Elliptische Kurven

HWS 2013

Inhaltsverzeichnis

1 Kurven in der projektiven Ebene **4**
- 1.1 Projektiver Raum, Nullstellenmengen homogener Polynome 4
- 1.2 Übergang von der affinen zur projektiven Ebene 7
- 1.3 Schnittpunkt einer Kurve mit einer Geraden 8
- 1.4 Algebraischer Einschub: Resultanten 11
- 1.5 Vielfachheit von Schnitten - Der Satz von Bezout 19

2 Elliptische Kurven und Weierstraßsche Normalform **34**
- 2.1 Weierstraßsche Normalform 43
- 2.2 CREMONA Transformation 45

3 Die Gruppenstruktur einer elliptischen Kurve **54**
- 3.1 Einschub: Elliptische Kurven über $\mathbb{C}$ 57
- 3.2 Gruppenoperation für Kurven in Weierstraßscher Normalform 58
  - 3.2.1 Algorithmus von Montgomery 63

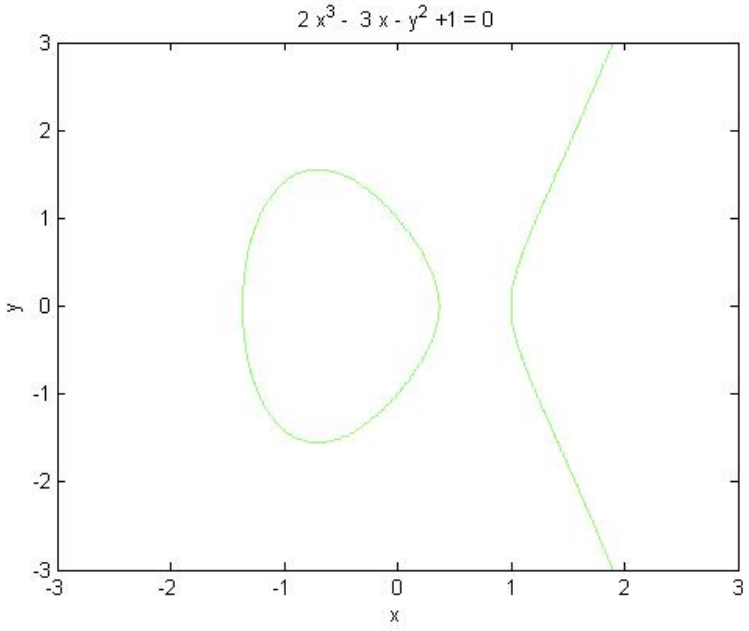
4 Anwendungen elliptischer Kurven **66**
- 4.1 Diskretes Logarithmenproblem 66
- 4.2 Kryptoverfahren auf Basis diskreter Logarithmen 68
  - 4.2.1 Schlüsselaustausch nach DIFFIE und HELLMAN 68
  - 4.2.2 Kryptoverfahren von MASSEY und OMURA 68
  - 4.2.3 Kryptoverfahren von ELGAMAL 69
  - 4.2.4 Kodierung nach KOBLITZ 69
  - 4.2.5 Kryptoverfahren von Koyama, Maurer, Okamoto und Vanstone 70
- 4.3 Elektronische Unterschriften mit elliptischen Kurven 71
  - 4.3.1 Das Verfahren von ELGAMAL 71
  - 4.3.2 Der Digitale Signatur Algorithmus DSA auf Basis elliptischer Kurven $E(\mathbb{F}_p)$ 72
  - 4.3.3 ECGDSA (Elliptic curve german digital signature algorithm) 74
- 4.4 Faktorisierung ganzer Zahlen 75
  - 4.4.1 POLLARDS-(p-1)-Methode 75
  - 4.4.2 Die elliptische Kurven Methode von Lenstra 76
- 4.5 Primzahltest mit elliptischen Kurven 77
  - 4.5.1 Klassisches Analogon 77
  - 4.5.2 POCKLINGTON-LEHMER-Test 78

5 Torsionspunkte **80**

1 Kurven in der projektiven Ebene

1.1 Projektiver Raum, Nullstellenmengen homogener Polynome

Beispiel einer elliptischen Kurve:



Allgemein, falls char$k \neq 2,3$: $y^2 = x^3 + ax + b$
k sei ein Körper. Wir identifizieren seine Punkte mit denen der Geraden $y = 0$ in der affinen Ebene k^2 mit den Koordinaten (x,y). Weiter sei $z = (0,-1)$, dann gibt es zu jedem Punkt $x \in k$ genau eine Gerade durch z und $(x,0)$. Umgekehrt schneidet jede Gerade durch z mit einer Ausnahme die x-Achse. Die Ausnahme ist $y = -1$.

Definition:
Die **Projektive Gerade** $\mathbb{P}^1(k)$ ist die Menge aller Geraden in k^2 durch einen festen Punkt $z \in k^2$.
Äquivalentes Modell:
$\mathbb{P}^1(k)$ ist die Menge aller eindimensionaler Untervektorräume von k^2.

Allgemein definieren wir:

Definition:
Ist k ein Körper und V ein k- Vektorraum, so bezeichnen wir die Menge aller eindimensionaler Untervektorräume von V als projektiven Raum $\mathbb{P}(V)$.
Für $n \in \mathbb{N}$ bezeichnen wir

$$\mathbb{P}^n = \mathbb{P}(k^{n+1})$$

als n-dimensionalen projektiven Raum.
$\mathbb{P}^1$ heißt projektive Gerade
$\mathbb{P}^2$ heißt projektive Ebene.

Zum besseren Rechnen ordnen wir den Punkten eines projektiven Raums sogenannte **homogene Koordinaten** zu.
Ist $U < V$ ein eindimensionaler Untervektorraum und $u \in U \backslash \{0\}$, so bezeichnen wir die Komponenten von u als homogene Koordinaten von u.

Konkret in $\mathbb{P}^2 = \mathbb{P}(k^3)$:
Ein eindimensionaler Untervektorraum $U < k^3$ besteht aus den Vielfachen des Vektors

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in k^3 \backslash \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

die homogene Koordinaten sind $(x : y : z)$.

Ist $\lambda \in k \backslash \{0\}$, so erzeugt
$\begin{pmatrix} \lambda \cdot x \\ \lambda \cdot y \\ \lambda \cdot z \end{pmatrix}$ denselben Untervektorraum wie $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$
d.h. $\left(\ x : y : z \ \right) = (x\lambda : y\lambda : z\lambda)$

Sei nun $f(x,y,z) = x^2 + y^2 + z^2 - 3$

dann ist $f(1,1,1) = 0$ aber $(1:1:1) = (2:2:2)$ und$f(2,2,2) = 9$

Definition:

a) Ein Polynom in n Variablen $x_1,\ldots,x_n$ über dem Körper k ist eine endliche Linearkombination von Monomen $x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}, e_i \in \mathbb{N}_0$

b) Der Grad eines solchen Monoms ist $e_1 + e_2 + \cdots + e_n$

c) Der Grad des Polynoms ist das Maximum der Grade der Monome

d) Das Polynom heißt homogen, wenn alle seine Monome den gleichen Grad haben.

Beispiel:
$x^3 + y^3 + z^3 + 5xyz$ ist homogen vom Grad 3

Ist f homogen vom Grad d und $\lambda \in k$ so ist

$$f(x_1,x_2,\ldots,x_n) = \lambda^d f(x_1,\ldots,x_n)$$

Falls $\lambda \neq 0$, verschwindet die linke Seite genau dann, wenn auch die rechte Seite verschwindet. Sind $(x_1,\ldots,x_n)$ die homogenen Koordinaten eines Punktes, so können wir also zwar nicht vom Funktionswert von f in diesem Punkt reden, aber wir können davon reden, ob f dort verschwindet oder nicht.

Definition:
Eine Teilmenge $C \subset \mathbb{P}^2$ heißt **ebene Kurve vom Grad d über dem Körper k**, wenn es ein nicht konstantes homogenes Polynom f vom Grad d über k gibt, so dass

$$C = \{(x:y:z) \in \mathbb{P}^2 \mid f(x,y,z) = 0\}$$

1.2 Übergang von der affinen zur projektiven Ebene

Wir bezeichnen die Koordinaten in k^3 mit x,y,z.
Jeder Punkt $(x:y:z) \in \mathbb{P}^2(k)$ mit $z \neq 0$ lässt sich auch schreiben in der Form $(x_0:y_0:1)$ mit $x_0 = \frac{x}{z}, y_0 = \frac{y}{z}, z = 1$.
Die Punkte mit homogenen Koordinaten

$$(x:y:z)$$

mit $z \neq 0$ entsprechen also eineindeutig den Punkten der affinen (x_0,y_0)-Ebene k^2. Dazu kommen die Punkte $(x:y:0)$, sie entsprechen den möglichen $x:y$ der Geraden durch $(0,0) = (0:0:1)$.
Nun sei

$$C = \{(x:y:z) \in \mathbb{P}^2 \mid f(x,y,z) = 0\}$$

eine Kurve vom Grad d und $(x_0,y_0) \in k^2$.
Wir identifizieren diesen Punkt mit $(x_0:y_0:1)$ aus $\mathbb{P}^3(k)$; er liegt also auf C, wenn $f(x_0,y_0,1) = 0$ ist. Das ist ein Polynom in x_0 und y_0, es ist i.A. nicht homogen. z.B.

- $f(x) = x^3 + y^3 + z^3 + 5xyz$ wird zu $x_0^3 + y_0^3 + 1 + 5x_0y_0$
- $g = z^2(x+y+z)$ wird zu $x_0 + y_0 + 1$
  affin: $x_0 + y_0 + 1 = 0 \Leftrightarrow y_0 = -x_0 - 1$

Geometrisch gesehen:
Interpretation von g: $g(x,y,z) = 0 \Leftrightarrow x+y+z = 0$ oder $z = 0$, d.h. die Kurve besteht aus zwei Geraden, eine davon im Unendlichen.
Umgekehrt:
Gegeben sei eine affine Kurve $\{(x_0,y_0) \in k^2 \mid f_0(x_0,y_0) = 0\}$,
f_0 Polynom in x_0,y_0.
Gesucht: Eine projektive Kurve $C = \{(x:y:z) \in \mathbb{P}^2 \mid f(x,y,z) = 0\}$, so dass $C \cap \{(x:y:z) \in \mathbb{P}^2(k) \mid z \neq 0\}$ gleich der gegebenen Kurve ist. Dazu füllen wir jedes Monom $x_0^a y_0^b$ von f_0 auf zu einem Monom $x^a y^b z^{d-a-b}$, wobei d den Grad von f_0 bezeichnet.

1.3 Schnittpunkt einer Kurve mit einer Geraden

Definition:
Eine ebene Kurve heißt **irreduzibel** in $\mathbb{P}^2(k), k$ algebraisch abgeschlossen, falls sie sich nicht schreiben lässt als Vereinigung zweier Kurven. Ist k nicht algebraisch abgeschlossen, dann bezeichnen wir eine Kurve

$$C = \{(x:y:z) \in \mathbb{P}^2 \mid f(x,y,z) = 0\}$$

als **irreduzibel**, wenn es keinen algebraisch abgeschlossenen Körper K gibt, der k enthält, so dass sich

$$C_K = \{(x,y,z) \in \mathbb{P}^2(K) \mid f(x,y,z) = 0\}, K \geq k$$

nicht als Vereinigung zweier Teilkurven schreiben lässt.

Ist $f = g \cdot h$,$f,g,h \in k[X,Y,Z], g,h$ nicht konstant, ist

$$V(f) = \{(x:y:z) \in \mathbb{P}^2 \mid f(x,y,z) = 0\} = V(g) \cup V(h)$$

Definition:
Ein Polynom $f \in k[X_1,\ldots,X_n]$ heißt **absolut irreduzibel**, wenn es keinen Erweiterungskörper $K \geq k$ gibt, mit nichtkonstanten Polynomen $g,h \in K[X_1,\ldots,X_n]$, so dass $f = g \cdot h$.

Beispiel:
$X^2+1 \in \mathbb{R}[X]$ ist irreduzibel, aber es ist nicht absolut irreduzibel, denn in $\mathbb{C}[X]$ ist $X^2+1 = (X+i)(X-i)$

Ist $f \in k[X,Y,Z]$ absolut irreduzibel, f homogen, so ist die Kurve

$$V(f) \subseteq \mathbb{P}^2(k)$$

irreduzibel.
Die Umkehrung gilt nicht, denn $V(f) = V(f^2) = V(f^3) = \ldots$.
Ist $f = \prod_{k=1}^{n} f_i^{e_i}, e_i \in \mathbb{N}$, so ist $V(f) = V(f_1) \cup V(f_2) \ldots V(f_r)$.
Wir nennen eine Kurve $V(f)$ **reduziert**, wenn f keine mehrfachen Faktoren hat.

k sei algebraisch abgeschlossen, und $f \in k[X,Y,Z]$ sei ein reduziertes homogenes Polynom vom Grad d, $C = V(f)$ und $G \subseteq \mathbb{P}^2(k)$ sei eine Gerade. G sei gegeben durch die lineare Gleichung $g(x,y,z) = 0$. Falls g Teiler von f ist, ist $G \subseteq C$, d.h. $G \cap C = G$. Wir nehmen an, dies sei nicht der Fall. Dann können wir eine Gerade finden, die keinen Punkt mit $G \cap C$ gemeinsam hat. Durch eine Koordinatentransformation lässt sich erreichen, dass diese Gerade die Gleichung $z = 0$ hat.

Betrachten wir die Einbettung

$$k^2 \hookrightarrow \mathbb{P}^2(k)$$

$$(x,y) \to (x : y : 1)$$

so liegen alle Punkte aus $G \cap C$ im Bild von k^2, d.h. wir können die Situation in k^2 statt in $\mathbb{P}^2(k)$ betrachten. Wenn wir uns nur für $G \cap C$ interessieren, können wir also affin rechnen. Durch einen weiteren Koordinatenwechsel können wir erreichen, dass der affine Teil von G in k^2 die Gleichung $y = 0$ hat. Die Gleichung des affinen Teils von C ist $f(x,y,1) = 0$. Die Punkte von $G \cap C$ sind dann jene Punkte $(x_0,0) \in k^2$ mit $f(x_0,0,1) = 0$.

Definition:
Der Punkt $(x_0,0)$ heißt **m-facher Schnittpunkt von** G **und** C, wenn x_0 eine m-fache Nullstelle des Polynoms f(x,0,1) ist.

Lemma
Ist k algebraisch abgeschlossen, f reduziert vom Grad d, $C = V(f) \subseteq \mathbb{P}^2(k)$ und G eine Gerade, so dass G keine Teilmenge von C ist, dann gilt:
Mit Vielfachheiten gezählt haben G und C genau d Schnittpunkte.

Beispiel:
C = Kreislinie $x^2 + y^2$, G=Gerade $x = a, a \in k$ fest.
Ein Koordinatenwechsel, der G auf die Gleichung $y = 0$ bringt wäre etwa:

$$(x,y) \to (y, x - a)$$

Schneller geht es, wenn wir direkt mir den vorhandenen Koordinaten rechnen, d.h. wir setzen $x = a$ ein in die Kreisgleichung.
$a^2 + y^2 = 1$ oder $y^2 = 1 - a$
Ist $a^2 = 1$, also $a \in \{-1,1\}$ so hat dies die doppelte Nullstelle $y = 0$, d.h. die Geraden $x = 1$ und $x = -1$ schneiden den Kreis im Punkt $(1,0)$ bzw $(-1,0)$ mit Vielfachheit 2. Andernfalls hat $y = 1 - a^2$ zwei einfache Nullstellen, d.h. die Gerade $x = 0$ schneidet die Kreislinie in den beiden Punkten $(a, \sqrt{(1-a^2)})$ und $(a, -\sqrt{(1-a^2)})$, jeweils mir Vielfachheit 1.

Lemma:
$C \subseteq \mathbb{P}^2(k)$ sei eine reduzierte Kurve vom Grad d und P sei ein Punkt, der nicht auf C liegt. Dann gibt es höchstens $d(d-1)$ Geraden durch P, die C nicht in d verschiedenen Punkten mit Vielfachheit 1 schneiden.

Beweis:
Wir wählen unser Koordinatensystem so, dass $P = (0,0,1)$. Die Kurve C habe die Gleichung $f(x,y,z) = 0$, f reduziert und homogen vom Grad d. Auf jeder Geraden durch P liegt genau ein Punkt der Form $(\lambda : \mu : 0)$. Die Gerade durch P und diesen Punkt bezeichnen wir mit $L_{\lambda,\mu}$.
$L_{\lambda,\mu} \setminus \{P\} = \{(\lambda : \mu : t) \mid t \in k\}$. Die Schnittpunkte von $L_{\lambda,\mu}$ mit C können deshalb berechnet werden als Nullstellen der Gleichung

$$F(\lambda, \mu, t) = 0$$

λ, μ fest, t variabel. Da $P \notin C$ ist das ein Polynom vom Grad d in t. Dieses Polynom hat genau dann eine mehrfache Nullstelle, wenn seine Diskriminante (siehe nächster Abschnitt) verschwindet. Diese ist ein homogenes Polynom vom Grad $d(d-1)$ in (λ, μ), also gibt es höchstens $d(d-1)$ Geraden, die mehrfache Schnittpunkte mit C haben. $\square$

1.4 Algebraischer Einschub: Resultanten

Problem: R sei ein Ring derart, dass wir im Polynomring $R[X]$ eine eindeutige Zerlegung in irreduzible Faktoren haben, z.B. $R = k$ Körper oder $R = k[x_1, \ldots, x_n]$ Polynomring über einem Körper.
Gegeben seien zwei Polynome $f, g \in R[X]$.
Wann haben f und g einen gemeinsamen Faktor positiven Grades?

Bemerkung:
Ist $R = k$ ein Körper, können wir das Problem lösen, in dem wir nach EUKLID den ggT von f und g berechnen. Das geht aber leider nur über Körpern.
Allgemein schreiben wir:

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$
$$g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$$

Angenommen f und g haben einen gemeinsamen Faktor h vom Grad d, mit $d \geq 1$.Dann gilt:

$$f = h f_0, \quad g = h g_0$$

dann ist

$$deg(f_0) = n - d, \quad deg(g_0) = m - d$$

und

$$f \cdot g_0 = h \cdot f_0 \cdot g_0 = f_0 \cdot h \cdot g_0 = f_0 \cdot g$$

ein Polynom vom Grad $n + m - d$;
Es gibt also ein gemeinsames Vielfaches von f und g, dessen Grad kleiner ist als die Summe der Grade von f und g.

Umgekehrt nehmen wir an, es gebe ein gemeinsames Vielfaches

$$u \cdot f = v \cdot g$$

mit $u, v \in R[X]$ vom Grad kleiner als $m + n$. Dann ist

$$deg\, u < deg\, g = m$$

und

$$deg\, v < deg\, f = n$$

Sei p ein irreduzibles Polynom, das f teilt, aber nicht v. Dann muss p den Faktor g teilen, d.h. f und g haben den Faktor p gemeinsam. Falls jeder irreduzible Faktor von p auch v teilt, muss wegen $deg\, v = deg\, f$ mindestens ein solcher Faktor p in f mit einer größeren Potenz vorkommen als in v.
Wir schreiben :

$$v = p^e \cdot v_0$$

wobei p kein Teiler von v_0 ist, und

$$f = p^e \cdot f_0$$

wobei p Teiler von f sein muss.
Aus der Gleichung $u \cdot f = v \cdot g$ folgt:

$$u \cdot f_0 = v_0 \cdot g$$

wobei $p \mid f_0$, aber $p \nmid v_0$. Da p Teiler von $v_0 \cdot g$ ist, aber nicht von v, muss p Teiler von g sein, d.h. p ist gemeinsamer Faktor von f und g.
Damit ist gezeigt:

f und g haben genau dann einen gemeinsamen Faktor positiven Grades, wenn es Polynome $u, v \in R[X]$ gibt mit $deg\, u < deg\, g$, $deg\, v < deg\, f$, so dass

$$u \cdot f = v \cdot g$$

ist.

Wir machen einen einen Ansatz mit unbestimmten Koeffizienten:

$$u = u_{m-1}x^{m-1} + \cdots + u_1 x + u_0$$
$$v = v_{n-1}x^{n-1} + \cdots + v_1 x + v_0$$

$u_0 \ldots u_{m-1}, v_0 \ldots v_{n-1}$ unbekannte Elemente von R.

Definition:
Der **Quotientenkörper** eines nullteilerfreien Rings R ist:

$$QuotR = \{\frac{f}{g} \mid f,g \in R, g \neq 0\}$$

Dabei ist $\frac{f}{g}$ die Äquivalenzklasse des Paares $(f,g) \in R \times R$ modulo der Äquivalenzrelation $(f_1,g_1) \sim (f_2,g_2) \Leftrightarrow f_1 \cdot g_2 = f_2 \cdot g_1$

Es genügt, wenn wir die Lösungen $u_0,\ldots,u_{m-1},v_0,\ldots v_{n-1} \in QuotR$ finden, denn da wir in $R[X]$ eindeutige Primzerlegung haben, haben wir sie erst recht in R und können daher eine Lösung aus $(QuotR)^{m+n}$ durch Multiplikation mit dem Hauptnenner zu einer aus R^{m+n} machen:
$u \cdot f = (u_{m-1}x^{m-1} + \cdots + u_1x + u_0)(a_nx^n + \cdots + a_1x + a_0)$
Ausmultiplizieren liefert:

$$\begin{aligned} a_nu_{m-1}x^{m+n-1} &+ (a_{n-1}u_{m-1} + a_nu_{m-2})x^{m+n-2} \\ &+ (a_{n-1}u_{m-1} + a_{n-1}u_{m-2} + a_nu_{m-1})x^{m+n-3} + \ldots \\ &+ (a_0u_2 + a_1u1 + a_2u_0)x^2 + (a_0u_1 + a_1u_0)x + a_0u_0 \end{aligned}$$

Ganz entsprechend ist

$$\begin{aligned} v \cdot g = b_mv_{n-1}x^{m+n-1} &+ (b_{m-1}v_{n-1} + b_mvn - 2)x^{n+m-2} + \ldots \\ &+ (b_0v_1 + b_1v_0)x + b_0v_0 \end{aligned}$$

Koeffizientenvergleich:

$$\begin{aligned} &a_nu_{m-1} - b_mv_{n-1} = 0 \\ &a_{n-1}u_{m-1} + a_nu_{m-2} - b_{m-1}v_{n-1} = 0 \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \\ &a_0u_1 + a_1u_0 - b_0v_1 - b_1v_0 = 0 \\ &a_0u_0 - b_0v_0 = 0 \end{aligned}$$

Dies ist ein homogenes lineares Gleichungssystem aus $m+n$ Gleichungen in den $m+n$ Unbekannten $u_{m-1},\ldots,u_0,v_{n-1},\ldots v_0$. Es hat genau dann eine nichttriviale Lösung, wenn seine Matrix Determinante Null hat.

Ist $(u_{m-1},\dots,u_0,v_{n-1},\dots v_0)$ eine nichttriviale Lösung dieses linearen Gleichungssystems, so ist $(u_{m-1},\dots,u_0,-v_{n-1},\cdots - v_0)$ eine nichttriviale Lösung des entsprechenden linearen Gleichungssystems in dem alle Minuszeichen durch Pluszeichen ersetzt wurden. Daher ist die nichttriviale Lösbarkeit der beiden Gleichungssysteme äquivalent und auch äquivalent dazu, dass die Determinante der folgenden Matrix verschwindet:

u_{m-1}	$u_m - 2$	$\dots$	u_1	u_0	v_{n-1}	v_{n-2}	$\dots$	v_1	v_0
a_n					b_m				
a_{n-1}	a_n				b_{m-1}	b_m			
a_{n-2}	a_{n-1}	a_{n-1}	a_n		b_{m-2}	b_{m-1}	b_m		
$\vdots$	$\vdots$	$\vdots$			$\vdots$	$\vdots$	$\vdots$		
a_0	a_1	a_2			b_0	b_1	b_2		

Die einzelnen Koeffizienten a_i, b_j stehen jeweils in Parallelen zur Hauptdiagonalen der Matrix. Innerhalb der Spalten sinken die Indizes von Zeile zu Zeile jeweils um 1, wobei der erste von Null verschiedene Eintrag bei den a s in der Diagonalen steht und a_n ist. Bei den b s steht er in der um m-1 Positionen nach rechts verschobenen Diagonalen und ist b_m. Die Determinante dieser Matrix verschwindet genau dann , wenn die der transponierten Matrix verschwindet. Diese transponierte Matrix heißt **Sylvestermatrix**, und ihre Determinante heißt **Resultante** $Res_X(f,g)$ von f und g bezüglich X.

$$Res_X(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & & a_0 & & & \\ & a_n & a_{n-1} & \cdots & & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_n & a_{n-1} & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & b_{m-1} & \cdots & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & b_m & b_{m-1} & \cdots & & b_0 \end{vmatrix}$$

Die Matrix setzt sich zusammen aus m Zeilen, in denen jeweils f um eins verschoben wird, und n Zeilen, in denen g verschoben wird.

