# Elliptische-Kurven-Kryptographie

Kevin Kappelmann, Lukas Stevens

23. April 2016

# Inhaltsverzeichnis



# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1 Einleitung und Motivation

Kryptosysteme wie RSA, Diffie-Hellman[1] und ElGamal[1], die sich auf die Schwere der Primafaktorzerlegung bzw. dem diskreten Logarithmenproblem über Ganzzahlen stützen, benötigen sehr große Schlüssellängen, um eine ausreichend hohe Sicherheit zu garantieren. Daraus ergibt sich sowohl eine hoher Energie- als auch Speicherbedarf für die Berechnung der Algorithmen, was vor allem für Microchips und eingebettete Systeme ein Problem darstellt.
Eine Lösung für dieses Problem sind elliptische Kurven. Diese algebraischen Kurven tragen eine Gruppenstruktur, über die das diskrete Logarithmenproblem deutlich schwerer lösbar ist, als über Gruppen mit Ganzzahlen. Kryptosysteme, die auf elliptische Kurven beruhen, kommen dadurch mit erheblich kürzeren Schlüsseln bei vergleichbarer Sicherheit aus. [2, Seite 53]
Nachfolgende Tabelle verdeutlicht diesen Sachverhalt. Spalte 1 kennzeichnet die maximale Sicherheit (in Bits) für den jeweiligen Algorithmus und der angegebenen Schlüssellänge (in Bits). Rot markierte Felder gelten als kryptographisch unsicher, grüne als aktuell sicher.

| Sicherheitsniveau | RSA/Diffie-Hellman[1] | Elliptische-Kurven |
|---|---|---|
| $\leq 80$ | 1024 | 160-223 |
| 112 | 2048 | 224-255 |
| 128 | 3072 | 256-383 |
| 192 | 7680 | 384-511 |
| 256 | 15360 | 512+ |

Tabelle 1: Vergleich Schlüssellängen

Die Verwendung elliptischer Kurven in der Kryptographie wurde Mitte der 1980er Jahre von Neal Koblitz [6] und Victor S. Miller [7] unabhängig voneinander vorgeschlagen. Aufgrund der vorteilhaften Eigenschaften gewinnt die **Elliptische-Kurven-Kryptographie** (kurz **ECC** für Elliptic Curves Cryptography) stets mehr an Bedeutung und löst ältere Verfahren wie RSA in den verschiedensten Bereichen ab. Vor allem in Umgebungen mit begrenzten Kapazitäten, wie z.B. Smartcards, ist ECC bereits weit verbreitet.
So verwendet beispielsweise Österreich seit 2004 als Vorreiter für alle gängigen Bürgerkarten ECC. [1] Aber auch die Reisepässe der meisten Europäischen Staaten nutzen inzwischen meist in einer Form ECC. [9]

# 2 Grundbegriffe

Um elliptische Kurven einführen zu können, müssen wir uns zunächst mit affiner und projektiver Geometrie und ihrer Verwandtheit auseinander setzen. Wir führen hierfür zunächst allgemein die Begriffe der affinen und projektiven Ebene ein und konstruieren uns eine projektive Ebene $\mathrm{PG}(2, \mathbb{F})$ über einen beliebigen Körper $(\mathbb{F}, +, *)$.

In den folgenden Kapiteln kürzen wir zu Gunsten der Notation den Körper $(\mathbb{F}, +, *)$ mit $\mathbb{F}$ ab.

[1] In der jeweiligen Implementierung als Gruppe über ganze Zahlen

## 2.1 Affine Ebenen

**Definition 2.1.** Es sei $\mathcal{A}$ eine Menge und $\mathcal{G}$ eine Teilmenge der Potenzmenge von $\mathcal{A}$, d.h. $\mathcal{G} \subseteq Pot(\mathcal{A})$. Die Menge $\mathcal{A}$ nennt man die **Punktmenge** und die Menge $\mathcal{G}$ die **Geradenmenge** der affinen Ebene $(\mathcal{A}, \mathcal{G})$, falls folgende drei Bedingungen erfüllt sind:

(A1) Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$ (durch zwei verschiedene Punkte geht genau eine Gerade).
Wir schreiben $\overline{a, b}$ für dieses G.

