

2. Februar 2006

Gruppenstrukturen auf elliptischen Kurven

Vortrag im Rahmen des Seminars *Geometrie algebraischer Kurven*
von Prof. Dr. Victor Pidstrygach im Wintersemester 2005/2006

Christian Bick

bick@math.uni-goettingen.de

<http://math.hlla.net>

Inhaltsverzeichnis

1 Gruppenstruktur auf Kubiken	3
1.1 Kubiken in Normalform	3
1.2 Definition einer Gruppenstruktur	4
2 Das Additionstheorem der \wp-Funktion	8
2.1 Wiederholung: Der Torus als nichtsinguläre Kubik	8
2.2 Das Abelsche Theorem	9
2.3 Das Additionstheorem und Gruppenstrukturen	11
3 Anwendungen in der Kryptographie	15
3.1 Einführung in die Kryptographie	15
3.2 Funktionsweise von ECC	16
3.3 Sicherheit von ECC	17
Literatur	19

1 Gruppenstruktur auf Kubiken

Im ersten Abschnitt wollen wir rein geometrisch Gruppenstrukturen auf einer regulären Kubik definieren und diese studieren.

1.1 Kubiken in Normalform

Definition 1.1

Sei K ein Körper mit $\text{char}(K) \neq 2, 3$ und $g_2, g_3 \in K$. Eine Kubik hat Weierstrass Normalform, wenn sie in der Form

$$y^2 = 4x^3 - g_2x - g_3$$

gegeben ist. Gilt zusätzlich $g_2^3 - 27g_3^2 \neq 0$, dann heißt diese Kubik elliptisch. Weiter bezeichne

$$\tilde{X}(g_2, g_3; K) := \{(x, y) \in K^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$$

die elliptische Kurve zu g_2, g_3 .

Bemerkung 1.2

1. Die Bedingung $g_2^3 - 27g_3^2 \neq 0$ sorgt dafür, dass die Nullstellen paarweise verschieden sind, also dass die Kubik regulär ist und in jedem Punkt eine wohldefinierte Tangente hat.
2. Man kann zeigen, dass unter den obigen Voraussetzungen an den Körper und die Kurve sich jede Kubik der allgemeinen Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

durch eine birationale Transformation auf Weierstrass-Normalform bringen lässt. Dieses kann man nachrechnen, eine Andeutung dazu findet man in [7, S. 22].

Vereinbarung

Im Folgenden sei immer $g_2^3 - 27g_3^2 \neq 0$ vorausgesetzt.

Bemerkung 1.3

Sei $f(x_1, x_2) = 4x_1^3 - g_2x_1 - g_3 - x_2^2 \in \mathbb{C}[x_1, x_2]$ und $V(f)$ die Nullstellenmenge von f in $\mathbb{A}^2(\mathbb{C})$. Sei weiter $F(x_0, x_1, x_2) = 4x_1^3 - g_2x_1x_0^2 - g_3x_0^3 - x_2^2x_0$ die durch die Inklusion

$$i : \begin{array}{ccc} \mathbb{A}^2(\mathbb{C}) & \longrightarrow & \mathbb{C}P^2 \\ (x_1, x_2) & \longmapsto & [1 : x_1 : x_2] \end{array}$$

gegebene Homogenisierung von f und $V(F)$ deren Nullstellenmenge in $\mathbb{C}P^2$. Dann gilt

$$V(F) \setminus i(V(f)) = \{[0 : 0 : 1]\},$$

das heißt, dass der unendlich ferne Teil der projektiven Kurve aus genau einem Punkt besteht.

Beweis

Betrachte $V(F)$, also die Lösungen von

$$x_0x_2^2 = x_1^3 - g_2x_1x_0^2 - g_3x_0^3$$

im bezüglich i unendlich fernen Teil, das heißt $x_0 = 0$.

Daraus folgt $x_1 = 0$ und x_2 beliebig. In $\mathbb{C}P^2$ sind allerdings alle diese Punkte äquivalent, also ist für $x_0 = 0$ nur $\infty := [0 : 0 : 1] \in V(F)$. □

1.2 Definition einer Gruppenstruktur

Definition 1.4

Wähle einen Punkt $\mathcal{O} \in \tilde{X}(g_2, g_3; K)$.

Seien $P, Q \in \tilde{X}(g_2, g_3; K)$. $P * Q$ bezeichne den dritten Schnittpunkt der Geraden durch P und Q und der Kurve, mit Vielfachheiten gerechnet. Insbesondere ist $P * P$ gegeben durch den Schnittpunkt der Tangente an P mit der Kurve. Beachte, dass $P * Q = \infty$ zugelassen ist.

