Reduktions- und Additionsverfahren für die Jacobische Varietät von Kurvenfamilien mit kryptographischen Anwendungen

Diplomarbeit

Humboldt Universität zu Berlin

Mathematisch-Naturwissenschaftliche Fakultät II

Institut für Mathematik

eingereicht von: Maria Petkova
geb.: am 05.10.1979 in: Sofia, Bulgarien
Betreuer: Prof. Dr. R.-P. Holzapfel
Berlin, 27. Oktober 2004

Inhaltsverzeichnis

1 Einführung

In der vorliegenden Arbeit werden zwei Hauptthemen betrachtet. Einerseits werden die Eigenschaften von hyperelliptischen Kurven untersucht. Es wird ein Reduktions- und Additionsalgorithmus in der Jacobischen Varietät von hyperelliptischen Kurven konstruiert. Mit Hilfe dieser expliziten Darstellung des Gruppengesetzes wird die Jacobische Varietät jeder hyperelliptischen Kurve zu einer abelschen Gruppe, die für kryptographische Zwecke geeignet ist. Es werden auch einige Verbesserungsvorschläge des Ursprungsalgorithmus diskutiert [*Hyperelliptic Curves and Cryptography*, Jacobson].
Zusätzlich wird die Kurvenfamilie $C : y^2 = xf_3(x^2)$ untersucht. Nach Aussortieren der singulären Kurven besteht die angegebene Familie aus hyperelliptischen Kurven vom Geschlecht 3. Im Rahmen der Arbeit werden die Isomorphieklassen der Familie unter der Koordinatentransformation

$$\begin{aligned} x &\mapsto u^2 x \\ y &\mapsto u^7 y, \quad u \in \mathbb{F}_q \end{aligned}$$

ausgerechnet und ihr Modulraum bestimmt. Mit Hilfe des definierten Cantorschen Reduktions- und Additionsalgorithmus erhalten wir auch eine explizite Divisorenaddition in der Jacobischen Varietät der betrachteten Kurven. Es werden auch explizite Beispiele für die Gruppenoperation in $Jac(C)$ ausgerechnet. Am Schluß werden die Grundideen des Cantorschen Algorithmus untersucht. Dabei lässt sich feststellen, dass D. Cantor in seinem Verfahren einerseits die Mumfordschen Koordinatenfunktionen bei der Darstellung der Divisoren verwendet hat. Andererseits wird die Gaußsche Reduktion implementiert, bekannt aus der Theorie der binären quadratischen Formen über $\mathbb{Z}$. Das ist ein schönes Beispiel für die Anwendung der Eigenschaften der quadratischen Formen in praktischen Aufgaben. Eine andere Anwendung wird in dem Anhang *Äquivalenz zwischen binären quadratischen Formen und Moduln quadratischer Ordnungen* angegeben. Hierbei werden quadratische Formen für die Bestimmung der Klassenzahl von Zahlkörpern benutzt.
Das zweite betrachtete Problem ist die explizite Darstellung der Gruppenstruktur der Jacobischen Varietät von den Kurvenfamilien $y^4 = p_4(x)$ und $y^4 = p_3(x)$. Dabei handelt es sich um nicht hyperelliptischen Kurven vom Geschlecht 3. Bei der Konstruktion des Reduktions- und Additionsalgorithmus bin ich von dem Artikel *Efficient Reduction on the Jacobian Variety of Picard Curves* von J. Estrada ausgegangen. Die dabei verwendete Idee ist eine Fortsetzung der geometrischen Addition von Punkten elliptischer Kurven. Ein ähnliches geometrisches Verfahren für hyperelliptische Kurven vom Geschlecht 2 wird in *The Equivalence of the Geometric and Algebraic Group Laws for Jacobians of Genus 2 Curves* von K. Lauter, definiert. Diese geometrische Konstruktion ist auf Grund des höheren Grades von hyperelliptischen Kurven vom Geschlecht 3 ungeeignet. Die kompliziertere Struktur der Jacobischen Varietät verlangt die Anwendung von Quadriken an Stelle der Sekanten und Tangenten im Fall von elliptischen Kurven. Jedem Divisor werden eindeutig drei Koordinatenfunktionen zugeord-

net. Die dabei definierte bijektive Korrespondenz liefert eine bequemere Darstellung der Divisoren, die für den Reduktions- und Additionsalgorithmus benötigt wird. Diese Idee, zuerst angegeben von D. Mumford in *Tata Lectures on Theta II*, wird auch bei dem Cantorschen Algorithmus angewendet. Somit werden die Divisoren zu Punkten einer Varietät, für welche die Koeffizienten der zu den Divisoren gehörigen Polynome Koordinaten sind.
Der dabei, für einige nicht hyperelliptischen Kurvenfamilien entstandene Algorithmus ist von geringerer Komplexität. In jedem Rekursionsschritt wird höchstens ein 4×4 lineares Gleichungssystem gelöst, sowie ein Polynom 3. Grades faktorisiert. Die dadurch konstruierten Divisoren gehören im schlechtesten Fall zu einer endlichen Erweiterung des Grundkörpers $k = \mathbb{F}_q$. Somit eignen sich auch nicht hyperelliptische Kurven für kryptographische Zwecke.

2 Hyperelliptische Kurven

Das Ziel dieses Kapitels ist die Struktur der Familie $C: \quad y^2 = xf_3(x^2)$ von nicht hyperelliptischen Kurven zu untersuchen. Dafür wird zuerst den Begriff *hyperelliptische Kurve* erläutert. Es lässt sich festellen, dass jede hyperelliptische Kurve vom Geschlecht $g(C) = g > 1$, eine kanonische Darstellung besitzt, die sogenannte *Weierstraß-Normalform.* Im Laufe des Kapitels werden die nicht singulären Kurven in $C: y^2 = xf_3(x^2)$ bestimmt, sowie die Anzahl der Isomorphieklassen hyperelliptischen Kurven ausgerechnet.

Definition 2.1 *C sei eine glatte geometrisch zusammenhängende Kurve über einem Körper k, und C sei vom Geschlecht $g \geq 1$. Dann heißt C hyperelliptische Kurve, falls ein endlich separabler Morphismus $C \to \mathbb{P}^1_k$ vom Grad 2 existiert. Der dazugehörige Funktionenkörper $F(C)$ heißt hyperelliptisch [Liu].*

Eine äquivalente Definition ist

Definition 2.2 *Ein hyperelliptischer Funktionenkörper über k ist ein Funktionenkörper F/k vom Geschlecht $g \geq 1$, der den rationalen Teilkörper $k(x) \subset F$ mit $[F : k(x)] = 2$ enthält [Stichtenoth].*

Lemma 2.3 *Ein Funktionenkörper F/k vom Geschlecht $g \geq 2$ ist hyperelliptisch genau dann, wenn ein Divisor $A \in Div_F$ mit $degA = 2$ und $dim\mathfrak{L}(A) \geq 2$ existiert.*

Beweis: Sei F/k hyperelliptisch. Wir wählen ein Element $x \in F$, so dass $[F : k(x)] = 2$ und betrachten den Divisor $A := (x)_\infty$. Dann gilt $degA = deg(x)_\infty = [F : k(x)] = 2$ und da die Elemente $1, x \in \mathfrak{L}(A)$ linear unabhängig über k sind, folgt $dim\mathfrak{L}(A) \geq 2$.
Umgekehrt sei F/k vom Geschlecht $g \geq 2$ und A ein Divisor mit $degA = 2$ und $dim\mathfrak{L}(A) \geq 2$. Dann existiert ein $A_1 \in Div_F$ mit $A_1 \geq 0$ und $A_1 \sim A$, so dass $degA_1 = 2$ und $dim\mathfrak{L}(A_1) \geq 2$. D.h., es existiert ein Element x mit

$x \in \mathfrak{L}(A_1)/k$. Dann gilt $(x)_\infty \leq A_1$. Dies liefert $[F : k(x)] = deg(x)_\infty \leq 2$. Weiterhin gilt $[F : k(x)] = 2$, da F/k nicht rational ist.

□

Bemerkung 2.4 *Ist F/k ein hyperelliptischer Funktionenkörper und $k(x)$ ist Teilkörper von F mit $[F : k(x)] = 2$, dann ist die Erweiterung $F/k(x)$ separabel und zyklisch mit dem dazugehörigen Automorphismen $id : (x, y) \mapsto (x, y)$ und der hyperelliptischen Involution $\sigma : (x, y) \mapsto (x, -y)$ mit $\sigma^2 = id$.*

Desweiteren betrachten wir die sogenannten *Weierstraß-Punkte*. Sie sind sehr wichtig für die algebraische Kurventheorie. Mit ihrer Hilfe lässt sich zeigen, dass jede Kurve C mit $g(C) \geq 2$ endlich viele Authomorphismen besitzt.

Definition 2.5 *Sei $P \in X$, X Riemannsche Fläche vom Geschlecht $g(X) = g \geq 2$ und $n \in \mathbb{N}, n \geq 1$. n heißt Lückenzahl in P genau dann, wenn $dim\mathfrak{L}(nP) = dim\mathfrak{L}((n-1)P)$. Mit anderen Worten ist n keine Lückenzahl in P, falls eine Funktion $f \in F(X)$ existiert mit Pol der Ordnung n in P und sonst regulär. [Miranda]*

Satz 2.6 *Die Anzahl der Lückenzahlen in P ist gleich g.*

Beweis: Wir betrachten die Folge

$$k = \mathfrak{L}(0) \subset \mathfrak{L}(P) \subset \mathfrak{L}(2P) \subset \cdots \subset \mathfrak{L}((n-1)P) \subset \mathfrak{L}(nP) \subset \cdots$$

Im n. Schritt gilt für die Dimension der Funktionenräume:

$$dim\mathfrak{L}(nP) = dim\mathfrak{L}((n-1)P), \quad oder$$
$$dim\mathfrak{L}(nP) = dim\mathfrak{L}((n-1)P) + 1$$

Für $n = 2g - 1$ ist die Dimension $dim\mathfrak{L}(nP) = deg(nP) + 1 - g = g$. Von nun an erhöht sich die Dimension mit jedem Schritt um eins. Es gilt noch $dim\mathfrak{L}(0P) = 1$, d.h. zwischen

$$\mathfrak{L}(0) \subset \mathfrak{L}(P) \subset \mathfrak{L}(2P) \subset \cdots \subset \mathfrak{L}(2g-1)$$

gibt es genau g Schritte, bei denen die Dimension unverändert bleibt. Dies bedeutet, dass es gibt genau g Lückenzahlen in P gibt.