(A2) Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$ (durch jeden Punkt geht genau eine Gerade, die zu einer gegebenen Gerade parallel ist).
Das sogenannte **Parallelenaxiom**.

(A3) Es existieren drei Elemente $a, b, c \in \mathcal{A}$ mit $c \notin \overline{a, b}$ (es gibt drei Punkte, die nicht alle auf einer Gerade liegen).

**Beispiel 2.2.** *Das **Minimalmodell** einer affinen Ebene umfasst genau 4 Punkte. [5, Seite 16]*

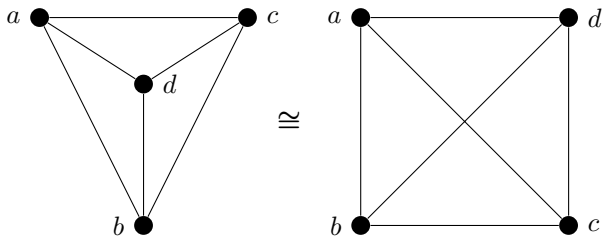



Abbildung 1: Minimalmodell einer affinen Ebene

**Beispiel 2.3.** *Die euklidische Ebene ("Der zweidimensionale Raum unserer Anschauung") ist eine affine Ebene, in der zusätzich Längen- und Winkelmaß definiert sind.*

## 2.2 Projektive Ebenen

**Definition 2.4.** ps sei $\mathcal{P}$ eine Menge und $\mathcal{G}$ eine Teilmenge der Potenzmenge von $\mathcal{P}$, d.h. $\mathcal{G} \subseteq Pot(\mathcal{P})$. Die Menge $\mathcal{P}$ nennt man die **Punktmenge** und die Menge $\mathcal{G}$ die **Geradenmenge** der projektiven Ebene $(\mathcal{P}, \mathcal{G})$, falls folgende drei Bedingungen erfüllt sind:

(P1) Zu je zwei Elementen $P, Q \in \mathcal{A}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$ (durch zwei verschiedene Punkte geht genau eine Gerade).
Wir schreiben $\overline{P, Q}$ für dieses G.

(P2) Für je zwei $G, H \in \mathcal{G}$ mit $G \neq H$ gilt $|G \cap H| = 1$ (zwei verschiedene Geraden schneiden sich in genau einem Punkt).

(P3) Es existieren vier verschiedene Elemente in $\mathcal{P}$, sodass immer höchstens zwei davon in jedem beliebigen $G \in \mathcal{G}$ liegen (es gibt vier Punkte, sodass nie drei davon auf derselben Gerade liegen).

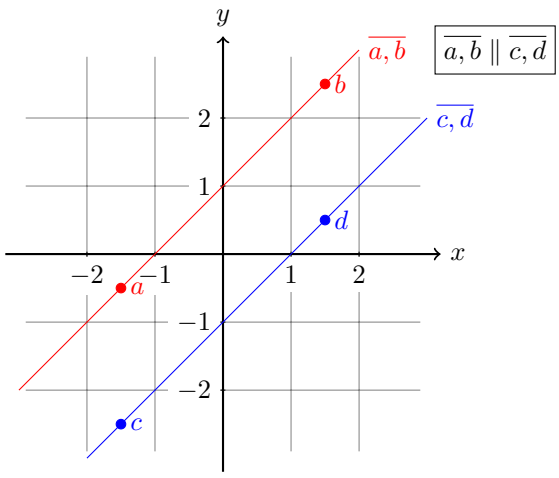



Abbildung 2: Parallelen in der euklidischen Ebene

Im wesentlichen Unterschied zu affinen Ebenen existieren in einer projektiven Ebene **keine Parallelen**.