Wir definieren folgende Verknüpfung:

$$\begin{aligned} + : \tilde{X}(g_2, g_3; K) \times \tilde{X}(g_2, g_3; K) &\longrightarrow \tilde{X}(g_2, g_3; K) \\ (P, Q) &\longmapsto P + Q := \mathcal{O} * (P * Q) \end{aligned}$$

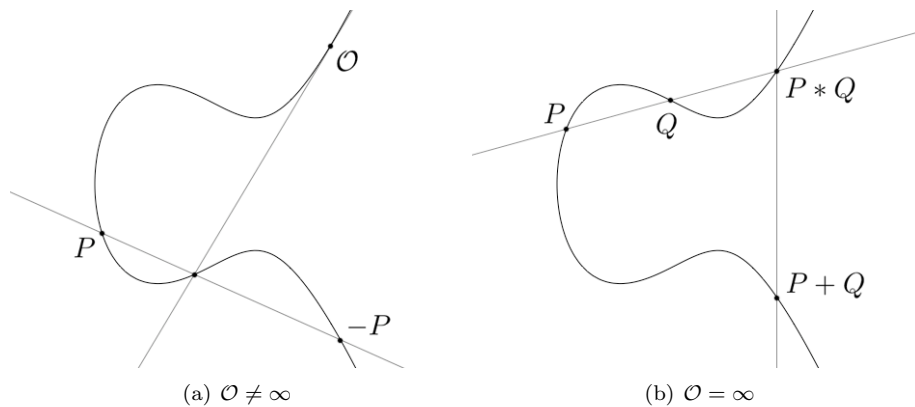


Abbildung 1: Additionen auf der Kubik im Reellen

Satz 1.5

$(\tilde{X}(g_2, g_3; K), +)$ ist eine abelsche Gruppe.

Beweis

Der Beweis soll an dieser Stelle nicht komplett formal durchgeführt werden, eine ausführlichere Argumentation ist in [7, S. 17-20] zu finden, denn anhand der Abbildungen ist das Meiste intuitiv erschließbar. Seien $P, Q, R \in \tilde{X}(g_2, g_3; K)$.

Die Kommutativität ist offensichtlich, denn es macht keinen Unterschied, ob die verbindende Gerade durch P, Q oder Q, P aufgespannt wird.

Für die Assoziativität genügt es zu zeigen, dass $(P + Q) * R = P * (Q + R)$. Die Assoziativität für den Fall $\mathcal{O} = \infty$ verdeutlicht die nachfolgende Zeichnung.

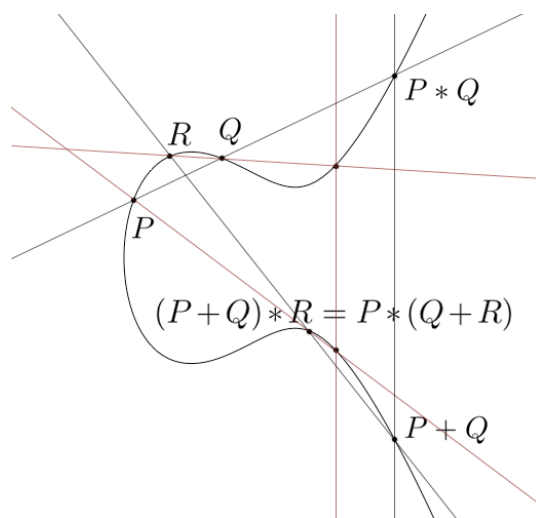


Abbildung 2: Assoziativität für $\mathcal{O} = \infty$ im Reellen

\mathcal{O} ist das neutrale Element, denn $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = P$, das inverse Element von P ist $-P = (\mathcal{O} * \mathcal{O}) * P$ (siehe Abbildung 1(a)).

□

Bemerkung 1.6

Die Wahl von \mathcal{O} ist unerheblich, denn

$$\varphi_{\mathcal{O}'} : P \mapsto P + (\mathcal{O}' - \mathcal{O})$$

liefert eine Bijektion von der Gruppe auf der Kurve mit neutralem Element \mathcal{O} zu der mit neutralem Element \mathcal{O}' durch Translation mit $\mathcal{O}' - \mathcal{O}$.

Beispiel 1.7

Sei $K = \mathbb{R}$ und $\mathcal{O} := [0 : 0 : 1] =: \infty$ in homogenen Koordinaten. Sei $P = (x, y)$ endlich. Dann ist $-P = (x, -y)$.

Beweis: Wir wollen zunächst die Tangente durch \mathcal{O} berechnen. Dazu gehen wir zu homogenen Koordinaten über und berechnen den Gradienten von

$$f(x_0, x_1, x_2) = x_1^3 - g_2 x_1 x_0^2 - g_3 x_0^3 - x_0 x_2^2.$$

Die Tangente im Punkt $[0 : 0 : 1]$ ist gegeben durch

$$\begin{aligned} 0 = t(x_0, x_1, x_2) &= \left(\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2} \right) \Big|_{[0:0:1]} \begin{pmatrix} x_0 \\ x_1 \\ x_2 - 1 \end{pmatrix} \\ &= (-1, 0, 0) \begin{pmatrix} x_0 \\ x_1 \\ x_2 - 1 \end{pmatrix} = -x_0. \end{aligned}$$

Somit ist die Tangente in \mathcal{O} die unendlich ferne Gerade. Da nach Bemerkung 1.3 \mathcal{O} der einzige unendlich ferne Punkt ist, hat die unendlich ferne Gerade einen dreifachen Schnittpunkt mit \mathcal{O} . Daraus folgt $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

