Elliptische Kurven (Teil 1)
Eine Einführung

Ausarbeitung zum Seminarvortrag vom 20.01.2011

Delf Lachmund
Universität Bremen

WS 2010/2011

Inhaltsverzeichnis

1 Vorwort

In der folgenden Ausarbeitung zu meinem Seminarvortrag vom 20.01.2011 möchte ich eine Einführung in das Gebiet der Elliptischen Kurven geben. Die Präsentation gliederte sich ein in eine Vortragsreihe „Faktorisierung und diskreter Logarithmus“. Sie lieferte Hintergrundwissen für die Folgevorträge über Faktorisierung und das diskrete Logarithmusproblem auf Elliptischen Kurven.

Das Gebiet der Elliptischen Kurven ist mitunter Gegenstand ein- oder zweisemestriger Vorlesungen. In einem zweistündigen Vortrag muss also rigoros gekürzt werden. Ziel ist es, grundlegende Definitionen zu nennen sowie einen Einblick in die wichtigsten strukturellen Resultate zu geben. Es wurde Wert auf Struktur gelegt und für den Leser, der sich noch nicht mit Elliptischen Kurven beschäftigt hat, wird der Einstieg zusätzlich mit Beispielen erleichtert.

2 Definition von Elliptischen Kurven

2.1 Definition

Eine Elliptische Kurve E ist der Graph, d.h. die Menge aller geordneten Lösungspaare (x, y), einer Gleichung der Form

$$y^2 = x^3 + Ax + B, \qquad \text{(Weierstrass-Gleichung)} \tag{1}$$

mit A, B (gegeben), x, y (variabel) $\in K$, K Körper[1].

2.2 Bemerkung

Für K werden im wesentlichen die Körper $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{F}_q$ mit $q = p^k$ betrachtet. Zur Vermeidung von mehrfachen Nullstellen wird zudem für die Koeffizienten

$$4A^3 + 27B^2 \neq 0 \tag{2}$$

gefordert[2].

[1] für die *verallgemeinerte Weierstrass-Gleichung* und die resultierende Addition vgl. [Coh] S.268ff.

[2] vgl [Was] S.9f.

Über $\mathbb{R}$ lassen sich Elliptische Kurven graphisch gut veranschaulichen.

2.3 Beispiel

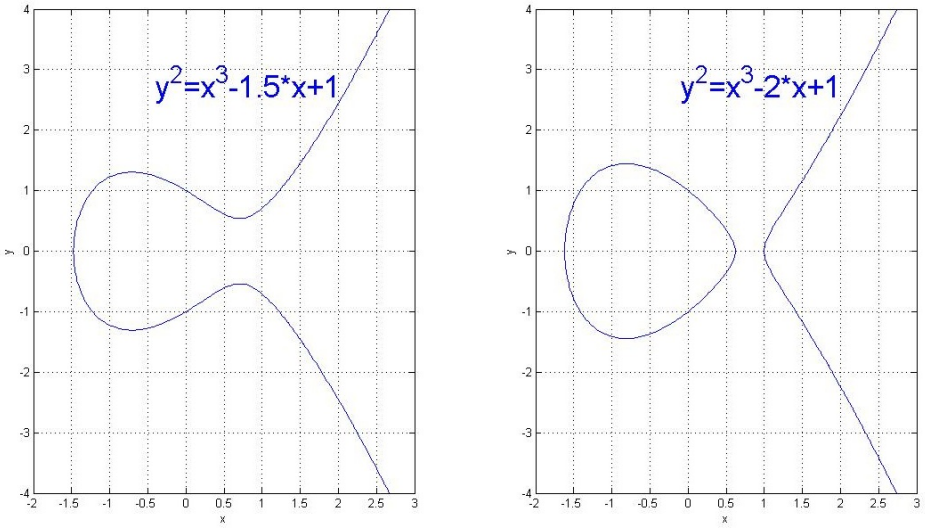

Abbildung 1: Beispiele von Elliptischen Kurven über $\mathbb{R}$

3 Elliptische Kurven als Gruppen

3.1 Addition (Geometrische Definition)

Es wird im Folgenden für eine Elliptische Kurve E über $\mathbb{R}$ eine Addition geometrisch definiert[3]. Für $P_1,\ P_2 \in E$ erhält man $P_3{:=}P_1 + P_2$ durch:

- Legen einer Geraden durch P_1 und P_2, die E in einem weiteren Punkt P_3' schneidet,
- anschließendes Spiegeln des Punktes P_3' an der x-Achse.