**Beispiel 2.5.** *Die **Fano-Ebene** ist das Minimalmodell einer projektiven Ebene und umfasst genau 7 Punkte (beachte: auch der Kreis gilt hier als Gerade!). [4, Seite 9]*
*Bemerkenswert ist die Tatsache, dass durch Entfernen einer beliebigen Gerade und den daraufliegenden Punkten eine affine Ebene entsteht. Dies ist kein Spezialfall sondern funktioniert immer, was wir auch im Abschnitt 2.2.2 zeigen werden.*

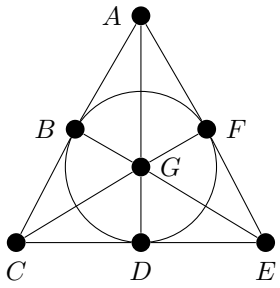



Abbildung 3: Fano-Ebene

### 2.2.1 Die projektive Ebene PG(2, $\mathbb{F}$)

Es sei $\mathbb{F}$ ein beliebiger Körper mit Nullelement 0 und $\mathbb{F}^3$ der dreidimensionale $\mathbb{F}$-Vektorraum mit Nullvektor $\mathbf{0}$. Wir definieren eine Äquivalenzrelation $\sim$ für alle $a, b \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$ wie folgt:

$$a \sim b :\Leftrightarrow \exists \lambda \in \mathbb{F} \setminus \{0\} : \lambda a = b$$

Für die Äquivalenzklassen von $a = (a_1, a_2, a_3) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$ schreiben wir $[a]$ oder auch $(a_1 : a_2 : a_3)$.

Weiters definieren wir die Menge aller Äquivalenzklassen als unsere Punktemenge:

$$\mathcal{P} \coloneqq \left\{[a] \mid a \in \mathbb{F}^3 \setminus \{\mathbf{0}\}\right\}$$

Für zwei verschiedene Punkte $P = [a] \in \mathcal{P}$ und $Q = [b] \in \mathcal{P}$ setzen wir die Verbindungsgerade zwischen $P$ und $Q$ fest mit:

$$\overline{P,Q} \coloneqq \left\{[\lambda a + \mu b] \mid \lambda, \mu \in \mathbb{F} \setminus \{0\}\right\}$$

Womit wir nun auch die Menge aller Geraden bilden können:

$$\mathcal{G} \coloneqq \{\overline{P,Q} \mid P, Q \in \mathcal{P} \wedge P \neq Q\}$$

### 2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

**Lemma 2.6.** *$\mathcal{P}_U$ und $\mathcal{G}_U$ definieren.*

# 3 Elliptische Kurven $E$

## 3.1 Die unendliche Gerade über PG(2, $\mathbb{F}$)

Um in 3.2 elliptische Kurven genau beschreiben zu können und in 3.3 eine affine Darstellung elliptischer Kurven herzuleiten, müssen wir $(\mathcal{P}, \mathcal{G})$ = PG(2, $\mathbb{F}$) nochmal betrachten. Wir wählen dazu eine Gerade $U \in \mathcal{G}$ aus. Prinzipiell kann dazu jede Gerade gewählt werden. Es ist jedoch von Vorteil eine bestimmte Gerade zu wählen um das Rechnen mit der Weierstraßgleichung(3.2) zu vereinfachen.

Dazu wählen wir die Verbindungsgerade $U = \overline{P,Q}$ der Punkte $P = (1 : 0 : 0)$ und $Q = (0 : 1 : 0)$, d.h. $U = \{(x : y : z) \in \mathcal{P} \mid z = 0\}$. Diese Menge $U$ bezeichnen wir im Folgenden als unendlich ferne Gerade. Im dreidimensionalen Raum ist das genau die $x, y$-Ebene mit $z = 0$.

