Vorschrift:

1. $-P_1 = -(x_1, y_1) = (x_1, -y_1)$
2. $P_1 + P_2 = P_3 = (x_3, y_3)$ *mit*

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

Beweis. Im Rahmen dieser Arbeit werden wir auf den Beweis verzichten. Er kann nachgelesen werden in [Wer02], Satz 2.3.13, S. 47ff. □

Beispiel (Elliptische Kurve über einem endlichen Körper)**.** Wir wollen ein konkretes Beispiels einer elliptischen Kurve über einem endlichen Körper betrachten. Nehmen wir die Gruppe der elliptischen Kurve $E_g(F)$ mit

$$g(X, Y, Z) = Y^2Z - X^3 - 2XZ^2 - 6Z^3$$

und $F = \mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}_7$. Zuerst einmal ist $E_g(F)$ wirklich eine elliptische Kurve, da g der Weierstraßform entspricht und die Diskriminante

$$\Delta = 4 \cdot 2^3 + 27 \cdot 6^2 = 1004 \not\equiv 0 \mod 5$$

ist. Nun wollen wir alle Punkte $P \in E_g(F)$ bestimmen. Den Punkt O kennen wir schon, weshalb wir nur noch die Lösungsmenge der affinen Weierstraßgleichung

$$y^2 = x^3 + 2x + 6$$

betrachten müssen. Wir werden dazu alle sieben möglichen $x \in \mathbb{Z}_7$ einsetzen und prüfen, ob sie quadratischer Rest modulo 7 sind. Dazu nehmen wir die Tabelle 1 zur Hilfe. Setzen wir nun x ein und berechnen jeweils die zugehörigen y, so dass

$y \mod 7$	0	1	2	3	4	5	6
$y^2 \mod 7$	0	1	4	2	2	4	1

Tabelle 1: Quadratische Reste modulo 7

f erfüllt ist, wie in Tabelle 2 gezeigt. Damit haben wir $E_g(F)$ bestimmt als die

$x \mod 7$	0	1	2	3	4	5	6
$x^3 + 2x + 6 = y^2 \mod 7$	6	2	4	4	1	1	3
$y \mod 7$	-	3, 4	2, 5	2, 5	1, 6	1, 6	-

Tabelle 2: Lösungsbestimmung für eine elliptische Kurve

Menge (mit affinen Koordinaten für $P \neq O$)

$$E_g(F) = \{O, (1,3), (1,4), (2,2), (2,5), (3,2), (3,5), (4,1), (4,6), (5,1), (5,6)\}.$$

Da also $E_g(F)$ eine Gruppe mit Ordnung 11 ist, ist $E_g(F)$ auch zyklisch und jeder Punkt $P \in E_g(F) \setminus \{O\}$ erzeugt $E_g(F)$. In Abbildung 5 ist die elliptische Kurve

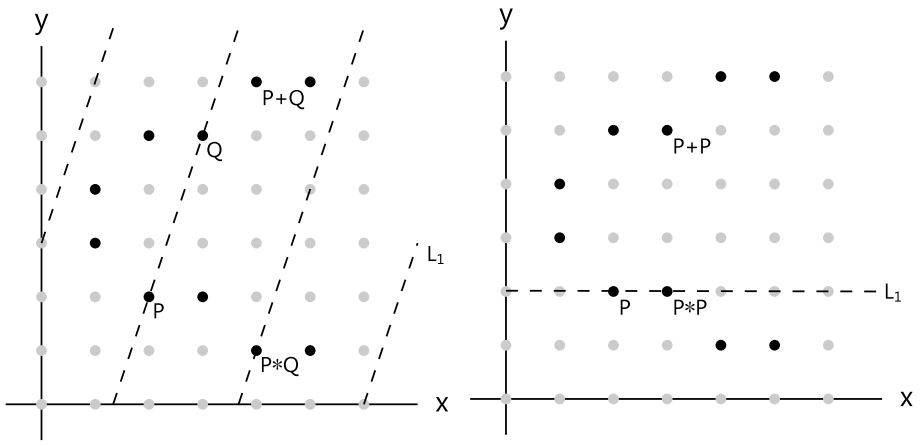

Abbildung 5: Elliptische Kurve über $\mathbb{Z}_7$

dargestellt. Zusätzlich zeigt sie eine geometrische Addition von zwei Punkten P und Q bzw. von P mit sich selbst, wobei die Geraden L_1 zwar jeweils kontinuierlich dargestellt sind, aber natürlich genau wie $E_g(F)$ auch nur über $\mathbb{Z}_7$ definiert sind. Dass die Gerade L_1, die in der rechten Abbildung zu sehen ist, wirklich die Tangente in P an $E_g(F)$ ist, ergibt sich aus folgender Rechnung

$$\begin{pmatrix} \frac{\partial g}{\partial X}(X,Y,Z) \\ \frac{\partial g}{\partial Y}(X,Y,Z) \\ \frac{\partial g}{\partial Z}(X,Y,Z) \end{pmatrix} = \begin{pmatrix} -3X^2 - 2Z^2 \\ 2YZ \\ Y^2 - 4XZ - 18Z^2 \end{pmatrix}.$$

Somit hat die Tangente $L(\alpha, \beta, \gamma)$ in $P = [2:2:1]$ die Koeffizienten

$$\begin{aligned} (\alpha, \beta, \gamma) &= \left(\frac{\partial g}{\partial X}(2,2,1), \frac{\partial g}{\partial Y}(2,2,1), \frac{\partial g}{\partial Z}(2,2,1) \right) \\ &= (-14, 4, -22) \equiv (0, 4, 6) \mod 7. \end{aligned}$$