Es gilt $-P \in \tilde{X}(g_2, g_3; K)$ wie man durch Einsetzen sofort sieht. Im Projektiven erhalten wir

$$\det \begin{pmatrix} 0 & 0 & 1 \\ 1 & x & y \\ 1 & x & -y \end{pmatrix} = x - x = 0.$$

Das heißt, dass $P, -P, \mathcal{O}$ komplanar sind, also auf einer projektiven Geraden liegen und somit $P * -P = \mathcal{O}$. Daraus folgt die Behauptung, denn

$$P + (-P) = \mathcal{O} * (P * -P) = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$

□

Um explizite Formeln für die Gruppenaddition zu finden, betrachte die paarweise verschiedenen Punkte

$$\begin{aligned} P_1 &= (x_1, y_1) \\ P_2 &= (x_2, y_2) \\ P_1 * P_2 &= (x_3, y_3) \\ P_1 + P_2 &= (x_3, -y_3) \end{aligned}$$

und die Gerade

$$y = mx + b$$

mit

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{und} \quad b = y_1 - mx_1 = y_2 - mx_2.$$

Diese Gerade verbindet nach Konstruktion P_1 und P_2 . Um den dritten Schnittpunkt zu berechnen, setzen wir gleich und erhalten

$$y^2 = (mx + b)^2 = 4x^3 - g_2x - g_3 =: f(x).$$

Nach Voraussetzung sind x_1, x_2, x_3 die Nullstellen des entstehenden Ausdrucks

$$m^2x^2 + 2mxb + b^2 - f(x) = 4(x_1 - x)(x_2 - x)(x_3 - x).$$

Koeffizientenvergleich am quadratischen Term liefert

$$m^2 = 4(x_1 + x_2 + x_3),$$

und somit gilt

$$P_1 + P_2 = (x_3, -y_3) = \left(\frac{m^2}{4} - x_1 - x_2, -mx_3 - b \right).$$

Für den Fall $P_1 = P_2$ ist die Vorgehensweise gleich, nur muss bei der Konstruktion der Geraden zur Tangentensteigung

$$m = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

übergegangen werden. Diese ist wohldefiniert wegen der Regularitätsbedingung an die Kurve.

Bemerkung 1.8

Nachdem nun eine Gruppenstruktur auf der Kurve definiert ist, kommen verschiedene Fragestellungen auf, z.B. ob die Gruppe endlich erzeugt ist oder welche Punkte auf der Kurve endliche Ordnung haben. Letzteres sind die Punkte P , für die es ein $n \in \mathbb{N}$ gibt, so dass $nP = \mathcal{O}$. Diese Frage wird unter einer anderen Herangehensweise am Ende des zweiten Abschnitts noch einmal behandelt werden.

Die Punkte der Ordnung zwei für den Fall $\mathcal{O} = \infty$ kann man direkt an der Kurve ablesen wie die nachfolgende Zeichnung illustriert.

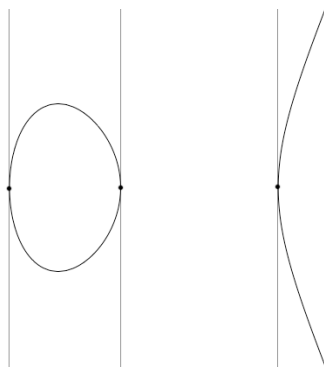


Abbildung 3: Punkte der Ordnung 2 bei $\mathcal{O} = \infty$

2 Das Additionstheorem der \wp -Funktion

Das Ziel dieses Abschnitts ist die Gruppenstruktur, die der Torus durch die Restklassenaddition gegeben hat, auf die Kubik zu übertragen, die durch die Differentialgleichung der \wp -Funktion bestimmt ist.

2.1 Wiederholung: Der Torus als nichtsinguläre Kubik

Die folgenden wichtigen Begriffe dienen nur der Wiederholung und werden im Folgenden als bekannt vorausgesetzt. Für mehr Informationen und Beweise siehe auch [3].

Definition 2.1

Sei Ω ein Gitter. Dann heißt

$$\wp(z; \Omega) := \wp(z) = \begin{cases} \frac{1}{z^2} + \sum_{\omega \in \Omega \setminus 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} & z \notin \Omega \\ \infty & z \in \Omega \end{cases}$$

Weierstrass'sche \wp -Funktion zum Gitter Ω .

Satz 2.2

\wp ist eine gerade, elliptische Funktion mit Polen zweiter Ordnung in den Gitterpunkten und holomorph in $\mathbb{C} \setminus \Omega$. \wp' ist eine ungerade Funktion mit Polen dritter Ordnung in den Gitterpunkten und es gilt die folgende Differentialgleichung:

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

$$\text{mit } g_2 = 60G_4 = 60 \sum_{\omega \in \Omega \setminus 0} \omega^{-4} \text{ und } g_3 = 140G_6 = 140 \sum_{\omega \in \Omega \setminus 0} \omega^{-6}.$$

Bemerkung 2.3

Im ersten Abschnitt bezeichneten g_2, g_3 die Koeffizienten der Kubik. Es stellt sich aber heraus, daß diese direkt mit dem Gitter zusammenhängen, das den Torus definiert. Deshalb werden sie Gitterkonstanten genannt und lassen sich direkt aus dem Gitter wie oben berechnen. Das führt zu folgender

Definition 2.4

Sei Ω ein Gitter mit Gitterkonstanten g_2, g_3 , dann heißt

$$X(g_2, g_3) := \{ (x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3 \}$$

die elliptische Kurve zum Gitter Ω und

$$\tilde{X}(g_2, g_3) := \{ [x_0 : x_1 : x_2] \in \mathbb{C}P^2 \mid x_2^2x_0 = 4x_1^3 - g_2x_1x_0^2 - g_3x_0^3 \}$$

der projektive Abschluss von $X(g_2, g_3)$.