□

Definition 2.7 *$G_P = \{n \in \mathbb{Z} | n \geq 1\}$ und es existiert kein $f \in F(X)$ mit $(f)_\infty = n\}$ heißt Weierstraß-Lückenfolge in P.*

Definition 2.8 *P heißt Weierstraß-Punkt genau dann, wenn die Lückenfolge von P $G_P = \{n_1, ..., n_g\}$ mit $n_1 < ... < n_g$ verschieden von $\{1, ..., g\}$ ist.*
Mit anderen Worten ist P Weierstraß-Punkt, falls eine meromorphe Funktion f existiert, holomorph auf $X \backslash \{P\}$, mit P Pol der Ordnung $\leq g$. Das letzte bedeutet $dim\mathfrak{L}(gP) \geq 2$.

Weierstraß-Punkte sind von großer Bedeutung für die Theorie der algebraischen Kurven, weil sie unter den Authomorphismen der Kurve ineinander übergehen. Daraus lässt sich schließen:

Satz 2.9 *Jede algebraische Kurve vom Geschlecht ≥ 2 hat nur endlich viele Authomorphismen [Miranda].*

Beweis: Sei C eine hyperelliptische Kurve. Dann sind ihre Authomorphismen verträglich mit der Überlagerung

$$\pi : C \to \mathbb{P}^1.$$

Somit werden sie zu Authomorphismen von $\mathbb{P}^1$, welche die $2g+2$ Verzweigungspunkte permutieren. Wir erhalten einen Homomorphismus $\sigma : Aut(C) \to S_{2g+2}$ mit Kern der Dimension 2, erzeugt durch die kanonische Involution π.
Im Fall von nicht hyperelliptischen Kurven lässt sich mit Hilfe von Cliffords Theorem [Griffiths&Harris] zeigen, dass die Anzahl der Weierstraß-Punkte $k \geq 2g+6$ ist. Jeder Authomorphismus permutiert diese Punkte und es existiert wieder ein Homomorphismus $\sigma : Aut(C) \to S_k$. Jeder Authomorphismus, der die Weierstraß-Punkte festhält ist trivial. Somit ist $Aut(C)$ eine endliche Gruppe.

□

Definition 2.10 *Sei C eine hyperelliptische Kurve und es gilt $P \in C$. P heißt Weierstraß-Punkt genau dann, wenn $dim\mathfrak{L}(2P) > 1$*
(d.h. falls eine Funktion $\varphi \in \mathfrak{L}(2P)$ existiert mit zweifachem Pol in P).

Bemerkung 2.11 *Im Fall von elliptischen Kurven (d.h. $g = 1$) ist jeder Punkt ein Weierstraß-Punkt. Ist $g > 1$, dann gibt es höchstens $2g+2$ Weierstraß-Punkte auf C und genau so viele, falls $char k \neq 2$.*

Definition 2.12 *Unter der Weierstraß-Gleichung einer hyperelliptischen Kurve C/k vom*
Geschlecht g verstehen wir

$$C : \quad y^2 + q(x)y = p(x),$$

wobei $q, p \in k[x]$ mit $deg(q) \leq g$ und $deg(p) = 2g+1$ [Lockhart].

Satz 2.13 *Für jede hyperelliptische Kurve (C, P) über k vom Geschlecht g existieren nicht konstante Funktionen $x, y \in F(C)$ mit $x \in \mathfrak{L}(2gP), y \in \mathfrak{L}((2g+1)P)$, so dass (C, P) einer Weierstraß-Gleichung genügt. Diese Gleichung ist* *bis auf die folgenden Koordinaten-Transformationen*

$$\begin{aligned} x &\mapsto u^2x' + r, \\ y &\mapsto u^{2g+1}y' + t(x') \end{aligned}$$

mit $u \in k^*$, $r \in k$ *und* $t \in k[x]$, $deg(t) \leq g$ *eindeutig bestimmt.*

Beweis: P sei $k-$rationaler Weierstraß-Punkt, d.h. es existiert eine nicht konstante Funktion $x \in F(C)$ mit zweifachem Pol in P. Nach dem Satz von Riemann-Roch, erhalten wir:

$$dim\mathfrak{L}(2gP) = g + 1, \quad dim\mathfrak{L}((2g+1)P) = g + 2.$$

Die Funktionen $1, x, x^2, ..., x^g$ bilden eine Basis von $\mathfrak{L}(2gP)$. Sei weiterhin $y \in \mathfrak{L}((2g+1)P) \backslash \mathfrak{L}(2gP)$. Wir betrachten die Funktionen

$$1, x, ..., x^{2g+1}, y, xy, ..., x^g y, y^2.$$

Jede dieser Funktionen liegt in dem Vektorraum $\mathfrak{L}((4g+2)P)$, dessen Dimension $3g + 3$ beträgt. Das bedeutet, dass die Funktionen $k-$linear abhängig sind und jede von ihnen hat in P einen Pol verschiedener Ordnung, bis auf die beiden Funktionen x^{2g+1}und y^2, die einen Pol der Ordnung $4g+2$ haben. Daraus folgt, dass die Koeffizinten vor den beiden Funktionen, in der $k-$lineare Relation, ungleich 0 sind. Nach Normierung erhalten wir für x, y eine Weierstraß-Gleichung vom Geschlecht g.
Seien x' und y' zwei weitere solche Funktionen. Da C eine hyperelliptische Kurve ist, gilt $dim\mathfrak{L}(2P) = 2$. Daraus erhalten wir $x = ax' + r$ und $y = by' + t(x')$, wobei $a \in k^*, r \in k, b \in k$ und $deg(t) \leq g$. Das liefert eine normierte Gleichung in x'^{2g+1} und y'^2, woraus $b^2 = a^{2g+1}$ folgt. Wir setzen $u = ba^{-g}$. Dann ist $u \in k^*$, $a = u^2$ und $b = u^{2g+1}$. Somit ist der Beweis abgeschlossen.

□

Bemerkung 2.14 *Bei* $char(k) \neq 2$ *lässt sich die Weierstraß-Gleichung von* C *durch quadratische Ergänzung auf die Form* $y^2 = f(x)$ *bringen. In diesem Fall lassen sich die Koordinatentransformationen vereinfachen, indem* $t = 0$ *eingesetzt wird.*

Weiterhin werden wir die hyperelliptische Kurvenfamilie

$$y^2 = xf_3(x^2)$$

mit $f_3 \in \mathbb{F}_q[X]$, $deg(f) = 3$ über dem endlichen Körpern $\mathbb{F}_q$ betrachten. Als Erstes wollen wir das Geschlecht von $C/\mathbb{F}_q$ ausrechnen. Dafür benötigen wir die folgenden Sätze.

Satz 2.15 *Sei F/k ein Funktionenkörper und $F' = F(y)$ mit $y^n = u \in F$, $n \neq 0 \mod char(k)$, und k enthält eine primitive n. Einheitswurzel. Desweitern sei $Q \in \mathbb{P}_F$ eine Stelle von F, so dass $ggT(\nu_Q(u), n) = 1$. Dann gilt:*

1. *k ist der volle Konstantenkörper von F'*
2. *F'/F ist eine zyklische Erweiterung vom Grad n*
3. *$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(n - r_P)degP$, mit $r_P = ggT(\nu_P(u), n)$ [Stichtenoth]*

Satz 2.16 *Sei $F = k(x,y)$ mit $char(k) \neq 2$ und $y^2 = f(x) = p_1(x)...p_s(x) \in k[x]$, wobei $p_1, ..., p_s$ verschiedene, irreduzible, normierte Polynome sind. $m = deg(f)$. Dann ist k der volle Konstantenkörper von F und F/k ist vom Geschlecht*

$$g(F) = \begin{cases} \frac{(m-1)}{2} & \text{falls } m \equiv 1 \mod 2, \\ \frac{(m-2)}{2} & \text{falls } m \equiv 0 \mod 2. \end{cases}$$

Beweis: Sei $F = F_0(y)$ mit $F_0 = k(x)$ und $f(x) = p_1(x)...p_s(x)$. Mit P_i bezeichnen wir die Nullstellen von $p_i(x)$, mit $P_i \in \mathbb{P}_{k(x)}$ und P_∞ der Pol von x in $k(x)$. Dann gilt $\nu_{p_i}(f(x)) = 1$, für $i = 1, ..., s$ und $\nu_{P_\infty}(f(x)) = -m$.
Nach dem vorigen Satz ist F/F_0 eine zyklische Erweiterung vom Grad 2 und es gilt

$$r_{P_i} = ggT(2, \nu_{P_i}(f(x))) = ggT(2, 1) = 1, i = 1, ..., s$$
$$r_{P_\infty} = ggT(2, -m) = \begin{cases} 1 & \text{falls } m \equiv 1 \mod 2, \\ 2 & \text{falls } m \equiv 0 \mod 2. \end{cases}$$

Desweiteren gilt

$$g(F) = 1 + 2(g(k(x)) - 1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(2 - r_P)degP$$

und

$$g(F) = \begin{cases} 1 + 2(0-1) + \frac{m}{2}(2-1) + \frac{1}{2}(2-1) & \text{falls } m \equiv 1 \mod 2, \\ 1 + 2(0-1) + \frac{m}{2}(2-1) + \frac{1}{2}(2-2) & \text{falls } m \equiv 0 \mod 2, \end{cases}$$

d.h.

$$g(F) = \begin{cases} -1 + \frac{m}{2} + \frac{1}{2} = \frac{m-1}{2} & \text{falls } m \equiv 1 \mod 2, \\ -1 + \frac{m}{2} = \frac{m-2}{2} & \text{falls } m \equiv 0 \mod 2. \end{cases}$$

□

Angewendet auf die Kurvenfamilie

$$C: \quad y^2 = xf_3(x^2)$$

mit $deg(xf_3(x)) = 7$ erhalten wir

$$g(C) = \frac{(7-1)}{2} = 3.$$

Weiterhin werden wir die Kurvenfamilie

$$C: \quad y^2 = xf_3(x^2) = a_3x^7 + a_2x^5 + a_1x^3 + a_0x$$

betrachten. Das ist eine hyperelliptische Kurvenfamilie vom Geschlecht 3. Nach linearer Transformation ist die obige Gleichheit äquivalent zu

$$y^2 = x^7 + a_2x^5 + a_1x^3 + a_0x = x(x^2 - \alpha_1)(x^2 - \alpha_2)(x^2 - \alpha_3).$$