Das Polynom $p \in F[x,y]$, das die affine Tangente erzeugt, ist also $p(x,y) = 4y+6$ und das verschwindet genau dann, wenn

$$4y + 6 \equiv 0 \Leftrightarrow y \equiv -6 \cdot 4^{-1} \equiv -6 \cdot 2 \equiv 2 \mod 7$$

ist. Laut Abbildung 5 ergibt sich also

$$(2,2) + (3,5) = (4,6) \qquad (2,2) + (2,2) = (3,5).$$

Dies deckt sich mit der algebraischen Berechnung nach Satz 3.2.4, denn es gilt für $P + Q := (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-2}{3-2} = 3 \equiv 3 \mod 7$$

$$x_3 = \lambda^2 - x_1 - x_2 = 3^2 - 3 - 2 = 4 \equiv 4 \mod 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 3(2-4) - 2 = -8 \equiv 6 \mod 7$$

und für $P + P := (x_4, y_4)$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = (3 \cdot 2^2 + 2)(2 \cdot 2)^{-1} \equiv 0 \cdot 4^{-1} \equiv 0 \mod 7$$

$$x_3 = \lambda^2 - x_1 - x_2 = 0 - 2 - 2 = -4 \equiv 3 \mod 7$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 0 - 2 = -2 \equiv 5 \mod 7.$$

3.3 Beweis der Gruppenstruktur mit Divisoren

Der Beweis mithilfe von Divisoren, dass $(E_g(F), \oplus)$ eine Gruppe ist, ist sehr elegant und ermöglicht einen tieferen Einblick als der geometrische Beweis. Er bedarf jedoch einiger weiterer Vorarbeit.

Falls für einen beliebigen Körper F die Menge $C_g(\overline{F})$ eine abelsche Gruppe ist, so ist die Menge $C_g(F)$ eine Untergruppe davon. Wir können daher in diesem Abschnitt annehmen, dass F selbst schon algebraisch abgeschlossen ist.

3.3.1 Definition (Divisoren)**.** *Sei $E_g(F)$ eine elliptische Kurve. Dann heißt eine formale Summe der Form*

$$D = \sum_{P \in E_g(F)} n_P P, \quad n_P \in \mathbb{Z}, \quad n_P \neq 0 \text{ für nur endliche viele } P$$

ein Divisor. Die Menge alle Divisoren schreiben wir als $\mathrm{Div}(E)$*. Seien nun $D, D' \in \mathrm{Div}(E)$ zwei Divisoren mit Koeffizienten n_P bzw. n'_P. Dann gilt:*

- $D + D' = \sum_{P \in E_g(F)} (n_P + n'_P)P$
- $-D = \sum_{P \in E_g(F)} (-n_P)P$

Damit lässt sich leicht nachrechnen, dass $(\mathrm{Div}(E), +)$ *eine abelsche Gruppe – die von E erzeugte freie abelsche Gruppe – ist. Um zwei Divisoren vergleichen zu können definieren wir noch folgendes:*

- $D \neq D' \Leftrightarrow n_P \neq n'_P$ *für mindestens eins P*
- $D \geq D' \Leftrightarrow n_P \geq n'_P$ *für alle P*
- $D > D' \Leftrightarrow D \geq D'$ *und* $D \neq D'$

Als Grad eines Divisors definieren wir die Summe der Koeffizienten

$$\deg(D) := \sum_{P \in E_g(F)} n_P.$$

Die Menge aller Divisoren mit Grad 0 schreiben wir als

$$\mathrm{Div}^0(E) := \{D \in \mathrm{Div}(E) : \deg(D) = 0\}.$$

Dies ist offensichtlich eine Untergruppe von $\mathrm{Div}(E)$*.*

3.3.2 Definition. *Sei $P \in E_g(F)$. Dann lässt sich P auf kanonische Weise ein Divisor zuordnen. Wir definieren dafür den Divisor (P) von P als*

$$(P) := \sum_{Q \in E_g(F)} n_Q \cdot Q, \quad n_Q := \begin{cases} 1, & P = Q \\ 0, & P \neq Q \end{cases}$$

3.3.3 Definition (Affiner Koordinatenring)**.** *Sei $E_f(F)$ der affine Teil einer elliptische Kurve, wobei f ein Polynom der Form*

$$y^2 = \pi(x) = (x - e_1)(x - e_2)(x - e_3)$$

ist, welches zerfällt für drei paarweise verschiedene Nullstellen e_1, e_2, e_3. Dann definieren wir den affinen Koordinatenring von E als

$$F[E] := F[x, y]/(y^2 - \pi(x)).$$

In diesem Ring ist insbesondere $y^2 = \pi(x)$.

3.3.4 Definition (Lokaler Ring)**.** *Sei $E_f(F)$ wie in der vorangegangenen Definition. Dann definieren wir den lokalen Ring von E an der Stelle P als*

$$F[E]_P := \{f/g : f, g \in F[E], g(P) \neq 0\}.$$

3.3.5 Definition (Ordnung)**.** *Seien $f, g \in F[E]$ teilerfremde Polynome. Dann definieren wir die Ordnung der rationalen Funktion f/g in P als*

$$\operatorname{ord}_P(f/g) := \begin{cases} \max\{n \in \mathbb{N}_0 : f/g \in M_P^n\}, & g = 1 \\ \operatorname{ord}_P(f) - \operatorname{ord}_P(g), & g \neq 1 \end{cases}$$

wobei M_P definiert ist als

$$M_P := \{f/g \in F[E] : g(P) \neq 0, f(P) = 0\}.$$

Die Ordnung von f/g in P ist also im Fall $(f/g)(P) = 0$ die Nullstellenordnung, im Fall $g(P) = 0$ die negative Polstellenordnung und sonst Null.

Beispiel. Sei gegeben der affine Teil $E_f(F)$ einer elliptischen Kurve mit

$$f : y^2 = \pi(x) = (x - e_1)(x - e_2)(x - e_3).$$

Dann ist $\operatorname{ord}_{(e_1,0)}(x - e_1) = 2$, denn es gilt

$$x - e_1 = \frac{y^2(x - e_1)}{y^2} = \frac{y^2(x - e_1)}{(x - e_1)(x - e_2)(x - e_3)} = \frac{y}{(x - e_2)} \cdot \frac{y}{(x - e_3)}.$$

Es ist also $(x - e_1) \in M_P^2$, jedoch lässt sich keine Zerlegung in drei Faktoren mit den nötigen Eigenschaften finden.