Satz 2.5

Die Abbildung

$$\lambda : \begin{array}{l} \mathbb{C}/\Omega \longrightarrow \mathbb{C}P^2 \\ [z] \longmapsto \begin{cases} [1 : \wp(z) : \wp'(z)] & z \notin \Omega \\ [0 : 0 : 1] & z \in \Omega \end{cases} \end{array}$$

ist eine Bijektion zwischen dem Torus \mathbb{C}/Ω zum Gitter Ω und der projektiven algebraischen Kurve $\tilde{X}(g_2, g_3)$.

2.2 Das Abelsche Theorem

Theorem 2.6

Eine elliptische Funktion zum Gitter Ω mit vorgegebenen Nullstellen a_1, \dots, a_n und Polstellen b_1, \dots, b_n existiert genau dann, wenn

$$a_1 + \dots + a_n \equiv b_1 + \dots + b_n \pmod{\Omega}$$

Bemerkung 2.7

Für den Beweis des Additionstheorems der \wp -Funktion ist nur die Richtung von Bedeutung in der auf die Kongruenz geschlossen wird, die andere Richtung soll an dieser Stelle nicht bewiesen werden. Sie ist die schwierigere und kann in [3, S. 297ff] nachgelesen werden.

Beweis

Sei f die elliptische Funktion mit den gegebenen Null- und Polstellen. Sei $a \in \mathbb{C}$, so dass für die verschobene Grundmasche des Torus

$$\mathcal{F}_a := \{a + \omega_1 t + \omega_2 s \mid t, s \in [0, 1)\}$$

gilt $a_j, b_j \notin \partial\mathcal{F}_a$. Mit geeigneter Wahl der Repräsentanten der a_j, b_j gilt dann auch $a_j, b_j \in \mathcal{F}_a^\circ$.

Sei g analytisch. Dann gilt $\text{Res}(g \frac{f'}{f}; a) = g(a) \text{ord}(f, a)$.

Betrachte folgendes Integral

$$I = \frac{1}{2\pi i} \int_{\partial\mathcal{F}_a} \zeta \frac{f'(\zeta)}{f(\zeta)} d\zeta.$$

Mit dem Residuensatz und $g(z) = z$ ergibt sich zusammen mit Obigem folgender Wert für das Integral

$$I = a_1 + \dots + a_n - b_1 - \dots - b_n.$$

Zu zeigen ist $I \in \Omega$. Betrachte dazu die Summe der Integrale über jeweils die gegenüberliegenden Seiten

$$\frac{1}{2\pi i} \left(\int_a^{a+\omega_1} \zeta \frac{f'(\zeta)}{f(\zeta)} d\zeta + \int_{a+\omega_1+\omega_2}^{a+\omega_2} \zeta \frac{f'(\zeta)}{f(\zeta)} d\zeta \right) \quad (*)$$

bzw. mit vertauschtem ω_1 und ω_2 . Es genügt zu zeigen, dass diese Summen jeweils in Ω liegen.

Setze $g(z) := z \frac{f'(z)}{f(z)}$.

$$\begin{aligned} (*) &= \frac{1}{2\pi i} \left(\int_a^{a+\omega_1} g(\zeta) d\zeta + \int_{a+\omega_1+\omega_2}^{a+\omega_2} g(\zeta) d\zeta \right) \\ &= \frac{1}{2\pi i} \left(\int_a^{a+\omega_1} g(\zeta) d\zeta - \int_a^{a+\omega_1} g(\zeta + \omega_2) d\zeta \right) = \frac{1}{2\pi i} \int_a^{a+\omega_1} g(\zeta) - g(\zeta + \omega_2) d\zeta \\ &= \frac{1}{2\pi i} \int_a^{a+\omega_1} \zeta \frac{f'(\zeta)}{f(\zeta)} - (\zeta + \omega_2) \frac{f'(\zeta + \omega_2)}{f(\zeta + \omega_2)} d\zeta \\ &= -\frac{\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(\zeta)}{f(\zeta)} d\zeta \end{aligned}$$

Mit einer analogen Rechnung für die beiden anderen gegenüberliegenden Seiten ergibt sich

$$I = \frac{\omega_1}{2\pi i} \int_a^{a+\omega_2} \frac{f'(\zeta)}{f(\zeta)} d\zeta - \frac{\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(\zeta)}{f(\zeta)} d\zeta.$$

Bleibt also nur noch zu zeigen, dass

$$\frac{1}{2\pi i} \int_a^{a+\omega_j} \frac{f'(\zeta)}{f(\zeta)} d\zeta \in \mathbb{Z}, \quad j = 1, 2.$$