**Lemma 3.1** (Isomorphismus von $\mathcal{P}_U$ und $\mathbb{F}^2$)**.** *Gegeben die projektive Ebene $(\mathcal{P}, \mathcal{G}) = PG(2, \mathbb{F})$ und die unendlich ferne Gerade $U$, dann ist die Abbildung*

$$\phi : \mathbb{F}^2 \to \mathcal{P}_U,\ (a, b) \mapsto (a : b : 1)$$

*bijektiv und bildet Geraden auf Geraden ab, d.h. $\phi$ ist ein Isomorphismus von affinen Ebenen.*

*Beweis.* Wie im Lemma 2.6 gezeigt wurde, erhält man eine affine Ebene, wenn man aus einer projektiven Ebene eine Gerade mitsamt allen ihren Punkten entfernt. Daraus folgt, dass es sich bei $(\mathcal{P}_U, \mathcal{G}_U)$ um eine affine Ebene handelt. Es sei $(a : b : c) \in \mathcal{P}_U$. Da gilt $(a : b : c) \notin U$, folgt $c \neq 0$. Das heißt $c^{-1}$ ist definiert, womit die Abbildung

$$\phi(ac^{-1}, bc^{-1}) = (ac^{-1} : bc^{-1} : 1) = (a : b : c)$$

surjektiv ist. Die Injektivität gilt auch, da mit $(a, b) \neq (a', b')$ die Vektoren $(a, b, 1)$ und $(a', b', 1)$ linear unabhängig sind, womit $(a : b : 1) \neq (a' : b' : 1)$ folgt.

Jede Gerade in $\mathbb{F}^2$ ist von der Form $\overline{a,b} = \{a + \lambda b \mid \lambda \in \mathbb{F} \wedge a, b \in \mathbb{F}^2 \wedge b \neq (0,0)\}$. Für einen Punkt $P = a + \lambda b \in \overline{a,b}$ gilt dann:

$$\begin{aligned}\phi(a + \lambda b) &= (a_1 + \lambda b_1 : a_2 + \lambda b_2 : 1) = (a_1 : a_2 : 1) + \lambda(b_1 : b_2 : 0) \\ &\sim \mu(a_1 : a_2 : 1) + \mu\lambda(b_1 : b_2 : 0)\end{aligned}$$

Hierbei ist zu beachten, dass $\mu \in \mathbb{F} \setminus \{0\}$ laut Definition der Äquivalenzrelation $\sim$ gilt. Man betrachte nun die Gerade

$$G \coloneqq \{u(a_1 : a_2 : 1) + v(b_1 : b_2 : 0) \mid (u, v) \in \mathbb{F}^2 \setminus \{(0,0)\}\}.$$

Alle Punkte der Bildmenge von $\phi$ liegen auf der Gerade $G$. Es wird nur ein Punkt nicht erreicht, nämlich der Punkt $R = (b_1 : b_2 : 0)$. Wie man sehen kann, gilt $G \cap U = R$. Es folgt $\phi(\overline{a,b}) = G \cap \mathcal{P}_U \in \mathcal{G}_U$. □

Insgesamt kann man sehen, dass man affine Geraden auf eine Teilmenge der projektiven Geraden abbilden kann. Außerdem bekommen diese affinen Geraden im Projektiven dann einen Schnittpunkt, der auf der unendlich fernen Gerade $U$ liegt.

## 3.2 Definiton elliptischer Kurven

Wir haben bereits die projektive Ebene PG(2, $\mathbb{F}$) über beliebige Körper $\mathbb{F}$ eingeführt.
Diese hat die folgende Punktemenge:

$$P = \{(u : v : w) \mid (u, v, w) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}\}$$

Nun wollen wir die Punktemenge $E$ der elliptischen Kurve einführen, welche eine Teilmenge der Punktemenge $\mathcal{P}$ ist, d.h. $E \subseteq \mathcal{P}$. Dazu benötigen wir Polynome in drei Unbekannten. Der Polynomring mit drei Unbekannten über $\mathbb{F}$ ist mit

$$\mathbb{F}[X, Y, Z] = \left\{ \sum_{k,l,m \geq 0} a_{k,l,m} X^k Y^l Z^m \mid a_{k,l,m} \in \mathbb{F} \right\}$$

definiert. $F(X, Y, Z) = \sum_{k,l,m \geq 0} a_{k,l,m} X^k Y^l Z^m \in \mathbb{F}[X, Y, Z]$ wird Polynom genannt.