3.3.6 Satz. *Sei $E_g(F)$ eine elliptische Kurve und $f \in F[E]^*$. Dann gilt:*

1. $\operatorname{ord}_P f \neq 0$ *für nur endliche viele* $P \in E_g(F)$

2. $\sum_{P \in E_g(F)} \operatorname{ord}_P f = 0$

Beweis. Die Beweise können in [Sil86], II.1.2 und II.3.1 nachgelesen werden. □

3.3.7 Definition und Satz (Hauptdivisoren)**.** *Wir definieren nun eine Abbildung, die einer rationalen Funktion einen Divisor zuordnet, in der folgenden Form:*

$$\operatorname{div} : F[E]^* \to \operatorname{Div}^0(E) : f \mapsto \sum_{P \in E_g(F)} \operatorname{ord}_P f \cdot P$$

Aufgrund der Eigenschaften von ord *gilt offensichtlich*

$$\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g)$$

und somit ist div *ein Homomorphismus. Damit ist das Bild dieser Abbildung eine Untergruppe von* $\operatorname{Div}^0(E)$*. Die Elemente dieser Untergruppe heißen Hauptdivisoren.*

3.3.8 Satz (Divisoren projektiver Geraden)**.** *Seien $E_g(F)$ eine elliptische Kurve und L eine projektive Gerade der Form*

$$\Lambda(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0.$$

Seien P, Q, R die drei Schnittpunkte von $E_g(F)$ und L. Dann hat der Divisor der affinen projektiven Gerade $\lambda = \Lambda/Z$ die Form

$$\operatorname{div}(\lambda) = (P) + (Q) + (R) - 3(O).$$

Beweis. Nach [Sha94], Theorem 1, entspricht die Ordnung von λ in P genau der Schnittvielfachheit gemäß Definition 1.4.5, falls P affin ist. Da jeder Hauptdivisor vom Grad 0 ist, und eine Polstelle nur im Punkt O auftreten kann, muss die Polstellenordnung in O genau die Summe der Schnittvielfachheiten in den affinen Punkten aufheben.
Damit ist die Aussage für drei paarweise verschiedene, affine Schnittpunkte gezeigt. Falls nun $P = Q$ ist, so gilt trotzdem weiter

$$\operatorname{div}(\lambda) = 2(P) + (Q) - 3(O) = (P) + (P) + (Q) - 3(O).$$

Auch im Fall, dass P ein Fernpunkt ist, also $P = O$, gilt immernoch

$$\operatorname{div}(\lambda) = (Q) + (R) - 2(O) = (O) + (Q) + (R) - 3(O).$$

Alle anderen Fälle ergeben sich analog. □

3.3.9 Definition (Divisorenklassengruppen)**.** *Zwei Divisoren $D, D' \in \operatorname{Div}(E)$ nennen wir äquivalent, falls ihre Differenz $D - D'$ ein Hauptdivisor ist. Wir schreiben dafür $D \sim D'$. Die Äquivalenzklasse eines Divisors D schreiben wir als $[D]$.*

3.3.10 Definition (Grad-0-Teil der Divisorenklassengruppe)**.** *Die Faktorgruppe*

$$\operatorname{Pic}^0(E) := \operatorname{Div}^0(E)/\sim$$

nennen wir Grad-0-Teil der Divisorenklassengruppe. Diese ist offensichtlich eine abelsche Gruppe, da die Bildung von Unter- und Faktorgruppen diese Eigenschaft erhält und $\operatorname{Div}(E)$*, wie wir schon gesehen haben, eine abelsche Gruppe ist.*

3.3.11 Definition (Kanonische Divisoren)**.** *Ein Divisor D heißt kanonischer Divisor, falls ein nicht verschwindendes Differential ω existiert mit* $\operatorname{div}(\omega) = D$.

3.3.12 Definition. *Zu einem Divisor $D \in \operatorname{Div}(E)$ definieren wir*

$$\mathcal{L}(D) := \{f \in F[E]^* : \operatorname{div}(f) \geq -D\} \cup \{0\}.$$

Dies ist ein F-Vektorraum.

Für den nachfolgenden Satz benötigen wir noch den Begriff des „Geschlechts“. Im Wesentlichen ist das Geschlecht einer Fläche definiert als die Anzahl der „Löcher“ der Fläche. So hat zum Beispiel die Kugeloberfläche das Geschlecht 0. Der Torus dagegen, hat das Geschlecht 1.

3.3.13 Satz (Riemann-Roch)**.** *Sei X eine kompakte riemannsche Fläche. Ihr Geschlecht sei $g \in \mathbb{N}_0$. Sei $D \in \operatorname{Div}(X)$ ein Divisor und $K \in \operatorname{Div}(X)$ ein beliebiger kanonischer Divisor. Dann gilt*

$$\dim(\mathcal{L}(D)) - \dim(\mathcal{L}(K - D)) = \deg D + 1 - g.$$

Beweis. Der Beweis kann nachgelesen werden in [Sil86], II.5.4 und II.5.5. □

3.3.14 Satz. *Bezüglich einer elliptischen Kurve ist der 0-Divisor ein kanonischer und das topologische Geschlecht einer elliptischen Kurve ist 1.*

Beweis. Es ist $\pi'(x) \cdot dx = d(\pi(x)) = d(y^2) = d(y)y + yd(y) = 2yd(y)$. Daraus folgt

$$\frac{dx}{dy} = \frac{2y}{\pi'(x)}.$$

In den Punkten $(e_i, 0)$ ist y eine Ortsuniformisierende und $\pi'(e_i) \neq 0$. Damit ist

$$\operatorname{ord}_{(e_i,0)}(dx) = \operatorname{ord}_{(e_i,0)}(dx/dy) = 1.$$

Im Punkt O ist $1/x$ eine Ortsuniformisierende, womit aufgrund von $dx = -x^2 d(1/x)$ folgt, dass $\operatorname{ord}_O(dx) = -3$ ist. Insgesamt ist also

$$\operatorname{div}(dx) = ((e_1, 0, 1)) + ((e_2, 0, 1)) + ((e_3, 0, 1)) - 3(O) = \operatorname{div}(y).$$

Damit ist der 0-Divisor

$$0 = \operatorname{div}(dx) - \operatorname{div}(y) = \operatorname{div}(dx/y)$$

der Divisor eines Differentials. Aus $\operatorname{div}(dx/y) = 0$ folgt auch, dass das Differential nirgends verschwindet und somit ist der 0-Divisor ein kanonischer Divisor.