Effiziente Berechnung der Resultante:
$f,g \in R[X]$ seien zwei Polynome. R ein Ring derart, dass es in $R[X]$ eindeutige Primzerlegung gibt. Angenommen f und g haben einen gemeinsamen Faktor p vom Grad $p \geq 1$ (nicht konstantes Polynom). Wir dividieren f durch g mit Rest :
$f : g = q$ Rest r oder $f = q \cdot g + r$
p teilt f und g, also auch $r = f - q \cdot g$.
Umgekehrt:
Ist p gemeinsamer Faktor von g und r, so auch von $f = q \cdot g + r$.
Also ist $Res_X(f,q) = 0 \Leftrightarrow Res_X(g,r) = 0$.
Wir betrachten die Polynomdivison mit Rest schrittweise zusammen mit ihren Auswirkungen auf die Sylvestermatrix:

$$f = a_n x^n + \cdots + a_1 x + a_0$$

$$g = b_m x^m + \ldots b_1 x + b_0$$

Sei zunächst $n = 0$:
Da die Sylvestermatrix m Zeilen aus Koeffizienten von f und n Zeilen aus Koeffizienten von g enthält, ist sie gleich:

$$\begin{pmatrix} a_0 & 0 & \cdots & 0 \\ 0 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_0 \end{pmatrix}$$

d.h. $Res_X(f,g) = a^m$.

Nun sein n beliebig. Wir dividieren g durch f:

$$g : f = q \quad Rest \quad h$$

Bei dieser Division wird g sukzessive ersetzt durch eine Folge von Po-

lynomen immer kleineren Grades, deren Letztes der Rest h ist.

$$g = g_0, g_1, \ldots, g_r = h$$

$$g_i = g_{i+1} - q_i x^j f$$

mit $j = deg\, g_i - deg\, f, \quad q_i \in QuotR.$

Die Zeilenvektoren der Sylvestermatrix sind Vektoren aus R^{n+m}. Die ersten m Zeilen sind die Koeffizientenvektoren der Polynome

$$x^{m-1}f, x^{m-2}f, \ldots xf, f$$

die restlichen n Zeilen sind die Koeffizientenvektoren von $x^{n-1}g, \ldots xg, g$.
Im ersten Divisionsschritt ersetzen wir g durch ein Polynom der Form

$$g - \lambda x^j f, \quad j = m - n, \lambda$$

so, dass in der Differenz der höchste Term verschwindet ($m \geq n$).

Der Koeffizientenvektor von $x^j f$ ist einer unserer Zeilenvektoren, der von g auch. Ersetzen wir den Letzteren durch den von

$$g_1 = g - \lambda x^j f$$

subtrahieren wir ein Vielfachen einer Zeile von einer anderen. Durch diese Zeilenoperation ändert sich die Determinante nicht. Auch alle anderen Schritte der Polynomdivison führen zu solchen Zeilenoperationen. Wir können also in der Sylvestermatrix g schrittweise durch $g_1, g_2 \ldots$ und schließlich h ersetzen, ohne dass sich die Determinante ändert.

Ist $h = c_s x^s + \cdots + c_1 x + c_0$ mit $s < m$, so wird h aufgefasst als Polynom vom Grad m:
$h = c_m x^m + \cdots + c_1 x + c_0$, mit $c_m = c_{m-1} = \cdots = c_{s+1} = 0$.
Wir haben also die Determinante:

$$\begin{vmatrix}
a_n & a_{n-1} & \cdots & & a_0 & & & \\
 & a_n & a_{n-1} & \cdots & & a_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & a_n & a_{n-1} & \cdots & & a_0 \\
c_m & c_{m-1} & \cdots & & c_0 & & & \\
 & c_m & c_{m-1} & \cdots & & c_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & c_m & c_{m-1} & \cdots & & c_0
\end{vmatrix}$$

Wegen $c_m = 0$ stehen in der ersten Spalte abgesehen von a_n oben links nur Nullen. Entwickeln wir nach der ersten Spalte, ist die Determinante also gleich
$a_n \cdot$ Determinante der Matrix ohne erste Zeile und Spalte.

Solange auch $(m-1) > s$ ist, d.h. $c_{m-1} = 0$, hat die neue Matrix die selbe Gestalt, d.h. wir können auch die zweite Zeile und Spalte der Ausgangsmatrix streichen, und erhalten einen weiteren Faktor a_n. Dies können wir wiederholen bis c_s in der ersten Spalte der reduzierten Matrix steht.
Wir erhalten also die Resultante von f und g:

$$\begin{aligned}
Res_X(f,g) &= a_n^{m-s} \cdot \begin{vmatrix}
a_n & a_{n-1} & \cdots & & a_0 & & & \\
 & a_n & a_{n-1} & \cdots & & a_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & a_n & a_{n-1} & \cdots & & a_0 \\
c_s & c_{s-1} & \cdots & & c_0 & & & \\
 & c_s & c_{s-1} & \cdots & & c_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & c_s & c_{s-1} & \cdots & & c_0
\end{vmatrix} \\
&= a_n^{m-s} \cdot Res_X(f,h)
\end{aligned}$$

Dieses Verfahren können wir iterieren, indem wir auch wieder das Polynom größeren Grades durch das andere dividieren usw. Da die Grade der Reste immer kleiner werden, erreichen wir schließlich, dass eines der Polynome konstant wird.

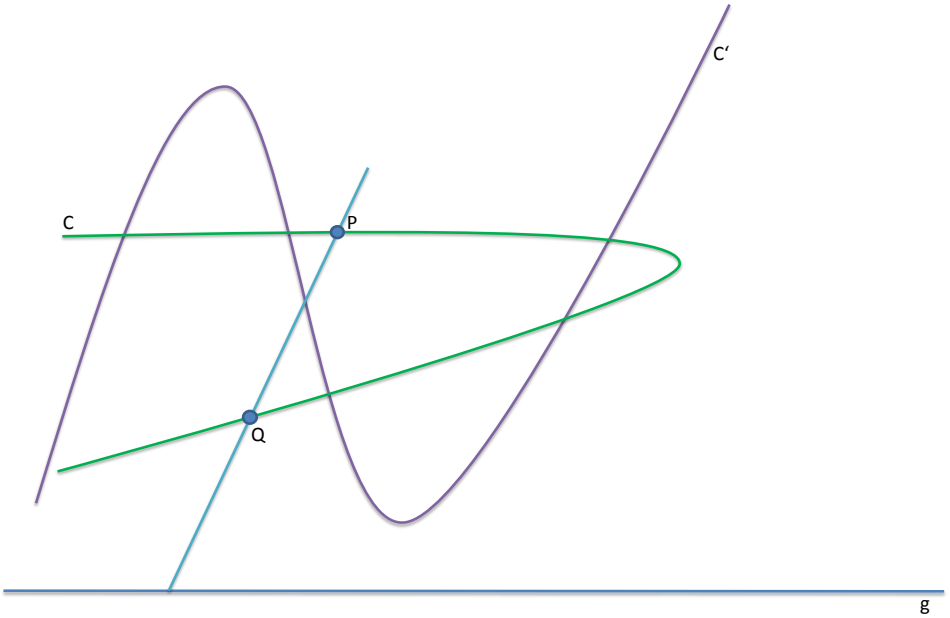
Lemma:
Ist $deg\, f = n$ und $deg\, g = m$, so ist

$$Res_x(f,g) = (-1)^{nm} \cdot Res_x(f,g)$$

Beweis:
Wir vertauschen die unterste f-Zeile nacheinander mit jeder der n g-Zeilen. Nach diesen m Vertauschungen steht sie unten. Dann verfahren wir genauso mit der nun untersten f Zeile usw. Die Gesamtanzahl der Zeilenvertauschungen ist mn. Damit könne wir die Resultante á la Euklid berechnen. □

1.5 Vielfachheit von Schnitten - Der Satz von Bezout

Ziel: Satz von Bezout
Zähle die Schnittpunkte zweier ebener Kurven C, C'. Sind D, D', D'' ebene Kurven, so auch $D \cup D'$ und $D \cup D''$, und ihre Schnittmenge enthält D, d.h. falls der Körper k algebraisch abgeschlossen ist, gibt es unendlich viele Schnittpunkte. Diesen Fall wollen wir ausschließen. Wir wählen einen Punkt $Q \in \mathbb{P}^2(k), k$ algebraisch abgeschlossener Körper, der auf keiner der beiden Kurven C, C' liegt, sowie eine Gerade g, die nicht durch Q geht, dann können wir die projektive Ebene $\mathbb{P}^2(k) \setminus \{0\}$ auf g projizieren, indem wir jeden Punkt $P \neq Q$ den Schnittpunkt der Geraden durch P und Q mit g zuordnen.



Wir wählen für $\mathbb{P}^2(k)$ ein Koordinatensystem derart, dass $Q = (0:0:1)$ ist, und g die durch $z = 0$ gegebene Gerade. Q entspricht einem eindimensionalen Untervektorraum U von k^3. Die Punkte von g sind ebenfalls eindimensionale Untervektorräume von k^3, es sind genau die, die in einem gewissen zweidimensionalen Untervektorraum $W \leq k^3$ liegen.
Nach Voraussetzung gilt:
$Q \notin g$, d.h. U ist kein Untervektorraum von W, d.h. $U \cap W = \{0\}$.
$b_1, b_2 \in k^3$ sei eine Basis von W, und b_3 sein eine von U.

Dann bilden b_1, b_2, b_3 eine Basis von k^3, d.h. jedes $v \in k^3$ lässt sich schreiben als :

$$v = xb_1 + yb_2 + zb_3$$

und mit diesen Koordinaten ist

$$W = \{v \in k^3 \mid z = 0\}$$

und

$$U = \{v \in k^3 \mid x = y = 0\}$$

Die Projektion von $\mathbb{P}^2 \backslash \{Q\}$ nach g ist dann einfach gegeben durch

$$(x : y : z) \longrightarrow (x : y : 0)$$

Im neuen Koordinatensystem sei

$$C = \{(x : y : z) \mid f(x,y,z) = 0\}$$

und

$$C' = \{(x : y : z) \mid \tilde{f}(x,y,z) = 0\}$$

$f \in k[x,y,z]$ sei homogen vom Grad d, $\tilde{f} \in k[x,y,z]$ homogen vom Grad e.Wir nehmen an, weder in f noch in $\tilde{f}$ sei ein irreduzibler Faktor mit einer höheren Potenz als 1. Außerdem sollen f und $\tilde{f}$ keinen gemeinsamen Faktor positiven Grades besitzen.
Konkret sei:

$$f(x,y,z) = a_0(x,y)z^d + a_1(x,y)z^{d-1} + \ldots a_{d-1}(x,y)z + a_d(x,y)$$

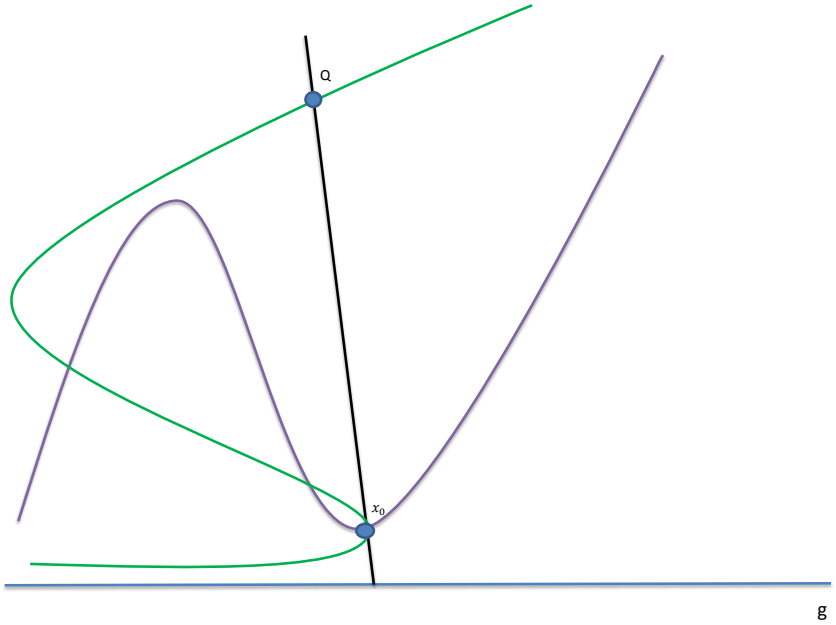
$$\tilde{f}(x,y,z) = b_0(x,y)z^e + b_1(x,y)z^{e-1} + \ldots b_{e-1}(x,y)z + b_e(x,y)$$

$a_i, b_i \in k[x,y]$ homogen vom Grad i.
$Q \notin C \cup C'$ d.h.

$$f(0,0,1) = a_0(0,0) \neq 0 \qquad \tilde{f}(0,0,1) = b_0(0,0) \neq 0$$

Wir fassen f und $\tilde{f}$ auf als Polynome in z mit Koeffizienten in $k[x,y]$ und betrachten $Res_z(f,\tilde{f})$. Das ist ein Polynom aus $k[x,y]$ und es ist nicht das Nullpolynom, da f und $\tilde{f}$ keinen gemeinsamen Faktor positiven Grades haben. Da alle a_i, b_i homogen sind, ist auch die Resultante

ein homogenes Polynom, ihr Grad ist $d \cdot e$.



Sei nun $P(x_0 : y_0 : z_0)$ ein Schnittpunkt von C und C', d.h.

$$a_0(x_0,y_0)_0 z^d + a_1(x_0,y_0)z_0^{d-1} + \ldots a_{d-1}(x_0,y_0)z_0 + a_d(x_0,y_0) = 0$$
$$b_0(x_0,y_0)z_0^e \; + \; b_1(x_0,y_0)z_0^{e-1} + \ldots b_{e-1}(x_0,y_0)z_0 + b_e(x_0,y_0) = 0$$

Die Polynome $f(x_0,y_0,z_0)$ und $\tilde{f}(x_0,y_0,z_0)$ haben also z_0 als gemeinsame Nullstelle, und $z - z_0$ als gemeinsamen Faktor. Somit verschwindet die Resultante der beiden Polynome. Da die Resultantenbildung und das Einsetzen der speziellen Werte $x = x_0$ und $y = y_0$ miteinander vertauschbar sind, folgt, dass

$$Res_z(f,\tilde{f})(x_0,y_0) = 0$$

sein muss. $Res_z(f,\tilde{f})(x_0,y_0)$ ist ein homogenes Polynom vom Grad $e \cdot d$, also gibt es höchstens $d \cdot e$ viele Punkte $(x_0 : y_0 : 0)$ auf g, für die sie verschwindet. Das bedeutet, dass es höchstens $e \cdot d$ Geraden durch Q gibt, insbesondere also endlich viele, die einen Schnittpunkt von C mit C' enthalten. Jede dieser endlich vielen Geraden enthält höchstens d Schnittpunkte mit C, also erst recht höchstens endlich viele Schnittpunkte von C und C'. Somit haben C und C' höchstens endlich viele

Schnittpunkte (nicht wie z.B. bei Sinus und Kosinus unendlich viele).

Lemma:
Es gibt höchstens de Schnittpunkte.

Beweis:
Angenommen es gäbe mehr Schnittpunkte, also mindestens $de+1$ Punkte

$$p^{(1)},\ldots,p^{(de+1)} \in C \cap C'$$

Wir wählen den Punkt Q nun so, dass er nicht auf C oder C' liegt und auch nicht auf der Verbindungsgeraden zweier Punkte $p^{(i)}$. g sei weiterhin irgendeine Gerade, die nicht durch Q geht. Bei der Projektion von

$$\mathbb{P}^2(k)\backslash\{Q\} \longrightarrow g$$

haben somit die $p^{(i)}$ allesamt verschiedene Bilder. Wir wählen unser Koordinatensystem wieder wie oben. Die Koordinaten von $p^{(i)}$ seien $(x_i : y_i : z_i)$. Da auf der Geraden auf $p^{(i)}$ und Q ein Schnittpunkt von C und C' liegt, ist

$$Res_Z(f,\tilde{f})(x^{(i)},y^{(i)}) = 0$$

Das gilt für $i = 1,2,\ldots de+1$, d.h. ein Polynom vom Grad de hat $de+1$ verschiedene Nullstellen.
Das geht nur für das Nullpolynom, d.h. $Res_Z(f,\tilde{f}) = 0$ also das Nullpolynom, im Widerspruch zur Voraussetzung, dass f und $\tilde{f}$ keinen gemeinsamen Faktor haben. □

Wir betrachten Q und g wie oben, verlangen jetzt aber, dass für keine zwei Schnittpunkte $P \neq P'$ der Punkt Q auf der Geraden durch P und P' liegt. Jeder Schnittpunkt von C und C' ist damit eindeutig bestimmt durch seine Projektion von Q auf g.
Seien C, C' Kurven:

$$F(x,y,z) = A_0(x,y)z^d + A_1(x,y)z^{d-1} + \cdots + A_d(x,y) = 0$$

$$G(x,y,z) = B_0(x,y)z^e + B_1(x,y)z^{e-1} + \cdots + B_e(x,y) = 0$$

Falls es einen Schnittpunkt $(c_0 : c_1 : c_2)$ gibt, ist dort

$$Res_z(F,G)(c_0,c_1) = 0$$

Die Vielfachheit der Nullstelle bezeichnen wir auch als Schnittmultiplizität von C, C' im Punkt (c_0, c_1, c_2). Damit folgt:

Satz von BEZOUT:
Zwei projektive ebene Kurven der Grade d und e die keine gemeinsame Komponente haben, schneiden sich mit Vielfachheiten gezählt in $\mathbb{P}^2(k), k$ algebraisch abgeschlossen, genau $d \cdot e$ mal.

Beweis:
Die Resultante $Res_Z(F,G)$ ist ein homogenes Polynom vom Grad de, d.h.

$$Res_Z(F,G) = \mu_{de}x^{de} + \mu_{de+1}x^{de+1}y + \cdots + \mu_0 y^{de}$$

Sei $r \in \mathbb{N}_0$ die kleinste Zahl, für die $\mu_{de-r} \neq 0$
Dann lässt sich die Resultante schreiben als

$$y^r(\mu_{de-r}x^{de-r} + \ldots \mu_0 y^{de-r})$$

wobei $\mu_{de-r} \neq 0$.
Damit haben wir eine r-fache Nullstelle im Punkt $(1:0)$. Das Polynom

$$\mu_{de-r}x^{de-r} + \mu_{de-r-1}x^{de-r-1} + \cdots + \mu_1 x + \mu_0$$

hat mit Vielfachheiten gezählt $de - r$ Nullstellen $x_1, \ldots, x_{de-r}$. Das homogene Polynom dazu hat also die Punkte $(x_i : 1)$ als Nullstellen, d.h.

$$Res_Z(F,G) = y^r \cdot \prod_{i=1}^{de-r}(x_i y - x)\mu_{de-r} \in k^\times$$

Für jeden dieser Punkte gibt es genau einen Schnittpunkt von C und C' auf der Verbindungsgeraden dieses Punktes mit $(0:0:1)$ und nach Definition ist die Schnittmultiplizität gleich der Vielfachheit des Faktors, d.h. die Schnittmultiplizitäten addieren sich zu de. □

Lemma:
Die oben definierte Schnittmultiplizität ist unabhängig von der Wahl des Koordinatensystems.

Beweis:
Wir gehen aus von Koordinaten $(x : y : z)$ wie oben., d.h.

$$(0:0:1) \notin C \cup C' \cup \bigcup L_{ij}$$

mit L_{ij}= Gerade durch den i-ten und j-ten Schnittpunkt von C und C'. Jedes andere Koordinatensystem erhalten wir daraus durch eine lineare Transformation

$$(x : y : z) \to (x' : y' : z')$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow A \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

Mit einer invertierbaren $3x3$ Matrix A.

Dabei soll $A \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ einen Punkt definieren, der nicht in $C \cup C' \cup \bigcup L_{ij}$liegt.

Explizit:
Sei

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{12} & a_{21} & a_{22} \end{pmatrix}$$

Dann ist

$$A \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{02} \\ a_{12} \\ a_{22} \end{pmatrix}$$

Ist $H \in k[X,Y,Z]$ das Produkt der Gleichungen von C und C' mal dem Produkt der linearen Polynome, die die L_{ij} definieren, so muss

$$H(a_{02}, a_{12}, a_{22}) \neq 0$$

sein. Wir fassen die Matrix auf als Punkt in k^9. $D(a_{00}, \ldots, a_{22})$ sei das Determinantenpolynom und

$$P(a_{00}, \ldots, a_{22}) = D(a_{02}, \ldots, a_{22}) \cdot H(a_{00}, a_{12}, a_{22})$$

Jeder Punkt $(a_{00}, \ldots a_{22}) \in k^9$, in dem P nicht verschwindet, definiert dann einen Koordinatenwechsel zu einem Koordinatensystem, das unseren Bedingungen genügt und umgekehrt.

Ein hier nicht bewiesener Satz aus der algebraischen Geometrie sagt uns, dass wir zwei Punkte aus k^9 , in denen P nicht verschwindet, durch einen Kantenzug verbinden können, derart, dass P in keinem Kurvenpunkt verschwindet.
Wir betrachten die Schnittmultiplizität von C und C' in einem Punkt $Q \in C \cap C'$ bezüglich der beiden Koordinatensysteme $(x : y : z)$ und (x', y', z'), wobei

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

Dann haben wir eine Kurve in

$$k^9 \setminus \{a_{00} \ldots, a_{22}) \in k^9 \mid P(a_{00}, \ldots, a_{22}) = 0\}$$

die den Punkt zur Einheitsmatrix mit dem zu A verbindet. Jeder Kurvenpunkt entspricht einem Koordinatensystem, das unsere Bedingungen erfüllt, so dass wir dort eine Schnittmultiplizität definieren können. Wir betrachten die Mengen aller Kurvenpunkte, in denen diese Schnittmultiplizität einen festen Wert r hat. Sie ist beschreibbar durch das verschwinden gewisser Polynome in $a_{00}, \ldots, a_{22}$. Diese Menge sei A_r und entsprechend definieren wir für andere vorkommende Schnittmultiplizitäten Mengen A_s Dann ist A die disjunkte Vereinigung endlich vieler solcher Mengen A_s und da A zusammenhängend ist, muss A gleich einem festen A_r sein, d.h. alle Schnittmultiplizitäten sind gleich.

□

Lemma:
C und C' seien Kurven ohne gemeinsame Komponente, und $P \in C \cap C'$. Dann gilt: Die Schnittmultiplizität von C und C' in P ist mindestens gleich dem Produkt der Vielfachheiten von P auf C bzw. C'. Sie ist genau dann gleich diesem Produkt, wenn die Tangenten durch P an C allesamt verschieden sind von denen durch P an C'.

Beweis:
r sei die Vielfachheit von P auf C, s die auf C'. Das Koordinatensystem $x : y : z$ sei so gewählt, dass $Q = (0 : 1 : 0)$ weder auf C noch auf C' noch auf der Verbindungsgeraden zweier Schnittpunkte, noch auf einer

Tangenten in P an C oder C' liegt.

$$F(x,y,z) = 0, \qquad G(x,y,z) = 0$$

seien die Gleichungen von C und C' und $P = (0:0:1)$.

$$f(x,y) = F(x,y,1), \qquad g(x,y) = G(x,y,1)$$

seien die entsprechenden Gleichungen in der affinen Ebene $z \neq 0$.
Wir betrachten f und g als Polynome in y mit Koeffizienten aus $k[x]$.
$R(f,g) \in k[x]$ sei die Resultante dieser beiden Polynome.

$$f(x,y) = f_0 y^d + f_1 y^{d-1} + \cdots + f_{d-r} y^r + f_{d-r-1} y^{r-1} + \cdots + f_d x^r y^0$$

$$g(x,y) = g_0 y^e + g_1 y^{e-1} + \cdots + g_{e-s} y^s + g_{e-s-1} y^{s-1} + \cdots + g_e x^s y^0$$

wobei $f_i, g_i \in k[x]$.