3.2 Bemerkung

Über die Betrachtung der elementarsymmetrischen Polynome dritten Grades bzw. einfaches Ausmultiziplieren von Klammern verifiziert man leicht die

[3] vgl hier und im Folgenden [Was] S.12ff.

folgende Beziehung:

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc.$$

3.3 Beispiel

Sei beispielsweise die Kurve E mit $A = 2$, $B = 1$ über dem Körper $\mathbb{R}$ gegeben, also $E : y^2 = x^3 + 2x + 1$. Seien zudem die Punkte $P_1 = (1, 2)$ und $P_2 = (8, 23)$ definiert. Es sind $P_1, P_2 \in E$, wie man durch Einsetzen überprüfen kann.

Das Ziel ist die Ermittlung des Punktes $P_3 := P_1 + P_2$ mit der Addition aus (3.1). Die Gerade $g_{P_1P_2}$ durch die beiden Punkte P_1 und P_2 ist gegeben durch die Geradengleichung $y = 3x - 1$.

Schneidet man nun g mit E, müssen die Schnittpunkte beide Gleichungen erfüllen. Setzt man die Geradengleichung in die Kurvengleichung ein, so erhält man die möglichen Werte für x:

$$\begin{aligned} g \cap E : \qquad (3x-1)^2 &= x^3 + 2x + 1 \\ 9x^2 - 6x + 1 &= x^3 + 2x + 1 \\ 0 &= x^3 - 9x^2 + 8x. \end{aligned}$$

Zwei Nullstellen (nämlich $x_1 = 1$ und $x_2 = 8$) kennen wir bereits nach Konstruktion. Die dritte ergibt sich in diesem speziellen Fall entweder durch Draufschauen (das absolute Glied verschwindet, also lässt sich x ausklammern, mit anderen Worten: $x_3 = 0$) oder - was immer möglich ist - mithilfe von Bemerkung (3.2):

Die Summe der drei Nullstellen entspricht dem negativen quadratischen Vorfaktor, also gilt weiter:

$$x_1 + x_2 + x_3 = 1 + 8 + x_3 = 9 \Rightarrow x_3 = 0, \quad \text{sowie} \quad y_3 = 3x_3 - 1 = -1,$$

Spiegeln an der x-Achse ergibt: $\Rightarrow P_3 = P_1 + P_2 = (1, 2) + (2, 8) = (0, 1).$