Wir werden zuerst die singulären Kurven bestimmen. Dafür betrachten wir die folgenden Fälle:

1. $char\mathbb{F}_q = 2$, dann gilt $x = \sqrt{\alpha_i}$ oder $x = -\sqrt{\alpha_i}$ ist doppelte Nullstelle und die Kurve C, angegeben durch die Gleichung $y^2 = xf_3(x^2)$, ist singulär.
2. $char\mathbb{F}_q \neq 2$.
   (a) $(0,0)$ ist mehrfache Nullstelle von C genau dann, wenn $a_0 = 0$. Wir können jede Kurve C eindeutig mit dem Koeffizienten-Tripel (a_2, a_1, a_0) identifizieren. Dann gilt für die Anzahl aller Kurven C mit mehrfachen Nullstellen in $(0,0)$

   $$\#C = q^2.$$

   (b) Sei jetzt $a_0 \neq 0$. Dann betrachten wir die folgenden Fälle:
      i. Seien $\alpha_1 = \alpha_2 = \alpha_3$ und $\alpha_i \neq 0$, dann gilt

      $$x(x^2 - \alpha_1)^3 = x(x^6 - 3\alpha_1x^4 + 3\alpha_1^2x^2 - \alpha_1^3) = x(x^6 + a_2x^4 + a_1x^2 + a_0)$$

      und nach Koeffizientenvergleich erhalten wir

      $$(a_2, a_1, a_0) = (-3\alpha_1, 3\alpha_1^2, -\alpha_1^3)$$

      woraus folgt

      $$\#C = q - 1.$$

      ii. Seien $\alpha_1 \neq \alpha_2$ und $\alpha_i \neq 0$, dann gilt

      $$\begin{aligned} xf_3(x^2) &= x(x^2 - \alpha_1)^2(x^2 - \alpha_2) \\ &= (x^4 - 2\alpha_1x^2 + \alpha_1^2)(x^2 - \alpha_2) \\ &= x(x^6 - (2\alpha_1 + \alpha_2)x^4 + (\alpha_1^2 + 2\alpha_1\alpha_2)x^2 - \alpha_1^2\alpha_2) \end{aligned}$$

      und wiederum nach Koeffizientenvergleich erhalten wir

      $$(a_2, a_1, a_0) = (-(2\alpha_1 + \alpha_2), \alpha_1^2 + 2\alpha_1\alpha_2, -\alpha_1^2\alpha_2)$$

      und folglich

      $$\#C = (q-1)(q-2).$$

Sei H die Menge aller singularitätenfreien Kurven dieser Familie. Dann gilt für die Anzahl der Elementen von H:

$$\#H = q^3 - (q^2 + (q-1) + (q-1)(q-2)) = q^3 - q^2 - (q-1)^2 = (q-1)(q^2 - q + 1)$$

Jede singularitätenfreie Kurve C der Kurvenfamilie $y^2 = xf_3(x^2)$ lässt sich einem Tripel (a_2, a_1, a_0) eindeutig zuordnen. Es gilt

$$(a_2, a_1, a_0) \in \mathbb{F}_q^3 \backslash S,$$

wobei S die Menge der Singularitäten ist.

$$S = (a_2, a_1, 0) \cup (-3\alpha_1, 3\alpha_1^2, -\alpha_1^3) \cup (-(2\alpha_1 + \alpha_2), \alpha_1^2 - 2\alpha_1\alpha_2, -\alpha_1^2\alpha_2),$$

mit $\alpha_1 \neq \alpha_2$ und $\alpha_1 \neq 0$ und $\alpha_2 \neq 0$.
Nachdem wir die Menge der singularitätenfreien Kurven der Familie bestimmt haben, d.h. die Menge der hyperelliptischen Kurven, wollen wir als Nächstes die Anzahl der Isomorphieklassen ausrechnen. Die Isomorphieklassen entsprechen dem Modulraum im Fall von endlichen Körpern. Dabei gehen wir wie in dem Artikel *Isomorphism Classes of Genus-2 Hyperelliptic Curves Over Finite Fields* von A. Menezes vor. Wir rechnen zuerst die Koordinaten-Transformationen für hyperelliptischen Kurven in dem Fall von $C : y^2 = xf_3(x)$.
Wir wissen, dass zu jeder hyperelliptischen Kurve eine Gleichung der Form $y^2 + q(x)y = p(x)$ existiert, die sogenannte Weierstraß-Gleichung. Die Letzte ist bis auf Koordinatentransformation der Form

$$\begin{aligned} x &\mapsto u^2x + r \\ y &\mapsto u^{2g+1}y + t(x) \end{aligned}$$

mit $u \in k^*, r \in k$ und $t \in k[x]$, $deg(t) \leq g$ eindeutig.
Es gilt für $C: \quad y^2 = x^7 + a_2x^5 + a_1x^3 + a_0x$ mit $g = 3:$

$$\begin{aligned} x &\mapsto u^2x + r \\ y &\mapsto u^{2g+1}y. \end{aligned}$$

Nach Bemerkung 2.14 können wir $t(x) = 0$ annehmen.
Angewendet auf die oben definierte Gleichung erhalten wir:

$$\begin{aligned} u^{14}y^2 = \quad & u^{14}x^7 \\ & + 7u^{12}rx^6 \\ & + (21u^{10}r^2 + a_2u^{10})x^5 \\ & + (35u^8r^3 + 5a_2u^8r)x^4 \\ & + (35u^6r^4 + 10a_2u^6r^2 + a_1u^6)x^3 \\ & + (21u^4r^5 + 10a_2u^6r^3 + 3a_1u^4r)x^2 \\ & + (7u^2r^6 + 5a_2u^2r^4 + 3a_1u^2r^2 + a_0u^2)x \\ & + r^7 + a_2r^5 + a_1r^3 + a_0r \end{aligned}$$

und nach Koeffizientenvergleich gilt $u^{14} = 1$. Aus

$$x^6 : 0 = 7u^{12}r$$

erhalten wir unter der Berücksichtigung von $u \in \mathbb{F}_q^*$, $r = 0$. Dann hat die Transformationsformel für C die folgende Form:

$$\begin{array}{rcl} x & \mapsto & u^2x \\ y & \mapsto & u^7y. \end{array}$$

Seien

$$C_1 : \quad y^2 = x^7 + a_2x^5 + a_1x^3 + a_0x$$

und

$$C_2 : \quad y^2 = x^7 + \bar{a}_2x^5 + \bar{a}_1x^3 + \bar{a}_0x,$$

die nach der Transformation erhaltene Kurve. Dann gilt

$$C_1 \sim C_2$$

und

$$\begin{aligned} a_2 &= u^4\bar{a}_2, \\ a_1 &= u^8\bar{a}_1, \\ a_0 &= u^{12}\bar{a}_0. \end{aligned} \tag{1}$$

Die Transformationen von C haben die Form

$$\begin{pmatrix} x \\ y \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} u^2 & 0 \\ 0 & u^7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

und wegen $u \in \mathbb{F}_q^*$, mit $u^{14} = 1$, bilden sie eine Untermenge von $SL_2(\mathbb{F}_q)$. Die 14. Einheitswurzeln haben die Form $u = e^{\frac{2\pi \mathrm{i}}{14}}$, mit $\mathrm{i} = 1, ..., 14$. Wir erhalten für die Werte von u^2 und u^7, bzw. für die Potenzen k_1, k_2 von $u^2 = e^{\frac{2\pi}{14}k_1}$ und $u^7 = e^{\frac{7i\pi}{14}k_2}$, die folgende Tabelle:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
k_1	2	4	6	8	10	12	14	2	4	6	8	10	12	14
k_2	7	14	7	14	7	14	7	14	7	14	7	14	7	14

Anhand der ausgerechneten Werte, können wir schliessen, dass die Menge der Transformationen isomorph zu dem Produkt $\mathbb{Z}_7 \times S_2$ ist. Jede Klasse äquivalenter Kurven entspricht genau einem Punkt des Quotientenraumes $\mathbb{P}^2/\mathbb{Z}_7 \times S_2$, den wir als Modulraum für die Kurvenfamilie erhalten.

Sei G die Gruppe der Transformationen von C, der Form $(x,y) \mapsto (u^2x, u^7y)$, mit $u \in \mathbb{F}_q^*$. Dann ist H/G die Menge der Isomorphieklassen von C. Um ihre Anzahl $|H/G|$ bestimmen zu können, betrachten wir die folgenden Mengen:

$$\begin{aligned} H_1 &= \{C \in H | a_2 = a_1 = 0, a_0 \neq 0\}, \\ H_2 &= \{C \in H | a_2 = 0, a_1a_0 \neq 0\}, \\ H_3 &= \{C \in H | a_1 = 0, a_2a_0 \neq 0\}, \\ H_4 &= H \backslash (H_1 \cup H_2 \cup H_3), \end{aligned}$$

wobei gilt

$$H_1 \cap H_2 \cap H_3 \cap H_4 = \varnothing.$$

Als Nächstes wollen wir die Mächtigkeit dieser Mengen bestimmen. Dabei müssen wir beachten, nur die singularitätenfreien Kurven zu zählen.
$H_1 = \{C \in H | a_2 = a_1 = 0, a_0 \neq 0\} = \{C : \quad y^2 = x^7 + a_0x\}$. Wir erhalten $|H_1| = q - 1$.

$H_2 = \{C \in H | a_2 = 0, a_1a_0 \neq 0\} = \{C : \quad y^2 = x^7 + a_1x^3 + a_0x\}$. Hier unterscheiden wir die folgenden Fälle:

1. C hat $3-$fache Nullstelle α_1. Dann lassen sich die Koeffizienten (a_2, a_1, a_0) als $(-3\alpha_1, 3\alpha_1^2, -\alpha_1^3)$ darstellen. Aus $a_2 = 0$ folgt $a_0 = 0$, was zum Widerspruch führt.

2. C hat $2-$fache Nullstelle α_1. Dann gilt für die Koeffizienten $(a_2, a_1, a_0) = (-(2\alpha_1 + \alpha_2), (\alpha_1^2 + 2\alpha_1\alpha_2), -\alpha_1^2\alpha^2)$. Aus $a_2 = 0$ erhalten wir $\alpha_2 = -2\alpha_1$. Die Kurven mit $2-$facher Nullstelle $\alpha_1 \neq 0$ und Nullstelle $\alpha_2 = -2\alpha_1$ gehören nicht zu H_2. Wir erhalten somit $|H_2| = (q-1)(q-1) - (q-1) = (q-1)(q-2)$.