Die Gleichungen der Tangenten von C bzw. von C' in P ist

$$f_{d-r}(0) y^r + \cdots + f_d(0) x^r = 0$$

$$g_{e-s}(0) y^s + \cdots + g_e(0) x^s = 0$$

Wenn die Tangenten an C paarweise verschieden sind von denen an C', haben diese Gleichungen keinen gemeinsamen Faktor, d.h. ihre Resultante ist von 0 verschieden. Außerdem gilt: Auf der Geraden PQ liegt kein Schnittpunkt von C und C'. Daraus folgt: Die Gleichungen $f(0,y) = 0$ und $g(0,y) = 0$ haben nur $y = 0$ als gemeinsame Nullstelle. Es gibt genau dann eine gemeinsame Tangente, wenn die Resultante:

$$D_1 = \begin{vmatrix} f_{d-r}(0) & \cdots & & f_d(0) & \\ \ddots & & & \ddots & \\ & f_{d-r}(0) & \cdots & & f_d(0) \\ g_{e-s}(0) & \cdots & & g_s(0) & \\ \ddots & & & & \ddots \\ & g_{e-s}(0) & \cdots & & g_s(0) \end{vmatrix}$$

verschwindet.
Falls alle Tangenten an C paarweise verschieden sind zu denen an C', ist also $D_1 \neq 0$. Auf der Geraden PQ liegt außer P kein Schnittpunkt

von C und C': Somit ist $y = 0$ die einzige gemeinsame Nullstelle der Gleichungen $f(0,y) = 0$ und $g(0,y) = 0$.

$$f_0(0)y^{d-r} + f_1(0)y^{d-r-1} + \cdots + f_{d-r}(0) = 0$$

und

$$g_0(0)y^{e-s} + g_1(0)y^{e-s-1} + \ldots y_{e-s}(0) = 0$$

haben keine gemeinsame Lösung, da $f_{d-r}(0) \neq 0$ und $g_{e-s}(0) \neq 0$.
Somit ist:

$$D_2 = \begin{vmatrix} f_0(0) & \cdots & f_{d-r}(0) & & \\ \ddots & & \ddots & & \\ & f_0(0) & \cdots & & f_{d-r}(0) \\ g_0(0) & \cdots & g_{e-s}(0) & & \\ \ddots & & & \ddots & \\ & g_0(0) & \cdots & & g_{e-s}(0) \end{vmatrix} \neq 0$$

Aus D_1 und D_2 können wir wie folgt zur Resultante von f und g kommen:
Wir starten mit $Res(f,g)$ und multiplizieren die $(e-s+1)$-te Zeile mit x, die nächste mit x^2 usw. analog multiplizieren wir die $(d+e-r+1)$-te Zeile mit x, die nächste mit x^2 usw. die letzte, d.h. die $(d+e)$-te mit x^r.Die Determinante wird also insgesamt multipliziert mit

$$x^{1+\cdots+r} \cdot x^{1+\cdots+s} = x^{\frac{r(r+1)+s(s+1)}{2}} \qquad (*)$$

Nun dividieren wir die letzte Spalte durch x^{r+s}, die vorletzte durch x^{r+s-1} usw. bis zur $(e+d-r-s+1)$-ten Spalte, die durch g geteilt wird. Die Determinante wird daher dividiert durch:

$$x^{1+2+\cdots+(r+s)} = x^{\frac{(r+s)(r+s-1)}{2}}$$

Vergleich mit $(*)$:

$$Res(f,g) = x^{rs} \cdot D \qquad (**)$$

$D =$Determinante der gerade modifizierten Matrix. Setzen wir in D die Variable x auf 0 erhalten wir eine Matrix, deren Zeilen und Spalten aus den Zeilen und Spalten von D_1 und D_2 zusammengesetzt sind. Entwicklung nach der Ersten Spalte zeigt:

$$D(0) = D_1 \cdot D_2$$

Wir wissen: $D_2 \neq 0$ und $D_1 = 0 \Leftrightarrow C$ und C' haben in P eine gemeinsame Tangente. $(**)$ zeigt, dass $Res(f,g)$ in 0 eine mindestens rs-fache Nullstelle hat, d.h. die Schnittmultiplizität ist $\geq rs$. Sie ist genau dann größer, wenn $D(0) = 0$. $D(0) = D_1 \cdot D_2$ verschwindet genau dann, wenn $D_1 = 0$, d.h. wenn C und C' in P eine gemeinsame Tangente haben. □

Nächstes Problem:
Gegeben seien endlich viele Punkte aus $\mathbb{P}^2(k)$. Gibt es Kurven vom Grad d, die durch alle diese Punkte gehen?
Angenommen C und C' sind zwei solche Kurven. C sei gegeben durch die Gleichung $F(X,Y,Z) = 0$ und C' durch die Gleichung $G(X,Y,Z) = 0$. $F,G \in k[X,Y,Z]$ homogen vom Grad d. Für $\lambda,\mu \in k, \lambda \cdot \mu \neq 0$, ist auch $\lambda F + \mu G$ ein homogenes Polynom vom Grad d, das ebenfalls in den gegebenen Punkten verschwindet. Die homogenen Polynome vom Grad d, die in gewissen vorgegebenen Punkten aus $\mathbb{P}^2(k)$ verschwinden, bilden also einen k-Vektorraum. Falls dies der Nullraum ist, gibt es keine Kurve vom Grad d, die durch alle solche vorgegebenen Punkte geht. Andernfalls definiert jedes Polynom aus diesem Raum, ungleich dem Nullpolynom, eine solche Kurve. Natürlich definieren F und λF, für $\lambda \in k \setminus \{0\}$ die selbe Kurve.

Beispiel: $d = 9$
Angenommen wir haben zwei Polynome F_1 und F_2 vom Grad 3, so dass $F = F_1 F_2^2$ in allen vorgegebenen Punkten verschwindet. Dann verschwindet auch $G = F_1^2 F_2$ in all diesen Punkten. Dies ist im Allgemeinen kein skalares Vielfaches von F.

Definition:
Ein **Divisor** ist eine formale Linearkombination

$$D = \sum_{i=1}^{r} a_i C_i \qquad r \in \mathbb{N}, a_i \in \mathbb{Z}$$

wobei C_i eine irreduzible Kurve, also die Nullstellenmenge eines irreduziblen Polynoms ist. Der Divisor heißt **effektiv**, in Zeichen $D \succ 0$, wenn die $a_i \geq 0$ sind und mindestens ein $a_i > 0$.

Ist $F \in k[X,Y,Z]$ ein homogenes Polynom mit Zerlegung $F = c \cdot F_1^{e_1} \dots F_r^{e_r}$ in irreduzible Polynome, so können wir F den Divisor

$$D = \sum_{i=1}^{r} e_i C_i$$

zuordnen

$$C_i = \{(x:y:z) \in \mathbb{P}^2(k) \mid F_i(x,y,z) = 0\}$$

Definition:
$D = \sum_{i=1}^{r} e_i C_i$ sei ein Divisor, C_i eine irreduzible Kurve vom Grad d. Dann heißt

$$\deg D = \sum_{i=1}^{r} e_i d_i$$

der **Grad** von D. Ist also $f = \prod_{i=1}^{r} f_i^{e_i}$ ein homogenes Polynom aus $k[X,Y,Z]$ vom Grad d, so hat auch der zugehörige Divisor $D = \sum_{i=1}^{r} e_i V(f_i)$ den Grad d.

$$V(f_i) = \{(x:y:z) \in \mathbb{P}^2(k) \mid F_i(x,y,z) = 0\}$$

Die homogenen Polynome vom Grad d bilden zusammen mit dem Nullpolynom einen Vektorraum der Dimension

$$\binom{d+2}{d}$$

Für $\lambda \in k \backslash \{0\}$ definieren f und λf denselben Divisor. Diese Divisoren bilden also einen projektiven Raum in einer Dimension weniger:

$$\binom{d+2}{d} - 1$$

Wir bezeichnen ihn als das lineare System der (effektiven) Divisoren vom Grad d, und betrachten im Folgenden lineare Teilsysteme davon, d.h. projektive Unterräume, die durch irgendwelche Bedingungen festgelegt sind, z.B. $f_1, \dots f_r$ homogene Polynome vom Grad d dann bilden die Divisoren zu den Polynomen $\lambda_1 f_1 + \dots + \lambda_r f_r$ mit $\lambda_i \in k$ nicht alle gleich Null, ein lineares System der Dimension $r-1$.

Meist spezifizieren wir lineare Systeme dadurch, dass die Divisoren mit einer gewissen Vielfachheit durch einen Punkt gehen sollen:
Ist $P \in \mathbb{P}^2(k)$ ein m_i-facher Punkt auf der Kurve C_i, wobei $m_i \neq 0$, falls $P \notin C_i$, so geht $D = \sum_{i=1}^{r} e_i C_i$ mit Vielfachheit $\sum_{i=1}^{r} e_i m_i$ durch P. Betrachten wir zunächst die Bedingung, dass D den Punkt P enthält, d.h. Vielfachheit ≥ 1. Ist

$$F(X,Y,Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-j}$$

und D der Divisor zu f, so bedeutet dies, dass für $P = (p_0, p_1, p_2)$ gelten muss:

$$f(p_0, p_1, p_2) = \sum_{i,j} a_{ij} p_0^i p_1^j p_2^{d-j} = 0$$

Das ist eine lineare Gleichung für die Koeffizienten a_{ij}, definiert also einen Untervektorraum des Vektorraums aller homogenen Polynome. Also hat der Vektorraum die Kodimension 1. Nun sei $m > 1$. Wir betrachten alle Polynome, die mit Vielfachheit $\geq d$ im Punkt P verschwinden. Wir wählen unser Koordinatensystem so, dass $P = (0:0:1)$.

$$f(0,0,1) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} a_{ij} 0^i 0^j 1^{d-j}$$

mit $0^0 = 1$, d.h. **einfache Nullstelle** bedeutet

$$a_{00} = 0$$

Doppelte Nullstelle: Jetzt dürfen auch die Terme $a_{10} X Z^{d-1}$ und $a_{01} Y Z^{d-1}$ nicht vorkommen , denn das sind die partiellen Ableitungen von f nach X bzw Y im Punkt P.
Bedingung:

$$a_{00} = a_{10} = a_{01} = 0$$

m-fache Nullstelle: Alle a_{ij} mit $i + j < m$ müssen verschwinden.
Für gegebenes $i \in \{0, \ldots, n-1\}$ gibt es $(m-i)$-Möglichkeiten für j, nämlich $j \in \{0, \ldots, m-i-j\}$ insgesamt also:

$$\sum_{i=0}^{m-1} (m-i) = m^2 - \sum_{i=0}^{m-1} i = m^2 - \frac{m(m-1)}{2} = \frac{2m^2 - m^2 + m}{2} = \frac{m(m+1)}{2}$$

Paare (i,j), für die $a_{i,j} = 0$ sein muss. Somit ist die Bedingung, dass P (mindestens) ein m-facher Punkt sein soll, äquivalent zu $\frac{m(m+1)}{2}$ linear unabhängigen Gleichungen in den Koeffizienten; das lineare System aller solcher Divisoren hat also die Kodimension

$$\frac{m(m+1)}{2}$$

Betrachten wir die Menge aller Divisoren vom Grad d, die Punkte $P_1,\dots,P_r$ jeweils mit Vielfachheit $m_1,\dots,m_r$ enthalten sollen, so hat das entsprechende lineare System also mindestens die Dimension

$$\binom{d+2}{2} - 1 - \sum_{i=1}^{r} \frac{m_i(m_i+1)}{2}$$

Definition:
r Punkte $P_1,\dots P_r \in \mathbb{P}^2(k)$ sind **in allgemeiner Lage** bezüglich Divisoren (bzw. Kurven) vom Grad d, wenn das lineare System aller Divisoren vom Grad d, die durch $P_1,\dots,P_r$ gehen, die maximal mögliche Dimension

$$\binom{d+2}{2} - 1 - r$$

hat, bzw. leer ist, falls diese Zahl negativ ist.

Beispiel:

- $d = 1, r = 3$.
  Drei Punkte sind genau dann in allgemeiner Lage bzgl. Kurven vom Grad 1 (Geraden), wenn sie nicht auf einer Geraden liegen, d.h. das entsprechende System leer ist.
- d=1, r=2
  $$\binom{d+2}{2} - 1 - 2 = 0$$
  d.h. zwei Punkte sind in allgemeiner Lage bzgl. Geraden, wenn es genau eine Gerade durch die beiden Punkte gibt, d.h. wenn sie verschieden sind

Grundsätzlich gilt:
Im Allgemeinen sind r Punkte $P_1,\dots P_r$ in allgemeiner Lage bzgl. Kurven vom Grad d.

Das soll bedeuten: Sind $P_1,\dots P_r$ in allgemeiner Lage, so betrachten wir die Menge aller r-Tupel $(Q_1,\dots Q_r) \in \mathbb{P}^2(k)^r$ mit der Eigenschaft, dass $Q_1,\dots Q_r$ nicht in allgemeiner Lage sind. Die Bedingung, dass der Divisor zum Polynom f vom Grad d durch $Q_1,\dots,Q_r$ gehen soll, stellt die r linearen Bedingungen

$$f(Q_1) = \cdots = f(Q_r) = 0$$

an die Koeffizienten von f.
Wenn diese Gleichungen nicht linear unabhängig sind, können wir dies ausdrücken durch das Verschwinden gewisser Determinanten in den Koeffizienten dieser Gleichungen, d.h. in Polynomen in den Koordinaten der Q_i. Diese Polynome sind nicht alle gleich dem Nullpolynom, denn da es Punkte $P_1,\dots P_r$ in allgemeiner Lage gibt, verschwinden zumindest für deren Koeffizienten nicht alle, d.h. die Koeffizienten müssen linear unabhängig sein. Somit gibt es endlich viele Polynome in den Koeffizienten der Q_i derart, dass $Q_1,\dots Q_r$ genau dann in allgemeiner Lage sind, wenn diese Polynome für $Q_,\dots,Q_r$ verschwinden.

Satz:
C und C' seien Kurven vom Grad d, die sich in genau d^2 verschiedenen Punkten schneiden. Wenn genau $d \cdot e$ dieser Punkte auf einer irreduziblen Kurve C'' vom Grad e liegen, liegen die restlichen $d \cdot (d-e)$ auf einer Kurve vom Grad $(d-e)$.

Beweis:
$F(X,Y,Z) = 0$ sei die Gleichung von C und $G(X,Y,Z) = 0$ die von C'. Wir betrachten das Büschel $\mathcal{L}$ der Kurven

$$\lambda F(X,Y,Z) + \mu G(X,Y,Z) = 0, \quad (\lambda : \mu) \in \mathbb{P}^1$$

Alle Kurven/ Divisoren aus $\mathcal{L}$ gehen durch die d^2 Schnittpunkte von C und C'. Sei $Q \in C''$, aber $Q \notin C$. Dann gibt es eine Kurve aus $\mathcal{L}$, die durch Q geht, denn dies stellt nur eine lineare Bedingung an die Elemente von $\mathcal{L}$. $\tilde{C}$ sei so eine Kurve.
C'' und $\tilde{C}$ schneiden sich einmal in den $d \cdot e$ Schnittpunkten von C und C'', außerdem noch in Q. Also haben C''und $\tilde{C}$ mindestens $de+1$ Schnittpunkte. Nach dem Satz von Bezout haben C'' und $\tilde{C}$ eine gemeinsame Komponente, die wegen der Irreduzibilität von C'' nur C'' selbst

sein kann. Also ist C'' eine Komponente von $\tilde{C}$, d.h.

$$\tilde{C} = C'' \cup C'''$$

mit einer (nicht notwendigerweise irreduziblen) Kurve C''' vom Grad $d - e$. Da alle d^2 Schnittpunkte von C und C' auf $\tilde{C}$ liegen und genau $d \cdot e$ davon auf C'', liegen die restlichen $d(d-e)$ auf C'''.

□

2 Elliptische Kurven und Weierstraßsche Normalform

k sei ein beliebiger Körper

Definition:
Eine **elliptische Kurve** über einem Körper k ist eine irreduzible ebene Kurve vom Grad 3 in $\mathbb{P}^2(k)$, die keine singulären Punkte hat und mindestens einen Punkt mit Koordinaten in k enthält.

Ist K irgendein Körper, der K enthält, und E eine elliptische Kurve über k, so bezeichnen wir mit $E(K)$ die Menge aller Punkte auf E mit Koordinaten in K.

Konkret:
Ist E gegeben durch das homogene kubische Polynom $F \in k[X,Y,Z]$, so ist für jeden Körper K, der k enthält,

$$E(K) = \{(x:y:z) \in \mathbb{P}^2(k) \mid F(x,y,z) = 0\}$$

Das lineare System aller Kurven/Divisoren vom Grad 3 in $\mathbb{P}^2(k)$ ist neundimensional, im Allgemeinen geht durch neun vorgegebene Punkte der projektiven Ebene genau eine Kurve vom Grad 3. Sind E, E' zwei kubische Kurven ohne gemeinsame Komponente, so gibt es über dem algebraischen Abschluss K von k mit Vielfachheiten gezählt, neun Schnittpunkte.

Satz:
E, E' seien kubische Kurven, die sich in genau neun Punkten schneiden und $\mathcal{L}$ sei das von E und E' erzeugte Büschel kubischer Kurven. Sind dann $P_1, \ldots P_8$ irgendwelche acht der neun Schnittpunkte, so geht jede kubische Kurve durch $P_1, \ldots P_8$ auch durch den neunten Schnittpunkt P_9.

Das lineare System $\mathcal{L}$ aller kubischer Kurven durch $P_1, \dots P_8$ ist gleich $\mathcal{L}$.

Beweis:

1. **Keine vier der Punkte $P_1, \dots, P_9$ liegen auf einer Geraden**
   Angenommen, die Gerade G enthalte vier der Punkte P_i. Wende Bezout an auf E und g bzw E' und g. Danach muss g Komponente von sowohl E als auch E' sein. Das geht nicht, da es genau neun Schnittpunkte gibt

2. **Keine sieben der Punkte $P_1, \dots, P_9$ liegen auf einer Quadrik**
   Wäre Q eine Quadrik, die sieben der Punkte enthält, würde sowohl $Q \cap E$, als auch $Q \cap E'$ mindestens sieben Punkte enthalten. Falls Q irreduzibel ist, folgt nach Bezout, dass Q gemeinsame Komponente von E und E' sein muss $\lightning$
   Ist $Q = g_1 \cup g_2$ irreduzibel, so müssen auf mindestens einer der beiden Geraden 4 P_i liegen. Das haben wir schon in (1) ausgeschlossen.

3. **Durch je 5 der Punkte geht genau eine Quadrik**
   Da das lineare System aller Quadriken in $\mathbb{P}^2(k)$ die Dimension 5 hat, gibt es auf jeden Fall eine Quadrik durch fünf vorgegebene Punkte. Angenommen, 5 der P_i liegen sowohl auf einer Quadrik Q, als auch auf einer davon verschiedenen Quadrik Q'. Nach Bezout müssen Q und Q' eine Gerade g als gemeinsame Komponente haben, d.h.
   $$Q = g \cup h, \qquad Q' = g \cup h'$$
   Auf g liegen höchstens 3 der P_i, denn nach (1) können keine 4 oder mehr drauf liegen, also liegen mindestens zwei der P_i sowohl auf h als auch auf h', d.h. $h = h'$ und $Q = Q'$.

4. **Wäre $\mathcal{L} \neq \mathcal{L}'$ so wären keine drei der P_i kollinear**
   Wenn $\mathcal{L} \neq \mathcal{L}'$, ist $\mathcal{L}' \subsetneq \mathcal{L}$, d.h. dim $\mathcal{L}' \geq 2$. Angenommen, drei der P_i sind kollinear, o.B.d.A seien P_1, P_2, P_3 Punkte auf der Geraden g. Die Punkte P_4, P_5, P_6, P_7, P_8 liegen nach (3) auf genau einer Quadrik Q. $P \in g$ sei verschieden von P_1, P_2, P_3 und $P' \in Q$ sei verschieden von $P_4, \dots P_8$. Da dim $\mathcal{L}' \geq 2$ ist, gibt es eine Kurve

$\hat{C} \in \mathcal{L}'$, mit $P, Q \in \hat{C}$. $\hat{C} \cap g \not\subseteq \{P_1, P_2, P_3, P_4\}$. Nach Bezout muss g eine Komponente von $\hat{C}$ sein, d.h. $\hat{C} = g \cup Q', Q'$ Quadrik.
$P_4, \ldots P_8 \notin g$, wegen (1). Also sind $P_4, \ldots P_8 \in Q'$. Da Q die einzige Quadrik durch $P_4, \ldots P_8$ ist, folgt $Q = Q'$, also ist $\hat{C} = g \cup Q$
$P' \in Q$, aber $P' \notin \hat{C}, P' \notin g$ $\lightning$

5. **Falls $\mathcal{L} \neq \mathcal{L}'$ liegen keine sechs der P_i auf einer Quadrik**
   Angenommen $P_1, \ldots P_6$ liegen auf einer Quadrik Q. Wegen (4) muss Q irreduzibel sein, sonst lägen 3 Punkte auf einer Geraden $\lightning$
   g sei die Gerade durch P_7 und P_8. Sei $P \in Q\{P_1, \ldots P_6\}, P' \in g'\{P_7, P_8\}$.
   Da dim $\mathcal{L}' \geq 2$ gibt es ein $\hat{C} \in \mathcal{L}' : P, P' \in \hat{C}$
   $\hat{C} \cap Q \not\subseteq \{P_1, \ldots P_6\}$, d.h. Q ist Komponente von $\hat{C} = Q \cup g'$. Wegen (2) sind $P_7, P_8 \notin Q$, also $P_7, P_8 \in g'$. Da $P_7, P_8 \in g \Rightarrow g = g'$ und $\hat{C} = Q \cup g$. Aber $P' \notin Q \cup g$, aber $P' \in \hat{C}$ $\lightning$

6. $\mathcal{L} = \mathcal{L}'$
   Angenommen, dies würde nicht gelten. g sei eine Gerade durch P_1 und P_2. Q die nach (3) eindeutige Quadrik durch $P_3, \ldots P_8$. Wähle $\tilde{P}_1\tilde{P}_2 \neq P_1P_2$. Da dim $\mathcal{L}' \geq 2$, da $\mathcal{L}' > \mathcal{L} : \exists \hat{C} \in \mathcal{L}'$ durch $\tilde{P}_1\tilde{P}_2$. Nach Bezout ist g Komponente von $\hat{C} \Rightarrow \tilde{C} = Q' \cup g, P_3, \ldots, P_7 \in Q'$ (da sie nicht auf g liegen) $\Rightarrow Q' = Q$.
   Also ist $\hat{C} = Q \cup g, P_8 \in \hat{C}$, aber $P_8 \notin g$ wegen (4) und $P_8 \in Q$ wegen (5) $\lightning$ da $P_8 \in \hat{C}$.

□

Wir betrachten die beiden Kurven
$y = x^4$ und $y = (x - \epsilon_1)(x - \epsilon_2)(x - \epsilon_3)(x - \epsilon_4)$ mit $\epsilon_i \neq 0$ und alle e_i verschieden. $y = x^4$ hat in $(0,0)$ die x-Achse $y = 0$ als Tangente. Setze $y = 0 \Rightarrow$ wir erhalten die Gleichung $x^4 = 0$, d.h. die x- Achse schneidet die Kurve im Punkt $(0,0)$ mit Vielfachheit 4. Bei der zweiten Kurve dagegen haben wir in jedem der vier Punkte $(\epsilon_i, 0)$ eine andere Tangente, die nur mit Vielfachheit zwei schneiden. Lassen wir die ϵ_i gegen Null gehen, fallen diese vier Tangenten zusammen; im Punkt $(0,0)$ der ersten Kurve liegt also eine besondere Situation vor. Für die kubische Parabel $y = x^3$ ist $y = 0$ ebenfalls Tangente im Nullpunkt; hier ist die Schnittmultiplizität gleich 3.

Definition:

a) Ein nichtsingulärer Punkt einer ebenen Kurve $C \subseteq \mathbb{P}^2(k)$ heißt **Wendepunkt** , wenn seine Tangente keine Komponente von C ist und die Schnittmultiplizität von C mit seiner Tangente in diesem Punkt dort größer oder gleich 3 ist.

b) Wir reden von einem r**-fachen Wendepunkt**, $r \geq 1$, falls diese Schnittmultiplizität $2 + r$ ist

Definition:
$C \subseteq \mathbb{P}^2(k)$ sei eine ebene Kurve, die nicht vollständig in Geraden zerfällt. Die **Hessesche**-Kurve $H_C \subseteq \mathbb{P}^2(k)$ ist die Nullstellenmenge der Hesseschen

$$\begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}$$

wobei F die Gleichung von C ist.
Ist d der Grad von F, so hat jede der partiellen Ableitungen von F den Grad $d-2$, die Hessesche ist also ein homogenes Polynom vom Grad $3(d-2)$ oder das Nullpolynom.

Beispiel:
$\deg F = 2$, dann gibt es eine symmetrische Matrix $A \in k^{3+3}$, so dass $F(X,Y,Z) = (XYZ) \cdot A \cdot (XYZ)^t$ ist, falls char $k \neq 2$. Die Determinante von $A = 0 \Leftrightarrow$ die Quadrik zerfällt in zwei Geraden.
Nachrechnen zeigt: $A = \frac{1}{2} \cdot$ Hessematrix, d.h. für eine nichtzerfallende Quadrik ist die Determinante ungleich Null. Man kann zeigen, ist diese Determinante für irgendein homogenes Polynom $F \in k[X,Y,Z]$ vom Grad d das Nullpolynom, so ist F Produkt von Linearfaktoren. In allen anderen Fällen ist H_c somit eine Kurve vom Grad $3(d-2)$. Speziell für $d = 3$ hat auch die Hessesche Kurve Grad 3.

Satz:
C sei eine Kurve, die keine Geraden als Komponente enthält, dann ist

$P \in C$ genau dann ein r- facher Wendepunkt von C, wenn sich C und H_C in P mit Schnittmultiplizität r schneiden.