3.4 Veranschaulichung

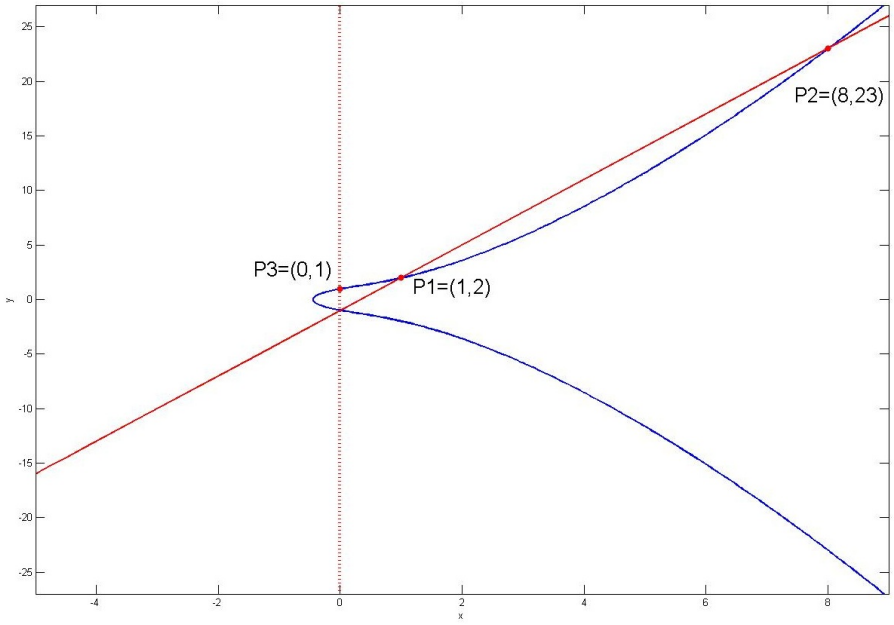

Abbildung 2: Veranschaulichung der Addition

3.5 Satz

Zusammen mit einem weiteren Element - bezeichnet mit „∞“ - bildet $(E, +)$ eine *abelsche Gruppe* mit der Addition aus (3.1).[4]

3.6 Addition (Algebraische Definition)

Es seien erneut die Bezeichnungen $P_k = (x_k, y_k)$, $k = 1, 2, 3$, $P_3 := P_1 + P_2$ gewählt.

In Übereinstimmung mit der vorherigen geometrischen Motivation ergibt sich

[4]Es soll zum Verständnis hier ausreichen, dass man zusätzlich ein neutrales Element benötigt, welches man künstlich einführt und einfach mit ∞ bezeichnet. Den Sinn der Bezeichnung samt einer tiefergehenden Erklärung mithilfe der projektiven Ebene findet man in [Was] S. 18ff.

für Elliptische Kurven (über beliebigen Körpern K) die folgende Addition[5]:

$a)$ $x_1 \neq x_2 \Rightarrow \boxed{P_3 = \left(m^2 - x_1 - x_2, m(x_1 - x_3) - y_1\right), \text{mit } m = \frac{y_2 - y_1}{x_2 - x_1},}$

$b)$ $x_1 = x_2, y_1 \neq y_2 \Rightarrow P_1 + P_2 = \infty$

$c)$ $P_1 = P_2, y_1 \neq 0 \Rightarrow \boxed{P_3 = \left(m^2 - 2x_1, m(x_1 - x_3) - y_1\right), \text{mit } m = \frac{3x_1^2 + A}{2y_1},}$

$d)$ $P_1 = P_2, y_1 = 0 \Rightarrow P_1 + P_2 = \infty,$

$e)$ $P + \infty = P, \ \forall P \in E.$

Die beiden wichtigen Fälle sind umrahmt. In Analogie zum reellen Fall lässt sich die Steigung bei $c)$ analytisch mithilfe von impliziter Differentiation herleiten.

3.7 Bemerkung: Graphische Spezialfälle

- Zu $c)$ und $d)$: Bei Elliptischen Kurven über $\mathbb{R}$ bedeutet $P_1 = P_2$, dass die Gerade tangential am Punkt anliegend gewählt wird.
- Zu $b)$: Falls P_2 der zu P_1 gespiegelte Punkt ist, verläuft die Gerade vertikal: dann ist $P_3 = \infty$. Mit anderen Worten: In $(E, +)$ gilt: $-(x_1, y_1) = (x_1, -y_1)$.

3.8 Bemerkung zum Beweis von Satz (3.5)

- Kommutativität: ist aus beiden Definitionen sofort ersichtlich; graphisch einfach wegen $g_{P_1P_2} \equiv g_{P_2P_1}$,
- Neutrales Element: ist per Definition „∞“,
- Inverses Element: $-P$ ist gespiegeltes P (vgl. Bemerkung (3.7)),
- Assoziativität: Sie ist das Überraschende und besonders Wertvolle an der definierten Addition. Der Beweis wird durch die nötigen Fallunterscheidungen sehr länglich[6].

[5] vgl. [Was] S.14

[6] Für einen möglichen Beweis vgl. z.B. [Was] S. 20ff.