**Definition 3.2** (Elliptische Kurve)**.** Eine elliptische Kurve $E$ ist durch die Lösung der Weierstraß-Gleichung

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

gegeben, wobei $a_i \in \mathbb{F}$ gilt und die Lösung keine Singularitäten besitzen darf. [8, Seite 54] Da der zugrundeliegende Raum PG(2, $\mathbb{F}$) eine projektive Ebene ist, handelt es sich um eine projektive Kurve. Wenn man die Gleichung als Polynom

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

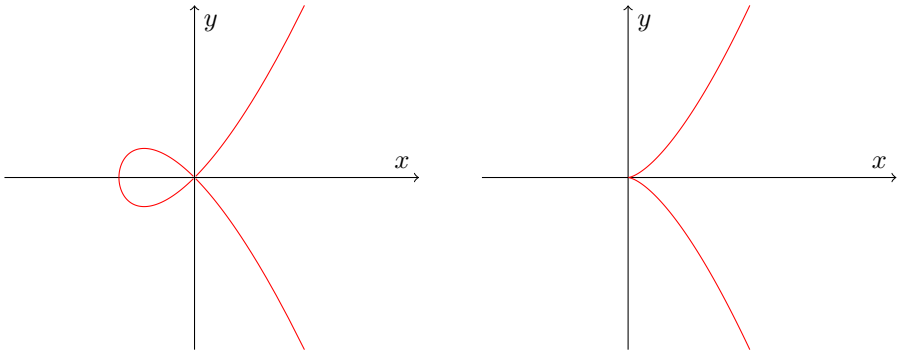
schreibt, dann ist $E$ genau die Nullstellenmenge des Polynoms $F$. Bemerkenswert ist hier, dass es sich um ein homogenes Polynom vom Grad 3 handelt, d.h. für jedes Summenglied $a_{k,l,m}X^kY^lZ^m$ mit $a_{k,l,m} \neq 0$ gilt $k + l + m = 3$.

**Definition 3.3** (Singularitäten)**.** Eine Kurve $E$ ist singulär in einem Punkt $P = (a : b : c) \in E$, wenn gilt

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$$

Man sagt auch, dass die partiellen Ableitungen des Polynoms $F$ im Punkt $P$ verschwinden. Falls die elliptische Kurve $E$ in keinem Punkt singulär ist, dann bezeichnet man sie als nicht-singulär. [3, Seite 227]

**Beispiel 3.4** (Singularitäten)**.** *Die folgenden Kurven sind jeweils in einem Punkt singulär. Damit gibt es mehrere Tangenten an diesen Punkt.*




(a) $y^2 = x^3 + x^2$ (b) $y^2 = x^3$

Abbildung 4: Kurven mit Singularitäten (Knoten und Spitze)

Wir hatten eine elliptische Kurve $E$ als Nullstellenmenge des Polynoms $F(X, Y, Z)$ mit $E \coloneqq \{(u : v : w) \in \mathcal{P} \mid F(u, v, w) = 0\}$ definiert. ¡¡¡¡¡¡¡ HEAD Jedoch handelt es sich bei Punkten in der projektiven Ebene und damit auch bei den Elementen von $E$ um Äquivalenzklassen. Deswegen müssen wir noch die Wohldefiniertheit der Nullstellen begründen. Wir rufen uns dazu noch einmal die Definition der Äquivalenzrelation $\sim$ ins Gedächtnis:

$$(u : v : w) \sim (u' : v' : w') \Leftrightarrow \exists \lambda \in \mathbb{F} \setminus \{0\} : (u, v, w) = \lambda(u', v', w')$$