Beweis:
Wir wählen das Koordinatensystem so, dass $P = (0:0:1)$ ist, und dass C dort die Gerade $y = 0$ als Tangente hat. Wir betrachten nur Punkte mit $z = 1$, rechnen also mit x und y als affinen Koordinaten. Die affine Gleichung von C geschnitten mit der affinen (x,y)-Ebene sei $f(x,y)$=0. Da $f(0,0) = 0$, hat f keinen konstanten Koeffizienten. Wir nehmen an, die Gerade $y = 0$ schneidet C in $(0,0)$ mit Vielfachheit $2 + r$, $r \in \mathbb{N}_0$.

$$f(x,y) = y \cdot u(x,y) + x^{r+2} \cdot v(x)$$

$u \in k[x,y],\ v \in k[x]\ , v(0) \neq 0,\ u(0,0) \neq 0$
Wir gehen zurück in die projektive Ebene, durch homogenisieren erhalten wir die Gleichung:

$$F(X,Y,Z) = Y \cdot U(X,Y,Z) + X^{r+2} \cdot V(X,Z)$$

Da $u(0,0) \neq 0 \Longrightarrow \frac{\partial U}{\partial Z}(0,0,1) \neq 0, U(0,0,1) \neq 0$.
Da $v(0) \neq 0$, ist $V(0,1) \neq 0$

$$\begin{aligned}
F_X(X,Y,Z) =& YU_X(X,Y,Z) + X^{r+2}V_X(X,Z) + (r+2)X^{r+1}V(X,Z)\\
F_Y(X,Y,Z) =& U(X,Y,Z) + YU_Y(X,Y,Z)\\
F_Z(X,Y,Z) =& YU_Z(X,Y,Z) + X^{r+2}V_Z(X,Z)\\
F_{XX}(X,Y,Z) =& YU_{XX}(X,Y,Z) + X^{r+2}V_{X,X}(X,Z) + 2(r+2)X^{r+1}(V_X(X,Z)\\
&+(r+1)(r+2)V(X,Z)X^r)\\
F_{XY} =& F_{YX} = YU_{XY}(X,Y,Z) + U_X(X,Y,Z)\\
F_{XZ} =& F_{ZX} = YU_{XZ}(X,Y,Z) + X^{r+2}V_{X,Z} + (r+2)V_Z(X,Z)\\
F_{YZ} =& F_{ZY} = U_Z(X,Y,Z) + YU_{YZ}(X,Y,Z)\\
F_{ZZ} =& YU_{ZZ}(X,Y,Z) + X^{r+2}V_{ZZ}(X,Z)
\end{aligned}$$

Da $V(0,1) \neq 0$, ist $V(X,Z)$ nicht durch X teilbar, d.h. die kleinste in F_{XX} vorkommende reine X-Potenz ist X^r. in den anderen zweiten

partiellen Ableitungen kommen, wenn überhaupt höchstens höhere reine x-Potenzen vor. Daher lässt sich die Determinante der Hesse-Matrix schreiben als

$$D(X,Y,Z) = YW(X,Y,Z) + X^r S(X,Z)$$

W, S homogene Polynome.

Nächstes Ziel: Schnittmultiplizität von C in H_C in P

1. Fall: r=0:
Setzen wir $(0:0:1)$ in D ein, erhalten wir

$$D(0,0,1) = DW(0,0,1) + S(0,1) = S(0,1) \neq 0$$

da X^r wirklich vorkommt. Also ist $(0:0:1) \notin C \cap H_C$
Die Schnittpunkte von C und H_C sind somit genau die Wendepunkte

2.Fall: r> 0:
P ist isolierter Schnittpunkt von C und H_C, d.h. C und H_C haben keine gemeinsame Komponente.
Noch zu zeigen:
Die Schnittmultiplizität von C und H_C in P ist r.
Wir nehmen an, dass das Koordinatensystem so gewählt ist, dass abgesehen von den bisherigen Bedingungen auch noch gilt:
Der Punkt $(0:0:1)$ liegt auf keiner Verbindungsgeraden zweier Schnittpunkte von C und H_C. Wir betrachten $Res_Y(F,D) \in k[X,Z]$. Die bezüglich Y konstanten Terme von F und D sind X^{r+2} und $X^r S(X,Z)$. Entwickeln wir die Determinante der Sylvestermatrix nach der ersten Spalte, erhalten wir:

$$Res_Y(F,D) = X^{r+2}V(X,Z)P(X,Z) + X^r S(X,Z)Q(X,Z)$$

mit geeigneten Polynomen $P, Q \in k[X,Z]$
$Q(0,1) \neq 0$, denn das ist die Resultante von $U(0,y,1)$ und $YV(0,Y,1)$. Würde sie verschwinden, so hätten die beiden Polynome eine gemeinsame Nullstelle Y, und $(0:Y.1)$ läge auf $C \cap H_C$ und auf der Geraden durch $(0:0:1)$ und $(0:1:0)$ $\lightning$ zur Wahl des Koordinatensystems.
Da auch $S(0,1) \neq 0$, ist $Res_Y(F,D)$ genau dann durch X^r teilbar, d.h.

wir haben im Punkt $P = (0:0:1)$ eine r-fache Nullstelle und damit Schnittmultiplizität r zwischen C und H_C. □

Satz:
C sei eine nichtsinguläre ebene Kurve vom Grad d in $\mathbb{P}^2(k)$, k algebraisch abgeschlossen und $d \geq 3$. Dann hat C mit Vielfachheiten gezählt $3d(d-2)$ Wendepunkte

Beweis:
H_C ist eine Kurve vom Grad $3(d-2)$, die nachdem vorherigen Satz keine Komponente mit C gemeinsam hat. Also gibt es nach dem Satz von Bezout mit Vielfachheiten gezählt $3d(d-2)$ Schnittpunkte, und die sind nach dem gerade bewiesenen Satz Wendepunkte von C mit derselben Vielfachheit. □

Korollar:
Eine elliptische Kurve über einem algebraisch abgeschlossenen Körper K hat genau 9 Wendepunkte, diese sind allesamt einfach.

Beweis:
P sei ein Wendepunkt der elliptischen Kurve E und g sei eine Wendetangente. Diese schneidet E in P mit Vielfachheit $r+2$, $r =$ Vielfachheit des Wendepunktes. Nach Bezout schneiden sich E und g mit Vielfachheiten gezählt in 3 Punkten, also ist P dreifacher Schnittpunkt und es gibt keine weiteren, d.h. $r = 1$.

□

Im Folgenden sei k ein beliebiger Körper und E eine elliptische Kurve über k. Nach Definition einer elliptischen Kurve gibt es mindestens einen Punkt P_0 auf E mit Koordinaten in K.
1. Fall: Es gibt einen Wendepunkt P_0 mit Koordinaten in k. Durch Koordinatenwechsel in der projektiven Ebene $\mathbb{P}^2(k)$ können wir erreichen, dass $P_0 = (0:1:0)$ ist, und $z = 0$ die Wendetangente. Die Gleichung von E schreiben wir als Polynom in Z :

$$F(X,Y,Z) = \phi_3(X,Y) + \phi_2(X,Y)Z + \phi_1(X,Y)Z^2 + \phi_0 Z^3$$

$\phi_i \in k[X,Y]$ homogen vom Grad $i, \phi_0 \in k$
Die Wendepunkte mit $z = 0$ können wir in Parameterform darstellen durch

$$(u : v) \to (u : v : 0)$$

Setzen wir das in F ein, erhalten wir $\phi_3(u,v)$. $P(0:1:0)$ ist aber der einzige Schnittpunkt der Wendetangente mit E. Also ist $\phi_3(u,v)$ durch u^3teilbar, d.h.

$$\phi_3(X,Y) = aX^3,\ a \neq 0,\ a \in k$$

Wir können annehmen, dass $a = 1$ ist, d.h. $\phi(X,Y) = X^3$
P_0 ist der einzige Punkt auf E mit Z-Koordinate 0. Um $E\backslash\{P_0\}$ zu untersuchen, können wir in der affinen Ebene $z \neq 0$ rechnen. Dort haben wir eine Gleichung der Form

$$X^3 + g(X,Z) = 0$$

wobei

$$g(X,Z) = \phi_2(X,Z) + \phi_1(X,Z) + \phi_0$$

höchstens den Grad 2 hat. Hätte g einen kleineren Grad als 2, würde in $P = (0,1)$ sowohl die partielle Ableitung nach X als auch die nach Y verschwinden, d.h. die Kurve hätte einen singulären Punkt, was nach Definition einer elliptischen Kurve ausgeschlossen ist. Insbesondere muss ein Term mit y^2 auftreten. Damit lässt sich die Kurvengleichung auch schreiben als:

$$aY^2 + \alpha(X)Y + \beta(X) = 0, \quad a \in k\backslash\{0\}$$

$\alpha(X)$ lineares Polynom, β kubisches Polynom.
Falls char $k \neq 2$ ist, können wir den Term $\alpha(X)Y$ durch quadratische Ergänzung zum verschwinden bringen und erhalten in neuen Koordinaten U,V eine Gleichung der Form:

$$V^2 = aU^3 + bU^2 + cU + d = g(U) \qquad (*)$$

Das Polynom g muss 3 verschiedene Nullstellen haben, denn wäre U_0 eine mehrfache Nullstelle, so würde im Punkt $(U_0,0)$ sowohl

$$\frac{\partial}{\partial V}(V^2 - aU^3 - bU^2 - cU - d) = 2V$$

als auch

$$\frac{\partial}{\partial U}(V^2 - g(U)) = \frac{\partial}{\partial U}g(U)$$

verschwinden
$(U_0, 0)$ wäre also ein singulärer Punkt. Multiplizieren wir $(*)$ mit a^2 und führen neue Koordinaten $Y = aV$ und $X = aU$ ein, erhalten wir die Gleichung:

$$\begin{aligned} Y^2 &= X^3 + bX^2 + acX + d \\ &= X^3 + pX^2 + qX + r \end{aligned}$$

Ist char$k \neq 3$, so können wir durch Verschiebung der X-Koordinate gemäß $X = X' - \frac{p}{3}$ auch noch den Term pX^2 zum Verschwinden bringen und erhalten die **WEIERSTRASSsche Normalform**

$$Y^2 = X^3 + aX + b$$

bzw homogen:

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

2.1 Weierstraßsche Normalform

$$Y^2Z + (dX + e)Y = X^3 + aX^2Z + bX + cZ^3$$

ist immer erreichbar. Bislang ist dies nur bewiesen, falls die Kurve einen Wendepunkt mit Koordinaten in k hat. Falls char $k \neq 2$, können wir erreichen, dass $d = e = 0$ ist. Falls char $k \neq 3$, können wir erreichen, dass $a = 0$ ist. Wir betrachten nun den Fall, dass die Kurve keinen Wendepunkt hat. Nach Definition einer elliptischen Kurve gibt es einen Kurvenpunkt P_0 mit Koordinaten in k. Da P_0 kein Wendepunkt ist, schneidet die Tangente an die Kurve E im Punkt P_0 nur mit Vielfachheit 2. Nach Bezout gibt es daher zumindest über dem algebraischen Abschluss von k einen weiteren Schnittpunkt P_1 dieser Tangente mit E. Tatsächlich liegt auch P_1 in $E(k)$. Setzen wir die Geradengleichung ein in die Gleichung der elliptischen Kurve, so erhalten wir (affin gerechnet) eine kubische Gleichung in einer Variablen für die x-Koordinate von P_1. Die x-Koordinate von P_0 ist eine zweifache Nullstelle dieser Gleichung. Abdividieren des entsprechenden quadratischen Faktors $(x - x_0)^2$ liefert eine lineare Gleichung und deren Lösung liegt in k. Da die Gleichung der Tangenten an P_0 Koeffizienten aus k hat, folgt daraus, dass auch die y-Koordinate in k liegt. Die Tangente an E im Punkt P_1 hat damit auch eine Gleichung mit Koeffizienten aus k. Dafür gibt es auf dieser Geraden weitere Punkte mit Koordinaten aus k.
Wir wählen einen solchen Punkt P_2 aus. Nun wählen wir unser Koordinatensystem so, dass $P_0 = (1:0:0), P_1 = (0:1:0)$ und $P_2 = (0:0:1)$ Die Tangente von E im Punkt P_0 ist die Gerade P_0P_1, sie hat also die Gleichung $Z = 0$. Die Tangente von E im Punkt P_1 ist die Gerade P_1P_2, sie hat die Gleichung $x = 0$. Die Gleichung von E sei

$$f(X,Y,Z) = \phi_3(X,Y) + \phi_2(X,Y)Z + \phi_3(X,Y)Z^2 + \phi_0 Z^3$$

ϕ_i homogenes Polynom vom Grad i in X und Y.
$Z = 0$ ist die Tangente im Punkt $P_0 = (1:0:0)$, da P_0 kein Wendepunkt ist, schneidet sie mit Vielfachheit 2, d.h. $\phi_3(X,Y)$ ist durch Y^2 teilbar. Somit kommen für ϕ_3 nur die Monome XY^2, Y^3 in Frage.
$P_1 = (0:1:0) \in E$ und $f(0,1,0) = \phi(0,1) = 0$ also kann $\phi_3(X,Y)$ keinen Y^3 Term enthalten. Da wir f mit einer Konstanten ungleich Null

multiplizieren dürfen, können wir annehmen, dass

$$\phi_3(X,Y) = XY^2$$

ist. Die Tangente P_1P_2 an E in P_1 hat die Gleichung $x = 0$, sie wird also parametrisiert durch die Abbildung:

$$\begin{cases} \mathbb{P}^1 \longrightarrow \mathbb{P}^2 \\ (u,v) \longrightarrow (0:u:v) \end{cases}$$

P_1 ist das Bild von $(1:0)$

$$f(0,u,v) = \phi_2(0,u)v + \phi_1(0,u)v^2 + \phi_0 v^3$$

Da die Tangente in P_1 mit Multiplizität 2 schneidet, muss dies durch v^2 teilbar sein. $\phi_2(X,Y)$ darf also keinen Y^2 Term enthalten. Damit ist

$$f(X,Y,Z) = XY^2 + (aX^2 + bXY)Z + (cX + dY)Z^2 + eZ^3$$

Affin betrachtet, in der Ebene $Z \neq 0$ entspricht dies der Gleichung

$$XY^2 + aX^2 + bXY + cX + dY + e = 0$$

Multiplikation mit X macht daraus:

$$(XY)^2 + aX^3 + bX(XY) + cX^2 + dXY + eX = 0$$

Diese Gleichung hat als Nullstellenmenge die elliptische Kurve E zusammen mit der Geraden $x = 0$.

2.2 CREMONA Transformation

Wir betrachten die Abbildung

$$\begin{cases} \mathbb{P}^2(k) \dashrightarrow \mathbb{P}^2(k) \\ (X:Y:Z) \to (\frac{1}{X}:\frac{1}{Y}:\frac{1}{Z}) = (YZ:XZ:XY) \end{cases}$$

Sie ist nicht definiert in jenen Punkten P_0, P_1 und P_2. Die Geraden P_0P_1, P_1P_2 und P_0P_2 werden zu Punkten kontrahiert:

$$P_0P_1 \longrightarrow P_2$$

$$P_0P_2 \longrightarrow P_1$$

$$P_1P_2 \longrightarrow P_0$$

Auf $\mathbb{P}^2(k)\backslash(P_0P_1 \cup P_0P_2 \cup P_1P_2)$ ist die Ableitung injektiv, denn dort sind x,y,z alle ungleich Null, und die Abbildung ist zu sich selbst invers. Affin betrachtet in der Ebene $z \neq 0$ hat die Cremona-Transformation die Form

$$(x,y) \longrightarrow (y:x:xy)$$

Die affine Abbildung

$$(x,y) \longrightarrow (x,xy)$$

kann in geeigneter Weise als Cremona-Transformation interpretiert werden. Wenden wir ihre Umkehrung an auf die Gleichung 4. Grades, erhalten wir eine Gleichung 3. Grades in neuen Variablen x,y der Form

$$y^2 + ax^3 + bxy + cx^2 + dy + e = 0$$

oder

$$y^2 + (cx + d)y = -(ax^3 + cx^2 + e)$$

Falls char $k \neq 2$ können wir durch quadratische Ergänzung erreichen, dass $b = d = 0$ ist, d.h. dass alle y-Terme verschwinden. Falls char $k \neq 3$, können wir rechts eine kubische Form ohne quadratischen Term bekommen, durch kubische Ergänzung.

$a = 1$ lässt sich im Fall, dass char $k \neq 2$ wie folgt erreichen:
Wir haben eine Gleichung der Form:

$$v^2 = au^3 + bu^2 + cu + d$$

Multipliziere mit a^2 und führe av und au als neue Variablen ein. Wir erhalten die Gleichung

$$y^2 = x^3 + ax^2 + bx + c$$

Wir wissen: Eine elliptische Kurve über einem algebraisch abgeschlossenen Körper k hat genau 9 Wendepunkte, alle sind einfach. E sei eine elliptische Kurve über dem algebraisch abgeschlossenen Körper k. Wir wählen unser Koordinatensystem so, dass $(0:1:0)$ und $(1:0:0)$ Wendepunkte sind, mit $x = 0$ und $y = 0$ als Wendetangente. Setzt man $x = 0$ oder $y = 0$ in die Kurvengleichung ein, verschwinden alle Terme außer Z^3. Daher enthält die Kurvengleichung außer Z^3 nur Monome, die sowohl durch X als auch durch Y teilbar sind, d.h. X^2Y, XY^2 und XYZ. Die Kurvengleichung hat also die Form:

$$XY(\alpha Z + \beta X + \gamma Y) + \delta Z^3 = 0$$

Da eine elliptische Kurve nichtsingulär ist, dürfen die drei partiellen Ableitungen der linken Seite in keinem Kurvenpunkt simultan verschwinden, also

$$\beta XY + Y(\alpha Z + \beta X + \gamma Y) \neq 0$$

oder

$$\gamma XY + X(\alpha Z) + \beta X + \gamma Y \neq 0$$

oder

$$\alpha XY + 3\delta Z^2 \neq 0$$

Damit müssen $\beta, \gamma, \delta \neq 0$ sein.
Sei etwa $\delta = 0$:
$XY(\alpha Z + \beta X + \gamma Y) = 0 \Rightarrow E$ besteht aus drei Geraden.
Die Schnittpunkte sind singulär.
$\beta = 0, \delta \neq 0$:

$$XY(\alpha Z + \gamma Y) + \delta Z^3 = 0$$

Ableitungen:

$$Y(\alpha Z + \gamma Y = 0) \Rightarrow \delta Z^3 = 0 \Rightarrow Z = 0$$

$$\gamma XZ + X(\alpha Z + \gamma Y) = \gamma XY$$

$$\Rightarrow X = 0 \quad oder \quad Y = 0$$
$$\Rightarrow \alpha XY + 3\delta Z^2 = 0$$

d.h. die Punkte $(1:0:0)$ und $(0:1:0)$ sind singulär
$\gamma = 0$: analog zu $\beta = 0$

Da k algebraisch abgeschlossen ist, gibt es dort mindestens eine dritte Wurzel $\tilde{\delta}$ von δ. Ersetzen wir Z durch $\tilde{\delta}Z$ erhalten wir eine Gleichung der Form

$$XY(\alpha Z + X + Y) + Z^3 = 0$$

Wir führen neue Koordinaten U, V, W ein, durch

$$3X = -\alpha W - U + 2V$$
$$3Y = -\alpha W + 2U - V$$
$$Z = W$$

Ab jetzt sei char$k \neq 2,3$.
Neue Gleichung:

$$(27 + \alpha^3)W^3 - 2U^3 + 3UV^2 - 2V^3 - 3\alpha W(U^2 + UV + V^2) = 0$$

Wobei $(U^2 - UV + V^2) = (U + \epsilon V)(U + \epsilon^2 V)$
ϵ Lösung von $\epsilon^2 + \epsilon + 1 = 0$

Für $k = \mathbb{C}$ ist $\epsilon = e^{\frac{2\pi i}{3}}$ und $\epsilon^2 = e^{\frac{4\pi i}{3}} = e^{-\frac{2\pi i}{3}}$
$3U^2V + 3UV^2 - 2U^3 - 2V^3$ ist bis auf das Vorzeichen gleich

$$(U + \epsilon V)^3 + (U + \epsilon^2 V)^3$$

Die neue Form der Gleichung ist dann:

$$(27 + \alpha^3)W^3 - ((U + \epsilon V)^3 + (U + \epsilon^2 V))^3 - 3\alpha W(U + \epsilon V)^3 + (U + \epsilon^2 V)^3) = 0$$

Neues Koordinatensystem, mit Koordinaten

$$X = U + \epsilon V, \qquad Y = U + \epsilon^2 V, \qquad Z = W$$

Dort ist die Gleichung:

$$(27 + \alpha^3)Z^3 - X^3 - Y^3 - 3\alpha ZXY = 0$$

Ersetze Z durch $\sqrt[3]{27+\alpha^3}\cdot Z$, falls $27+\alpha^3 \neq 0$,
X durch $-X, Y$ durch $-Y$
Dies führt zu der neuen Gleichung

$$Z^3 + X^3 + Y^3 + \lambda XYZ = 0$$

für geeignetes $\lambda \in k$, die **HESSE-Normalform**.

Hessesche Kurve dazu:
Sei

$$F = X^3 + Y^3 + Z^3$$

Dann ist

$F_X = 3X^2 + \lambda YX \qquad F_{XX} = 6X$
$F_Y = 3Y^2 + \lambda XZ \qquad F_{YY} = 6Y$
$F_Z = 3Z^3 + \lambda XY \qquad F_{ZZ} = 6Z$
$F_{XY} = F_{YX} = \lambda Z \qquad F_{XZ} = F_{ZX} = \lambda Y \qquad F_{YZ} = F_{ZY} = \lambda X$

$$\Longrightarrow H_F = \begin{vmatrix} 6X & \lambda Z & \lambda Y \\ \lambda Z & 6Y & \lambda X \\ \lambda Y & \lambda X & 6Z \end{vmatrix} = 6\lambda^2(X^3+Y^3+Z^3) + (216+2\lambda^3)XYZ$$

Sowohl E als auch seine Hesse-Kurve liegen also im eindimensionalen linearen System der Kurven

$$\alpha(X^3+Y^3+Z^3) + \beta XYZ = 0, \quad (\alpha:\beta) \in \mathbb{P}^1(k)$$

Wir betrachten eine Kurve aus diesem System:
Ist $\alpha = 0$, wird die Gleichung zu:

$$XYZ = 0$$

die Kurve besteht also aus drei Geraden, die ein Dreieck bilden.

Ausgangskurve: $\alpha = 1, \beta = \lambda$
Angenommen

$$\lambda^3 + 27 = 0 \Rightarrow \lambda \in \{-3, -3\epsilon, -3\epsilon^2\}$$

Umständliche, aber elementare Rechnung zeigt:
Für $\lambda = -3$ erhalten wir:

$$(X+Y+Z)(Z+\epsilon X+\epsilon^2 Y)(Z+\epsilon y+\epsilon^2 X) = 0$$

Für $\lambda = -3\epsilon$:

$$(X + \epsilon Y + Z)(Z + \epsilon X + Y)(Z + \epsilon^2 X + \epsilon^2 Y) = 0$$

Für $\lambda = -3\epsilon^2$:

$$(X + \epsilon^2 Y + Z)(Z + \epsilon X + \epsilon Y)(Z + \epsilon^2 X + Y) = 0$$

Also jeweils drei Geraden, von denen sich jeweils zwei in einem Punkt schneiden.
Unser lineares System wird aufgespannt von je zwei Kurven daraus, also beispielsweise von den beiden Kurven

$$XYZ = 0, \qquad X^3 + Y^3 + Z^3 = 0$$

Alle Kurven aus dem linearen System schneiden sich in den selben Punkten,d.h in den Schnittpunkten der Kurven $XYZ = 0$ und $X^3 + Y^3 + Z^3 = 0$
Ist $X = 0 \Longrightarrow Y^3 = -Z^3 \Longrightarrow Y = -Z$ oder $Y = -\epsilon Z$ oder $Y = -\epsilon^2 Z$ also drei Punkte

$$(0 : -1 : 1), (0 : -\epsilon : 1), (0 : -\epsilon^2 : 1)$$

$Y = 0, Z = 0$ analog.
Auch die Kurven zu $\lambda \in \{-3, -3\epsilon, -3\epsilon^2\}$ gehen durch diese Punkte, genauso die Kurve $XYZ = 0$ und diese vier Kurven bestehen jeweils aus drei Geraden. Somit gibt es 12 Geraden derart, dass die neun Schnittpunkte auf der Vereinigung einer Geraden liegen.
Ist $X^3 + Y^3 + Z^3 + \lambda XYZ = 0$ eine elliptische Kurve, also nichtsinguläre, so sind alle neun Wendepunkte unabhängig von λ, die neun gerade berechneten Punkte. Alle diese Kurven gehen durch die neun Punkte:

$$\begin{array}{lllll} X = 0: & P_{00} = (0 : -1 : 1), & P_{01} = (0 : -\epsilon : 1), & P_{02} = (0 : -\epsilon^2 : 1) \\ Y = 0: & P_{10} = (1 : 0 - 1), & P_{11} = (1 : 0 : -\epsilon), & P_{12} = (1 : 0 : -\epsilon^2) \\ Z = 0: & P_{20} = (-1 : 1 : 0), & P_{21} = (-\epsilon : 1 : 0), & P_{22} = (-\epsilon^2 : 1 : 0) \end{array}$$

und sofern die Gleichung eine elliptische Kurve beschreibt, sind dies die Wendepunkte der Kurve.