3.9 Skalare Multiplikation

Für die Rechnerimplementation ist es wichtig zu bemerken, dass

$$k \cdot P = P + P + \cdots + P \text{ (k Summanden)}$$

deutlich schneller durch schrittweises Verdoppeln berechnet werden kann. Beispielsweise sind für die Berechnung von

$$1.048.577P = (2^{20} + 1)P = 2 \cdot (2 \cdot (\cdots (2 \cdot P) \cdots)) + P$$

statt 1.048.576 Additionen nur 21 auszuführen.[7]

Es sei weiterhin angemerkt, dass bei $E(\mathbb{Q})$ die Stellenzahl im Zähler und Nenner der Koordinaten sehr schnell zunimmt, sodass hier eine Berechnung wieder problematisch wird. Dies ist bei $E(\mathbb{F}_p)$ kein Problem, da man schrittweise (mod p) rechnen kann.

4 Strukturelle Resultate

4.1 Überblick

Über die evtl. je nach (A, B) variierende Gruppenstruktur einer Elliptischen Kurve über einem Körper K lassen sich für die verschiedenen Körper K wichtige Isomorphien beweisen:

- K endlich: dann ist $E(K)$ stets eine endliche abelsche Gruppe,
- $K = \mathbb{Q}$: vgl. Mordell-Weil-Theorem (4.2),
- $K = \mathbb{R}$: dann ist $E = E(\mathbb{R}) \cong S^1$ oder $E(\mathbb{R}) \cong S^1 \oplus \mathbb{Z}_2$,
- $K = \mathbb{C}$: dann ist $E(\mathbb{C}) \cong \mathbb{R}^2/\mathbb{Z}^2 \cong$ (flacher) Torus.

In den folgenden beiden Unterkapiteln beschäftigen wir uns kurz mit den beiden Fällen $K = \mathbb{Q}$ und $K = \mathbb{F}_q$.

[7] Natürlich muss man den entsprechenden Faktor vorher binär entwickeln. Für genauere Informationen zu verwendeten Verfahren vgl. [Hof] S.292ff.; ein Pseudo-Code samt Beispielen findet sich in [Coh] S.271f.

4.2 Mordell-Weil-Theorem

4.2.1 Theorem

Sei E eine Elliptische Kurve über $\mathbb{Q}$. Dann ist $E(\mathbb{Q})$ eine endlich erzeugte abelsche Gruppe[8].

4.2.2 Bemerkung

Endliche abelsche Gruppen sind isomorph zu Gruppen der Form

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s},$$

wobei $n_i | n_{i+1}$ für $i = 1, 2, ..., s-1$. [9]

Eine Gruppe G heißt endlich erzeugte abelsche Gruppe, falls es eine endliche Teilmenge $\{g_1, g_2, \ldots, g_k\} \subset G$ gibt, sodass jedes Element $h \in G$ (nicht notwendigerweise eindeutig) in der Form

$$h = \sum_{i=1}^{k} m_i g_i \ , \quad \text{mit } m_i \in \mathbb{Z}$$

dargestellt werden kann.

Man kann weiterhin zeigen, dass eine endlich erzeugte abelsche Gruppe isomorph zu einer Gruppe der Form

$$\mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s},$$

mit $r \geq 0$ und $n_i | n_{i+1}$ für $i = 1, 2, ..., s-1$ ist. Die Untergruppe $T \leq G$ mit $T \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ wird dabei als Torsionsuntergruppe (sie ist isomorph zur Untergruppe der Elemente endlicher Ordnung in G) und r als Rang bezeichnet.

Die Gestalt von T und die Größe von r bei einer gegebenen Elliptischen Kurve E kann man (teilweise sehr aufwändig) berechnen. Man vermutet, dass es Elliptische Kurven von beliebig großem Rang r gibt. Trotzdem kennt man bisher erst Beispiele mit $r \lesssim 28$. [10]

[8] Ein Beweis findet sich beispielsweise in [Was] S. 206ff.

[9] vgl. hier und im Folgenden [Was] S. 404ff.

[10] vgl. [Elk]; zur Erklärung des Ungefährzeichens: im entsprechenden Beispiel wird nicht der exakte Rang bestimmt, sondern lediglich $r \geq 28$ gezeigt; ein Rang größer als 28

4.3 Elliptische Kurven über endlichen Körpern

Sei im Folgenden E eine Elliptische Kurve über $\mathbb{F}_q$, $q = p^n$, p prim. Wichtige Fragen sind: Welche und wieviele Elemente enthält $E(\mathbb{F}_q)$?