$f(z)$ hat nach Voraussetzung weder Pol- noch Nullstellen auf dem Integrationsweg, also ist der Integrand dort eine holomorphe Funktion, und es existiert eine Stammfunktion in einer kleinen Umgebung um den Weg. Mit $f(z) = \exp(h(z))$ ist $h(z)$ Stammfunktion des Integranden, denn

$$f'(z) = h'(z) \exp(h(z)) = h'(z) f(z) \Rightarrow h'(z) = \frac{f'(z)}{f(z)}.$$

Es folgt

$$\int_a^{a+\omega_j} \frac{f'(\zeta)}{f(\zeta)} d\zeta = h(a + \omega_j) - h(a),$$

und wegen

$$\exp(h(a + \omega_j)) = f(a + \omega_j) = f(a) = \exp(h(a))$$

gilt

$$h(a + \omega_j) - h(a) = 2\pi i k, \quad k \in \mathbb{Z}.$$

Zusammengesetzt ergibt sich

$$\frac{1}{2\pi i} \int_a^{a+\omega_j} \frac{f'(\zeta)}{f(\zeta)} d\zeta = k \in \mathbb{Z},$$

was zu zeigen war. □

2.3 Das Additionstheorem und Gruppenstrukturen

Satz 2.8

Es gilt

$$\det \begin{pmatrix} 1 & \wp(u+v) & -\wp'(u+v) \\ 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \end{pmatrix} = 0$$

Beweis

Wähle Punkte $u, v \notin \Omega$ mit $\wp(u) \neq \wp(v)$. Betrachte die Funktion

$$f(z) = \det \begin{pmatrix} 1 & \wp(z) & -\wp'(z) \\ 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \end{pmatrix} = A + B\wp(z) + C\wp'(z)$$

mit $C \neq 0$. Diese Funktion ist elliptisch und hat in den Gitterpunkten Pole dritter Ordnung wegen der Eigenschaft von \wp' .

f hat Nullstellen in $z = u$ und $z = v$. Sei w die dritte Nullstelle modulo Ω . Dann gilt nach dem Abelschen Theorem

$$u + v + w \equiv 0 \pmod{\Omega}.$$

Wegen der Elliptizität von f bezüglich Ω ist $w = -(u + v)$ eine Nullstelle und Einsetzen liefert die Behauptung. □

Corollar 2.9 (Analytische Form des Additionstheorems)

Seien $z, w \in \mathbb{C}$ mit $z + w, z - w, z, w \notin \Omega$. Dann gilt

$$\wp(z + w) = \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2 - \wp(z) - \wp(w)$$

Beweis

Betrachte die paarweise verschiedenen Punkte

$$\begin{aligned} (x_1, y_1) &= (\wp(u), \wp'(u)) \\ (x_2, y_2) &= (\wp(v), \wp'(v)) \\ (x_3, y_3) &= (\wp(u + v), -\wp'(u + v)). \end{aligned}$$

Nach Satz 2.8 verschwindet die Determinante, d.h. die Punkte liegen auf einer Geraden

$$y = mx + b$$

mit der Steigung

$$m = \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}.$$

Einsetzen in die Kurvengleichung liefert

$$4x^3 - g_2x - g_3 = (mx + b)^2$$

mit den Nullstellen x_1, x_2, x_3 . Der Wurzelsatz von Vieta liefert für den quadratischen Term

$$x_1 + x_2 + x_3 = \frac{m^2}{4}.$$

Also

$$\wp(z + w) = \frac{1}{4}m^2 - \wp(z) - \wp(w).$$

□

Bemerkung 2.10

Ein Vergleich der Rechnung im obigen Beweis mit der aus Beispiel 1.7 zeigt die Analogie zwischen der geometrisch definierten Gruppenstruktur und dem Additionstheorem auf.

Corollar 2.11 (Verdoppelungsformel)

Sei $z \in \mathbb{C}$ mit $2z, z \notin \Omega$. Dann gilt

$$\wp(2z) = \frac{1}{4} \left(\frac{\wp''(z)}{\wp'(z)} \right)^2 - 2\wp(z)$$

Beweis

Corollar 2.8 mit Grenzübergang $w \rightarrow z$

□

Corollar 2.12 (Geometrische Form des Additionstheorems)

Drei Punkte $u, v, w \in \tilde{X}(g_2, g_3)$ haben genau dann die Summe 0, wenn sie auf einer Geraden liegen.

Beweis

Die Punkte $u = [u_1 : u_2 : u_3], v = [v_1 : v_2 : v_3]$ und $w = [w_1 : w_2 : w_3]$ liegen genau dann auf einer Geraden, wenn $(u_1, u_2, u_3), (v_1, v_2, v_3), (w_1, w_2, w_3)$ linear abhängig sind.

Dies ist aber gerade gleichbedeutend mit Satz 2.8.

□

Bemerkung 2.13

Corollar 2.12 liefert den Zusammenhang zwischen den im ersten Teil definierten Gruppenstrukturen auf einer elliptischen Kurve und der Restklassenaddition auf dem Torus. Corollar 2.12 besagt nämlich, dass die Struktur, die durch λ auf der Kurve induziert wird, genau diejenige mit $\mathcal{O} = \infty$ ist.