Die Mächtigkeit von H_3 bestimmen wir genau wie die von H_2. Es gilt $|H_3| = (q-1)(q-2)$.

$H_4 = \{C \in H | a_2a_1a_0 \neq 0\} = H \backslash (H_1 \cup H_2 \cup H_3)$. Die Anzahl der Elemente von H_4 ist gleich $|H_4| = |H| - |H_1| - |H_2| - |H_3| = (q-1)(q^2 - 3q + 4)$.
Weiter seien G_1, G_2, G_3, G_4, die zu den Gruppen H_1, H_2, H_3, H_4 gehörigen Stabilisatoren.

$$\begin{aligned} G_1 &= \{u \in \mathbb{F}_q^* | y^2 - x^7 - a_0x \mapsto y^2 - x^7 - \bar{a}_o x\} = \{u \in \mathbb{F}_q^* | u^{12} = 1\} \\ G_2 &= \{u \in \mathbb{F}_q^* | y^2 - x^7 - a_1x^3 - a_0x \mapsto y_2 - x^7 - \bar{a}_1x^3 - \bar{a}_o x\} \\ &= \{u \in \mathbb{F}_q^* | u^8 = 1 \quad und \quad u^{12} = 1\} = \{u \in \mathbb{F}_q^* | u^4 = 1\} \\ G_3 &= \{u \in \mathbb{F}_q^* | y^2 - x^7 - a_2x^5 - a_0x \mapsto y_2 - u^{14}x^7 - \bar{a}_2x^5 - \bar{a}_o x\} \\ &= \{u \in \mathbb{F}_q^* | u^4 = 1 \quad und \quad u^{12} = 1\} = \{u \in \mathbb{F}_q^* | u^4 = 1\} \\ G_4 &= \{u \in \mathbb{F}_q^* | a_2a_1a_0 \neq 0\} = \{u \in \mathbb{F}_q^* | u^4 = 1 \quad und \quad u^8 = 1 \quad und \quad u^{12} = 1\} \\ &= \{u \in \mathbb{F}_q^* | u^4 = 1\} \end{aligned}$$

Die Gruppen G_2, G_3, G_4 sind gleich und entsprechend gilt für die Mächtigkeiten $|G_2| = |G_3| = |G_4|$. Dann gilt $G \sim \mathbb{F}_q^*$ und $|G| = q-1$, wegen $u \in \mathbb{F}_q^*$ für ein Erzeugende g von G. Folglich erhalten wir:

1. Ist $u \in G_i, i = 2,3,4$, dann gilt wegen $G_i \subset G$, dass $u = g^k$ für ein $k \leq q-1$. Es gilt $g^{4k} = u^4 = 1 = g^{s(q-1)}$ für ein $s \in \mathbb{N}$. Aus $k \leq (q-1)$ erhalten wir $s \leq 4$. $q-1$ ist immer durch zwei teilbar und wir betrachten daher nur die folgenden Fälle:
   (a) $4|(q-1)$. Wegen $s \leq 4$ erhalten wir vier Werte für s oder $|G_i|$ ist in diesem Fall gleich 4.
   (b) $4 \nmid (q-1)$. Dann muss gelten $2|s$ und wegen $s \leq 4$ kann s nur die Werte 2 oder 4 annehmen und $|G_i| = 2$.
2. Sei jetzt $u \in G_1$. Dann gilt $u = g^k, k \leq (q-1)$ und $g^{12k} = u^{12} = 1 = g^{s(q-1)}$. Aus $k \leq (q-1)$ erhalten wir diesmal $s \leq 12$. Wir betrachten die folgenden Fälle
   (a) $3|(q-1)$ und $4|(q-1)$. Entsprechend der Werte von s ist $|G_1| = 12$.
   (b) $3|(q-1)$ und $4 \nmid (q-1)$. Dann ist $2|s$ und s kann die Werte $s = 2,4,6,8,10,12$ annehmen. In diesem Fall gilt $|G_1| = 6$.
   (c) $3 \nmid (q-1)$ und $4|(q-1)$. Dann ist $3|s$, $s = 3,6,9,12$ und $|G_1| = 4$.

Mit Hilfe der Bahnformel und dem Satz von Lagrange erhalten wir für die Anzahl der Isomorphieklassen

$$\begin{aligned}
|H/G| &= \frac{|H_1|}{|B_1|} + \frac{|H_2|}{|B_2|} + \frac{|H_3|}{|B_3|} + \frac{|H_4|}{|B_4|} \\
&= \frac{|H_1|}{(G:G_1)} + \frac{|H_2|}{(G:G_2)} + \frac{|H_3|}{(G:G_3)} + \frac{|H_4|}{(G:G_4)} \\
&= \frac{|H_1||G_1|}{|G|} + \frac{|H_2||G_2|}{|G|} + \frac{|H_3||G_3|}{|G|} + \frac{|H_4||G_4|}{|G|} \\
&= |G_1| + (q-2)|G_2| + (q-2)|G_3| + (q^2-3q+4)|G_4|.
\end{aligned}$$

In Abhängigkeit der Werte von $|G_i|, i = 1,2,3,4$, unterscheiden wir die folgenden Fälle:

$$\begin{array}{lll}
3|(q-1) \quad \textit{und} & 4|(q-1) & \Longrightarrow |H/G| = 4q^2 - 4q + 12 \\
3|(q-1) \quad \textit{und} & 4 \nmid (q-1) & \Longrightarrow |H/G| = 4q^2 - 2q + 6 \\
3 \nmid (q-1) \quad \textit{und} & 4|(q-1) & \Longrightarrow |H/G| = 4q^2 - 4q + 4.
\end{array}$$

Wir erhalten drei verschiedene Möglichkeiten für die Anzahl der F_q-Isomorphieklassen in Abhängigkeit von den Werten von q.

3 Cantorscher Algorithmus

3.1 Der Cantorsche Algorithmus

In diesem Kapitel wird der Cantorsche Algorithmus *Computing in the Jacobian of a Hyperelliptic Curve* von D. Cantor, 1994, dargestellt. Das ist eine effiziente und elegante Methode, um Elemente der Jacobischen Varietät einer hyperelliptischen Kurve, beliebiges Geschlechtes, explizit addieren zu können. Bei der Untersuchung der Struktur der Jacobischen Varietät werden wir zuerst in jeder Divisorenäquivalenzklasse ein ausgezeichnetes Element definieren, den sogenannten reduzierten Divisor. Für die Menge der reduzierten Divisoren werden wir entsprechend des Algorithmuses für binäre quadratische Formen, einen Additionsalgorithmus konstruieren. Mit Hilfe dieses Rechenvorgangs lässt sich die Gruppenoperation auf der Jacobischen Varietät explizit darstellen. Somit wird die Jacobische Varietät jeder hyperelliptischen Kurve zu einer abelschen Gruppe, welche für kryptographische Zwecke geeignet ist.
Bei der Konstruktion des Kapitels habe ich mich hauptsächlich auf den Artikel *An Ellementary Introduction to Hyperelliptic Curves* von A. Menezes orientiert. Sei $C : y^2 - h(x)y = f(x)$ eine hyperelliptische Kurve vom Geschlecht g über einem endlichen Körper $k = \mathbb{F}_q$. Um die Struktur der Jakobischen Varietät $Jac(C)$ erklären zu können, werden wir zuerst einige Grundbegriffe definieren.

Definition 3.1 *Sei $P = (x_0, y_0) \neq P_\infty$ ein endlicher Punkt von C. Der Punkt $\tilde{P} = (x_0, -y_0 - h(x_0))$ heißt das Inverse von P und es gilt $\tilde{P} \in C$. Das Inverse von P_∞ ist der unendliche Punkt selbst.*
Gilt für einen Punkt $P \neq P_\infty$ und $P = \tilde{P}$, dann heißt P speziell, sonst gewöhnlicher Punkt.

Definition 3.2 *C sei eine hyperelliptische Kurve über dem Grundkörper k.*

$$k[C] = k[x, y]/(y^2 + h(x)y - f(x))$$

heißt der Koordinatenring von C über k und

$$\bar{[}C] = \bar{k}[x, y]/(y^2 + h(x)y - f(x))$$

der Koordinatenring von C über $\bar{k}$, wobei $\bar{k}$ ein algebraischer Abschluss von k ist.

Definition 3.3 *Ein Element $p \in \bar{k}[C]$ heißt Polynomialfunktion von C.*

Bemerkung 3.4 *$\bar{k}[C]$ ist ein Integrationsbereich.*

Sei $p \in \bar{k}[C]$ eine Polynomialfunktion. Aus der Kurvengleichung von C lässt sich y^2 als $y^2 = f(x) - h(x)y$ darstellen. Somit ist p gleich einem eindeutigen Polynom der Form

$$a(x) - b(x)y, \quad mit \quad a(x), b(x) \in \bar{k}[x].$$

Definition 3.5 *Das Polynom* $\bar{p} = a(x) + b(x)h(x) + y \in \bar{k}[C]$ *heißt das Konjugierte von* p.
Für $p = a(x) - b(x)y$ *lässt sich die Norm* $N(p) = p\bar{p}$ *definieren.*

Lemma 3.6 *Die Norm von* p *hat die folgenden Eigenschaften.*

1. $N(p) \in \bar{k}[x]$
2. $N(\bar{p}) = N(p)$
3. $N(pq) = N(p)N(q), q \in \bar{k}[C]$.

Beweis: Sei $p = a - by$, $q = c - dy$ mit $a, b, c, d \in \bar{k}[C]$.

1. $\bar{p} = a + b(h+y)$. $N(p) = p\bar{p} = (a-by)(a+b(h+y)) = a^2 + abh - b^2 f \in \bar{k}[x]$.
2. $\bar{\bar{p}} = a - by = p \Rightarrow N(\bar{p}) = \bar{p}\bar{\bar{p}} = \bar{p}p = N(p)$
3. $pq = (ac + bdf) - (bc + ad + bdh)y$ und

$$\begin{aligned} \overline{pq} &= (ac + bdf) + (bc + ad + bdh)(h + y) \\ &= (a + b(h + y))(c + d(h + y)) = \bar{p}\bar{q} \end{aligned}$$

und somit erhalten wir $N(pq) = pq\overline{pq} = pq\bar{p}\bar{q} = p\bar{p}q\bar{q} = N(p)N(q)$.