Satz:
Jede elliptische Kurve über einem algebraisch abgeschlossenen Körper mit char$k \neq 2,3$ hat neun Wendepunkte, dazu gibt es zwölf Geraden, auf denen jeweils drei der Wendepunkte liegen. Genauer liegen die folgenden Tripel auf einer Geraden:

1. P_{ij}, i konstant, $j = 0,1,2$
2. P_{ij}, j konstant, $i = 0,1,2$
3. Wir betrachten formal die Determinante

$$\begin{vmatrix} P_{00} & P_{01} & P_{02} \\ P_{10} & P_{11} & P_{12} \\ P_{20} & P_{21} & P_{22} \end{vmatrix}$$

und entwickeln nach SARRUS: Jedes dabei auftretende Dreierprodukt entspricht einem Tripel von Punkten, die auf einer Geraden liegen.

Beweis:
Die zwölf Gleichungen sind

$$X = 0, Y = 0 \text{ und } Z = 0$$

sowie die 3×3 -Linearfaktoren der zerfallenden Kurven

$$X^3 + Y^3 + Z^3 + \lambda XYZ$$

mit $\lambda \in \{-3, -3\epsilon, -3\epsilon^2\}$, $\epsilon = \frac{1}{2}(1 + \sqrt{-3})$
Durch Einsetzen der zwölf Punktetripel in die jeweils richtige Gleichung folgt die Behauptung.

□

Wir kennen drei Normalformen elliptischer Kurven:
$Y^2Z = X^3 + aXZ + bZ^3$ (Weierstraß)
$Y^2Z = X(X - Z)(X - \lambda Z)$ (Legendre)
$X^3 + Y^3 + Z^3 + \mu XYZ = 0$ (Hesse)
Wann bestimmen zwei Weierstraßgleichungen

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

und

$$Y^2Z = X^3 + a'XZ^2 + b'Z^3$$

die selbe Kurve?
Haben wir die gleiche Punktmenge in der projektiven Ebene, dann nur für $a = a'$ und $b = b'$. Dieselbe in dem Sinne, dass die Kurven durch eine projektive (lineare) Transformation ineinander überführt werden können.

Aus der speziellen Gestalt der Weierstraßschen Normalform folgt, das ein Koordinatenwechsel, der eine elliptische Kurve in Weierstraßnormalform in eine andere überführt nur von der Form sein kann, dass jede Koordinate in ein skalares, nichtverschwindendes Vielfaches überführt wird.

$$(X : Y : Z) \longrightarrow (\alpha X : \beta Y : \gamma Z), \quad \alpha, \beta, \gamma \neq 0$$

Da wir homogene Koordinaten haben, können wir o.B.d.A annehmen, dass $\beta = 1$ ist, d.h.

$$(X : Y : Z) \longrightarrow (\alpha X : Y : \gamma Z)$$

Liegt (X:Y:Z) auf der Kurve $Y^2Z = X^3 + aXZ + bZ^3$ so ist
$Y^2Z = X^3 + aZ^2 + bZ^3$.

Beh:
Die Kurven

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

und

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

lassen sich durch eine projektive Transformation ineinander überführen.

Betrachten wir die folgende Transformation:

$$(X : Y : Z) \longrightarrow (\lambda^2 X : \lambda^3 Y : Z)$$

Ist

$$(\lambda^3 Y)^2 Z = (\lambda^2 X)^3 + a(\lambda^2 X)Z^2 + bZ^3$$

so ist

$$\lambda^6 Y^2 Z = \lambda^6 X^3 + \lambda^2 a X Z^2 + b Z^3$$

Division durch λ^6 liefert:

$$Y^2 Z = X^3 + (\lambda^4 a) X Z^2 + (\lambda^{-6} b) Z^3$$

Die Transformation führt also die Kurven zu (a,b) und $(\lambda^{-4}a, \lambda^{-6}b)$ ineinander über. In Gegenrichtung die zu (a,b) und die zu $(\lambda^4 a, \lambda^6 b)$. Mit $\mu = \sqrt{\lambda}$ ist dies die Kurve zu $(\mu^2 a, \mu^3 b)$.
Die Kurven $Y^2Z = X^3 + aXZ^2 + bZ^3$ und $Y^2Z = X^3 + a'XZ^2 + b'Z^3$ lassen sich also genau dann ineinander überführen, wenn es ein $\mu \in k$ gibt:
$a' = \mu^2 a$ und $b' = \mu^3 b$.
Das ist offensichtlich genau dann der Fall, wenn

$$\frac{a^3}{b^2} = \frac{(a')^3}{(b')^2}$$

Wenn $a' = \mu^2 a$ und $b' = \mu^3 b$, so folgt:

$$\frac{(a')^3}{(b')^2} = \frac{\mu^6 a^3}{\mu^6 b^2} = \frac{a^3}{b^2}$$

Ist $\frac{a^3}{b^2} = \frac{(a')^3}{(b')^2}$, so gibt es ein α, so dass $(\alpha')^3 = \alpha a^3, (b')^2 = \alpha b^2$.
Setzen wir dann $\mu = \sqrt[6]{\alpha}$, so ist

$$(\alpha')^3 = \mu^6 a^3 = (\mu^2 a)^3, (b')^2 = \mu^6 b^2 = (\mu^3 b)^2$$

Mit der richtigen sechsten Wurzel μ ist also $a' = \mu^2 a, b' = \mu^3 b$.
Wir wissen vom 5.Übungsblatt: $Y^2Z = X^3 + aXZ + bZ^3$ definiert genau dann eine elliptische Kurve, wenn die Diskriminante $\Delta = 4a^3 + 27b^2 \neq 0$. Ersetzt man a durch $\mu^2 a$ und b durch $\mu^3 b$, so wird Δ ersetzt durch $\mu^6 \Delta$

Definition:

$$j = \frac{12^3 a^3}{\Delta} = \frac{12^3 a^3}{4a^3 + 27b^2}$$

heißt **j-Invariante** der elliptische Kurve $Y^2Z = X^3 + aXZ^2 + bZ^3$
Damit gilt auch: Zwei Kurven in Weierstraßgestalt sind genau dann

projektiv-äquivalent (d.h. bis auf Koordinatenwechsel sind es die gleichen Kurven), wenn sie die gleiche j-Invariante haben.

Wichtig: Um die 6. Wurzel ziehen zu können, haben wir vorausgesetzt, dass k algebraisch abgeschlossen ist. Über $\mathbb{R}$ haben die beiden Kurven $Y^2Z = X^3 + Z^3$ und $Y^2 = X^3 - Z^3$ beide $j = 0$, aber reell ist kein Koordinatenwechsel möglich, denn reell lassen sich die beiden Kurven nicht ineinander überführen.
Über $\mathbb{Q}$ haben alle Kurven $Y^2Z = X^3 + pZ$, p prim j-Invariante Null, sind aber alle verschieden.

3 Die Gruppenstruktur einer elliptischen Kurve

k sei ein Körper, $E \subseteq \mathbb{P}^2(k)$ eine elliptische Kurve. Für eine Gruppenstruktur brauchen wir zwei Abbildungen:

$$+ : \begin{cases} E \times E \longrightarrow E \\ (P,Q) \longrightarrow P+Q \end{cases}$$
$$- : \begin{cases} E \longrightarrow E \\ P \longrightarrow -P \end{cases}$$

Außerdem benötigen wir ein neutrales Element O.
Idee:
Sind $P,Q \in E$, schneidet die Gerade PQ die Kurve E über dem algebraischen Abschluss nach Bezout noch in einem dritten Punkt, da wir eine Kurve dritten Grades betrachten.Wir wissen aus den Übungen, dass dieser dritte Schnittpunkt Koordinaten aus k hat. Aber so können wir die Addition nicht definieren. Für alle $P \in E$ muss gelten: $P+O=P$, d.h. die Gerade durch P und O muss in P mit Vielfachheit 2 schneiden, also Tangente sein. Ein Punkt O mit dieser Eigenschaft existiert praktisch nie. Für die Abbildung $-$ bietet sich folgendes an:
Wähle für $-P$ den dritten Schnittpunkt der Geraden OP mit E. Dann sind die Punkte O,P und $-P$ kollinear, liegen also auf einer Geraden und ihre Summe ist Null.
Modifizierte Summendefinition:
$P+Q+R=0 \Leftrightarrow P,Q$ und R sind kollinear.
Die Konstruktion von $P+Q$ geht dann folgendermaßen:
R sei der dritte Schnittpunkt der geraden PQ mit E, dann ist $P+Q$ der dritte Schnittpunkt der Geraden OR mit E. Es sollte dann gelten:
$O+O+O=O$, d.h. die Tangente an den Punkt O muss mit Vielfachheit 3 schneiden,d.h. O ist Wendepunkt.

Beh:
Mit der so definierten Verknüfung und Inversenabbildung ist E eine abelsche Gruppe mit Neutralelement O

Beweis:
Das **Kommutativgesetz** ist klar, denn die Gerade durch P und Q ist gleich der durch Q und P und $P+Q$ hängt nur ab von dieser Geraden und von O.
Existenz des Inversen: $P,-P$ und O sind kollinear. Zur Berechnung von $P+(-P)$ betrachten wir den dritten Schnittpunkt der Geraden durch P und $-P$ und E. Das ist O. Dann betrachten wir die Tangente an O. Da sie eine Wendetangente ist, ist O auch der dritte Schnittpunkt, also ist $P+(-P)=O$
Neutralelement: $P+O=O+P=P$.
Die Gerade OP schneidet E außerdem in $-P$, die durch O und $-P$ hat P als dritten Schnittpunkt.
Bleibt noch das **Assoziativgesetz:** $(P+Q)+R=P+(Q+R)$
Setze $P+Q=S,\ S+R=T,\ Q+R=U$ damit wird die Aussage zu:

$$T=P+U$$

Dies ist äquivalent dazu, dass P,U und $-T$ auf einer Geraden liegen:

- g_1 sei die Gerade durch P,Q und $-S$
- g_2 sei die Gerade durch S,R und $-T$
- g_3 sei die Gerade durch O,U und $--U$
- h_1 sei die Gerade durch S,O und $-S$
- h_2 sei die Gerade durch Q,R und $-U$

$C=g_1\cup g_2\cup g_3$ ist eine konstante kubische Kurve. Wir betrachten ihren Durchschnitt mit E, er besteht aus den neun Punkten

$$O,P,Q,R,S,-S,-T,U,-U$$

$O,R,S,-S,Q,-U$ liegen auf der Quadrik $h_1\cup h_2$. Nach nach einem

früheren Satz gilt, falls von den neun Schnittpunkten zweier kubischer Kurven sechs auf einer Quadrik liegen, liegen die restlichen drei auf einer Geraden. In unserem Fall also $P, -T, U$, somit ist $T = P + U$, das Assoziativgesetz gilt also. □

Lemma:
Ein Punkt $P \in E$ ist genau dann Wendepunkt, wenn $P + P + P = O$ ist

Beweis:
Die Tangente durch P schneidet genau dann mit Vielfachheit 3, wenn $P + P + P = 0$ ist . □

Korollar
Die Anzahl der Wendepunkte von E ist $1, 3$ oder 9.

Beweis:
Die Wendepunkte bilden eine Untergruppe von E, denn ist $3P = O$, so ist nach dem Kommutativgesetz und Assoziativgesetz auch $3(P + Q) = O$, d.h. auch $P + Q$ ist Wendepunkt, insbesondere ist auch $P + P = -P$ Wendepunkt, und O war als Wendepunkt gewählt.
Jetzt sei $\bar{k}$ ein algebraisch abgeschlossener Körper, der k enthält, und $E(\bar{k}) \subseteq \mathbb{P}^2(\bar{k})$ sei die durch die Gleichung von E definierte elliptische Kurve in $\mathbb{P}^2(\bar{k})$. $E(\bar{k})$ hat 9 Wendepunkte. Die neun Wendepunkte bilden also eine Gruppe. Die Gruppe der Wendepunkte auf E ist deren Schnittmenge mit E, also insbesondere eine Untergruppe. Dafür kommen nach LAGRANGE nur die Gruppenordnungen $1, 3$ und 9 in Frage. □

3.1 Einschub: Elliptische Kurven über $\mathbb{C}$

Wir betrachten Funktionen

$$f : \mathbb{C} \longrightarrow \mathbb{C} \text{ z.B. } f(z) = e^{2\pi i z}$$

Für jede ganze Zahl m ist $f(z+m) = f(z)$, denn $e^{2\pi i} = 1$.
Also ist f periodisch mit Periode 1.
Angenommen $\tau \in \mathbb{C}\backslash\mathbb{R}$, dann bilden 1 und τ eine $\mathbb{R}$-Basis von $\mathbb{C}$.
Frage: Gibt es eine Funktion $f : \mathbb{C} \longrightarrow \mathbb{C}$, für die gilt:
$f(z+1) = f(z) \quad \forall z \in \mathbb{C}$ und $f(z+\tau) = f(z) \quad \forall z \in \mathbb{C}$?
Nach LIOUVILLE ist eine komplex differenzierbare Funktion
$f : \mathbb{C} \longrightarrow \mathbb{C}$ konstant. Wir können aber Funktionen betrachten, die auf dem Parallelogramm nicht überall definiert sind, sondern in den Ecken den Wert ∞ annehmen.

$$\wp(z) = \sum_{n,m \in \mathbb{Z}} \frac{1}{(z-n-m\tau)^2}$$

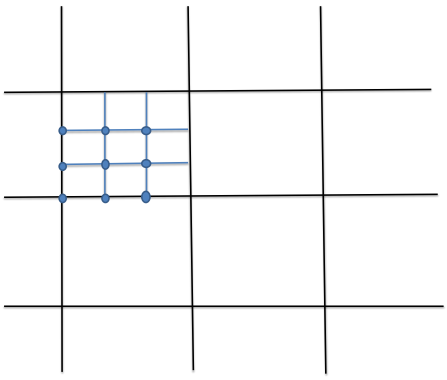
Die Funktionen $\wp$ und $\wp'$ nehmen auf $\mathbb{Z} + \mathbb{Z}\tau$ den Wert ∞ an.

Die Abbildung $\begin{cases} \mathbb{C} \longrightarrow \mathbb{P}^2(\mathbb{C}) \\ z \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1)\,, & z \notin \mathbb{Z} + \mathbb{Z}\tau\,, \\ (0:1:0)\,, & sonst \end{cases} \end{cases}$

identifiziert $C/\mathbb{Z} + \mathbb{Z}\tau$ mit einer elliptischen Kurve $E \subseteq \mathbb{P}(\mathbb{C})$

$$y^2 z = 4x^3 - g_2(\tau) x z^2 - g_3(\tau)$$

Außerdem ist diese Abbildung ein Gruppenhomomorphismus.



3.2 Gruppenoperation für Kurven in Weierstraßscher Normalform

Sei char $k \neq 2,3$

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \quad \in \mathbb{P}^2(k)$$

Dies ist die affine Kurve

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

plus dem einen unendlich fernen Punkt $O = (0:1:0)$

Wann liegen O und zwei weitere Punkte $(x_1 : y_1 : z_1)$ und $(x_2 : y_2 : z_2)$ auf einer Geraden? Die Gerade durch $(x_1 : y_1 : z_1)$ und $O = (0:1:0)$ besteht aus allen Punkten

$$\lambda(x_1 : y_1 : z_1) + \mu O = (\lambda x_1 : \lambda y_1 + \mu : \lambda z_1)$$

mit $(\lambda : \mu) \in \mathbb{P}^1(k)$
$\lambda = 0 \Rightarrow O$ erfüllt die Eigenschaft
$\lambda \neq 0$: Dann ist auch die z-Koordinate des obigen Punktes ungleich Null, denn für eine Weierstraß Gleichung gilt: $z \neq 0 \Rightarrow Punkt = O$. Die von Null verschiedenen Punkte der Geraden sind:

$$(x_1 : y_1 + \mu : z_1), \mu \in k$$

d.h. es sind die Punkte der affinen Geraden $x = \frac{x_1}{z_1}$ in k^2. Damit ist klar wie zu $P = (x,y) \in k^2$ der Punkt $-P$ aussieht. Die Gerade OP ist parallel zur y-Achse. $-P$ als dritter Schnittpunkt mit dieser Kurve muss also die gleiche x-Koordinate haben wie P:
Da

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

d.h. zu festem $x = x_1$ ist

$$y = \pm\sqrt{x_1^3 + ax_1 + b}$$

also ist

$$-P = (x_1, -y_1)$$

Falls $x_1^3 + ax_1 + b \neq 0$, ist $-P = O$. Andernfalls ist $-P = P$, also $2P = O$. Punkte mit $2P = O$ sind damit einmal $P = O$, sowie jene

Punkte$(x,0)$, mit $x^3+ax+b=0$ Ist $\bar{k}$ der algebraisch abgeschlossene Körper, der k enthält, gibt es in $\bar{k}$ drei verschiedene x-Werte, für die dies gilt. Es gibt also genau 4 solche Punkte. Wenn wir nur Punkte mit Koordinaten in k zulassen, brauchen wir Nullstellen von $x^3+ax+b\in k$, davon gibt es $0,1$ oder 3. Also gibt es $1,2$ oder 4 Punkte P mit $2P=O$.

Bemerkung:
Diese Punkte bilden eine Untergruppe von E. Denn wenn gilt: $2P=O$ und $2Q=O$ so ist

$$2(P+Q)=2P+2Q=O+O=O$$

und

$$2(-P)=O$$

da $P=-P$.Die Punkte aus $E(\bar{k})$ mit $2P=O$ bilden eine Gruppe der Ordnung 4. Die aus E sind eine Untergruppe, deren Ordnung 4 teilen muss.
Reelles Bild: Konstruktion von $P+Q, P=(x_1,y_1), Q=(x_2,y_2), P\neq Q$. Wir müssen die Gerade PQ betrachten:

1.Fall: $x_1=x_2$**:**
Dann ist

$$Q=-P$$

denn P und $-P$ sind die einzigen Punkte mit x-Koordinate x_1.
Dann ist

$$P+Q=O$$

2.Fall: $x_1\neq x_2$**:**
Dann hat PQ die Gleichung

$$y=\frac{y_2-y_1}{x_2-x_1}(x-x_1)+y_1=m(x-x_1)+y_1$$

Zur Berechnung des dritten Schnittpunkts setzen wir dies ein in die Weierstraßgleichung:

$$m(x-x_1)^2=x^3+ax+b$$

das ist eine kubische Gleichung der Form

$$x^3-m^2x^2+px+q,\ p,q\in k$$

Über $\bar{k}$ zerfällt dieses Polynom in Linearfaktoren, d.h.

$$\begin{aligned} x^3 - m^2x^2 + px + q &= (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha,\beta,\gamma \in \bar{k} \\ &= x^3 - (\alpha+\beta+\gamma)x^2 + \dots \\ &\Rightarrow m^2 = \alpha+\beta+\gamma \end{aligned}$$

Da P,Q auf der Kurve liegen, sind x_1,x_2 Lösungen. Für den dritten Schnittpunkt (x_3,y_3) ist x_3 die dritte Lösung, d.h.

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 = (\frac{y_2-y_1}{x_2-x_1})^2 - x_2 - x_1 \\ y_3 &= m(x_3 - x_1) + y_1 \end{aligned}$$

$P+Q$ ist der Punkt

$$(x_3,-y_3) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$$

mit $m = \frac{y_2-y_1}{x_2-x_1}$

Fehlt nur noch der Fall $P = Q \neq O$:
Sei $P = (x_1,y_1)$. Die „Gerade durch P und P“ ist die Tangente im Punkt P. Betrachte y als Funktion von x. Da $y^2 = x^3 + ax + b$, folgt: $2yy' = 3x^2 + a$. Also ist $y' = {}_{\bar{3}}x^2 + a2y$, falls $y \neq 0$. Ist $y_1 = 0$, so ist $2P = O$ und wie sind fertig.
Andernfalls hat die Tangente in (x_1,y_1) die Steigung $m = \frac{3x^2+a}{2y}$ und ist die Gerade $y = m(x - x_1) + y_1$.
Einsetzen ergibt: $(m(x - x_1) + y_1)^2 = x^3 + ax + b$, also

$$x^3 - m^2x^2 + px + q = 0, p,q \in k$$

Die Summe aller drei Nullstellen ist wieder $-m^2$ und x_1 ist doppelte Nullstelle, da wir eine Tangente haben. Die dritte Nullstelle ist $x_3 = m^2 - 2x_1$. Der Punkt $2P$ ist also $(m^2 - 2x_1, m(x_3 - x_1) + y_1)$, mit $m = \frac{3x^2+a}{2y}$
Damit können wir für zwei beliebige Punkte P,Q der elliptischen Kurve $P+Q$ und $-P$ berechnen.

Anwendung:
Bestimme alle Punkte $P \in E(\bar{k})$ mit $3P = O$, d.h. die Tangente schneidet dreimal, d.h. wir suchen die Wendepunkte:
Klar: $P = O$ ist eine Lösung. Alle anderen liegen in der affinen Ebene $z \neq 0$. Ist $3P = O$, so ist $2P = -P$. Für $P \neq O$ und $3P = O$ liegen auch $2P$ und $-P$ in der affinen Ebene. $2P$ kann nicht gleich O sein, denn ist $3P = O$ und $P = O$ so auch $2P$.
Sei $P = (x,y)$, $2P = -P$ wird zur Gleichung:

$$m^2 - 2x = x, m = \frac{3x^2 + a}{2y}$$

für die x-Koordinaten

$$m^2 = \frac{(3x^2 + a)}{4y^2} = \frac{3x^2 + a}{4(x^3 + ax + b)}$$

Damit wird

$$m^2 = 3x$$

zu

$$(3x^2 + a)^2 = 12x(x^3 + ax + b)$$

oder

$$3x^4 + 6ax^2 + 12bx - a^2 = 0$$

Betrachte die Resultante zwischen dem Polynom und der Ableitung:

$$Res_X(f, f') = -12^4(4a^3 + 27b^2)^2$$

Da für eine Weierstraß Gleichung $4a^2 + 27b^2 \neq 0$ sein muss, hat f vier verschiedene Nullstellen in $\bar{k}$. Ist $3P = O$, so ist auch $3(-P) = O$, also gibt es zu jeder Nullstelle x zwei mögliche y-Werte, wir bekommen also acht, zusammen mit O neun Punkte P mit $3P = O$. Die bilden eine Untergruppe. Die Punkte daraus mit Koordinaten in k bilden eine Untergruppe, d.h. davon gibt es $1,3$ oder 9 Punkte.

Gegeben: $N \in \mathbb{N}, P \in E, E : y^2 = x^3 + ax + b$ elliptische Kurve über einem Körper k, char $k \neq 2,3, NP = P + P + \cdots + P$ mit N Summanden.

Ist $N = \sum_{i=0}^{k} n_i 2^i, \qquad n_i \in \{0,1\}$
die Binärdarstellung von N, so ist

$$NP = \sum_{i=0}^{k} n_i 2^i P = \sum_{i=0, n_i \neq 0}^{k} 2^i P$$

k Verdoppelungen
Anzahl Additionen= Anzahl der Einsen in Binärdarstellung -1.

3.2.1 Algorithmus von Montgomery

Berechne nacheinander die Punkte N_lP und $(N_l+1)P$, wobei N_l die Zahl ist, die durch die ersten l Binärziffern von N dargestellt wird.

$$N_l = \sum_{i=k+1-l}^{k} n_i 2^{i-1-(k-l)}$$

Offensichtlich ist $N_{k+1} = N$.
Wir setzen

$$U_l = N_lP, \quad V_l = (N_l+1)P$$

Dann ist $U_0 = O, V_0 = P, N_0 = 0$
Rekursion: $N_l = 2N_{l-1} + n_{k+1-l}$
d.h.