Daraus folgt mit [Sil86], II.5.5.b, auch, dass $0 = \deg(0) = 2g - 2$ und somit das Geschlecht einer elliptischen Kurve 1 ist. □

3.3.15 Lemma (Riemann-Roch für elliptische Kurven)**.** *Sei $E_g(F)$ eine elliptische Kurve und $D \in \operatorname{Div}(E)$ ein Divisor. Dann gilt:*

1. $\dim(\mathcal{L}(D)) - \dim(\mathcal{L}(-D)) = \deg D$

2. $\deg D > 0 \;\Rightarrow\; \dim(\mathcal{L}(D)) = \deg D \;\wedge\; \dim(\mathcal{L}(-D)) = 0$

Beweis. Folgt direkt mit den Sätzen 3.3.13 und 3.3.14. □

Nun lasst sich relativ einfach beweisen, dass $(E_g(F), \oplus)$ eine abelsche Gruppe ist. Der zugehörige Satz lautet wie folgt:

3.3.16 Satz. *Sei $E_g(F)$ eine elliptische Kurve. Dann ist die Abbildung*

$$\varphi : E_g(F) \to \mathrm{Pic}^0(E) : P \mapsto [(P) - (O)]$$

ein Isomorphismus.

Beweis. Zu zeigen sind die Bijektivität und die Homomorphie von φ.

1. Surjektivität: Sei $D \in \mathrm{Div}^0(E)$. Dann ist $\deg(D + (O)) = 1 > 0$ woraus mit Satz 3.3.15 folgt, dass $\dim(\mathcal{L}(D + (O))) = 1$ ist. Es existiert also ein $f \in F[E]^*$ mit $\mathrm{div}(f) \geq -D - (O)$. Da $\deg(-D - (O)) = -1 \neq 0 = \deg(\mathrm{div}(f))$ ist, existiert ein Punkt $P \in E_g(F)$, so dass $\mathrm{div}(f) = -D - (O) + (P)$ ist. Da $\mathrm{div}(f)$ definitionsgemäß ein Hauptdivisor ist, folgt somit

   $$(P) - (O) = D + \mathrm{div}(f) \sim D.$$

   Es ist also $\varphi(P) = [D]$.

2. Injektivität: Sei $[(P) - (O)] = [(Q) - (O)]$. Dann ist $(P) - (O) \sim (Q) - (O)$ und somit auch $(P) - (Q) \sim 0$. Also ist $(P) - (Q)$ ein Hauptdivisor. Sei nun f eine rationale Funktion mit $\mathrm{div}(f) = (P) - (Q)$. Es gilt $\mathrm{div}(f) \geq -(Q)$. Mit $\deg((Q)) = 1$ und Satz 3.3.15 folgt dann, dass $\dim(\mathcal{L}((Q))) = 1$ ist. Also muss $\mathcal{L}((Q))$ der Grundkörper F sein und $f \in \mathcal{L}((Q))$ somit eine konstante Funktion. Es folgt also $(P) - (Q) = \mathrm{div}(f) = 0$ und daher ist $P = Q$.

3. Homomorphie: Es gilt zu zeigen, dass $\varphi(P \oplus Q) = \varphi(P) + \varphi(Q)$ ist. Das ist äquivalent zur Bedingung

   $$(P \oplus Q) - (O) \sim (P) + (Q) - 2(O).$$

   Sei nun $R = P * Q$, also der Hilfspunkt, der bei der geometrischen Konstruktion von $P \oplus Q$ benötigt wird. Weiter seien die beiden Konstruktionsgeraden L und L' mit den zugrundeliegenden Polynomen

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

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

   gegeben, wobei L die Punkte P, Q, R und die L' die Punkte $R, O, P \oplus Q$ enthalten. Dann gilt, falls wir durch Division mit der Ferngerade $Z = 0$ zur affinen Darstellung übergehen:

   $$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(O)$$

   $$\mathrm{div}(f'/Z) = (P \oplus Q) + (R) - 2(O)$$

   Es folgt also $(P \oplus Q) - (P) - (Q) + (O) = \mathrm{div}(f/Z) - \mathrm{div}(f'/Z) \sim 0$ woraus durch Umstellen die Behauptung folgt. □

Damit ist $(E_g(F), \oplus)$ isomorph zu einer abelschen Gruppe und selbst eine abelsche Gruppe.

4 Kryptographie auf elliptischen Kurven

Nun sind wir in der Lage elliptische Kurven für kryptographische Zwecke zu nutzen. Im Rahmen dieser Arbeit soll nicht genauer auf die verschiedenen Konzepte und Motivationen für kryptographische Verfahren eingegangen werden. Eine sehr gute poplärwissenschaftliche Einführung in die geschichtliche Entwicklung der Kryptographie gibt [Sin99].

4.1 Verschlüsselungsverfahren

Bei der Verschlüsselung geht es darum, eine Botschaft mithilfe eines geheimen Wortes so zu verändern, dass es ohne Kenntnis dieses Geheimnisses nicht (oder nur sehr schwer) möglich ist, die ursprüngliche Botschaft herauszufinden. Andererseits muss es mit Kenntnis des Geheimnisses leicht möglich sein, die Botschaft zurückzuerhalten.

Formal sieht es dann so aus: Sei K der Klartext, also die zu verschlüsselnde Botschaft. Als C bezeichnen wir den Geheimtext, also die verschlüsselte Variante vom Klartext. Das geheime Wort, auch Schlüssel genannt, sei G. Dann ist ein Verschlüsselungsverfahren ein Paar von zwei Scharen von Abbildungen (ϕ_G, ϕ_G^-) derart, dass

$$\phi_G : K \mapsto C$$

$$\phi_G^- : C \mapsto K$$

Es es also eine Vorschrift, die für jeden möglichen (bzw. zulässigen) Schlüssel zwei Abbildungen definiert, wovon eine den Klartext in Geheimtext überführt und die andere diesen Geheimtext wieder in Klartext zurückführt. Man unterscheidet drei Arten von Verschlüsselungsverfahren:

Symmetrische Verschlüsselungsverfahren: In diesem Fall wird zur Ver- und Entschlüsselung das gleiche Geheimnis G verwendet. Es ist also

$$\phi_G \circ \phi_G^- = \mathrm{id}\,.$$

Dies hat zur Folge, dass zwei Partner, die verschlüsselt kommunizieren möchten, sich zuerst über einen sicheren Kanal auf ein gemeinsames Geheimnis einigen müssen. Häufig verwendete Vertreter sind z.B. AES und DES.