□

Der Koordinatenring $k[C]$ reicht nicht aus, um die Struktur der Jacobischen Varietät beschreiben zu können. Aufgrund dessen definieren wir:

Definition 3.7 $k(C) = Quotk[C]$ *heißt der Funktionenkörper von* C *über* k, *entsprechend* $\bar{k}(C) = Quot\bar{k}[C]$ *der Funktionenkörper von* C *über* $\bar{k}$.
Die Elemente von $\bar{k}(C)$ *werden rationale Funktionen genannt.*

Sei $r \in \bar{k}(C)$ und $P \in C \setminus \{P_\infty\}$. r ist in P definiert, falls zwei Polynomialfunktionen $p, q \in \bar{k}[C]$ existieren mit $r = \frac{p}{q}$ und $q(P) \neq 0$. $r(P) = \frac{p(P)}{q(P)}$ heißt der Wert von r in P und ist unabhängig von der Darstellung von r.

Definition 3.8 *Sei* $p(x, y) = a(x) - b(x)y \in \bar{k}[C] \setminus \{0\}$. *Dann heißt*

$$deg(p) = max\{2deg_x(a(x)), 2g + 1 + 2deg_x(b(x))\}$$

der Grad von p.

Lemma 3.9 *Für den Grad von* p *lassen sich die folgenden Eigenschaften nachweisen:*

1. $deg(p) = deg_x(N(p))$
2. $deg(pq) = deg(p) + deg(q)$
3. $deg(p) = deg(\bar{p})$.

Beweis:

1. Sei $p = a(x) - b(x)y$ mit $d_1 = deg_x(a(x)), d_2 = deg_x(b(x))$. Die Norm von p ist gleich $a(x)^2 + a(x)b(x)h(x) - b(x)^2 f(x)$ und aus der Definition von C wissen wir, dass $deg_x(h(x)) \leq g$ und $deg_x(f(x)) = 2g + 1$. Wir betrachten die folgenden Fälle:

   (a) Sei $deg(p) = 2d_1$, d.h. $2d_1 > 2g+1+2d_2$. Dann gilt $2d_1 \geq 2g+2+ad_2$ oder äquivalent dazu $d_1 \geq g + 1 + d_2$. Somit erhalten wir

   $$deg_x(a(x)^2) = 2d_1 \geq d_1+g+1+d_2 > d_1+d_2+g \geq deg_x(a(x)b(x)h(x))$$

   (b) Sei $deg(p) = 2g + 1 + 2d_2$, d.h. $2d_1 < 2g + 1 + 2d_2$. Daraus folgt $2d_1 \leq 2g + 2d_2 \Leftrightarrow d_1 \leq g + d_2$ und

   $$\begin{aligned} deg_x(a(x)b(x)h(x)) &\leq d_1 + d_2 + g \leq 2g + 2d_2 < 2g + 2d_2 + 1 \\ &= deg_x(b(x)^2 f(x)). \end{aligned}$$

   Insgesamt erhalten wir $deg_x(N(p)) = max\{2d_1, 2g + 1 + 2d_2\} = deg(p)$.

2. $$\begin{aligned} deg(pq) &= deg_x(N(pq)) = deg_x(N(p)N(q)) \\ &= deg_x(N(p)) + deg_x(N(q)) = deg(p) + deg(q). \end{aligned}$$

3. Die Behauptung folgt aus der Normeigenschaft $N(p) = N(\bar{p})$.

$\square$

Nachdem wir den Wert einer rationalen Funktion $r \in \bar{k}(C)$ an einer Stelle $P \neq P_\infty$ erklärt haben, wollen wir jetzt auch $r(P_\infty)$ definieren.

Definition 3.10 *Sei $r = \frac{p}{q} \in \bar{k}(C)$.*

1. *Gilt $deg(p) < deg(q)$, dann ist $r(P_\infty) := 0$.*
2. *Falls $deg(p) > deg(q)$, dann ist r in P_∞ nicht definiert.*
3. *Falls $deg(p) = deg(q)$, gilt $r(P_\infty) = \frac{k_1}{k_2}$, wobei k_1, k_2 die Haupkoeffizienten von p, q bezüglich dem Grad sind.*

Als nächstes werden wir die Begriffe *Nullstelle und Pol* einer rationalen Funktion, sowie *lokaler Parameter* und ihre Eigenschaften erklären.

Definition 3.11 *Sei $r \in \bar{k}(C)^*$ und $P \in C$.*

1. *P heißt Nullstelle von r, falls $r(P) = 0$.*
2. *P heißt Pol von r, falls r in P nicht definiert ist. Dann gilt $r(P) = \infty$.*

Lemma 3.12 *Für $p \in \bar{k}[C]$, $P \in C$ und $p(P) = 0$ gilt $\bar{p}(\tilde{P}) = 0$.*

Beweis: Sei $p = a(x) - b(x)y$ und $P = (x_0, y_0)$. Entsprechend haben $\bar{p}, \tilde{P}$ die Form $\bar{p} = a(x) + b(x)(y + h(x))$ und $\tilde{P} = (x_0, -y_0 - h(x_0))$.

$$\bar{p}(\tilde{P}) = a(x_0) + b(x_0)(-y_0 - h(x_0) + h(x_0)) = a(x_0) - y_0 b(x_0) = p(P) = 0.$$

□

Definition 3.13 *Sei $P \in C$. Dann existiert eine Funktion $u \in \bar{k}(C)$ mit $u(P) = 0$ und den folgenden Eigenschaften:*

1. *Für jedes $p \in \bar{k}[C]^*$ existiert ein $d \in \mathbb{Z}$ und $s \in \bar{k}(C)$ mit $s(P) \neq 0, \infty$ und $p = u^d s$.*
2. *d ist unabhängig von der Wahl von u.*

Eine solche Funktion heißt lokaler Parameter.
Existenzbeweis für lokalen Parameter in [Menezes/Stichtenoth].

Mit Hilfe des lokalen Parameters definieren wir:

Definition 3.14 *Seien p und P wie in der obigen Definition angegeben. Dann heißt d die Ordnung von p in P und wird mit $ord_P(p) = d$ bezeichnet.*

Lemma 3.15 *Für zwei Polynome $p, q \in \bar{k}[C]^*$ mit $ord_P(p) = d_1$ und $ord_P(q) = d_2$ und $P \in C$ gilt*

1. *$ord_P(pq) = ord_P(p) + ord_P(q)$.*
2. *Sei $p \neq -q$, dann gilt*

$$\begin{aligned} ord_P(p+q) &= min\{d_1, d_2\}, falls \quad d_1 \neq d_2 \\ ord_P(p+q) &\geq min\{d_1, d_2\}, sonst. \end{aligned}$$

Beweis: Sei u ein lokaler Parameter in P. Dann haben p, q die Darstellung $p = u^{d_1} s_1$ und $q = u^{d_2} s_2$ mit $s_1, s_2 \in \bar{k}(C)$ und $s_i(P) \neq 0, \infty, i = 1, 2$. O.B.d.A. $d_1 \geq d_2$.

1. $ord_P(pq) = ord_P(u^{d_1+d_2} s_1 s_2) = d_1 + d_2$.
2. $p + q = u^{d_2}(u^{d_1-d_2} s_1 + s_2)$.
   (a) Falls $d_1 > d_2$, dann gilt $u^{d_1-d_2} s_1(P) = 0$ und $s_2(P) \neq 0$. Daraus folgt $ord_P(p+q) = d_2$.
   (b) Falls $d_1 = d_2$, dann gilt $(s_1 + s_2)(P) \neq \infty$ und $ord_P(p+q) \geq d_2$.

□

Lemma 3.16 *Für $p \in \bar{k}[C]^*$ gilt $ord_P(p) = ord_{\tilde{P}}(\bar{p})$.*

Beweis: Wir betrachten die folgenden Fälle

1. Sei $P = P_\infty$ oder $\tilde{P} = P_\infty$, dann ist $ord_P(p) = -deg(p)$ und $ord_{\tilde{P}}(\bar{p})$ und $deg(p) = deg(\bar{p})$.

2. Sei $P = (x_0, y_0)$ ein endlicher Punkt.
$p = a(x) - b(s)y = (x - x_0)^d s(x, y)$, d sei die größte Potenz von $(x - x_0)$ die beiden $a(x)$ und $b(x)$ teilt. Falls $s(P) \neq 0$ setzen wir $d = 0$, sonst ist d die größte Potenz von $(x - x_0)$, die $N(s)$ teilt.
Es gilt $\bar{p} = (x - x_0)^d \bar{s} = (x - x_0)^d ((a_0(x) + b_0(x)h(x)) + b_0(x)y)$, mit $s = a_0(x) - b_0(x)y$. $s(P) = 0$ ist äquivalent zu $\bar{s}(\tilde{P}) = 0$. Da $(x - x_0)$ nicht $a_0(x) + b_0(x)y$ und $b_0(x)$ gleichzeitig teilen kann, wegen $(x - x_0) \nmid a_0(x)$, ist d die höchste Potenz mit $(x - x_0)^d | N(s) = N(\bar{s})$. Somit ist die Behauptung bewiesen.

□

Satz 3.17 *Sei $p \in \bar{k}[C]^*$, dann hat p nur endlich viele Null- und Polstellen und es gilt $\sum_{P \in C} ord_P(p) = 0$.*

Beweis: Sei $deg(p) = n$, dann gilt $deg_x N(p) = n$ und $N(p) = p\bar{p} = (x - x_1)(x - x_2)...(x - x_n)$, wobei nicht alle $x_i \in \bar{k}$ verschieden sein müssen. Der einzige Pol von p ist in P_∞ mit $ord_{P_\infty}(p) = -n$.
Seien $P_i = (x_i, y_i) \in C$ $n-$Punkte mit $x-$Koordinaten wie oben.
Ist P_i gewöhnlicher Punkt, dann gilt $ord_{P_i}(x - x_i) = 1$ und $ord_{\tilde{P}_i}(x - x_i) = 1$.
Ist P_i spezieller Punkt, dann gilt $ord_{P_i}(x - x_i) = 2$.
In beiden Fällen hat $(x - x_i)$ keine weiteren Nullstellen. Somit erhalten wir, dass $N(p)$ nur endlich viele Nullstellen hat und folglich auch p.
$\sum_{P \in C \setminus \{P_\infty\}} ord_P(N(p)) = 2n$ und wegen $ord_P(p) = ord_{\tilde{P}}(\bar{p})$ gilt
$\sum_{P \in C \setminus \{P_\infty\}} ord_P(p) = \sum_{P \in C \setminus \{P_\infty\}} ord_P(\bar{p})$ und damit auch die Behauptung.