- falls $n_{k+1-l} = 0, U_l = 2U_{l-1}, V_l = U_{l-1} + V_{l-1}$
- falls $n_{k+1-l} = 1$ ist $U_l = U_{l-1} + V_{l-1}, V_l = 2V_{l-1}$

Die x- Koordinaten von U_l, V_l können berechnet werden nur aus den x-Koordinaten von P und den Vorgängern, d.h. den U_{l-1}, V_{l-1}:
Ist $P = (x_1, y_1)$, so hat $2P$ die x- Koordinate

$$m^2 - 2x_1$$

mit

$$m = \frac{3x_1^2 + a}{2y_1} \Rightarrow m_2 = \frac{(3x_1^2+a)^2}{4y_1^2} = \frac{(3x_1^2+a)^2}{4(x_1^3+ax_1+b)}$$

Die x-Koordinate von $2P$ ist also

$$\frac{(3x_1^2+a)^2}{4(x_1^3+ax_1+b)} - 2x_1 = \frac{(x_1^2-a)^2 - 8bx_1}{4(x_1^3+ax_1+b)}$$

Nun sei $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ und $x_1 \neq x_2$.
Die x- Koordinate von $P_1 + P_2$ ist dann

$$x_+ = m^2 - x_1 - x_2, \qquad m = \frac{y_2 - y_1}{x_2 - x_1}$$

$P_1 - P_2 = P_1 + (-P_2)$ und $-P_2 = (x_2, -y_2)$
$P_1 - P_2$ hat daher die x-Koordinate :

$$x_- = n^2 - x_1 - x_2, \qquad n = \frac{-y_2 - y_1}{x_2 - x_1}$$

Dann ist:

$$\begin{aligned} x_+x_- &= (m^2 - x_1 - x_2)(n^2 - x_1 - x_2) \\ &= (mn)^2 - (x_1 + x_2)(m^2 + n^2) + (x_1 + x_2)^2 \end{aligned}$$

wobei

$$\begin{aligned} mn &= -\frac{y_2^2 - y_1^2}{(x_2 - x_1)^2} = -\frac{x_2^3 - x_1^3 + a(x_2 - x_1)}{(x_2 - x_1)^2} \\ &= -\frac{x_2^2 + x_1x_2 + x_1^2 + a}{x_2 - x_1} \\ m^2 + n^2 &= \frac{(y_1 - y_2)^2 + (y_1 + y_2)^2}{(x_2 - x_1)^2} = 2 \cdot \frac{y_1 + y_2}{(x_2 - x_1)^2} \\ &= 2 \cdot \frac{x_1^3 + x_2^3 + a(x_1 + x_2) + 2b}{(x_2 - x_1)^2} \end{aligned}$$

Einsetzen und Ausmultiplizieren führt auf:

$$x_+x_- = \frac{(x_1x_2 - a)^2 - 4b(x_1 + x_2)}{(x_2 - x_1)^2}$$

Im Algorithmus von Montgomery müssen wir die Punkte

$$U_{l-1} \text{ und } V_{l-1} \text{ addieren.}$$

$U_{l-1} = N_{l-1}P, \quad V_{l-1} = (N_{l-1} + 1)P \Rightarrow V_{l-1} - U_{l-1} = P$
Ist also u_{l-1} die x- Koordinate von U_{l-1} und v_{l-1} die x- Koordinate von V_{l-1}
so ist

$$\frac{(u_{l-1}v_{l-1} - a)^2 - 4b(u_{l-1} + v_{l-1})}{(u_{l-1} - v_{l-1}^2x_1)}$$

die x-Koordinate von $U_{l-1} + V_{l-1}$
Die y- Koordinate y_* von $NP = U_{k+1}$ lässt sich folgendermaßen bestimmen:
$V_{k+1} = (N + 1)P = U_{k+1} + P$

Nach der Additionsformel ist also

$$\begin{aligned} v_{k+1} &= (\frac{y_* - y_1}{u_{k+1} - x_1})^2 - u_{k+1} - x_1 \\ &= \frac{y_*^2 - 2y_1y_* + y_1^2}{u_{k+1} - x_1})^2 - u_{k+1} - x_1 \\ &= \frac{u_{k+1}^3 + au_{k+1} + b - 2y_1y_* + y_1^2}{u_{k+1} - x_1})^2 - u_{k+1} - x_1 \end{aligned}$$

$$y_* = \frac{u_{k+1}^3 + au_{k+1} + b + y_1^2 - (v_{k+1} + u_{k+1} + x_1)(u_{k+1} - x_1)^2}{2y_1}$$

Betrachten wir x_1, y_2 als Variable, so stellen die Formeln für die u_l jedes u_l dar als rationale Funktion von x_1. Insbesondere ist die $x-$Koordinate von NP als rationale Funktion $r_N(x_1)$ darstellbar.
Da

$$\frac{1}{y_1} = \frac{y_1}{y_1^2} = \frac{y_1}{x_1^3 + ax + b}$$

ist, lässt sich die y- Koordinate y_* von NP ausdrücken als

$$y_1 s_N(x_1), s_N(x_1) \in k(x_1)$$

rationale Funktion von(x_1):

$$NP = (r_N(x_1), y_1 s_N(x_1))$$

4 Anwendungen elliptischer Kurven

4.1 Diskretes Logarithmenproblem

G sei eine zyklische Gruppe und a ein erzeugendes Element. Dann haben wir die leicht berechenbare Funktion :

$$\begin{cases} \mathbb{N}_0 \longrightarrow G \\ n \longrightarrow n \cdot a = \underbrace{a + \cdots + a}_{n-mal} \end{cases}$$

Sie ist injektiv auf $\{0,1,\ldots,\#G-1\}$
Die Umkehrabbildung

$$\begin{cases} \mathbb{G} \longrightarrow \{0,1,\ldots \#G-1\} \\ n \cdot a \longrightarrow n \end{cases}$$

heißt diskreter Logarithmus zur Basis a.

Beispiel:
$G = \mathbb{Z}/N\{0,\ldots,N-1\}$ Erzeugendes ist z.B. $a = 1$, dann ist der diskrete Logarithmus die Identität. Für a lässt sich auch eine andere Zahl wählen. Falls $ggT(a,N) = 1$, sind die Vielfachen von a modulo N alle Elemente von $\mathbb{Z}/N$. Dann gibt es ein b so dass $ab \equiv 1 \mod N$.
Der diskrete Logarithmus ist die Multiplikation mit b modulo N.

Beispiel:
$G = \mathbb{F}^\times = \{1,\ldots,p-1\}$ mit Multiplikation modulo p. Dies ist eine zyklische Gruppe mit $p-1$ Elementen.
Die Abbildung

$$\begin{cases} \{0,\ldots,p-1\} \longrightarrow \mathbb{F}_p^\times \\ n \longrightarrow a^n \end{cases}$$

ist für alle a leicht berechenbar.
Wählt man für a ein Erzeugendes, ist die Abbildung bijektiv .

Die Umkehrabbildung ist für große p schwer zu berechnen.

$$\begin{cases} \mathbb{F}_p^\times \longrightarrow \{0,\dots,p-1\} \\ a^n \longrightarrow n \end{cases}$$

Alternative:
E sei eine elliptische Kurve über einem endlichen Körper, P sei ein Punkt aus E, G die von P erzeugte zyklische Gruppe

$$G = \{0, P, 2P, 3P, \dots\}$$

Wieder ist $\mathbb{N}_0 \to G, n \to nP$ einfach zu berechnen, die Umkehrabbildung aber nicht.

4.2 Kryptoverfahren auf Basis diskreter Logarithmen

4.2.1 Schlüsselaustausch nach DIFFIE und HELLMAN

A und B möchten über eine unsichere Leitung einen Schlüssel für ein klassisches Kryptoverfahren vereinbaren. Sie wählen eine zyklische Gruppe G mit erzeugendem Element P, zum Beispiel die Gruppe aller Vielfachen eines Punktes P einer elliptischen Kurve über einem endlichen Körper.
Jeder wählt eine geheimzuhaltende Zahl. Bei A sei dies a bei B b.

- A schickt $U = aP$ an B
- B schickt $V = bP$ an A.
- A berechnet $aV = abP$
- B berechnet $bU = abP$

Dieser Punkt abP ist nun A und B bekannt.
Ein Angreifer kennt nur G, P, U, V

4.2.2 Kryptoverfahren von MASSEY und OMURA

1. A und B vereinbaren eine elliptische Kurve über einem endlichen Körper. Sie habe N Punkte.
2. A kodiert seine Nachricht durch einen Punkt M der Kurve E
3. A wählt eine natürliche Zahl m_A mit $ggT(N, m_A) = 1$.
   Er schickt $M_1 = m_A \cdot M$ an B
4. B wählt eine natürliche Zahl m_B mit $ggT(N, m_B) = 1$.
   Er schickt $M_2 = m_B \cdot M_1$ an A
5. A berechnet eine Zahl n_A mit $n_A \cdot m_A \equiv 1 \mod N$ und schickt $M_3 = n_A M_2$ an B
6. B berechnet eine Zahl n_B mit $n_B m_B \equiv 1 \mod N$ und berechnet damit $M_4 = n_B M_3$

Insgesamt ist

$$M_4 = n_B n_A m_B m_A M = (n_B m_B)(n_A m_A) M = M$$

4.2.3 Kryptoverfahren von ELGAMAL

Hier handelt es sich um ein Verfahren mit öffentlichen Schlüsseln, d.h. jeder Teilnehmer veröffentlicht in einer Art Telefonbuch einen Schlüssel. Dieser besteht bei ELGAMAL aus

- einer elliptischen Kurve E über einem endlichen Körper
- einem Punkt P auf E
- einem Vielfachen $B = sP$ von P

$s \in \mathbb{N}$ ist der geheime Schlüssel.
Will jemand eine Nachricht an den Inhaber dieses Schlüssels schicken, kodiert er diese als einen Punkt $M \in E$. Er wählt eine (geheime) Zufallszahl k und berechnet $M_1 = kP$ und $M_2 = M + kB$.
(M_1, M_2) geht an den Empfänger. Dieser berechnet:

$$\begin{aligned} M_2 - sM_1 &= (M + kB) - skP \\ &= (M + kB) - kB \\ &= M \end{aligned}$$

4.2.4 Kodierung nach KOBLITZ

Kodierung einer Nachricht durch einen Punkt der elliptischen Kurve

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

nach Koblitz. Die Kurve sei definiert über $\mathbb{F}_p$. Für die Nachricht m gelte $0 \leq m < \frac{p}{100}$. Betrachte für $j = 0, 1, 2, \ldots$ die Zahlen

$$x_j = 100m + j \quad \in \mathbb{F}_p$$

und berechne dazu

$$x_j^3 + ax_j + b$$

bis eine dieser Zahlen in $\mathbb{F}_p$ als Quadrat eines Elements y_j darstellbar ist. Die Nachricht wird kodiert als Punkt (x_j, y_j).
Betrachte die Abbildung:

$$\begin{cases} \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \\ x \longrightarrow x^2 \end{cases}$$

Ihr Kern besteht aus 1 und $p-1$, hat also zwei Elemente. Also hat das Bild $\frac{p-1}{2}$ Elemente. Von den p Elementen von $\mathbb{F}_p$ sind also $\frac{p+1}{2}$ Quadrate. Zufällig gewähltes Element ist daher mit einer Wahrscheinlichkeit von ziemlich genau 0,5 Quadrat. Wenn wir davon ausgehen, dass die Elemente $x_j^3 + ax_j + b$ sich wie zufällig verhalten, ist die Wahrscheinlichkeit, dass sie für $j = 0,\ldots k-1$ keine Quadrate sind $\sim 2^- k$. Speziell für $k = 100 : p \approx 2^{-100} \approx 10^{-30}$.
Wie erkennt man Quadrate in $\mathbb{F}_p$ und bestimmt die Wurzel?
Am einfachsten geht das, wenn $p \equiv 3 \bmod 4$ ist. Angenommen, $c = y^2$ ist ein Quadrat in $\mathbb{F}_p$. Dann ist zunächst

$$c^{\frac{p+1}{4}} = c^{\frac{p+1}{2}} = y^{p+1} = y^{p-1} = 1 \cdot y^2 = c$$

d.h. in diesem Fall ist $c^{\frac{p+1}{4}}$ eine Quadratwurzel von c. Um zu testen, ob c ein Quadrat ist, berechnet man also $y = c^{\frac{p+1}{4}}$, falls das Quadrat $y^2 = c$ ist, ist c Quadrat und y Wurzel, sonst ist c kein Quadrat. In der Praxis lässt sich also schnell und effizient ein $x_j = 100m + j$ mit $j \leq 99$ finden, so dass $x_j^3 + ax_j + b$ Quadrat eines $y_j \in \mathbb{F}_p$ ist. Die Nachricht m wird dann kodiert durch den Punkt $m_j = (x_j, y_j)$.
Aus m_j lässt sich m bestimmen als $m = [\frac{x_j}{100}]$

4.2.5 Kryptoverfahren von Koyama, Maurer, Okamoto und Vanstone

Der Empfänger wählt zwei große Primzahlen p und q aus, für die gilt:

$$p \equiv q \equiv 2 \mod 3$$

und berechnet $n = pq$. Weiter wählt er die Zahlen e,d mit $ed \equiv 1 \bmod kgV(p-1,q-1)$. n und e werden als öffentlicher Schlüssel bekannt gegeben. Wer ihm eine Nachricht schicken will, geht fogendermaßen vor:
Die Nachricht wird als Zahlenpaar (m_1,m_2) dargestellt. $M = (m_1,m_2)$ wird aufgefasst als Punkt der elliptischen Kurve

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

mit

$$b = (m_2^2 - m_1^3) \mod n$$

Dort wird $C = e \cdot M$ berechnet und als verschlüsselte Nachricht abgeschickt. Der Empfänger berechnet

$$d \cdot C = deM$$

Man kann zeigen: Die elliptische Kurve der Form

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

über einem endlichen Körper k hat so viele Punkte, wie k Elemente hat. Ist $ed \equiv 1 \mod \#k - 1$, so ist $ed \cdot M = M$. Dies gilt hier für $k = \mathbb{F}_p$ und $k = \mathbb{F}_q$, also nach dem chinesischen Restesatz auch über $\mathbb{Z}/n$.

4.3 Elektronische Unterschriften mit elliptischen Kurven

4.3.1 Das Verfahren von ELGAMAL

Der Unterschreibende legt folgende Daten fest:

- Eine elliptische Kurve E über einem Körper $\mathbb{F}_p$, p prim
- Einen Punkt $A \in E(\mathbb{F}_p)$, dessen Ordnung N möglichst groß ist , beispielsweise eine große Primzahl
- Einen geheimen Multiplikator $a \in \mathbb{N}$ und $B = a \cdot A$ und eine Funktion $f : E(\mathbb{F}_p) \to \mathbb{Z}$ z.B. die x-Koordinate via der Identifizierung $\mathbb{F}_p = \{0, \ldots p-1\}$

öffentlicher Schlüssel:

$$E, \mathbb{F}_p, f, A, B$$

geheimer Schlüssel:

$$a$$

Unterschrift unter die Nachricht $m < N$:
Wähle für jede Unterschrift eine neue Zufallszahl $k < N$ mit

$$ggT(k, N) = 1$$

und berechne

$$R = k \cdot A$$

Sodann wird

$$s = (k^{-1}(m - af(R))) \mod N$$

berechnet.
Die unterschriebene Nachricht ist:

$$(m, R, s)$$

Verifikation der Unterschrift (m, R, s):
Berechne $V_1 = f(R)B + sR$ und $V_2 = mA$.
Mit $B = aA$ und $R = kA$ folgt:

$$\begin{aligned} V_1 &= f(R)aA + skA \\ &= f(R)aA + (m - af(R))A \\ &= mA \\ &= V_2 \end{aligned}$$

Die Unterschrift wird somit akzeptiert, wenn $V_1 = V_2$ ist.

4.3.2 Der Digitale Signatur Algorithmus DSA auf Basis elliptischer Kurven $E(\mathbb{F}_p)$

p sei eine Primzahl, E elliptische Kurve über $\mathbb{F}_p$. $G \in E(\mathbb{F}_p)$ Punkt der Ordnung q, q von p verschiedene Primzahl. Sicherheitsanforderungen der Bundesnetzagentur: Bis Ende 2015 muss q mindestens 224 Bit haben, bis Ende 2019 mindestens 250. Außerdem muss

$$r_0 = \min(r \cdot q | p^r - 1) > 10^4$$

sein, und die Klassenzahl der Hauptordnung zum Endomorphismenring von E muss mindestens 200 sein.
Weiter wählt der Unterzeichnende ein zufälliges $A \in \{1, 2, \ldots q-1\}$ als geheimen Schlüssel, dazu berechnet er den Punkt

$$Q = a \cdot G$$

Der öffentliche Schlüssel besteht aus

$$\mathbb{F}_p, E, q, G, Q$$

Unterschriften:
Für jede Unterschrift wird eine Zufallszahl $k \in \{1,\ldots,q-1\}$ gewählt, und

$$R = k \cdot G$$

wird berechnet. R habe Koordinaten (x,y). Zum Unterschreiben einer Nachricht $m \in \{0,\ldots,q-1\}$ wird

$$s = k^{-1}(m + ax) \mod q$$

berechnet. Das unterschriebene Dokument ist:

$$(m,R,s)$$

Verifikation der Unterschrift:

1. Berechne $u_1 = s^{-1} \cdot m \mod q$ und $u_2 = s^{-1} \cdot x$
2. Berechne $V = u_1 G + u_2 Q$
3. Die Unterschrift wird akzeptiert, wenn $V = R$ ist

Grund:

$$\begin{aligned} V &= u_1 G + u_2 Q \\ &= s^{-1} m G + s^{-1} x Q \\ &= s^{-1}(mG + xaG) \\ &= s^{-1}(m + ax)G \end{aligned}$$

$$s = k^{-1}(m + ax) \Rightarrow s^{-1} = k(m + ay)^{-1}$$

d.h.

$$V = k(m + ax)^{-1} \cdot (m + ax)G = kG = R$$

Weitere Variante:

4.3.3 ECGDSA (Elliptic curve german digital signature algorithm)

Wir gehen wieder aus von einer elliptischen Kurve E über $\mathbb{F}_p$ und einem Punkt $G \in \mathbb{F}_p$ der Ordnung q. Geheimer Schlüssel $a \in \{1,\ldots,q-1\}$ und dem zugehörigen öffentlichen Punkt $Q = a^{-1} \cdot G$.
Unterschrift unter Nachricht m:
Wähle $k \in \{1,\ldots q-1\}$ zufällig und setze

$$r = kG = (x,y)$$

berechne

$$r = x \mod q$$

Falls $r = 0$: Wähle neues k.
Berechne:

$$s = (kr - m) \cdot a \mod q$$

Falls $s = 0$: Wähle neues k
Unterschrift:

$$(r,s)$$

Verifikation:
Berechne

$$r^{-1} \mod q$$

$$u_1 = r^{-1}m \mod q, \qquad u_2 = r^{-1}s \mod q$$

$$V = u_1G + u_2Q \qquad v = x \mod q$$

Die Unterschrift wird akzeptiert, falls

$$v = r$$

ist.
Grund: Im wesentlichen dieselbe Rechnung wie oben.

4.4 Faktorisierung ganzer Zahlen

4.4.1 POLLARDS-(p-1)-Methode

Faktorisiert werden soll eine Zahl n.
Annahme: Einer der Primfaktoren p von n hat folgende Eigenschaft:
Jede Primzahlpotenz q^e, die $p-1$ teilt, ist kleiner oder gleich einer Schranke B. Für die anderen Primteiler von n gelte das nicht. Wir rechnen in $\mathbb{F}_p^\times$; seine Elemente werden durch Restklassen mod n repräsentiert. Wir gehen aus von einer Zahl $a \geq 2$. Für jede Primzahl $p \leq B$ ersetzen wir das jeweilige a durch a^{p^e}, wobei p^e die größte p-Potenz $\leq B$ ist (Alle Rechnungen modulo n). Das Endergebnis sei b. Dann ist

$$b = a^m \mod n \text{ wobei } m = \prod p_i^{e_i}, \{p_i\} = \{\text{Primzahlen} \leq B\}, e_i$$

so, dass $p_i^{e_i} \leq B,\ p_i^{e_i+1} \geq B$.
Wenn unsere Annahme stimmt, ist $(p-1 \mid m)$ und nach Fermat ist

$$a^{p-1} \equiv 1 \mod p$$

Für andere Primteiler q von p ist wohl im Allgemeinen

$$a^{p-1} \not\equiv 1 \mod q \text{ und } a^m \not\equiv 1 \mod q$$

p ist Teiler von $a^m - 1$, da mit a^{p-1} auch $a^m \equiv 1 \mod p$ ist.
Berechne $ggT(n, b-1)$. Wir können hoffen, dass dies gleich p ist, oder zumindest ein nichttrivialer Teiler von n.
Nachteil: Wir wissen nie, ob unsere Annahme erfüllt ist
Vorteil: Wenn die Methode funktioniert, liefert sie oft mit verhältnismäßig geringem Aufwand recht große Faktoren.
Verallgemeinerung: Ersetze $\mathbb{F}_p^\times$ durch eine andere Gruppe G_p. Dann haben wir Erfolgsaussichten, wenn die Gruppenordnung von G_p ($\#G_p$) nur durch kleine Primzahlpotenzen teilbar ist.
Schlimmster Fall für die (p-1)-Methode:
Alle Primteiler p von n haben die Form $p = 2q+1$, q prim.

4.4.2 Die elliptische Kurven Methode von Lenstra

HASSE:
Für eine elliptische Kurve E über $\mathbb{F}_p$ gilt:

$$p+1-\sqrt{2p} < \#E(\mathbb{F}_p) < p+1+2\sqrt{2p}$$

FREY, RÜCK:
Zu jeder natürlichen Zahl aus diesem Intervall gibt es eine elliptische Kurve über $\mathbb{F}_p$ mit entsprechender Elementanzahl.

Beispiel:
$N = 4453, \quad E : y^2 = 10x - 2, \quad p =$ gesuchter Primfaktor von N
Wir rechnen $\mod N$ in der von $(1,3)$ erzeugten zyklischen Gruppe.
Wir berechnen $3P$.
Dazu bestimmen wir zunächst $2P$ nach der Verdoppelungsformel:
Die Tangentensteigung im Punkt (x,y) ist $m = \frac{3x^2+10}{2y}$ in $(1,3)$ also

$$m = \frac{13}{16} \mod p$$

Da wir p nicht kennen, versuchen wir dies modulo N zu berechnen, d.h. wir wenden den erweiterten Euklidischen Algorithmus an auf N und 6 und erhalten eine Darstellung:

$$ggT(N,6) = a \cdot N + b \cdot 6$$

Falls der $ggT(N,6) = 1$ ist

$$b \cdot 6 = 1 - a \cdot N \equiv 1 \mod N$$

d.h. modulo N ist b invers zu 6.
Wir erhalten als Ergebnis: $ggT(N,6) = 1$ und $b = 3711$.
Also ist $m = 13 \cdot 3711 \mod N$ und $2P = (x,y)$ mit $x = 4332, y = 3230$
$3P = 2P + P$. Die Gerade durch P und $2P$ hat die Steigung

$$m = \frac{3230-3}{4332-1} = \frac{3227}{4331}$$

Wende den erweiterten Euklidischen Algorithmus an auf 4331 und $N = 4453$:

$$4453 : 4331 = 1 \; Rest \; 122$$
$$4331 : 122 = 35 \; Rest \; 61$$
$$122 : 61 = 2 \; Rest \; 0$$

Also ist $ggT(4331, N)$=61, es gibt also kein Inverses zu 4331 modulo 4453. $4453 : 61 = 73$. Unsere Rechnung zeigt: Wenn wir E über $\mathbb{F}_{61}$ betrachten, ist $3P = O$, über $\mathbb{F}_{73}$ betrachtet aber nicht. Vor allem aber zeigte sie uns, dass 61 ein Faktor von 4453 ist. Modulo N müsste man E nach dem chinesischen Restesatz zerlegen in E mod 61 und E mod 73.

Allgemeine Vorgehensweise:
Gegeben sei eine natürliche Zahl N.
Gesucht: Ein Faktor p von N

1. Man wähle einige $(10 - 20)$ zufällige elliptische Kurven
$$E_i : y^2 = x^3 + a_i x + b_i \mod N$$
und auf jeder einen Punkt $P_i \in E(\mathbb{Z}/N)$
2. Wähle eine Suchschranke $B(\sim 10^8)$ und ersetze für jede Primzahl $p < N$ die Punkte P_i durch $p^e P_i$, p^e größte p-Potenz $< B$

Wir hoffen, dass bei mindestens einer Kurve und einer Primzahl $p^e P_i$ nicht berechenbar ist, da der Nenner der Steigung nicht teilerfremd zu N ist. Dann haben wir einen Faktor gefunden.
Falls sich Schritt 2 bis zum Ende durchführen lässt, war der Ansatz erfolglos; man kann dann versuchen, B zu erhöhen oder mehr elliptische Kurven betrachten.
In der Praxis funktioniert die Methode recht gut für Faktoren bis etwa 10^{40}.

4.5 Primzahltest mit elliptischen Kurven

4.5.1 Klassisches Analogon

Kleiner Satz von FERMAT: p prim, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \mod p$
Umkehrung: $p \nmid a$, $a^{p-1} \not\equiv 1 \mod p \Rightarrow p$ ist nicht prim .

Angenommen, wir kennen alle Primteiler von $p-1$.
Falls gilt:

$$a^{p-1} \equiv 1 \mod p$$

und für jeden Primteiler l von $p-1$

$$a^{\frac{p-1}{l}} \not\equiv 1 \mod p$$

dann ist p prim. Denn dann ist die Ordnung von $a \mod p$ ein Teiler von $p-1$ aber für $l|p-1$ kein Teiler von $\frac{p-1}{l}$, d.h. sie ist $p-1$. Also ist $(\mathbb{Z}/p)^\times$ die von a erzeugte zyklische Gruppe mit $p-1$ Elementen, d.h. p ist prim.

4.5.2 POCKLINGTON-LEHMER-Test

Sei $p > 1$ und $p-1 = r \cdot s$, mit $r > \sqrt{p}$. Falls es für jeden Primteiler l von r ein a_l gibt, so dass

$$a_l^{p-1} \equiv 1 \mod p$$

und

$$ggT(a_l^{\frac{p-1}{l}} - 1, p) = 1$$

dann ist p prim.