Wir setzen ein:

$$F(u', v', w') = F(\lambda u, \lambda v, \lambda w) = \lambda^3 F(u, v, w).$$

Die zweite Äquivalenz folgt aus der Homogenität des Polynoms. Daraus folgt, dass die Nullstellen von $F$ in $\mathcal{P}$ wohldefiniert sind:

$$F(u, v, w) = 0 \Leftrightarrow F(\lambda u, \lambda v, \lambda w) = 0.$$

Wir wollen nun noch eine Einschränkung treffen; die Charakteristik des Körpers $\mathbb{F}$ soll nicht 2 und nicht 3 sein. Wir schreiben $char\, \mathbb{F} \neq 2$ bzw. $char\, \mathbb{F} \neq 3$. Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, oder anders gesagt: Wenn wir das neutrale Element der Multiplikation 2 bzw. 3 mal addieren, dann erhalten wir nicht das neutrale Element der Addition, welches kein multiplikatives Inverses hat. Dadurch wird die Allgemeinheit für den Fall, dass $\mathbb{F}$ eine dieser Charakteristiken hat, eingeschränkt.

Wir können jetzt die Weierstraßgleichung(3.2), welche die Form

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

hat, umformen. Zuerst können wir, wenn $char\,\mathbb{F} \neq 2$ gilt, den Term $XYZ$ mit folgendem Variablenwechsel eliminieren:

$$X' = X,\ Y' = Y + \frac{a_1}{2}X,\ Z' = Z$$

Anschließen könnnen wir auch noch die Terme $X^2$ und $Y$ eliminieren, falls $char\,\mathbb{F} \neq 2, 3$ gilt:

$$X' = X + \frac{a_2}{3},\ Y' = Y + \frac{a_3}{2},\ Z' = Z$$

Damit lautet das Ergebnis

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{1}$$

## 3.3 Affine Darstellung elliptischer Kurven

Wir wollen eine affine Darstellung herleiten. Dazu zeigen wir zunächst, dass nur ein Punkt der unendlich fernen Gerade $U$, nämlich der Punkt $\mathcal{O} = (0 : 1 : 0)$, auf $E$ liegt. Für $P \in U$ gilt $P = (u : v : 0)$ mit $u, v \in \mathbb{F}$. Es gibt drei Möglichkeiten Punkte zu erzeugen, die 0 als Z-Koordinate haben: $P = (1 : 0 : 0)$, $Q = (u : v : 0)$ mit $u, v \in \mathbb{F} \setminus 0$ und $\mathcal{O} = (0 : 1 : 0)$. Wenn wir diese Punkte in die Gleichung 1 einsetzen, dann löst nur $\mathcal{O}$ die Gleichung.
Für jeden Punkt $P \in E$ mit $P \neq \mathcal{O}$ gilt also $P \in \mathcal{P}_U$. Aufgrund der Äquivalenzrelation $\sim$ können wir ohne Einschränkung der Allgemeinheit annehmen, dass $P \in \{(u : v : 1) \mid u, v \in \mathbb{F}\}$. Wenn wir also nur diese Punkte betrachten können wir die Gleichung 1 vereinfachen und erhalten die affine Gleichung $y^2 = x^3 + ax + b$ oder als Polynom:

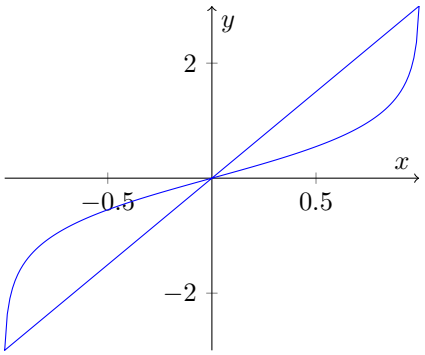
$$f(x, y) \coloneqq y^2 - x^3 - ax - b \tag{2}$$