□

3.2 Divisoren

In diesem Teil werden wir die Struktur der Jacobischen Varietät einer hyperelliptischen Kurve C studieren. Dafür benötigen wir noch die folgenden Begriffe: Unter einen *Divisor* $D \in Div(C)$ verstehen wir eine formale Summe $D = \sum_{P \in C} m_P P$ mit $m_P \in \mathbb{Z}$. Die Zahl $deg(D) = \sum_{P \in C} m_P$ heißt der Grad von D und m_P bezeichnet die Ordnung von D in P ($ord_P D = m_P$). $supp(D) := \{P \in C | m_p \neq 0\}$ ist der *Träger* von D. Die Gesamtheit aller Divisoren von C bildet unter der Divisorenaddition

$$\sum P \in C m_P P + \sum_{P \in C} n_P = \sum_{P \in c} (m_P + n_P) P$$

eine abelsche Gruppe $Div(C)$. Die Menge der Hauptdivisoren $H = div(r) = \sum_{P \in C} ord_P(r) P, r \in \bar{k}(C)^*$ ist eine Untergruppe $Princ(C)$ von $Div(C)$.

Hat r die Form $r = \frac{p}{q}$, dann gilt für den Divisor von r, dass $div(r) = div(p) - div(q)$.
Unter dem größten gemeinsaxmmen Faktor zweier Divisoren D_1, D_2 verstehen wir den Divisor

$$ggT(D_1, D_2) = \sum_{P \in C} min\{m_P, n_P\}P - (\sum_{P \in C} min\{m_P, n_P\}P)P_\infty$$

und es gilt $ggT(D_1, D_2) \in Div_0(C)$. Hierbei bezeichnet $Div_0(C)$ die Menge der Divisoren vom Grad 0.

Bemerkung 3.18 *Für einen Punkt $P = (x_0, y_0)$ gilt*

1. *$div(x - x_0) = P + \tilde{P} - 2P_\infty$, falls P ein gewöhnlicher Punkt ist.*
2. *$div(x - x_0) = 2P - 2P_\infty$, falls P spezieller Punkt ist.*

Wegen $ord_P(p) = ord_{\tilde{P}}(\bar{p})$, $p \in \bar{k}[C]$ gilt $div(p) = \sum_{P \in C} m_p P$ und $div(\bar{p}) = \sum_{P \in C} m_p \tilde{P}$.

Definition 3.19 *Die Quotientengruppe $Jac(C) = Div_0(C)/Princ(C)$ heißt die Jacobische Varietät von C.*
Zwei Divisoren werden äquivalent $D_1 \sim D_2$ genannt, falls $D_1 - D_2 \in Princ(C)$.

Sei σ ein Automorphismus von $\bar{k}$ über k. C sei eine hyperelliptische Kurve und $P = (x_0, y_))$ ein Punkt auf C. Dann gilt für den Punkt $P^\sigma = (x_0^\sigma, y_0^\sigma)$, dass $P^\sigma \in C$.

Definition 3.20 *Ein Divisor $D = \sum m_P P$ ist über dem Körper k definiert, falls $D^\sigma := \sum m_P P^\sigma \sim D$ für jeden Automorphismus $\sigma \in (Gal\bar{k}/k)$.*

Nicht jeder Punkt eines Divisors D über k ist ein $k-$rationaler Punkt. Ein Hauptdivisor H ist definiert über k genau dann, wenn H der Divisor einer rationalen Funktion mit Koeffizienten in k ist. Die Menge $Jac(k)$ aller Divisorenklassen in $Jac(C)$, die einen Repräsentanten über k haben, bildet eine Untergruppe von $Jac(C)$. Der Beweis der letzteren Aussage wird das Ziel der folgenden Betrachtungen sein.

Definition 3.21 *Ein semi-reduzierter Divisor ist ein Divisor der Gestalt $D = \sum P_i - (\sum m_i)\infty$, wobei $m_i \geq 0$, $P_i \neq P_\infty$, und falls $P_i \in Supp(D)$ dann $\tilde{P}_i \notin Supp(D)$. Für $P_i = \tilde{P}_i$ gilt $m_i = 1$.*

Lemma 3.22 *Zu jedem Divisor $D \in Div_k^0(C)$ existiert ein äquivalenter semi-reduzierter Divisor.*

Beweis: Sei $D = \sum_{P \in C} m_P P$ und (C_1, C_2) sei eine Zerlegung der Menge der gewöhnlichen Punkte von C, so dass $P \in C_1$ genau dann, wenn $\tilde{P} \in C_2$. $P \in C_1$

bedeutet, dass $m_P \geq m_{\tilde{P}}$. Weiterhin sei C_0 die Menge der speziellen Punkte von C. Dann lässt sich D wie folgt darstellen:

$$D = \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P + \sum_{P \in C_0} m_P P - m\infty$$

Wir betrachten den folgenden Divisor:

$$D_1 = D - \sum_{P=(x',y') \in C_2} m_p div(x - x') - \sum_{P=(x',y') \in C_0} \lfloor \frac{m_P}{2} \rfloor div(x - x')$$

Es gilt $D \sim D_1$ und nach Bemerkung 3.18 erhalten wir

$$D_1 = \sum_{P \in C_1} (m_P - m_{\tilde{P}})P + \sum_{P \in C_0} (m_P - 2\lfloor \frac{m_P}{2} \rfloor)P - m_1\infty$$

für ein $m_1 \in \mathbb{Z}$. Anhand der Form von D_1 lässt sich feststellen, dass D_1 ein semi-reduzierter Divisor ist.

□

Um besser mit semi-reduzierten Divisoren rechnen zu können, brauchen wir eine bequemere Darstellung der Divisoren. Hierbei werden jedem Divisor D eineindeutig zwei Polynome $a(x)$ und $b(x)$ zugeordnet, wobei

$$a(x) = \prod_{P_i \in supp(D)} (x - x_i)^{m_i}, \quad P_i = (x_i, y_i)$$

und $b(x)$ sei das eindeutige Polynom mit

1. $deg_x(b(x)) < deg_x(a(x))$
2. $b(x_i) = y_i$, für jedes i mit $m_i \neq 0$
3. $a(x) | \left(b(x)^2 + b(x)h(x) - f(x)\right)$.

Lemma 3.23 *Sei $P = (x_0, y_0)$ ein gewöhnlicher Punkt auf C und $R \in \bar{k}(C)$ eine rationale Funktion ohne Pol in P. Dann existieren für jedes $t \geq 0$ eindeutige Elemente $c_0, c_1, ..., c_t \in \bar{k}$ und $R_t \in \bar{k}(C)$, so dass*

$$R = \sum_{0}^{t} c_i(X - x_0)^i + (X - x_0)^{t+1} + R_t,$$

wobei R_t keinen Pol in P hat.

Beweis: Potenzreihenentwicklungssatz.

□

Lemma 3.24 *Sei $P = (x_0, y_0)$ wie oben ein gewöhnlicher Punkt auf C. Dann existieren für jedes $t \geq 1$ eindeutige Polynome $b_t(X) \in \bar{k}[X]$, so dass*

1. *$deg_x b_t < t$*
2. *$b_t(x_0) = y_0$*
3. *${b_t}^2(x) + b_t(x)h(x) \equiv f(x) \pmod{(x - x_0)^t}$*

Beweis: Sei $y = \sum_{i=0}^{t-1} c_i(x - x_0)^i + (x - x_0)^t R_{t-1}$ mit $c_i \in \bar{k}$ und $R_{t-1} \in \bar{k}(C)$. Wir definieren $b_t(X) = \sum_{i=0}^{t-1} c_i(x - x_0)^i$. Nach der Anwendung von Lemma 3.23 auf $r = y$ erhalten wir $c_0 = y_0$ und somit $b_t(x_0) = y_0$. Wegen $y^2 + h(x)y = f(x)$ und nach Reduktion der beiden Seiten modulo $(x - x_0)^t$ folgt ${b_t}^2(x) + b_t(x)h(x) \equiv f(x) \pmod{(x - x_0)^t}$. Die Eindeutigkeit lässt sich leicht mittels Induktion zeigen.

$\square$

Satz 3.25 *Sei $D = \sum m_i P_i - (\sum m_i)\infty$ ein semi-reduzierter Divisor, wobei $P_i = (x_i, y_i)$. Sei $a(X) = \prod (x - x_i)^{m_i}$ und b sei das eindeutige Polynom mit*

1. *$deg_x b < deg_x a$*
2. *$b(x_i) = y_i$ für jedes i mit $m_i \neq 0$*
3. *$a(x) | \left(b(x)^2 + b(x)h(x) - f(x)\right)$*

Dann gilt $D = ggT(div(a(x)), div(b(x) - y))$.
Wir werden weiterhin die Schreibweise $div(a, b)$ für $ggT(div(a(x)), div(b(x) - y))$ verwenden.

Beweis: Sei C_1 die Menge aller gewöhnlichen Punkte in $Supp(D)$, C_0 die Menge der speziellen Punkte und mit C_2 bezeichnen wir die Menge $\{\tilde{P} | P \in C_1\}$. Dann lässt sich D darstellen als

$$D = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m\infty, m_i, m \in \mathbb{Z}_{\geq 1}.$$

Wir zeigen zuerst, dass ein eindeutiges Polynom $b(x)$ existiert, das die vorgegebenen Bedingungen erfüllt. Nach Lemma 3.24 existiert für jedes $P_i \in C_1$ ein eindeutiges Polynom $b_i(x) \in \bar{k}$ mit den Eigenschaften

1. $deg_x b_i < m_i$
2. $b_i(x_i) = y_i$
3. $(x - x_i)^{m_i} | {b_i}^2(x) + b_i(x)h(x) - f(x)$.