Asymmetrische Verschlüsselungsverfahren: In diesem Fall sind die Abbildungen ϕ_G und ϕ_G^- nicht invers zueinander. Eine Nachricht, die mit einem Schlüssel G verschlüsselt wurde, kann nur mit einem bestimmten anderen Schlüssel G' entschlüsselt werden. Als Beispiel sei hier das RSA-Verfahren genannt. Bei diesem Verfahren hat jeder der Kommunikationspartner einen geheimen und einen öffentlichen Schlüssel. Will z.B. Alice an Bob eine Nachricht verschicken, so besorgt sie sich Bobs frei zugänglichen öffentlichen Schlüssel. Um diese Nachricht dann wieder zu entschlüsseln, benutzt Bob seinen privaten Schlüssel, den nur er kennt. Natürlich darf sich der private Schlüssel nicht aus dem öffentlichen Schlüssel herleiten lassen. Jedoch muss sich der öffentliche aus dem privaten ableiten lassen. Im Wesentlichen besteht der private Schlüssel aus zwei großen

Primzahlen p und q und der öffentliche Schlüssel aus dem Produkt $N = pq$. RSA verlässt sich also darauf, dass das Faktorisierungsproblem für große Zahlen schwierig ist. Wie dies genau funktioniert, ist in [Wer02], S. 2f, kurz beschrieben.

Hybride Verschlüsselungsverfahren: Dies ist eigentlich keine eigene Kategorie. Hybride Verschlüsselungsverfahren bedienen sich asymmetrischer Verfahren, um einen Schlüsselaustausch zu ermöglichen. Mit diesem Schlüssel wird dann der eigentliche Klartext mithilfe eines symmetrischen Verfahrens verschlüsselt.

4.2 Diffie-Hellmann-Schlüsselaustausch

4.2.1 Definition (Diskreter Logarithmus)**.** *Sei $(G, \cdot)$ eine endliche zyklische Gruppe der Ordnung n und sei $g \in G \setminus \{e\}$ ein Erzeuger von G. Dann ist die Abbildung*

$$\exp_g : \mathbb{Z}/n\mathbb{Z} \to G : x \mapsto g^x$$

ein Gruppenisomorphismus, genannt diskrete Exponentation. Die Umkehrfunktion

$$\log_g : G \to \mathbb{Z}/n\mathbb{Z} : x \mapsto log_g x$$

heißt diskreter Logarithmus.

Der diskrete Logarithmus lässt sich auch auf additiven Gruppen definieren. In diesem Fall gibt der diskrete Logarithmus zu einem Element h das Element $a \in G$ an, so dass gilt:

$$ah = g$$

4.2.2 Definition (Problem des diskreten Logarithmus)**.** *Vorgelegt seien eine abelsche Gruppe $(G, +)$, ein Element $P \in G$, $n = ord(P)$ und ein Element $Q \in \langle P \rangle$. Die Suche nach dem Element $k \in \mathbb{Z}/n\mathbb{Z}$, mit*

$$kP = Q$$

heißt Problem des diskreten Logarithmus, kurz DL-Problem.

4.2.3 Definition (Diffie-Hellmann-Problem)**.** *Vorgelegt seien eine abelsche Gruppe $(G, +)$, ein Element $P \in G$ der Ordnung n und die Ergebnisse aP und bP, wobei $a, b \in \mathbb{Z}$ nicht bekannt sind. Dann heißt das Problem der Berechnung des Elementes abP aus diesen Informationen heraus Diffie-Hellmann-Problem, kurz DH-Problem.*

Offensichtlich lässt sich das DH-Problem in einer Gruppe, in der sich das DL-Problem lösen lässt, ebenfalls lösen. Ob jedoch die Lösung des DL-Problems auch notwendig dafür ist, ist bisher nicht bekannt.

4.2.4 Algorithmus (Diffie-Hellmann-Schlüsselaustausch)**.** Sei eine abelsche Gruppe G gegeben, in der das Diskrete-Logarithmus-Problem und das Diffie-Hellmann-Problem hinreichend schwierig zu lösen ist. Wenn nun zwei Personen (hier Alice und Bob) über einen öffentlichen und unsicheren Kanal einen Schlüssel austauschen wollen, so können sie dies wie folgt tun:

1. Alice und Bob einigen sich auf ein Element $P \in G$, dessen Ordnung $n = \#\langle P \rangle$ hinreichend groß ist.

2. Alice überlegt sich eine geheime zufällige Zahl $a \in \mathbb{Z}_n$ und Bob überlegt sich eine geheime zufällige Zahl $b \in \mathbb{Z}_n$.

3. Alice schickt das Ergebnis von aP an Bob und Bob schickt das Ergebnis bP an Alice.

4. Nun teilen beide ein gemeinsames Geheimniss - das Ergebnis von abP.

Ein Angreifer (hier Eva), der nun ebenfalls dieses Geheimnis kennen möchte, besitzt, falls er alles abgehört hat, folgende Informationen: Die Gruppe G, das Element $P \in G$, das Ergebnis $aP \in G$ und das Ergebnis $bP \in G$. Da vorausgesetzt war, dass das DL- und DH-Problem hinreichend schwierig in G ist, hat Eva zunächst keine Chance, an das Geheimnis abP zu gelangen, obwohl sie jeglichen Nachrichtenaustausch von Alice und Bob abgehört hat. Dass sich der DH-Schlüsselaustausch nur durch Lösen des DL-Problems knacken lässt, ist allerdings nicht bewiesen. Es könnte also auch einen alternativen Ansatzpunkt geben, mit dem sich das Geheimnis abP aus den gegebenen Informationen erhalten lässt.