Beweis:
q sei ein Primfaktor von p und l^e sei die größte l-Potenz, die r teilt. Sei $b = a_l^{\frac{p-1}{l^e}} \mod q$. Dann ist

$$b^{l^e} = a_l^{p-1} \equiv 1 \mod q$$

aber

$$b^{l^{e-1}} = a_l^{\frac{p-1}{l}} \not\equiv 1 \mod q$$

Also hat b modulo q die Ordnung l^e. Somit teilt l^e insbesondere $q-1$. Das Produkt aller l^e ist r also folgt: $r|q$. Das gilt für jeden Primteiler q von p, d.h. jeder Primteiler von p ist $\geq r > \sqrt{p}$. Damit ist gezeigt, dass p prim ist.

Übertragung auf elliptische Kurven:

Satz:
Sei $p \in \mathbb{N}$ und E eine elliptische Kurve modulo p. Falls es Primzahlen $l_1 \dots l_k$ gibt, und Punkte $P_i \in E \backslash \{O\}$, so dass gilt:

1. $l_i P_i = O$, für $i = 1, \dots k$
2. $\prod_{i=1}^{k} l_i > (\sqrt[4]{p} + 1)^2$

so folgt, dass p eine Primzahl ist.

Beweis:
q sei ein Primfaktor von p, $p = q^f \cdot n$, $ggT(n,q) = 1$.

$$E(\mathbb{Z}/p) = E(\mathbb{Z}/q^f) \oplus E(\mathbb{Z}/n)$$

P_i definiert auch einen Punkt ungleich O in $E(\mathbb{Z}/q^f)$ sowie $E(\mathbb{Z}/q)$, da l_i prim ist, hat P_i auch modulo q die Ordnung l_i. Also teilt nach dem Satz von Lagrange l_i die Elementanzahl von $E(\mathbb{F}_q)$ für alle i, d.h.

$$\prod_{i=1}^{k} l_i | \#E(\mathbb{F}_q)$$

Somit ist nach dem Satz von Hasse

$$(\sqrt[4]{p} + 1)^2 < \prod_{i=1}^{k} l_i \leq \#E(\mathbb{F}_q) < q + 1 + 2\sqrt{q} = (\sqrt{q} + 1)^2$$

Also ist

$$\sqrt{q} + 1 > \sqrt[4]{p} + 1 \Longrightarrow q > \sqrt{p}$$

Das geht nicht, also muss p prim sein.

□

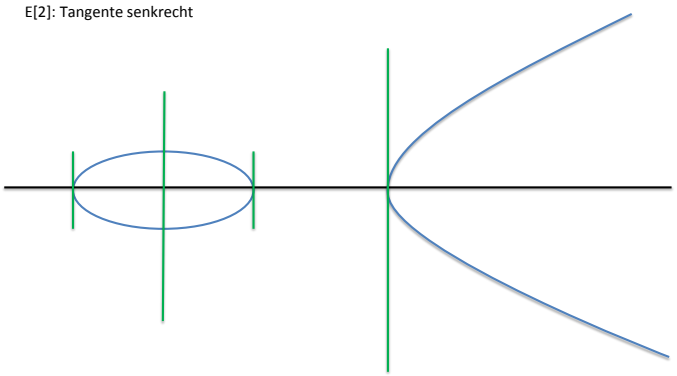
5 Torsionspunkte

k sei ein Körper, $\bar{k}$ ein algebraisch abgeschlossener Körper der k enthält, E eine elliptische Kurve über k.

Definition:
$E[n] = \{P \in E(\bar{k}) \mid nP = O\}$ heißt die Menge der n-**Torsionspunkte** von E, $n \in \mathbb{N}$
Sei char $k \neq 2,3 \quad E : y^2 = x^3 + ax + b, \quad a,b \in k$

$$E[1] = \{O\}$$

$$E[2] = \{O,(\gamma_1,0),(\gamma_2,0),(\gamma_3,0)\}, \quad x^3 + ax + b = \prod_{i=1}^{3}(x - \gamma_i)$$



$E[3]$= Menge aller Wendepunkte von $E[\bar{k}]$, dies ist eine neunelementige Menge

Als abstrakte Gruppe ist

$$E[1] \cong < 0 >$$

$$E[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

$P = (\gamma_1,0) + (\gamma_2,0)$
$2P = 2(\gamma_1,0) + 2(\gamma_2,0) = O + O = O$
Somit ist $(\gamma_1,0) + (\gamma_2,0) = (\gamma_3,0)$

Gruppentafel:

+	O	$(\gamma_1,0)$	$(\gamma_2,0)$	$(\gamma_3,0)$
O	O	$(\gamma_1,0)$	$(\gamma_2,0)$	$(\gamma_3,0)$
$(\gamma_1,0)$	$(\gamma_1,0)$	O	$(\gamma_3,0)$	$(\gamma_2,0)$
$(\gamma_2,0)$	$(\gamma_2,0)$	$(\gamma_3,0)$	O	$(\gamma_1,0)$
$(\gamma_3,0)$	$(\gamma_3,0)$	$(\gamma_2,0)$	$(\gamma_1,0)$	O

Also ist

$$E[2] \cong \{O,(\gamma_1,0)\} \times \{O,(\gamma_2,0)\}$$
$$P + Q \longleftarrow (P,Q)$$

$E[3] \cong \mathbb{Z}/3 \times \mathbb{Z}/3, P \neq O$ sei ein Wendepunkt; er erzeugt eine zyklische Gruppe $\{O,P,2P\}, Q \notin \{O,P,2P\}$ sei ein weiterer Wendepunkt.

Behauptung:
$\begin{cases} E[3] \cong \{O,P,2P\} \times \{O,Q,2Q\} \\ R + S \longleftarrow (R,S) \end{cases}$

Beweis:
Das Bild von ϕ besteht aus allen Punkten der Form

$$rP + sQ, \quad r,s \in \{0,1,2\}$$

Je zwei dieser Punkte sind verschieden, denn sonst gäbe es eine nichttriviale Darstellung

$$O = rP + sQ, \quad r,s \in \mathbb{Z}\backslash\{0\}$$

d.h. $rP = -sQ$, d.h. P und Q erzeugen die gleiche zyklische Gruppe, $\lightning$ Wir haben eine bijektive Abbildung, denn jede surjektive Abbildung

zwischen zwei gleichmächtigen endlichen Mengen ist injektiv, also auch bijektiv. Homomorphismus, klar.

□

Gruppenstruktur auf einem Produkt:
$(G,+),(H,+)$ seien Gruppen. Für $(g_1,h_1),(g_2,h_2) \in G \times H$ ist

$$(g_1,h_1)+(g_2,h_2) = (g_1+g_2,h_1+h_2)$$

$$-(g_1,h_1) = (-g_1,-h_1),$$

Neutralelement: $(0,0)$

Ziel: Falls char $k \nmid n$, ist $E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$
$E[n]$ ist der Kern des Gruppenhomomorphismus

$$\begin{cases} E[\bar{k}] \longrightarrow E[\bar{k}] \\ P \quad \longrightarrow n \cdot P \end{cases}$$

Wir wollen diese Abbildung auch geometrisch betrachten.

Definition:
Eine rationale Funktion mit Koeffizienten aus k in x,y ist ein Quotient $r(x,y) = \frac{p(x,y)}{q(x,y)}, p,q \in k[x,y]$ Polynome in x,y, $\quad q \neq$ Nullpolynom. Die Menge aller rationaler Funktionen wird mit $k(x,y)$ bezeichnet. Aus den Regeln der Bruchrechnung folgt: $k(x,y)$ ist ein Körper.

Definition:
E,E' seien zwei elliptische Kurven über k.
Ein Morphismus $\phi : E \to E'$ ist gegeben durch zwei rationale Funktionen $r,s \in k(x,y)$:

$$\phi((x,y)) = (r(x,y),s(x,y))$$

Da $\phi(P) \in E' : y^2 = x^3 + a'x + b'$, für alle Punkte $P \in E : y^2 = x^3 + ax + b$, muss gelten:

$$s(x,y)^2 = r(x,y)^3 + a'r(x,y) + b, \quad \forall (x,y) \in E$$

Beispiele:
Ist $Q \in E$ ein fester Punkt, so ist die Abbildung

$$\begin{cases} E \longrightarrow E \\ P \longrightarrow P + Q \end{cases}$$

ein Morphismus.
Für jedes $n \in \mathbb{N}$ ist auch

$$\begin{cases} E \longrightarrow E \\ P \longrightarrow n \cdot P \end{cases}$$

ein Morphismus. Die Funktionen r_n, s_n hierzu haben wir mit dem Algorithmus von Montgomery bestimmt.

Definition:
Ein Endomorphismus einer elliptischen Kurve E ist ein Morphismus

$$E \to E'$$

der gleichzeitig ein Gruppenhomomorphismus ist.

Endomorphismen können addiert werden:
Für $\phi, \psi : E \to E$ ist $\phi + \psi$ die Abbildung $: E \to E$ mit:

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

auch

$$\phi \circ \psi = \begin{cases} E \longrightarrow E \\ P \longrightarrow \phi(\psi(P)) \end{cases}$$

ist wieder ein Endomorphismus. Somit ist die Menge aller Endomorphismen ein Ring, der Endomorphismenring End E. Da die Multiplikation mit $n \in \mathbb{N}$ ein Endomorphismus ist und $P \to -P$ auch, ist auch $P \to -nP$ ein Endomorphismus.

$$\begin{cases} E \to E \\ P \to O \end{cases}$$

ist das additive Neutralelement von End E; wir haben also für jedes $n \in \mathbb{Z}$ einen Endomorphismus $P \to nP$. Für $n \neq m$ sind diese verschieden: Ansonsten wäre $(n-m)P = O$ für alle $P \in E(\bar{k})$, d.h. $E(\bar{k}) \subseteq E[n-m]$. Da $E[n-m]$ Kern eines Morphismus ist, wird es in der x-Koordinate durch das Verschwinden des Nenners von $r_N(x)$ definiert,

$$\begin{cases} E \to E \\ P \to nP = (r_N(x), y s_N(x)), P = (x,y) \end{cases}$$

daher ist $E[n-m]$ endlich, $E(\bar{k})$ aber nicht, da jeder algebraisch abgeschlossene Körper unendlich ist. Somit können wir $\mathbb{Z}$ einbetten als Unterring in End E.

In char k gibt es immer noch einen weiteren Endomorphismus, den Frobenius-Endomorphismus:

$$\begin{cases} E \to E \\ (x,y) \to (x^p, y^p) \end{cases}$$

denn $(x+y)^p = x^p + y^p, (xy)^p = x^p y^p$; auch seine Potenzen sind Endomorphismen.

Elliptische Kurve über endlichen Körper lassen sich in Untergruppe einbetten in $\mathbb{Z} \mod m \times \mathbb{Z} \mod m$.

Definition:
$C \subseteq k^2$ sei eine ebene Kurve und $P \in C$. Eine **Ortsuniformisierende** oder **lokale Koordinate** in P ist eine rationale Funktion $\mu_P \in k(X,Y)$ für die gilt:

1. $\mu_P(P) = O$
2. Ist f irgendeine rationale Funktion auf C, so gibt es ein $d \in \mathbb{Z}$, so dass gilt:

   $$f = \mu_P^d g$$

   wobei g eine rationale Funktion ist, deren Zähler und Nenner beide nicht in P verschwinden

d.h. g hat in P weder Nullstellen noch Polstellen (y-Koordinate=0)

Beispiel: $C = \{y = 0\}$:
Die rationalen Funktionen von C sind gerade die rationalen Funktionen in X. Ortsuniformisierende in $(x_0, 0)$ ist z.B. $X - x_0$
1. ist klar
2. $f = \frac{p(X)}{q(X)}$ sei irgendeine rationale Funktion, $ggT(p,q) = 1$.
Falls $p(x_0) = 0$ gibt es ein $d \in \mathbb{N}$, so dass

$$p(X) = (X - x_0)^d \tilde{p}(X), \quad \tilde{p}(x_0) = 0$$

und

$$f = (X - x_0)^d \frac{\tilde{p}(X)}{q(X)}$$

Falls $q(x_0) = 0$:
$q(X) = (X - x_0)^e \tilde{q}(X), \tilde{q}(x_0) \neq 0$ und $f = (X - x_0)^e \frac{p(x)}{\tilde{q}(x)}$.
Falls $p(x_0) \neq 0$ und $q(x_0) \neq 0$, können wir $d = 0$ und $g = f$ setzen.
Projektiv betrachtet haben wir noch einen unendlichfernen Punkt. Hier ist $\frac{1}{X}$ die Ortsuniformisierende.

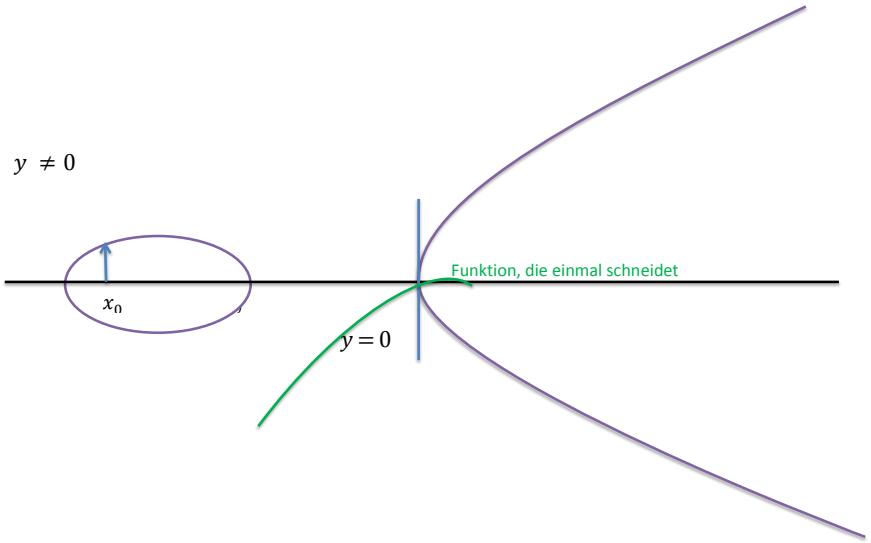
Auf einer elliptischen Kurve

$$E : y^2 = x^3 + ax + b$$

lässt sich jede rationale Funktion auf E realisieren durch ein Element von $k(X)[Y]/(Y^2 - X^3 - aX - b) \cong k(X) \oplus k(X)Y$. Jede rationale Funktion auf E lässt sich also schreiben in der Form

$$r(x,y) = s(x) + y \cdot t(x), \quad s,t \in k(x)$$

Für einen Punkt $(x_0, y_0) \in E$ mit $y_0 \neq 0$ ist wieder $X - x_0$ eine Ortsuniformisierende. Für die Punkte $(x_0, 0)$ ist y eine Ortsuniformisierende.
Im unendlichfernen Punkt O ist $\frac{Y}{X}$ eine Ortsuniformisierende



Definition:
f sei eine rationale Funktion auf der elliptischen Kurve $E, P \in E$ und μ_p eine Ortsuniformisierende in P. Ist $f = \mu_p^d \cdot g$, wobei weder Zähler noch Nenner in g verschwindet, heißt d die **Ordnung** von f in P, $d = ord_P f$
Ist $d = ord_P f > 0$, hat f eine d-fache Nullstelle in P, ist $d < 0$ eine $(-d)$-fache Polstelle

Ein Morphismus $\phi : E_1 \to E_2$ zwischen elliptischen Kurven ist gegeben durch zwei rationale Funktionen r, s auf E_1:

$$\phi(P) = (r(P), s(P))$$

falls r, s keine Pole in P haben.
Wir nehmen wie üblich an, dass E_1 und E_2 durch Weierstraß-Gleichungen gegeben sind.

$$E_i : y^2 = x^3 + a_i x + b_i$$

Für jeden Punkt $P \in E_1$ gilt dann:

$$s(P)^2 = r(P)^3 + a_2 r(P) + b_2 \quad (*)$$

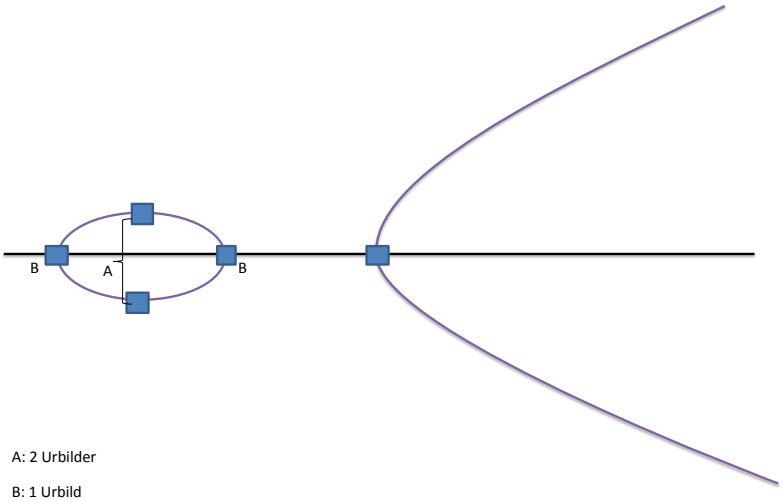
μ sei Ortsuniformisierende im Punkt $P \in E_1$.
$s(P) = \mu^d \cdot \tilde{s}(P), \tilde{s}(P) \neq 0, \infty, \quad r(P) = \mu^e \cdot \tilde{r}(P), \tilde{r}(P) \neq 0, \infty$

Da (*) gilt, müssen im Falle $d < 0$ oder $e < 0$ die Polordnungen links und rechts gleich sein, d.h. $2d = 3e$. Der Wert $\phi(P)$ in einem solchen Punkt ist

$$(\tilde{r}(P), \tilde{s}(P))$$

Definition:
E sei elliptische Kurve, $P \in E, g$ sei eine nichtkonstante rationale Funktion auf E. μ sei eine Ortsuniformisierende in $g(P) \in \mathbb{P}^1$.
Der **Verzweigungsindex** von g in P ist

$$\epsilon_g(P) = ord_P(\mu \circ g)$$



Beispiel:
$g(x,y) = x$, für $P = (x_0, y_0)$ ist $g(P) = x_0$, wir können also $\mu = X - x_0$ nehmen. Dann ist auch

$$\mu \circ g = X - x_0$$

Falls $y_0 \neq 0$ ist $\mu \circ g$ somit eine Ortsuniformisierende von P auf E, d.h.

$$\epsilon_g(P) = ord_P(X - x_0) = 1$$

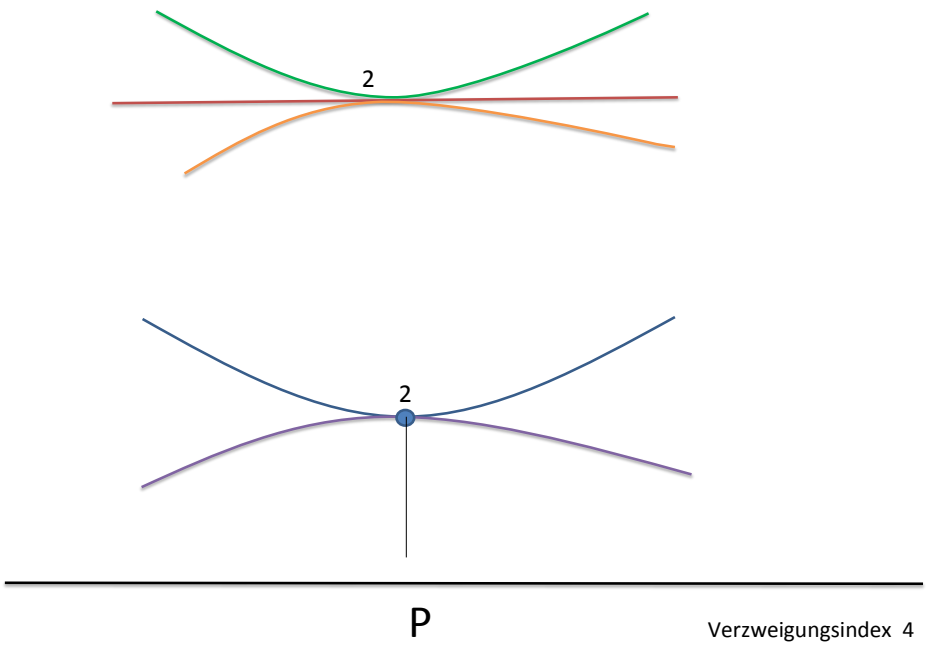
Falls $y_0 = 0$ ist $X - x_0$ keine Ortsuniformisierende, sondern z.B. Y.
$X - x_0$ hat in (x_0, y_0) eine doppelte Nullstelle (Tangente), d.h.

$$\epsilon_g(P) = ord_p(X - x_0) = 2$$

Definition:
E_1, E_2 seien elliptische Kurven, $P \in E_1$ und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus(gegeben durch ein Paar rationaler Funktionen, oder projektiv durch Tripel homogener Polynome desselben Grads).
Ist μ eine Ortsuniformisierende im Punkt $\phi(P)$, so heißt

$$\epsilon_g(P) = ord_P(\mu \circ \phi)$$

der **Verzweigungsindex** in P.
Allgemein sagen wir , eine Abbildung zwischen zwei Kurven sein **unverzweigt** in einem gegebenen Punkt, wenn der Verzweigungsindex dort 1 ist, ansonsten ist sie dort **verzweigt**.



Lemma:
Sind $\phi : E_1 \to E_2, \psi : E_2 \to E_3$ Morphismen zwischen elliptischen Kurven, so gilt für $P \in E_1$:

$$\epsilon_{\psi\circ\phi}(P) = \epsilon_\phi(P) \cdot \epsilon_\psi(\phi(P))$$

□

Lemma:
$\phi : E_1 \to E_2$ sei eine Isogenie (also zusätzlich ein Gruppenhomomorphismus). Dann ist der Verzweigungsindex $\epsilon_\phi(P)$ unabhängig von $P \in$

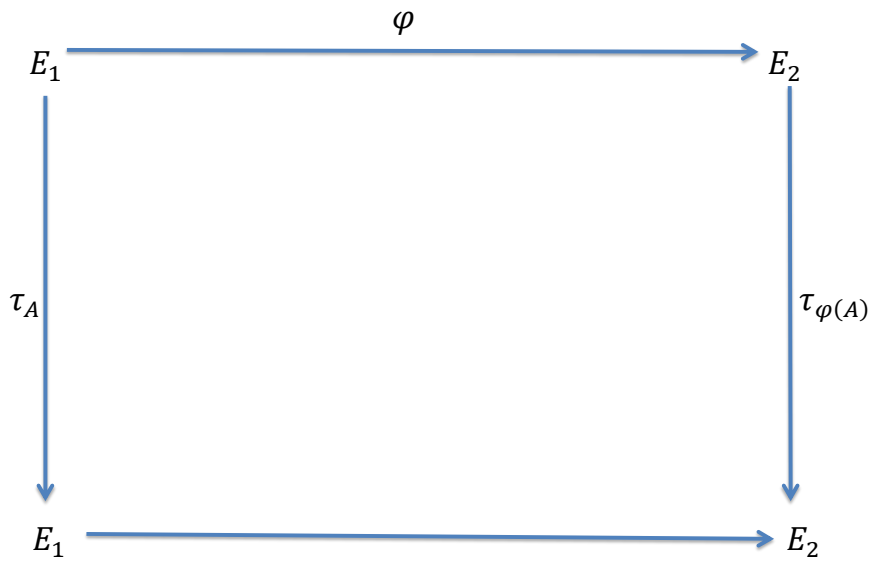
E_1

Beweis:
Für alle $P, Q \in E_1$ ist $\phi(P+Q) = \phi(P) + \phi(Q)$. Bezeichnet allgemein

$$\tau_A = \begin{cases} E \longrightarrow E \\ P \longrightarrow P + A \end{cases}$$

für eine elliptische Kurve E und einen Punkt $A \in E$ die Addition von A, so ist

$$(*)\tau_{\phi(A)} \circ \phi = \phi \circ \tau_A$$



denn $\tau_{\phi(A)} \circ \phi(P) = \phi(P) + \phi(A)$ und $\phi \circ \tau_A(P) = \phi(P+A)$.
Im Punkt $O \in E_1$ ist

$$\epsilon_{\phi \circ \tau_A}(O) = \epsilon_{\tau_A}(O) \cdot \epsilon_\phi(A) = \epsilon_\phi(A)$$

denn τ_A ist unverzweigt

$$\epsilon_{\phi(A) \circ \phi}(O) = \epsilon_\phi(O) \cdot \epsilon_{\tau_{\phi(A)}}(\phi(A)) = \epsilon_\phi(O)$$

denn $\tau_{\phi(A)}$ ist unverzweigt, also ist auch $\epsilon_\phi(A) = \epsilon_\phi(O)$. Da A beliebig war, sind alle $\epsilon_\phi(A)$ gleich. □

Definition:
$\phi : E_1 \to E_2$ sei eine Isogenie (surjektiv), gegeben durch

$$P \to (r(x), y \cdot s(x)), \quad r,s \in k(x)$$

ϕ heißt **separabel**, wenn die Funktion $r'(x)$ nicht identisch verschwindet.