Die Anwendung von $\varphi_{\mathcal{O}'}$ entspricht einer Translation des Gitters um einen Urbildpunkt von P . Somit erhält man über die Addition auf dem Urbildraum alle Gruppenstrukturen durch Anwenden von λ .

Corollar 2.14

λ ist ein Gruppenisomorphismus zwischen \mathbb{C}/Ω und $\tilde{X}(g_2, g_3)$.

Bemerkung 2.15

Dieser Gruppenisomorphismus bietet nun eine neue Möglichkeit die letzte Fragestellung aus Bemerkung 1.8, die Frage nach Punkten endlicher Ordnung auf der Kurve, zu beantworten, indem wir die Addition mit Hilfe von λ zurückziehen und Punkte n -ter Ordnung auf dem Torus finden. Diese sind aber direkt ablesbar. Es bezeichne \mathcal{P}_n die Punkte der Ordnung n .

$$\mathcal{P}_n = \left\{ \frac{s}{n}\omega_1 + \frac{t}{n}\omega_2 \mid t, s \in \{0, \dots, n-1\} \right\}.$$

\mathcal{P}_n ist eine Untergruppe von \mathbb{C}/Ω .

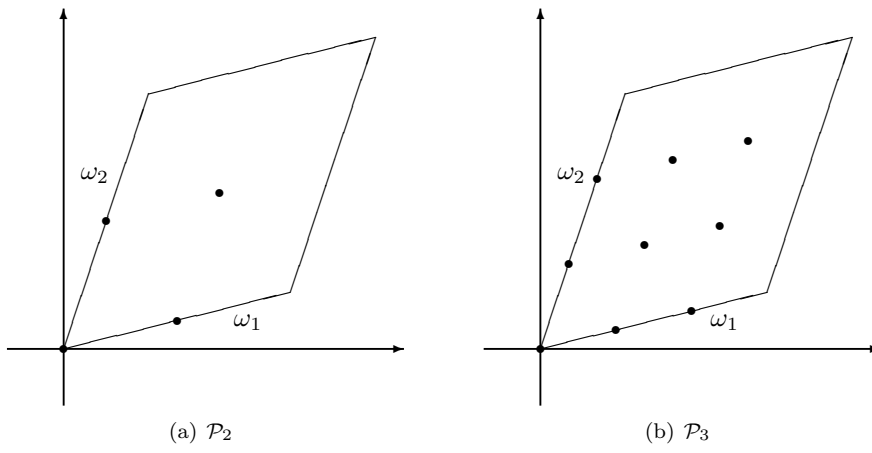


Abbildung 4: Untergruppen endlicher Ordnung

3 Anwendungen in der Kryptographie

Der letzte Abschnitt soll eine moderne Anwendung des in den vorigen Abschnitten behandelten Stoffes aufzeigen, beginnend mit einer kleinen Einführung in die Funktionsweise von Verschlüsselungsverfahren.

3.1 Einführung in die Kryptographie

Die Kryptographie ist ein uraltes Thema, das schon seit Jahrtausenden die Menschen beschäftigt. Vor allem zu Kriegszeiten wurde eifrig nach neuen Verschlüsselungsmethoden geforscht, aber auch in unserer modernen Informationsgesellschaft spielen Kryptographie und die Existenz von sicheren Verschlüsselungsalgorithmen eine immer wichtiger werdende Rolle. Heutzutage unterscheidet man prinzipiell zwischen zwei grundlegenden Arten der Verschlüsselung, nämlich der symmetrischen und der asymmetrischen Verschlüsselung.

Bei der symmetrischen Verschlüsselung existiert ein vorher vereinbarter Schlüssel, den sowohl Sender als auch Empfänger vorher auf einem sicheren Kanal ausgetauscht haben müssen. Dieser Schlüssel dient sowohl zum ver- als auch zum entschlüsseln. Der Vorteil der symmetrischen Verschlüsselung ist die Schnelligkeit verglichen zu asymmetrischer Verschlüsselung. Nachteilig hingegen ist z.B. die Tatsache, dass wenn n Teilnehmer jeweils verschlüsselt kommunizieren wollen, entsprechend viele Schlüssel bereitgestellt werden müssen. Außerdem ist ad-hoc Kommunikation schwierig, da vorher der gemeinsame Schlüssel vereinbart werden muss. Ein antikes Beispiel für einen symmetrischen Algorithmus ist die Cäsar Verschlüsselung, bei der einfach die Buchstaben im Alphabet um drei Stellen verschoben wurden. Modernere Vertreter sind der Data Encryption Standard (DES) und dessen Nachfolger Advanced Encryption Standard (AES), der heute als sehr sicher gilt.

Asymmetrische Verschlüsselung läuft etwas anders ab. Jeder Teilnehmer hat einen sogenannten öffentlichen und einen privaten Schlüssel. Auf den öffentlichen Schlüssel haben alle anderen Kommunikationspartner Zugriff, z.B. über ein öffentliches Verzeichnis. Will Alice jetzt Bob eine verschlüsselte Nachricht senden, so nimmt sie dazu Bobs öffentlichen Schlüssel und verschlüsselt die Nachricht damit. Sie kann sie selbst nicht wiederherstellen, nur Bob kann nach Erhalt der Nachricht diese wieder mit seinem privaten Schlüssel entziffern. Der wohl prominenteste Vertreter der asymmetrischen Verschlüsselung ist der RSA Algorithmus. Dieses Verfahren kann einige Nachteile der symmetrischen Verschlüsselung beseitigen, ist aber im Vergleich zur symmetrischen Verschlüsselung relativ langsam.