4.2.5 Satz (Schranke für Gruppenordnung endlicher elliptischer Kurven)**.** *Sei $\mathbb{F}_q$ ein endlicher Körper und $E_g(\mathbb{F}_q)$ eine elliptische Kurve über diesem. Dann ist die Ordnung der Gruppe $E_g(\mathbb{F}_q)$, die aus dem Punkt O und den Lösungen der affinen Weierstraßgleichung*

$$f(x, y) = y^2 - x^3 - ax - b$$

besteht, nach oben beschränkt durch

$$\#E_g(\mathbb{F}_q) \leq 2q + 1.$$

Beweis. Man kann in f genau q-viele verschiedene x einsetzen. Für ein konkretes $x_0 \in \mathbb{F}_q$ erhalten wir damit eine quadratische Gleichung in y der Form

$$h(y) := y^2 - r \quad \text{mit} \quad r := x_0^3 - ax_0 - b \in \mathbb{F}_q.$$

Daher gibt es zu jedem $x_0 \in \mathbb{F}_q$ maximal zwei verschiedene $y \in \mathbb{F}_q$, so dass $i(x_0, y) \in E_g(\mathbb{F}_q)$ liegt. □

Damit also das DL- und DH-Problem schwierig in $E_g(F)$ ist, muss der Grundkörper F hinreichend groß sein, da sonst $\#E_g(F)$ nicht groß sein kann und somit auch für jedes $P \in E_g(F)$ das Erzeugnis $\langle P \rangle$ nicht groß sein kann. In kleinen zyklischen Gruppen lassen sich das DL- und DH-Problem jedoch durch einfaches Durchprobieren lösen.

Eine wesentlich bessere Abschätzung für die Gruppenordnung liefert der folgende Satz, den wir jedoch im Rahmen dieser Arbeit nicht beweisen werden.

4.2.6 Satz (Hasse)**.** *Sei $E_g(F)$ eine elliptische Kurve über dem endlichen Körper $F = \mathbb{F}_q$. Dann lässt sich die Gruppenordnung von $E_g(F)$ abschätzen durch*

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

Beweis. Der Beweis kann in [Sil86], Theorem 1.1 nachgelesen werden. □

4.2.7 Anwendung. Sei $\mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und sei q hinreichend groß. Sei $E_g(\mathbb{F}_q)$ eine elliptische Kurve über diesem Körper mit hinreichend großer Ordnung $\#E_g(\mathbb{F}_q)$. Sei weiter P ein Punkt aus $E_g(\mathbb{F}_q)$, der eine hinreichend große Untergruppe $\langle P\rangle$ erzeugt, wobei wir $n = \#\langle P\rangle$ als die Ordnung dieser Untergruppe bezeichnen.

Dann können sich Alice und Bob mithilfe von $\mathbb{F}_q$, $E_g(\mathbb{F}_q)$ und P, die sie öffentlich vereinbaren, und mithilfe des DH-Schlüsselaustausches auf ein gemeinsames Geheimnis verständigen. Dieses Geheimnis können sie als Schlüssel für ein symmetrisches Verschlüsselungsverfahren benutzen, um gesichert zu kommunizieren.

In diesem Kapitel haben wir öfter Formulierungen wie „hinreichend sicher“ oder „schwierig“ verwendet. Was damit genau gemeint ist, soll im Folgenden erläutert werden.

4.3 Komplexität

4.3.1 Definition (Landau Symbole)**.** *Sei $k \in \mathbb{N}$ und seien f, g Abbildungen*

$$f : \mathbb{N}^k \to \mathbb{R} \qquad g : \mathbb{N}^k \to \mathbb{R}$$

Dann schreiben wir

$$f \in \mathcal{O}(g),$$

falls es einen Faktor $C \in \mathbb{R}_+$ und eine Schranke $B \in \mathbb{R}_+$ gibt, so dass für alle $x = (n_1, \ldots, n_k) \in \mathbb{N}^k$ mit $n_i \geq B$ die Gleichung $f(x) \leq Cg(x)$ gilt. Wir sagen in diesem Fall auch, dass f nicht wesentlich schneller wächst als g. Falls unter denselben Bedingungen $f(x) \geq Cg(x)$ gilt, so schreiben wir

$$f \in \Omega(g)$$

und sagen, dass f nicht wesentlich langsamer wächst als g. Falls sowohl $f \in \mathcal{O}(g)$ als auch $f \in \Omega(g)$ gilt, so schreiben wir

$$f \in \Theta(g)$$

und sagen, dass f im Wesentlichen genauso schnell wächst wie g.

Mithilfe der Landau Symbole können wir nun die benötigte Rechenzeit von Algorithmen kategorisieren. Falls wir z.B. einen Algorithmus haben, der als Eingabeparameter k verschiedene Werte aus $\mathbb{N}$ benötigt, so können wir versuchen, eine Funktion f zu bestimmen, die in Abhängigkeit der k Eingabeparameter einen Wert ausgibt, welcher für die Rechenzeit steht. Zum Beispiel wäre das Zählen elementarer Rechenoperationen eine solche Möglichkeit f zu bestimmen. Die benötigte Rechenzeit wird in Bezug auf die Bitlänge der Eingabeparameter angegeben. Als praktisch unlösbare Probleme bezeichnet man Berechnungen, deren benötigte Rechenzeit nicht wesentlich langsamer wächst als eine exponentielle Funktion. Falls eine Berechnung eine Rechenzeit hat, die nicht wesentlich schneller wächst als eine polynomielle Funktion, so gilt sie als effizient lösbar. Jedoch sollte in diesem Fall der Grad des Polynoms eher klein sein.
Wir werden statt Rechenzeit auch Aufwand oder Komplexität sagen. Man kann auch andere Komplexitäten wie den Speicherverbrauch betrachten. Wir wollen uns jedoch ausschließlich mit der benötigten Rechenzeit befassen.

4.3.2 Lemma. *Für die Landau Symbole gelten folgende leicht nachzuweisende Zusammenhänge:*

- *Für jedes positive reelle α gilt:* $\mathcal{O}(\alpha) = \mathcal{O}(1)$
- *Für jedes Polynom p vom Grad n gilt:* $\mathcal{O}(p) = \mathcal{O}(x^n)$

Dies gilt analog auch für Ω und Θ.