Eine Möglichkeit, für kleine q die Elemente herauszufinden, ist es, eine Liste der möglichen Werte für x sowie von $x^3 + x + 1 \pmod q$ und der zugehörigen Quadratwurzeln y zu erstellen. Dazu betrachten wir das folgende Beispiel.

4.3.1 Beispiel

Sei E die Elliptische Kurve $E: \ y^2 = x^3 + x + 1$ über $\mathbb{F}_5$. [11]

Liste möglicher Punkte:

x	$x^3 + x + 1 \pmod 5$	y	Punkte
0	1	± 1	(0,1), (0,4)
1	3	/	/
2	1	± 1	(2,1), (2,4)
3	1	± 1	(3,1), (3,4)
4	4	± 2	(4,2), (4,3)
∞		∞	∞

Also hat die gegebene Elliptische Kurve $E(\mathbb{F}_5)$ die Ordnung 9.

Zur generellen Gruppenstruktur von Elliptischen Kurven über endlichen Körpern hat man das folgende Theorem.

4.3.2 Theorem

Sei E eine Elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Dann ist $E(\mathbb{F}_q) \cong \mathbb{Z}_n$ oder $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, mit $n_1 | n_2$. [12]

4.3.3 Hasse-Theorem

Sei E eine Elliptische Kurve über $\mathbb{F}_q$. Dann erfüllt die Gruppenordnung von $E(\mathbb{F}_q)$ folgende Ungleichung[13]:

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

erscheint natürlich unwahrscheinlich

[11] vgl. [Was] S.89f.

[12] Ein Beweis findet sich in [Was] S.91 zusammen mit S.75f.

[13] Für einen Beweis vgl. [Was] S.91 und 92ff.

4.3.4 Bemerkung

Sei $P \in E(\mathbb{F}_q)$. Die Ordnung von P ist die kleinste positive ganze Zahl k, sodass $kP = \infty$. Mit anderen Worten: Nach dem Satz von Lagrange ist das Erzeugnis $< P > \leq E$ eine Untergruppe und $\# < P > | \#E$.
Zusammen mit Hasses Theorem kann man bei Kenntnis eines Punktes großer Ordnung häufig die Ordnung der Elliptischen Kurve E selbst schnell herausfinden. Vergleiche dazu das folgende Beispiel[14].

4.3.5 Beispiel

Sei E die Kurve $y^2 = x^3 + 7x + 1$ über $\mathbb{F}_{101}$. Man kann zeigen, dass der Punkt $(0, 1)$ die Ordnung 116 hat. Also ist $\#E(\mathbb{F}_{101})$ Vielfaches von 116. Nach Hasse gilt zudem:

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

also

$$\begin{aligned} & 101 + 1 - 2\sqrt{101} \leq && \#E(\mathbb{F}_{101}) \leq && 101 + 1 + 2\sqrt{101} \\ \Rightarrow \quad & 82 \leq && \#E(\mathbb{F}_{101}) \leq && 122. \end{aligned}$$

Also folgt insgesamt $\#E(\mathbb{F}_{101}) = 116$, und $E(\mathbb{F}_{101})$ ist zyklisch und wird (u.a.) von dem Element $(0, 1)$ erzeugt.

[14] vgl. [Was] S.101

Literatur

[Coh] Cohen, Frey et al.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics and its Applications, Boca Ration (Florida) 2006, Chapman & Hall/CRC

[Elk] Elkies, Noam D.: Three lectures on elliptic surfaces and curves of high rank, September 2007, `http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.2908v1.pdf`

[Hof] Hoffstein, Pipher, Silverman: An Introduction to Mathematical Cryptography. Undergraduate Texts in Mathematics, New York 2008, Springer

[Was] Washington, Lawrence C.: Elliptic Curves. Number Theory and Cryptography, Boca Raton (Florida) 2003, Chapman & Hall/CRC

Abbildungsverzeichnis

Anmerkung: Beide Abbildungen wurden mit Matlab R2007b selbst erstellt.