Es gilt zusätzlich für $P_i \in C_0$, dass $b_i(x) = y_i$.
Nach dem Chinesischen Restsatz existiert ein eindeutiges Polynom $b(x) \in \bar{k}[x]$ mit $deg_x b < \sum m_i$ und

$$b(x) \equiv b_i(x) \pmod{(x-x_i)^{m_i}}, \quad \forall i.$$

Es lässt sich jetzt nachprüfen, dass $b(x)$ die Bedingungen des Theorems erfüllt. Sei

$$div(a(x)) = div \prod (x-x_i)^{m_i} = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \tilde{P_i} - (*)\infty$$

und

$$div(b(x)-y) = \sum_{P_i \in C_0} t_i P_i + \sum_{P_i \in C_1} s_i P_i + \sum_{P_i \in \{C_0 \cup C_1 \cup C_2 \cup \infty\}} m_i P_i - (*)\infty,$$

wobei jedes $s_i \geq m_i$, da $(X-x_i)^{m_i} | N(b-y) = b^2 + hb - f$. Sei $P = (x_0, y_0) \in C_0$, dann teilt $(x - x_0)$ das Polynom $b^2 + bh - f$ und nach Ableiten dieses Polynomes in $X = x_0$ erhalten wir

$$\begin{aligned}
&2b(x_0)b'(x_0) + b'(x_0)h(x_0) + b(x_0)h'(x_0) - f'(x_0) \\
&= b'(x_0)(2y_0 + h(x_0)) + (h'(x_0)y_0 - f'(x_0)) \\
&= h'(x_0)y_0 - f'(x_0), \quad da \quad 2y_0 + h(x_0) = 0 \\
&\neq 0.
\end{aligned}$$

Somit ist $x = x_0$ einfache Nullstelle von $N(b-y) = b^2 + bh - f$ und $t_i = 1$ für alle i. Daraus folgt

$$ggT(a(x), b(x)-y) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m\infty = D.$$

□

Korollar 3.26 *Seien $a(x), b(x) \in \bar{k}[x]$ mit $deg_x b < deg_x a$. Gilt $a | (b^2 + bh - f)$, dann ist $div(a, b)$ ein semi-reduzierter Divisor.*

Beweis: Folgt aus dem vorigen Satz mit $D = ggT(a, b - y)$.

□

Definition 3.27 *Sei $D = \sum m_i P_i - (\sum m_i)\infty$ ein semi-reduzierter Divisor für den zusätzlich noch gilt $\sum m_i < g$, mit $g = g(C)$, dann heißt D reduzierter Divisor.*

Definition 3.28 *Die Zahl*

$$|D| = \sum_{P \in C} |m_P|$$

heißt Norm des Divisors $D = \sum m_p P$.

Satz 3.29 *Zu jedem Divisor $D \in Div^0$ existiert ein eindeutig bestimmter zu D äquivalenter reduzierter Divisor.*

Beweis: Wir zeigen zuerst die **Existenz**.
Nach Lemma 3.22 existiert ein semi-reduzierter Divisor D' mit $D' \sim D$ und $|D'| \leq |D|$. Gilt $|D'| \leq g$, dann ist D' ein reduzierter Divisor und die Existenz ist bewiesen.
Seien sonst $P_1, P_2, ..., P_{g+1}$ endliche Punkte aus $Supp(D')$, nicht unbedingt verschiedene. Jeder dieser Punkte kann höchstens $ord_P(D')$ mal in D vorkommen und $div(a(x), b(x))$ sei die Polynomialdarstellung des Divisors

$$D = P_1 + P_2 + \cdots + P_{g+1} - (g+1)P\infty.$$

Wegen $deg_x(b) \leq g$ haben wir $deg(b(x) - y) = 2g + 1$ und

$$div(b(x) - y) = P_1 + P_2 + \cdots + P_{g+1} + Q_1 + \cdots + Q_g - (2g+1)P\infty,$$

für einige endliche Punkte $Q_1, ..., Q_g$. Nach Subtraktion dieses Divisors von D' erhalten wir ein Divisor D'', wobei es gilt $D'' \sim D' \sim D$ und $|D''| < |D'|$. Wir wiederhollen diesen Schritt bis wir letzendlich einen Divisor D_1 konstruiert haben mit $|D_1| \leq g$.
Eindeutigkeit:
Seien D_1, D_2 zwei reduzierte Divisoren mit $D_1 \sim D_2$ und $D_1 \neq D_2$. Nach Lemma 3.22 existiert ein semi-reduzierter Divisor D_3 mit $D_3 \sim D_1 - D_2$. Wegen $D_1 \neq D_2$ gibt es ein Punkt P, so dass $ord_P(D_1) \neq ord_P(D_2)$. O.B.d.A. $ord_P(D_1) = m_1 \geq 1$ und es gilt entweder 1) $ord_P(D_2) = 0$ oder 2) $ord_P(D_2) = m_2$ mit $1 \leq m_2 < m_1$ oder 3) $ord_{\tilde{P}}(D_2) = m_2$ und $1 \leq m_2 \leq m_1$. Ist P spezieller Punkt, dann kommt nur Fall 1) in Frage.
Im Fall 1) gilt $ord_P(D_3) = m_1 \geq 1$,
im Fall 2) ist $ord_P(D_3) = (m_1 - m_2) \geq 1$ und
im Fall 3) ist $ord_P(D_3) = (m_1 + m_2) \geq 1$.
In allen Fällen gilt $ord_P(D_3) \geq 1$, so dass $D_3 \neq 0$. Also $|D_3| \leq |D_1 - D_2| \leq |D_1| + |D_2| \leq 2g$. Sei jetzt r eine rationale Funktion in $\bar{k}(C)^*$, so dass $div(r) = D_3$. Wegen $D_1 \sim D_2$ und $D_3 \sim D_1 - D_2$ erhalten wir, dass D_3 ein Hauptdivisor ist, was die Existenz der Funktion r garantiert. Da r keine endliche Polstellen hat, muss r eine Funktion sein. D. h. $= a(x) - b(x)y$ für geeignete $a, b \in \bar{k}[x]$. Wegen $deg(y) = 2g + 1$ und $deg(r) = |D_3| \leq 2g$ erhalten wir, dass $b(x) = 0$. Angenommen $deg_x(a(x)) \geq 1$ und $x_0) \in \bar{k}$ ist eine Nulstelle von $a(x)$. Sei $P = (x_0, y_0)$ ein Punkt auf C. Ist P ein gewöhnlicher Punkt, dann sind beide $P, \tilde{P}$ Nullstellen von r, was der Semi-Reduziertheit von D_3 widerspricht. Ist aber P ein spezieller Punkt, dann ist P eine Nullstelle von G von mindestens Ordnung 2, was wieder der Semi-Reduziertheit von D_3 widerspricht. Damit ergibt sich, dass $deg_X(a(X)) = 0$ und $D_3 = 0$ ist. Widerspruch.

$\square$

3.2.1 Addition reduzierter Divisoren

Seien $D_1 = div(a_1, b_1)$ und $D_2 = div(a_2, b_2)$ zwei reduzierte Divisoren definiert über k, d.h. $a_1, b_1, a_2, b_2 \in k[X]$. Mittels des folgenden Algorithmus wird ein semi-reduzierte Divisor $D = (a, b)$ mit $a, b \in k[X]$ konstruieret, so dass $D \sim D_1 + D_2$. Dieses Verfahren entspricht der Struktur der Komposition bei binären quadratischen Formen.

Algorithm 1

<u>Eingabe:</u> Reduzierte Divisoren $D_1(a_1, b_1)$ und $D_2 = (a_2, b_2)$ definiert über k

<u>Ausgabe:</u> Semi-reduzierter Divisor $D = div(a, b)$ definiert über k mit $D \sim D_1 + D_2$

1. Finde Polynome $d_1, e_1, e_2 \in k[X]$ mittels des erweiterten euklidischen Algorithmus, so dass $d_1 = ggT(a_1, a_2)$ und $d_1 = e_1 a_1 + e_2 a_2$.
2. Finde Polynome $d, c_1, c_2 \in k[X]$, so dass $d = ggT(d_1, b_1 + b_2 + h)$ und $d = c_1 d_1 + c_2(b_1 + b_2 + h)$
3. Seien $s_1 = c_1 e_1, s_2 = c_1 e_2$ und $s_3 = c_2$, so dass
$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$$
.
4. Definiere
$$a = a_1 a_2 / d^2$$
und
$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \pmod{a}$$

Wir zeigen jetzt, dass dieser Algorithmus zu der Konstruktion eines semi-reduzierten Divisors führt.

Satz 3.30 *Seien $D_1 = div(a_1, b_1)$ und $D_2 = div(a_2, b_2)$ zwei semi-reduzierte Divisoren und a und b wie in dem Algorithmus definiert. Dann ist der Divisor $D = div(a, b)$ semi-reduziert und es gilt $D \sim D_1 + D_2$.*

Beweis: Wir werden zuerst zeigen, dass b ein Polynom ist. Mit Hilfe der im Schritt 3) angegebenen Darstellung von d erhalten wir

$$\begin{aligned} &\frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \\ &= \frac{b_2(d - s_2 a_2 - s_3(b_1 + b_2 + h)) + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \\ &= b_2 + \frac{s_2 a_2 (b_1 - b_2) - s_3({b_2}^2 + b_2 h - f)}{d}. \end{aligned}$$

Aus $d|a_2$ und $a_2|({b_2}^2 + b_2h - f)$ folgt, dass b ein Polynom ist.
Sei jetzt $b = sa + (s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f))/d$ mit $s \in k[x]$. Dann ist

$$\begin{aligned} b - y &= \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f) - dy}{d} + sa \\ &= \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f) - s_1a_1 - s_2a_2y - s_3(b_1 + b_2 + h)y}{d} + sa \\ &= \frac{s_1a_1(b_2 - y) + s_2a_2(b_1 - y) + s_3(b_1 - y)(b_2 - y)}{d} + sa. \qquad (2) \end{aligned}$$

Aus der letzteren Beziehung ergibt sich $a|(b^2 + bh - f) = (b - y)(b + y + h) = N(b - y)$. Um dies einzusehen, müssen wir zeigen, dass a_1a_2 das Produkt von $(s_1a_1(b_2 - y) + s_2a_2(b_1 - y) + s_3(b_1 - y)(b_2 - y))$ mit seinem Konjugierten teilt. Das folgt aus $a_1|({b_1}^2 + b_1h - f) = (b_1 - y)(b_1 + y + h)$ und $a_2|({b_2}^2 + b_2h - f) = (b_2 - y)(b_2 + y + h)$.
Aus Korollar 3.26 erhalten wir, dass $D = div(a, b)$ semi-reduzierter Divisor ist. Es bleibt noch $D \sim D_1 + D_2$ zu zeigen. Dafür berechnen wir zuerst die Ordnung von D in den Punkten $P \in supp(D_1) \cup supp(D_2)$. Dabei unterscheiden wir zwei Fälle.