Beispiel:
E sei eine elliptische Kurve über $\mathbb{F}_p$

$$F : \begin{cases} E \to E \\ (x,y) \to (x^p, y^p) \end{cases}$$

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

$$\Rightarrow (y^p)^2 = (y^2)^p = (x^3 + ax + b)^p = x^3 p + a^p x^p + b^p = (x^p)^3 + ax^p + b$$

denn für alle Elemente von $\mathbb{F}_p$ ist $a^p = a$.
Hier ist

$$r(x) = x^p \Rightarrow r'(x) = p \cdot x^p - 1 = 0$$

$$s(x) = (x^3 + ax + b)^{\frac{p-1}{2}}$$

Damit ist F nicht separabel.

Lemma:
Eine Isogenie ist genau dann separabel, wenn sie unverzweigt ist.

Beweis:
$\phi : E_1 \to E_2$ sei gegeben durch $(x,y) \to (r(x), ys(x))$. Falls ϕ separabel ist, ist $r'(X)$ nicht identisch Null, es gibt also Punkte $(x,y) \in E_1$ mit $r'(x) \neq 0, y \neq 0$.

$$\epsilon_\phi((x,y)) = ord_{(x,y)}(r(X) - r(x))$$

$r(X) - r(x)$ verschwindet in x nur mit Multiplizität 1, da die Ableitung $r'(X)$ in x nicht verschwindet, ($r(x)$ ist eine Konstante, deren Ableitung ist Null.)

Somit ist $\epsilon_\phi(x,y) = 1$, also ist er überall gleich 1 (nach obigem Lemma).
Umkehrung: genauso (es reicht zu zeigen, dass es einen Punkt gibt, an dem die Ableitung nicht verschwindet, denn ist sie inseparabel, so ist sie überall gleich Null). □

Definition:
Der Grad $\deg\phi$ einer Isogenie $\phi : E_1 \to E_2$ ist $\epsilon_\phi \cdot \#\ker\phi$

Lemma:
Sind $\phi : E_1 \to E_2$ und $\psi : E_2 \to E_3$ Isogenien, so ist

$$\deg(\psi \circ \phi) = \deg\phi \cdot \deg\psi$$

Beweis:
$\#\ker(\psi \circ \phi) = \#\ker\psi \cdot \#\ker\phi$ und $\epsilon_{\phi\circ\psi} = \epsilon_\phi \cdot \epsilon_\psi$

□

Im Folgenden bezeichnen wir mit

$$[n] : \begin{cases} E \to E \\ P \to nP \end{cases}$$

die Multiplikation mit n, d.h.

$$E[n] = \ker[n]$$

Konkret: $[n]((x,y)) = (r_n(x), y \cdot s_n(x))$

$$r_1(x) = x, \quad s_1(x) = 1$$

$$r_2(x) = \frac{(3x^2 + a^2)}{4(x^3 + ax + b)} - 2x = \frac{F'(x)^2}{4F(x)} - 2$$

mit $F(x) = x^3 + ax + b$

$$s_2(x) = -\frac{F'(x)^2}{2F(x)}(r_2(x) - x) - 1 = -\frac{F'(x)}{2F(x)}\left(\frac{F'(x)^2}{4F(x)} - 3x\right) - 1$$

Ist

$$\lambda_n = \frac{ys_n - y}{r_n - x} \Rightarrow \lambda_n^2 = F(x)\left(\frac{s_n - 1}{r_n - x}\right)^2$$

und

$$r_{n+1} = \lambda_n^2 - r_n - x$$

$$ys_{n+1} = -\lambda_n(r_{n+1} - x) - y = y\left(\left(\frac{s_n - 1}{r_n - x}\right)(r_{n+1} - x) - 1\right)$$

$$\Rightarrow r_{n+1}(x) = F(x) \cdot \left(\frac{s_n(x) - 1}{r_n(x) - x}\right) - r_n(x) - x$$

$$s_{n+1}(x) = -\frac{s_n(x) - 1}{r_n(x) - x}(r_{n+1}(x) - x) - 1$$

Lemma:
Für jedes $n \in \mathbb{N}$ ist

$$r_n'(x) = ns_n(x)$$

d.h. $[n]$ ist separabel, sofern n und p teilerfremd sind.

Beweis: durch vollständige Induktion:
n=1: trivial
n=2:

$$r_2'(x) = \frac{8F(x)F'(x)F''(x) - 4F'(x)^3}{16F(x)^2} - 2$$

da $F''(x) = 6x$, folgt:

$$r_2'(x) = 3x \cdot \frac{F'(x)}{F(x)} - \frac{F'(x)^3}{4F(x)^2} - 2 = 2s_2(x)$$

Induktionsschritt $n \to n+1$:
Angenommen $r_n'(x) = ns_n(x)$, zu zeigen:

$$r_{r+1}'(x) = (n+1)s_{n+1}(x)$$

Abkürzungen: $r_n = r$, $s_n = s$, $r_{n+1} = R$, $s_{n+1} = S \Rightarrow \lambda = \lambda_n = \frac{s-1}{r-x}$
zz: $R' = (n+1)S$
Nach obigen Formeln ist:

$$R' = F'\lambda^2 + 2F\lambda\lambda' - r' - 1$$
$$(n+1)S = -(n+1)F\lambda^3 + (n+1)\lambda(r+2x) - (n+1)$$

$$\begin{aligned}\Delta &= R' - (n+1)S \\ &= \lambda^2(F' + (n+1)F\lambda) + \lambda(2F\lambda' - (n+1)(r+2x)) - (ns-n)\end{aligned}$$

$$\frac{\Delta}{s-1} = \frac{s-1}{(r-x)^2}(F' + (n+1)F\lambda) + \frac{1}{r-x}(2F\lambda' - (n+1)(r+2x)) - n$$

$$\lambda' = \frac{s'}{r-x} = -\frac{(s-1)(ns-1)}{(r-x)^2} \quad \text{nach Induktionsannahme.}$$

$$\begin{aligned}\frac{(r-x)^3}{s-1}\Delta =& (s-1)(r-x)F' + \underbrace{(n+1)F(s-1)^2}_{A} + 2F(r-x)s' \\ & \underbrace{-2F(s-1)(ns-1)}_{B} - (n+1)(r+2x)(r-x)^2 - n(r-x)^3\end{aligned}$$

$$\begin{aligned}A - B =& (Fs^2 - F)(1-n) \\ n(x,y) =& (r, ys) \in E \\ \Rightarrow& (ys)^2 = r^3 + ar + b \\ \Rightarrow& F's^2 + 2Fss' = 3r'r^2 + ar' \\ (ys)^2 =& y^2s^2 = Fs^2, r' = ns\end{aligned}$$

$$\begin{aligned}\Rightarrow A - B &= (1-n)(r^3 + ar + b - x^3 - ax - b) \\ &= (1-n)(r-x)(r^2 + rx + x^2 + a)\end{aligned}$$

$$\begin{aligned}\Rightarrow \frac{(r-x)^2}{s-1}\Delta =& (s-1)F' + (1-n)(r^2 + rx + x^2 + a) + 2Fs' \\ & -(n+1)(r+2x)(r-x) - n(r-x)^2F's + 2Fs' \\ =& 3nr^2 + an\end{aligned}$$

Also ist

$$\begin{aligned}\frac{(r-x)^3}{s-1}\Delta =& (s-1)F' + (1-n)(r^2 + rx + x^2 + a) + 3nr^2 + an \\ & -F's - (n+1)(r^2 + rx - 2x^2) - n(r^3 - 2rx + x^2) \\ =& -F' + 3x^2 + a = 0 \quad \text{denn } F = x^3 + ax + b \Rightarrow F' = 3x^2 + a\end{aligned}$$

Also ist $\Delta = 0$, d.h. $r'_{n+1} = (n+1)s_{n+1}$. □

Zur Erinnerung:

$$\begin{cases} P \to nP \\ (x,y) \to (r_n(x), y \cdot s_n(x)) \end{cases}$$

$$E : y^2 = x^3 + ax + b$$

also ist $(ys_n(x))^2 = r_n(x)^3 + ar_n(x) + b$ für alle $(x,y) \in E$
$\Rightarrow (x^3 + ax + b)s_n(x)^2 = r_n(x)^3 + ar_n(x) + b$ für alle x.
Damit sind die Ableitungen gleich
$\Rightarrow (3x^2 + a)s_n(x)^2 + 2(x^3 + ax + b)s_n(x)s'_n(x) = 3r_n(x)^2 r'_n(x) + ar'_n(x)$.
Da $r'_n(x) = ns_n(x)$ erhalten wir

$$s'_n(x) = \frac{n(3r_n(x)^2 + a) - s_n(x)(3x^2 + a)}{2(x^3 + ax + b)}$$

$r''_n(x) = ns'_n(x)$ folgt:

$$r''_n(x) = \frac{n^2(3r_n(x)^3 + a) - r'_n(x)(3x^2 + a)}{2(x^3 + ax + b)}$$

Sei $P = (x_0, 0) \in E[2] \to 2P = O, 3P = P; \ldots,$, d.h.

$$nP = \begin{cases} O, \text{ falls n gerade} \\ P, \text{ falls n ungerade} \end{cases}$$

Lemma:
Ist $(x_0, 0) \in E[2]$, so ist $s_n(x_0) = n$ für alle ungeraden n

Beweis: Induktion nach n:
Sei $F(x) = x^3 + ax + b$, $G(x) = \frac{1}{2}F'(x)$.
In einem Erweiterungskörper von k können wir F faktorisieren als

$$F(x) = (x - x_0)(x - x_1)(x - x_2)$$

also ist x_0 Nullstelle erster Ordnung von F, d.h. $G(x_0) \neq 0$
n=1: $ys_1(x) = y \Rightarrow s_1(x) = 1$

n>1: Vorbereitung: x_0 ist Nullstelle von $r_n(x) - x$
n=3: Im vorherigen Beweis haben wir gesehen, dass

$$r_2(x) = \frac{G(x)^2}{F(x)} - 2x$$

und

$$s_2(x) = -\frac{G(x)^3}{F(x)^2} + 3x\frac{G(x)}{F(x)} - 1$$

$r_3(x) = F(x)H(x)^2 - r_2(x) - x$
$s_3(x) = -H(x)(r_3(x) - x) - 1$ mit $H(x) = \frac{s_2(x)-1}{r_2(x)-x}$
Einsetzen liefert:

$$H(x) = \frac{1}{F(x)} \underbrace{(-\frac{-6(x)^3 + 3xG(x)F(x) - 2F(x)^2}{G(x)^2 - 3xF(x)})}_{h_0(x)} = \frac{h_0(x)}{F(x)}$$

An der Stelle x_0 ist $h_0(x) = -G(x_0) \neq 0$

$$\begin{aligned} s_3(x) &= -H(x)(F(x)H(x)^2 - \frac{G(x)^2}{F(x)}) - 1 \\ &= -H(x) \cdot \frac{(h_0(x) - G(x))(h_0(x) + G(x))}{F(x)} - 1 \end{aligned}$$

$h_0(x) + G(x) = \cdots = -\frac{2F(x)^2}{G(x)^2 - 3xF(x)} \Rightarrow h_0(x_0) + G(x_0) = 0$

$$\begin{aligned} s_3(x) &= -H(x)F(x) \underbrace{(h_0(x) - G(x)\frac{-2}{G(x)^2 - 3xF(x)})}_{h_1(x)} - 1 \\ &= -\frac{h_0(x)}{F(x)}F(x)h_1(x) - 1 \end{aligned}$$

$h_1(x_0) = -2G(x_0) \cdot \frac{-2}{G(x_0)^2} = \frac{4}{G(x_0)}$
$\Rightarrow s_3(x_0) = -(-G(x_0))\frac{4}{G(x_0)} - 1 = 4 - 1 = 3$
n>3:
$r_{n+2}(x) = m^2 - r_n(x) - r_2(x), \quad m = y\frac{s_n(x)-s_2(x)}{r_n(x)-r_2(x)}$
$ys_{n+2} = -m(r_{n+2}(x) - r_n(x)) - ys_n(x)$

Einsetzen der Formeln für $r_2(x), s_2(x)$ ergibt:

$$m = \frac{y}{F(x)} \underbrace{\left(\frac{F(x)^2(s_n(x)+1) + G(x)^3 - 3xG(x)F(x) + F(x)^2}{F(x) - G(x)^2 + 3xF(x)}\right)}_{h(x)}$$

wobei $h(x_0) = -G(x_0) \neq 0$
$\frac{m}{y} = \frac{h(x)}{F(x)}$ hat also einen einfachen Pol an der Stelle $x = x_0$.

$$m^2 = y^2 \frac{h(x)^2}{F(x)^2} = \frac{h(x)^2}{F(x)}$$
$$m^3 = y \frac{h(x)^3}{F(x)^2}$$
$$s_{n+2} = -\frac{h(x)}{F(x)} \cdot \left(\frac{(h(x) - G(x))(h(x) + G(x))}{F(x)}\right) - s_n(x)$$

Ähnlich wie bei $n = 3$ erhalten wir

$$h(x) + G(x) = \frac{F(x)^2(s_n(x)+1) + G(x)F(x)(r_n(x) - x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)}$$

an der Stelle x_0 ist dies Null.
$r_n(x)$ ist nicht konstant. $r_n(x_0) = x$, $r_n(x) - x$ verschwindet in x_0.x_0 ist einfache Nullstelle von F, d.h. wir können F als Ortsuniformisierende benutzen, es gibt also eine Funktion $t_n(x)$, so dass

$$r_n(x) - x = F(x) \cdot t_n(x)$$

Damit ist

$$s_{n+2}(x) = -\frac{h(x)}{F(x)}\left((h(x) - G(x))F(x)\frac{s_n(x) + 1 + G(x)t_n(x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)}\right.$$
$$\left. - 2F(x)t_n(x)\right) - s_n$$

Kürze das $F(x)$ im Nenner und setze x_0 ein. Ergebnis:

$$s_{n+2}(x_0) = n + 2, \quad da\ s_n(x_0) = n$$

□

Lemma:
Falls n kein Vielfaches der Charakteristik ist, gilt:

$$\deg r_n = 2, \quad \deg s_n = O, \qquad \frac{r_n}{x}(O) = \frac{1}{n^2}, \quad s_n(O) = \frac{1}{n^3}$$

Beweis: Durch Induktion:
n=2: folgt aus der expliziten Form für r_2 und s_2. Nun seien n,m zwei ganze Zahlen, so dass weder n noch m noch $n \pm m$Vielfaches von p ist. Angenommen, die Behauptung sei richtig für jede ganze Zahl $< n+m$ zu zeigen: Sie stimmt für $n+m$:

$$R_{n+m}(x) = \lambda - r_n(x) - r_m(x), \quad \lambda = \frac{s_n(x) - s_m(x)}{r_n(x) - r_m(x)}$$

Nach Induktionsannahme ist:

$$\frac{r_{n+m}}{\lambda}(O) = \left(\frac{\frac{1}{n^3} - \frac{1}{m^3}}{\frac{1}{n^2} - \frac{1}{m^2}}\right)^2 - \left(\frac{1}{n^2} + \frac{1}{m^2}\right) = \frac{1}{(n+m)^2}$$

□

Definition:

a) Ein **Divisor** auf einer elliptischen Kurve E ist eine formale Summe der Form

$$D = \sum_{i=1}^{r} e_i P_i, \quad e_i \in \mathbb{Z}, \ P_i \text{ Punkte}$$

von E mit Koordinaten im algebraischen Abschluss des Grundkörpers.

b) f sei eine rationale Funktion auf E; die Nullstellen und Polstellen von f seien die Punkte $P_1, \ldots P_r$. Der Divisor von f ist

$$div(f) = \sum_{i=1}^{r} ord_{P_i}(f) \cdot P_i$$

c) Für eine endliche Menge M von Punkten auf E schreiben wir

$$(M) = \sum_{P \in M} P$$

Wir schreiben Divisoren in der Form

$$D = \sum c_p(P), \quad c_p \in \mathbb{Z}$$

(P) Divisor vom Grad 1, bestehend nur aus P.
Die Divisoren bilden eine Gruppe $Div(E)$: $D + D' = \sum(c_p + c'_p)(P)$.
Es gibt einen Homomorphismus

$$Div(E) \longrightarrow E$$

$$\underbrace{\sum c_p(P)}_{\text{Addition in Div } E} \longrightarrow \underbrace{\sum c_p P}_{\text{Addition auf } E}$$

$Div(E)$ hat als Untergruppe

$$Div^0(E) = \{D = \sum c_p(P) \mid \deg D = \sum c_p = 0\}$$

Satz von Abel -Jacobi
$\mathcal{H} = \{\sum ord_p(f)(P) \mid f \in k(E)\}$, die Gruppe der Hauptdivisoren liegt in $Div^0(E)$ und ϕ induziert einen Isomorphismus

$$Div^0(E)/\mathcal{H} \to E$$

(ohne Beweis)

Lemma:
$0 \neq n \neq \pm m \in \mathbb{Z}$ seien so, dass weder m noch n, noch $n+m$, noch $n-m$ Vielfaches der Charakteristik ist. Dann gilt:

$$div(r_n - r_m) = (E[n+m]) + (E[n-m]) - 2(E[n]) - 2(E[m])$$

Beweis:
Ist P eine Nullstelle von $r_n - r_m$, so haben nP und mP die gleiche x-Koordinate, d.h. $(n-m)P = O$ oder $(n+m)P = O$
Ist P ein Pol von $r_n - r_m$, ist $(r_n - r_m)(P) = \infty$, d.h. $r_n(P) = \infty$ oder $r_m P = \infty$, d.h. $nP = O$ oder $m(P) = O$.
Zu zeigen bleibt: Die Koeffizienten in der Behauptung stimmen.

1.Fall:
$P = O \in E[n+m] \cap E[n-m] \cap E[n] \cap E[m]$ er sollte also nach der obigen Formel in $div(r_n - r_m)$ liegen mit Koeffizient -2. Wir wissen aus dem vorherigen Lemma, dass

$$\frac{r_n - r_m}{x}(O) = \frac{1}{n^2} - \frac{1}{m^2} = \frac{m^2 - n^2}{n^2 m^2} = \frac{(m+n)(m-n)}{n^2 m^2} \neq 0, \infty$$

Also ist die Ordnung von $\frac{r_n - r_m}{x}$ in O gleich 0, d.h. $r_n - r_m$ hat dort die gleiche Ordnung wie x, also -2.
2.Fall:
$P \in E[n] \cap E[m] \Rightarrow P \in E[n \pm m]$
$\Rightarrow$ in obiger Formel sollte P Koeffizient -2 haben.
Zu zeigen: $ord_p(r_n - r_m) = -2$. Wir wissen: Für die Translation

$$\tau_p : \begin{cases} E \to E \\ Q \to P + Q \end{cases}$$

und jede Funktion $f \in k[E]$ ist $ord_{P+Q}(f) = ord_Q(f \circ \tau_p)$. Also lässt sich dieser Fall via τ_p zurückführen auf den 1. Fall.
3.Fall:
$P \in E[n-m] \backslash E[n+m] \Rightarrow nP = mP(*) \Rightarrow P$ Nullstelle von $r_n - r_m$ und $nP \neq -mP(*) \Rightarrow nP$ und mP haben verschiedene y-Koordinaten. Aus (*) folgt:

$$nP \neq -nP \Rightarrow 2nP \neq O$$

$$mP \neq -mP \Rightarrow 2mP \neq O$$

$\Rightarrow P$ ist $\notin E[2], P \notin E[n], P \notin E[m] \Rightarrow$ Koeffizient rechts ist 1. Da $P \notin E[2]$, ist $s_n(P) = s_m(P)$. Da $r_n'(P) = n s_n(P)$ folgt:
$(r_n - r_m)'(P) = (n-m)s_n(P) \neq 0$.
Also ist P einfacher Pol von $r_n - r_m$.
Die übrigen Fälle gehen ähnlich $\square$

Satz:
Ist n kein Vielfaches der Charakteristik, so ist $\#E[n] = n^2$

Beweis:
Wir können jede Zahl $r \in \mathbb{Z} \backslash p\mathbb{Z}$ schreiben als $r = n + m$, wobei $n, m \in$

$\mathbb{Z}$ die Behauptung erfüllen. Beweis durch Induktion über alle Paare (n,m) mit dieser Eigenschaft. Induktionsvoraussetzung ist jeweils:
Es gilt für alle (n',m') mit dieser Eigenschaft, für die $n'+m' < n+m$ ist:

$n+m=1 : E[1] = \{O\}$
$n+m=2 : \#E[2] = 4 = 2^2$
$n+m>3 :$

Sei $d_r = \#E(r)$
Nach dem gerade bewiesenen Lemma, hat $div(r_n - r_m)$ den Grad $d_{m+n} + d_{m-n} - 2d_n - 2d_m$.
Als Hauptdivisor hat $div(r_n - r_m)$ Grad 0, d.h.

$$\begin{aligned} d_{m+n} &= 2d_n + 2d_m - d_{m-n} \\ &= 2n^2 + 2m^2 - (m-n)^2 \\ &= 2n^2 + 2m^2 - m^2 + 2mn - n^2 \\ &= n^2 + m^2 + 2mn \\ &= (n+m)^2 \end{aligned}$$

□

Struktursatz für endliche abelsche Gruppen:
Jede endliche abelsche Gruppe ist isomorph zu einer Gruppe der Form:

$$\mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_r$$

wobei $n_r \mid n_{r-1} \mid n_{r-2} \mid \cdots \mid n_2 \mid n_1$

Satz:
Ist E elliptische Kurve über einem Körper k der Charakteristik p, so ist entweder $E[p] = \{O\}$ oder $E[p]$ ist eine zyklische Gruppe der Ordnung p (supersingulärer Fall).

□

Nun sei E eine elliptische Kurve über einem endlichen Körper k.

$E(k)$= Gruppe der Punkte mit Koordinaten aus k. $E(k)$ ist endlich, ihre Ordnung sei N. Dann ist $E(k) \leq E[N] \leq \mathbb{Z}/N \times \mathbb{Z}/N$. Außerdem ist nach dem Struktursatz:

$$E[k] \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$$

Also ist $r \leq 2$ und $n_2 \mid n_1 \mid N$. Somit gibt es natürliche Zahlen $n_1, n_2, n_2 \mid n_1$ so dass $E(k) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$

Bemerkung:
Man kann zeigen, dass außerdem gilt: $n_2 \mid (\#k - 1)$, falls n_1 teilerfremd ist zu $\#k - 1$, ist also $E(k) \cong \mathbb{Z}/n_1$

Beweisskizze für den Struktursatz für endliche abelsche Gruppen:
A sei eine endliche abelsche Gruppe.

1. $a \in A$ habe Ordnung n, b Ordnung m.
   Falls $ggT(n,m) = 1$, hat $a + b$ die Ordnung nm:
   $$nm(a+b) = m(na) + n(mb) = 0 + 0 = 0$$
   Wäre r echter Teiler von nm und $r(a+b) = 0$, so wäre für
   $a' = ggT(r,n) \cdot a$: $\quad ma' = 0, \quad na' = 0.$
   $ggT(m,n)a' = 0 \Rightarrow a' = 0,$
   d.h. die Ordnung von a ist $\leq ggT(r,n) \leq n$
   Genauso: die Ordnung von b ist $\leq ggT(r,m) \leq m$ mit mindestens einem echten $<$ $\quad \lightning$

2. $\#A = N = N_1 \cdot N_2$, $ggT(N_1, N_2) = 1$. Dann ist $A \cong A_1 \times A_2, \#A_j = N_j$.
   Sei $a \in A$ beliebig $\Rightarrow Na = 0$.
   Sei $a_1 = N_2 a, \quad a_2 = N_1 a \quad \Rightarrow N_1 a_1 = N_2 a_2 = O$
   Schreibe:
   $$1 = ggT(N_1, N_2) = r_1 N_1 + r_2 N_2$$
   $\Rightarrow a = (r_1 N_1 + r_2 N_2)a = \underbrace{r_1 a_2}_{ord \mid N_2} + \underbrace{r_2 a_1}_{ord \mid N_1}$ Ist $A_j = \{a \in A \mid N_j a = 0\}$,
   so definiert
   $$\begin{cases} A \to A_1 \times A_2 \\ a \to (r_2 a_1, r_1 a_2) \end{cases}$$
   einen Isomorphismus.

3. Sei $N = \prod_i p_i^{e_i}$. Induktiv folgt: A ist Produkt von Gruppen A_i der Ordnung $p_i^{e_i}$ diese wiederum sind Produkte von zyklischen Gruppen mit p_i-Potenzen als Ordnungen

4. Chinesischer Restesatz:
   Ist $ggT(n,m) = 1$, dann ist $\mathbb{Z}/n \times \mathbb{Z}/m \cong \mathbb{Z}/nm$.
   Sei $n_1 = \prod_i P_i^{\text{maximal vorkommender Exponent}}$ und $n_2 = \prod_i p_i^{\text{2. höchster Exponent}}$
   usw. bis es keine Faktoren mehr gibt

□