In der Praxis werden heutzutage meist Hybridalgorithmen eingesetzt, also Algorithmen, die die Vorteile von symmetrischer und asymmetrischer Verschlüsselung ausnutzen. So wird der langsame asymmetrische Algorithmus eingesetzt um den Schlüssel zu übertragen, mit dem dann die weitere Kommunikation symmetrisch abläuft.

Jeder eingesetzte Algorithmus ist knackbar, sei es durch bloßes Ausprobieren aller Möglichkeiten (brute force) oder durch gezieltere Angriffe durch Krypto-

analyse. Ein Algorithmus gilt dann als sicher, wenn es mit realistischem Aufwand genügend lange dauert ihn zu knacken. Bei asymmetrischen Algorithmen ist man speziell auf der Suche nach "one way"-Funktionen, das heißt Operationen, die einfach durchzuführen ist, deren Inverse aber sehr aufwendig sind.

3.2 Funktionsweise von ECC

Wir wollen jetzt ein Verfahren betrachten, welches man mit Hilfe der Gruppenstruktur auf elliptischen Kurven realisieren kann und das ähnlich wie die asymmetrischen Verfahren zwei Schlüssel einsetzt, aber nur einen gemeinsamen Schlüssel produziert, der dann zur symmetrischen Kommunikation eingesetzt werden kann (Diffie-Hellman Key Exchange). Dieses wird im Folgenden mit ECC (Elliptic Curve Cryptography) bezeichnet.

Elliptische Kurven sind über jedem Körper definiert. Für ECC sind speziell elliptische Kurven über einem endlichen Körper F_q , $q = p^r$, p prim interessant, denn generell werden Verschlüsselungsalgorithmen auf einem Rechner implementiert, der nur eine endliche Anzahl von Zuständen kennt. In der Anwendung benutzen wir einen Körper F_{2^m} , denn ein Rechner manipuliert typischerweise Bitketten.

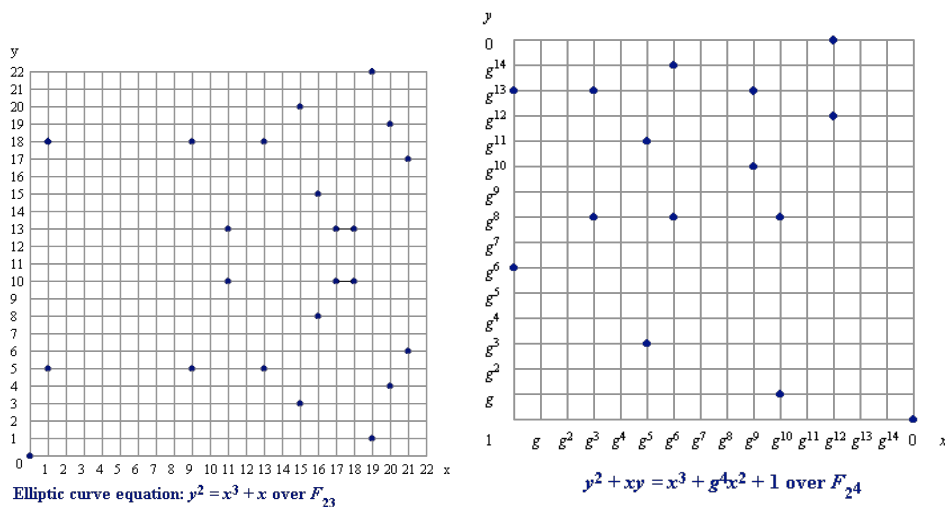
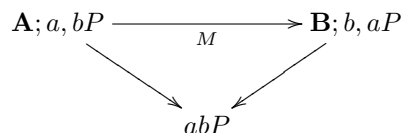


Abbildung 5: Elliptische Kurven über endlichen Körpern

Für die Kommunikation müssen nun eine geeignete elliptische Kurve E und einen Punkt $P \in E$ festgelegt werden, der eine möglichst große Untergruppe erzeugt, am besten die gesamte Kurve. Alice will Bob nun eine Nachricht schicken; dazu besitzen beide jeweils eine geheime Zufallszahl, Alice a und Bob b . Daraus lassen sich die öffentlichen Schlüssel berechnen, die publiziert werden, indem die entsprechenden Vielfachen von P gebildet werden. Das heißt der öffentliche Schlüssel von Alice ist aP und der von Bob ist bP . Sei der öffentliche Schlüssel von Bob nun Alice bekannt. Es ist außerordentlich schwierig aus bP Bobs privaten Schlüssel b zu berechnen (siehe Abschnitt 3.3). Der Schlüsselaus-

tausch läuft nun wie folgt ab



Alice verschlüsselt nun die Nachricht M mit einem Schlüssel, der sich aus $a(bP)$ zusammensetzt und gibt diese Nachricht an Bob weiter. Er kann diese nun entschlüsseln, indem er $b(aP) = abP = a(bP)$ ausrechnet, welches den selben Schlüssel ergibt den Alice zum Verschlüsseln benutzt hat.