Da kryptographische Algorithmen in der Regel von Computern ausgeführt werden, dabei aber jeder Computer, was Hard- und Software betrifft, etwas unterschiedlich ist, wollen wir den Aufwand einer Berechnung unabhängig von solchen „äußeren Faktoren“ angeben. Die Angabe des Aufwands soll lediglich vom konkreten Algorithmus und von einem grundlegenden Modell einer imaginären Rechenmaschine abhängen.

4.3.3 Definition (Bitlänge)**.** *Sei x eine ganze nicht-negative Zahl gegeben in der 2-adischen Darstellung*

$$x = x_k \cdot 2^k + x_{k-1} \cdot 2^{k-1} + \ldots + x_1 \cdot 2^1 + x_0 \cdot 2^0 \qquad x_i \in 0, 1.$$

Das heißt x wird dargestellt als eine endliche Folge von Nullen und Einsen, wobei wir die einzelnen Ziffern als Bits bezeichnen. Dann ist die Bitlänge von x definiert als

$$\operatorname{size} x := k = \lceil \log_2 x \rceil$$

4.3.4 Satz (Komplexität elementarer Ganzzahlarithmetik)**.** *Sei eine Rechenmaschine gegeben, die mit ganzen nicht-negativen Zahlen, welche in der 2-adischen Darstellung gegeben sind, rechnen kann. Wir nehmen an, dass die Rechenmaschine in der Lage ist, zwei Bits mit konstantem Aufwand, also in $\mathcal{O}(1)$, zu addieren. Dann lässt sich der Rechenaufwand für die Addition, Multiplikation und Division mit Rest berechnen als*

- *$a + b$ benötigt* $O(\max\{\operatorname{size} a, \operatorname{size} b\})$
- *$a - b$ benötigt* $O(\max\{\operatorname{size} a, \operatorname{size} b\})$
- *$a \cdot b$ benötigt* $O(\operatorname{size} a \cdot \operatorname{size} b)$
- *$a \div b = qb + r$ benötigt* $O(\operatorname{size} b \cdot \operatorname{size} q)$

Beweis. Dieser Satz lässt sich einfach beweisen durch Betrachten des jeweiligen Algorithmus und Zählen der jeweils benötigten Operationen. Der Beweis lässt sich im Einzelnen nachlesen in [Buc99], Abs. 2.5, S. 8ff. □

Nun zahlt sich die Angabe des Aufwands mit der Landau-Notation aus. Zum Beispiel macht es keinen Unterschied, ob man, wie wir angenommen haben, auf einem Computer arbeitet, der pro Rechenzyklus nur 1 Bit verarbeiten kann, oder ob pro Rechenzyklus mehrere Bits verarbeitet werden können. Hätten wir einen Rechner, der 32 Bit simultan verarbeiten könnte, so wäre der Aufwand für die Addition von einem Bit $\mathcal{O}(1/32)$. Nach Lemma 4.3.2 gilt aber $\mathcal{O}(1/32) = \mathcal{O}(1)$. Der vorangegangene Satz gibt also weiterhin eine gültige Aussage über den Aufwand.

4.3.5 Satz (Komplexität für den erweiterten euklidschen Algorithmus)**.** *Sei eine Rechenmaschine wie in Satz 4.3.4 gegeben. Dann lassen sich zu zwei positiven ganzen Zahlen a und b zwei ganze Zahlen r und q berechnen, so dass gilt*

$$ra + qb = \gcd(a, b),$$

mit einem Rechenaufwand von $\mathcal{O}(\operatorname{size} a \cdot \operatorname{size} b)$.

Beweis. Der Beweis lässt sich nachlesen in [Buc99], Theorem 2.10.5, S. 18ff. □

Beispiel (Komplexität des DH-Problems in $\mathbb{Z}_p$)**.** Wir wollen nun untersuchen, warum sich der Körper $\mathbb{Z}_p$ mit p prim für einen Diffie-Hellmann-Schlüsselaustausch nicht eignet. Seien ein Element $x \in \mathbb{Z}_p$, ein Koeffizient $a \in \mathbb{Z}_p$ und das Ergebnis $y := ax$ gegeben. Um nun aus x und y den Koeffizienten a zu berechnen, also das Diffie-Hellmann-Problem zu lösen, reicht es offensichtlich, das multiplikative Inverse von x zu berechnen, denn es gilt

$$ax = y \;\Leftrightarrow\; a = yx^{-1}.$$

Dazu können wir uns des erweiterten euklidschen Algorithmus bedienen. Der Aufwand, das DH-Problem in $\mathbb{Z}_p$ zu lösen, lässt sich demnach wie folgt angeben: Die Berechnung von x^{-1} benötigt $\mathcal{O}(\operatorname{size} x \cdot \operatorname{size} p)$ und die Berechnung von yx^{-1} benötigt $\mathcal{O}(\operatorname{size} y \cdot \operatorname{size} x^{-1})$. Da nun x, x^{-1} und y kleiner als p sind, lässt sich der Gesamtaufwand abschätzen durch

$$\mathcal{O}((\operatorname{size} p)^2 + (\operatorname{size} p)^2) = \mathcal{O}((\operatorname{size} p)^2)$$

und somit ist das DH-Problem in $\mathbb{Z}_p$ effizient zu lösen. Daher würde ein Diffie-Hellmann-Schlüsselaustausch in $\mathbb{Z}_p$ keine Sicherheit bieten.