Wir wissen aus Lemma 2.6, dass $\mathcal{P}_U$ genau die Punktemenge einer affinen Ebene ist. Wenn wir zusätzlich die Abbildung $\phi$ aus Lemma 3.1 auf $\mathcal{P}_U$ anwenden, dann zerfällt die Punktemenge der elliptischen Kurve $E$ in zwei Teilmengen, einen affinen Teil und den unendlichen Punkt $\mathcal{O}$:

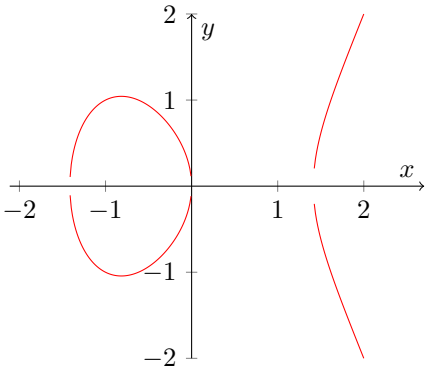
$$E = \big\{(u : v : 1) \mid (u, v) \in \mathbb{F}^2 \wedge f(u, v) = 0\big\} \cup \{\mathcal{O}\}$$

Wir können im Anschluss nur den affinen Teil betrachten, wenn wir den Punkt $\mathcal{O}$ nicht außer Acht lassen.

**Beispiel 3.5.** *Skizzen elliptischer Kurven über dem Körper* $\mathbb{R}$




(a) $y^2 = x^3 + 0.3x + 2$




(b) $y^2 = x^3$

# 4 Eine Gruppe über $E$

Macht Kevin bis 4.3

## 4.1 Tangenten elliptischer Kurven

## 4.2 Schnittpunkte von Geraden mit elliptischen Kurven

Unendlich ferne Gerade mit Schnittpunkt $\mathcal{O}$, Affine Geraden, Parallele zur y-Achse

## 4.3 Die Schnittpunkt-Verknüpfung $\oplus$ über $E$

Definition, Beweis der Abgeschlossenheit, graphische Interpretation

## 4.4 Die Gruppe $(E, +)$

Macht Lukas bis fertig
Gruppe ist abelsch mit neutralem Element $\mathcal{O}$, Beispiel

# 5 Anwendung elliptischer Kurven in der Kryptologie

## 5.1 ElGamal

Welche Charakteristiken für elliptische Kurven, Domänenparameter

## 5.2 Noch einen für Signaturen

Welche Charakteristiken für elliptische Kurven, Domänenparameter

# Literaturverzeichnis


[1] Elliptische Kurven (Elliptic Curve Cryptography - ECC). https://www.a-sit.at/de/technologiebeobachtung/ecc_curves/index.php. Abgerufen am 15.04.2016.

[2] Elaine Barker. Recommendation for Key Management. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, 2016. Abgerufen am 15.04.2016.

[3] Hubert Kiechle Christian Karpfinger. *Kryptologie: Algebraische Methoden und Algorithmen*. 2010.

[4] Schirin Gratzer. Diskrete Geometrien. http://www.uni-graz.at/~baurk/lehre/WS2014-LAK-Seminar/4_Gratzer.pdf, 2014. Abgerufen am 23.04.2016.

[5] Hans-Wolfgang Henn. Elementare Geometrie und Algebra, 2003.

[6] Neal Koblitz. Elliptic curve cryptosystems, 1987.

[7] Victor S. Miller. Use of elliptic curves in cryptography, 1985.

[8] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[9] Zdeněk Říha. Electronic passports. https://web.archive.org/web/20100215182600/http://www.buslab.org/SummerSchool2008/slides/Zdenek_Riha.pdf. Archiviert vom Original, abgerufen am 15.04.2016.