Hier werden die Unterschiede zu RSA deutlich, denn während man bei asymmetrischen Verschlüsselungsverfahren die einmal mit dem öffentlichen Schlüssel des Partners chiffrierte Nachricht selbst nicht mehr entschlüsseln kann, wird hier ein für jeweils zwei Kommunikationspartner einzigartiger Schlüssel erzeugt, nämlich abP , mit dem dann verschlüsselt kommuniziert werden kann.

3.3 Sicherheit von ECC

ECC Verschlüsselung gilt bei geeigneter Wahl der Kurve bei weitaus kleineren Schlüssellängen als bei RSA schon als sehr sicher. Das macht ECC gerade interessant bei Medien, auf denen die Schlüssellängen begrenzt sind, wie z.B. Smartcards.

Die Sicherheit von ECC beruht sehr stark auf der Lösung des Problems des diskreten Logarithmus:

Problem

Sei (G, \circ) eine endliche Gruppe, $\alpha \in G$ und

$$\beta \in H := \{\alpha^i \mid i \geq 0\} \subset G$$

Gesucht ist das eindeutige $a \in \mathbb{N}$ mit $0 \leq a \leq |H| - 1$ und $\beta = \alpha^a$.

Bezeichnung: $a = \log_{\alpha}(\beta)$

Die Bezeichnung diskreter Logarithmus basiert auf der multiplikativen Schreibweise einer Gruppe, bei der der Exponent gesucht ist. Im Fall der elliptischen Kurven wird die Gruppenverknüpfung additiv geschrieben, entspricht der diskrete Logarithmus der "Division" durch P . Denn in diesem Fall ist ein a mit $aP = Q$ gesucht und naives Rechnen würde " $a = Q/P$ " ergeben.

Generell ist dieses Problem nicht ohne erheblichen Rechenaufwand zu lösen. Es gibt effizientere Algorithmen als das Durchprobieren aller Möglichkeiten, z.B. den Baby-Step-Giant-Step-Algorithmus, aber bei geeigneter Kurvenwahl ist der

Aufwand im Vergleich zur Schlüssellänge mindestens exponentiell. Bei unglücklicher Kurvenwahl vereinfacht sich das Problem und macht Angriffe mit subexponentiellem Aufwand möglich.

Wir haben die ganze Zeit über eine "geeignete Kurvenwahl" gesprochen, nun stellt sich die Frage von welchen Faktoren die Wahl einer Kurve abhängt. Grundsätzlich muss eine Kurve, die zur Verschlüsselung eingesetzt werden soll, natürlich genügend viele Elemente besitzen. Diese Zahl kann nach dem Satz von Hasse [6] abgeschätzt werden.

Satz

Sei E eine elliptische Kurve über einem Körper K mit $|K| = k$. Dann gilt

$$k + 1 - 2\sqrt{k} < |E| < k + 1 + 2\sqrt{k}$$

Bemerkung

Eine elliptische Kurve über einem endlichen Körper hat nur endlich viele Elemente.

Satz (Silver-Pohlig-Hellman)

Sei G eine endliche abelsche Gruppe mit $|G| = p_1^a p_2^a \cdots p_s^a$. Dann lässt sich das diskrete Logarithmusproblem in G auf das Lösen von Logarithmenproblemen in Gruppen der Ordnung p_1, \dots, p_s zurückführen.

Ein weiteres wichtiges Kriterium ist, dass die Ordnung einer geeigneten Kurve einen möglichst hohen Primfaktor haben sollte.

Für mehr Informationen und Details siehe auch [4] und [5].

Literatur

- [1] CERTICOM: *Online Elliptic Curve Cryptography Tutorial*. URL http://www.certicom.com/index.php?action=ecc_tutorial,home
- [2] ESSLINGER, Bernhard ; BÜGER, Matthias ; BARTOL, Filipovic ; KOY, Henrik ; OYONO, Roger ; SCHNEIDER, Jörg C.: *CrypTool-Skript: Mathematik und Kryptographie*. URL <http://www.cryptool.de>. Stand 17. Juli 2003
- [3] FREITAG, Eberhard ; BUSAM, Rolf.: *Funktionentheorie 1*. 3. Aufl. Berlin : Springer, 2000. - ISBN 3-540-67641-4
- [4] KOBLITZ, Neil: *A course in Number Theory and Cryptography*. 2. Aufl. New York : Springer, 1994. - ISBN 0-387-94293-9
- [5] KOBLITZ, Neil: *Algebraic Aspects of Cryptography*. 1. Aufl. Berlin : Springer, 1998. - ISBN 3-540-63446-0
- [6] SILVERMAN, J.: *The arithmetic of elliptic curves*. 1. Aufl. New York : Springer, 1986. - ISBN 0-387-96203-4
- [7] SILVERMAN, J. ; TATE, J.: *Rational points on elliptic curves*. 1. Aufl. New York : Springer, 1992. - ISBN 0-387-97825-9