4.3.6 Satz (Komplexität von Addition und Inversion auf elliptischen Kurven)**.** *Sei $E_g(\mathbb{Z}_p)$ eine elliptische Kurve über dem Körper $\mathbb{Z}_p$. Seien nun $P_1, P_2 \in E_g(\mathbb{Z}_p)$ mit $P_1, P_2 \neq 0$ und $P_1 \neq P_2$. Dann lassen sich die arithmetischen Operationen auf $E_g(\mathbb{Z}_p)$ berechnen mit einem Aufwand von*

	$+$	-	$\cdot$	$^{-1}$	*Aufwand*
$-P_1$	*0*	*1*	*0*	*0*	$\mathcal{O}(\operatorname{size} p)$
$2P_1$	*1*	*4*	*6*	*1*	$\mathcal{O}(5(\operatorname{size} p) + 7(\operatorname{size} p)^2) = \mathcal{O}((\operatorname{size} p)^2)$
$P_1 + P_2$	*0*	*6*	*3*	*1*	$\mathcal{O}(6(\operatorname{size} p) + 4(\operatorname{size} p)^2) = \mathcal{O}((\operatorname{size} p)^2)$

Beweis. Die Zählung der einzelnen benötigten Operationen in $\mathbb{Z}_p$ ergibt sich aus Satz 3.2.4. Daraus ergibt sich der Gesamtaufwand direkt aus Satz 4.3.4. □

In einer Gruppe $E_g(\mathbb{Z}_p)$ lässt sich also effizient die Addition und die Inversion berechnen. Anders ist das nach heutigem Kenntnisstand mit dem DH-Problem in elliptischen Kurven. Es ist keine effiziente Methode bekannt, so dass man heute davon ausgeht, dass sich dieses Problem nur durch Durchprobieren aller möglichen Koeffizienten berechnen lässt.

4.3.7 Satz (Komplexität des DH-Problems in $E_g(\mathbb{Z}_p)$)**.** *Sei $E_g(\mathbb{Z}_p)$ eine elliptische Kurve und sei $P \in E_g(\mathbb{Z}_p)$. Sei n die Ordnung des Erzeugnisses $\langle P \rangle$ und $Q \in \langle P \rangle$. Dann lässt sich das $a \in \mathbb{Z}_n$ mit $aP = Q$ finden, indem man sukzessive*

alle möglichen Punkte $P, 2P, 3P, \ldots, (n-1)P$ berechnet und sie auf Gleichheit mit Q prüft. Im ungünstigen Fall - es ist erst $(n-1)P = Q$ - benötigt man dafür offensichtlich $n-2$ Additionen in $E_g(\mathbb{Z}_p)$. Nach Satz 4.3.6 beträgt die benötigte Rechenzeit in diesem Fall also

$$\mathcal{O}((n-2) \cdot (\operatorname{size} p)^2) = \mathcal{O}(2^{\operatorname{size} n - 2} \cdot (\operatorname{size} p)^2) = \mathcal{O}(2^{\operatorname{size} n}).$$

Das DH-Problem ist also in $E_g(\mathbb{Z}_p)$ in exponentieller Zeit lösbar. Dass es jedoch nicht schneller geht, ist nicht bewiesen. Es sind zur Zeit nur keine effizienteren Algorithmen bekannt, die für beliebige elliptische Kurven funktionieren. Für spezielle Klassen von elliptischen Kurven sind jedoch effizientere Lösungsverfahren bekannt. So können zum Beispiel supersinguläre elliptische Kurven unter gewissen Voraussetzungen mit dem MOV-Algorithmus oder aber anormale Kurven mit dem SSSA-Algorithmus angegangen werden, um das DH-Problem in subexponentieller Zeit zu lösen.

5 Fazit

Wir haben mit grundlegenden Kenntnissen der linearen Algebra ein solides theoretisches Fundament der Mathematik der elliptischen Kurven entwickelt. Darauf aufbauend haben wir eine geometrisch motivierte Verknüpfung auf der Punktmenge einer elliptischen Kurve definiert und bewiesen, dass diese Verknüpfung sogar eine Gruppenstruktur definiert. Anhand eines konkreten Beispiels haben wir uns dann noch einmal von der Korrektheit unserer Überlegungen überzeugt und gesehen, wie die zuvor abstrakt definierten Abläufe konkret aussehen.

Nach einer knappen Einführung in die Kryptographie haben wir dann mithilfe des Diffie-Hellmann-Problems und -Schlüsselaustausches ein Beispiel dafür gesehen, wie sich elliptische Kurven für kryptographische Zwecke nutzen lassen. Nach einer ebenso knappen Einführung in grundlegende Ideen der Komplexitätstheorie haben wir die benötigte Rechenzeit der arithmetischen Operationen auf elliptischen Kurven studiert.

Zum Abschluss soll noch ein kleiner Ausblick geben werden: Obwohl elliptische Kurven schon seit Jahrzehnten bekannt sind, sind sie noch lange nicht in allen Einzelheiten verstanden. Beweise, die wesentlich für die Sicherheit bestimmter krpytographischer Verfahren auf elliptischen Kurven sind, wie z.B. dass das DL- und DH-Problem wirklich schwierig zu lösen sind, stehen noch aus.

Elliptische Kurven lassen sich nicht nur zur Kryptographie sondern auch zur Kryptoanalyse (das Gegenstück der Kryptographie, welches zum Ziel hat verschlüsselte Nachrichten auch ohne Kenntnis des Schlüssels zu entschlüsseln) verwenden. So existieren Algorithmen mit elliptischen Kurven, die bei der Faktorisierung von bestimmten Zahlen schneller sind, als die naiven Ansätze und sie werden so auch benutzt, um z.B. Schwächen im RSA-Algorithmus aufzudecken.

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich die vorliegende Bachelorarbeit mit dem Titel „Kryptographie auf elliptischen Kurven“ selbständig verfasst sowie die benutzten Quellen und Hilfsmittel vollständig angegeben habe und dass die Arbeit nicht bereits als Prüfungsarbeit vorgelegen hat.

Braunschweig 18. November 2010, ...
Christian Hoffmeister

Literatur

[Buc99] Johannes Buchmann. *Einführung in die Kryptographie*. Springer, 1999.

[HMV04] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer Verlag, 2004.

[Sha94] Igor' Rostislavovich Shafarevich. *Basic algebraic geometry 1 (2nd)*. Springer, 1994.

[Sil86] J.H. Silvermann. *The arithmetic of elliptic curves*. Springer, 1986.

[Sin99] Simon Singh. *Geheime Botschaften*. Deutscher Taschenbuch Verlag, 1999.

[Wer02] Annette Werner. *Elliptische Kurven in der Kryptographie*. Springer Verlag, 2002.