1. Sei $P = (x_0, y_0)$ ein gewöhnlicher Punkt.

   (a) Sei $ord_P(D_1) = m_1, ord_{\tilde{P}}(D_1) = 0, ord_P(D_2) = m_2$ und $ord_{\tilde{P}}(D_2) = 0$, mit $m_1 \geq 0, m_2 \geq 0$. Dann ist $ord_P(a_1) = m_1, ord_P(a_2) = m_2, ord_P(b_1 - y) \geq m_1, ord_P(b_2 - y) \geq m_2$. Ist $m_1 = 0$ oder $m_2 = 0$ oder beide , dann ist $ord_P(d_1) = 0$ was $ord_P(d) = 0, ord_P(a) = m_1 + m_2$ liefert. Ist aber $m_1 \geq 1$ und $m_2 \geq 1$, dann folgt $ord(d) = 0$ und $ord_P(a) = m_1 + m_2$, wegen $(b_1 + b_2 + h)(x_0) = 2y_0 + h(x_0) \neq 0$. Aus der Relation 1) erhalten wir, dass

   $$ord_P(b - y) \geq min\{m_1 + m_2, m_2 + m_1, m_1 + m_2\} = m_1 + m_2,$$

   und daraus folgt $ord_P(D) = m_1 + m_2$.

   (b) Sei $ord_P(D_1) = m_1, ord_{\tilde{P}}(D_2) = m_2$, $m_1 \geq m_2 \geq 1$. Wir haben $ord_P(a_1) = m_1, ord_P(a_2) = m_2, ord_P(d_1) = m_2, ord_P(b_1 - y) \geq m_1, ord_P(b_2 - y) = 0$ und $ord_{\tilde{P}}(b_2 - y) \geq m_2$. Aus der letzteren Ungleichung geht hervor, dass $ord_P(b_2 + h + y) \geq m_2$, was $ord_P(b_1 + b_2 + h) \geq m_2$ oder $(b_1 + b_2 + h) = 0$ zur Folge hat. D.h. $ord_P(d) = m_2$ und $ord_P(a) = m_1 - m_2$. Wie in dem Fall zuvor erhalten wir aus 1)

   $$ord_P(b - y) \geq min\{m_1 + 0, m_2 + m_1, m_1 + 0\} - m_2 = m_1 - m_2,$$

   was $ord_P(D) = m_1 - m_2$ ergibt.

2. Sei jetzt $P = (x_0, y_0)$ ein spezieller Punkt.

   (a) Sei $ord_P(D_1) = 1, ord_P(D_2) = 1$. Dann gilt $ord_P(a_1) = 2, ord_P(a_2) = 2, ord_P(d_1) = 2$. Nun ist $(b_1 + b_2 + h)(x_0) = 2y_0 + h(x_0) = 0$, was $ord_P(b_1 + b_2 + h) \geq 2$ oder $(b_1 + b_2 + h) = 0$ liefert. Daraus folgt $ord_P(d) = 2$ und $ord_P(a) = 0$ und damit $ord_P(D) = 0$.

(b) Seien $ord_P(D_1) = 1$ und $ord_P(D_2) = 0$. Dann gilt $ord_P(a_1) = 2$, $ord_P(a_2) = 0$ und deswegen auch $ord_P(d_1) = ord_P(d) = 0, ord_P(a) = 2$. Aus $ord_P(b_1 - y) = 1$ gilt nach Relation 1), dass $ord_P(b - y) \geq 1$. Wir zeigen $ord_P(b - y) = 1$. Dazu bemerken wir $ord_P(b - y) \geq 2$ nur gelten kann, falls $ord_P(s_2a_2 + s_3(b_2 - y)) \geq 1$. In diesem Falle wäre $ord_P(s_2a_2 + s_3(b_2 + h + y)) \geq 1$, woraus $ord_P(s_2a_2 + s_3(b_1 + b_2 + h)) \geq 1$ oder $s_2a_2 + s_3(b_1 + b_2 + h) = 0$ folgt. Mittels Schritt 3) des Algorithmus erhalten wir $ord_P(d) \geq 1$, was zum Widerspruch führt. Folglich gilt $ord_P(b - y) = 1$ und $ord_P(D) = 1$.

Weiterhin betrachten wir den Divisor $T = (D_1 + D_2) - D$. Nach dem gerade Ausgerechnete, gilt für die Ordnung von $(D_1 + D_2) - D$ in $P \in supp(D_1) \cup supp(D_2)$

1. $ord_P((D_1 + D_2) - D) = (m + 1 + m_2) - (m_1 + m_2) = 0$, wobei P ein gewöhnlicher Punkt ist und $ord_P(D_1) = m_1, ord_P(D_2) = m_2$.
   Dann gilt für die Einschränkung des Divisors T auf P, $T = (D_1 + D_2 - D)_{|P} = 0P - 0P_\infty = 0$ und ist somit Hauptdivisor.

2. $ord_P((D_1 + D_2) - D) = (m_1 + 0) - (m_1 - m_2) = m_2$, falls Pgewöhnlicher Punkt ist und es gilt $ord_P(D_1) = m_1$ und $ord_{\tilde{P}}(d_2) = m_2$.
   Entsprechend gilt für $T_{|P \cup \tilde{P}} = m_2P + m_2\tilde{P} - 2m_2P_\infty$. Dies ist nach Bemerkung 3.18 ein Hauptdivisor.

3. In dem Fall, dass P ein spezieller Punkt ist, erhalten wir $ord_P(D_1 + D_2 - D) = (1 + 1) - 0$, wobei $ord_P(D_1) = ord_P(D_2) = 1$. $T_{|P} = 2P - 2P_\infty$ ist wiederum nach Bemerkung 3.18 ein Hauptdivisor.

4. Ist aber $ord_P(D_1) = 1$ und $ord_P(d_2) = 0$, dann gilt $ord_P(D) = 1$ und $T_{|P} = 0P - 0P_\infty = 0$.

Die Menge der Hauptdivisoren bildet eine additive Gruppe. Daher gilt $T = D_1 + D_2 - D$ ist ein Hauptdivisor und die Behauptung ist bewiesen.

□

3.2.2 Reduktion semi-reduzierter Divisoren

Die im Algorithmus 1 angegebene Konstruktion liefert keinen eindeutigen semi-reduzierten Divisor. Damit wir je zwei Divisoren D_1, D_2 einen eindeutigen Divisor zuordnen können müssen wir den gefundenen semi-semireduzierten Divisor $D \sim D_1 + D_2$ reduzieren, d.h. zu D ein äquivalenten reduzierten Divisor finden. Dies erfolgt nach dem Algorithmus 2.

Algorithmus 2
Eingabe: $D = div(a, b)$ semi-reduzierter Divisor definiert über k
Ausgabe: Der eindeutige reduzierte Divisor $D' = (a', b')$ mit $D' \sim D$.

1. Definiere:
$$a' = (f - hb - b^2)/a$$
und
$$b' = -h - b \mod a'$$
2. Falls $deg_X a' > g$ dann setze $a' \mapsto a$ und $b' \mapsto b$ und gehe zum Schritt 1
3. Sei c der Hauptkoeffizient von a', dann setze $c^{-1}a' \mapsto a'$
4. $D' = div(a', b')$

Es bleibt noch zu zeigen, dass die Anwendung vom Algorithmus 2 zu der Konstruktion eines reduzierten Divisors äquivalent zu D führt.

Satz 3.31 *Sei $D = div(a, b)$ ein semi-reduzierter Divisor, dann ist der nach Algorithmus 2 erhaltene Divisor $D' = div(a', b')$ reduziert und äquivalent zu D.*

Beweis: Seien $a' = (f - bh - b^2)/a$ und $b' = -h - b \mod a'$ Wir werden zeigen:

1. $deg_x(a') < deg_x(a)$
2. $D' = div(a', b')$ ist semi-reduziert und
3. $D \sim D'$

Die Behauptung des Satzes folgt nach Wiederholung der Reduktionprozese aus Algorithmus 2.

1. Sei $m = deg_x a, n = deg_x b$ mit $m > n, m \geq g + 1$.Dann ist $deg_x a' = max\{2g+1, 2n\} - m$. Ist $m > g+1$, dann gilt für das Maximum $max\{2g+1, 2n\} \leq 2(m-1)$, was $deg_x a' \leq m - 2 < deg_x a$ ergibt. Ist $m = g + 1$, dann ist $max\{2g+1, 2n\} = 2g + 1$ und damit $deg_x a' = g < deg_x a$.
2. Es gilt $aa' = f - bh - b^2$. Durch Reduktion der beiden Seiten modulo a' erhalten wir
$$f + (b' + h)h - (b' + h)^2 \equiv 0 \mod a'$$
oder äquivalent dazu
$$f - b'h - (b')^2 \equiv 0 \mod a'.$$
Daraus folgt $a'|(f - b'h - (b')^2)$, und nach Korollar 3.26 ist der Divisor $div(a', b')$ semi-reduziert.
3. Sei $C_0 = \{P \in Supp(D)|P = \tilde{P}\}$, $C_1 = \{P \in Supp(D)|P \neq \tilde{P}$ und $C_2 = \{\tilde{P}|P \in C_1\}$. Wie in dem Beweis vom Satz 3.25 können wir schreiben:
$$D = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - (*)\infty.$$

und

$$div(a) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \tilde{P}_i - (*)\infty$$

$$div(b-y) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} n_i P_i + \sum_{P_i \in C_1} 0\tilde{P}_i + \sum_{P_i \in C_3} s_i P_i - (*)\infty,$$

wobei $n_i \geq m_i, C_3 = C - (C_0 \cup C_1 \cup C_2 \cup \{\infty\}), s_i \geq 1, s_i = 1$, falls P_i spezieller Punkt ist. Aus $b^2 + bh - f = N(b-y)$ folgt wegen $div\bar{D} = \sum_{P \in C} m_P \tilde{P}$ für jeden Divisor $D = \sum_{P \in C} m_P P$, dass

$$\begin{aligned} div(b^2+bh-f) = &\sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} n_i P_i + \sum_{P_i \in C_1} n_i \tilde{P}_i + \sum_{P_i \in C_3} s_i P_i \\ &+ \sum_{P_i \in C_3} s_i \tilde{P}_i - (*)\infty, \end{aligned}$$

und folglich

$$\begin{aligned} div(a') &= div(b^2+bh-f) - div(a) \\ &= \sum_{P_i \in C_1{}'} t_i P_i + \sum_{P_i \in C_1{}'} t_i \tilde{P}_i + \sum_{P_i \in C_3} s_i P_i + \sum_{P_i \in C_3} s_i \tilde{P}_i - (*)\infty, \end{aligned}$$

wobei $t_i = n_i - m_i$ und $C_1{}' = \{P_i \in C_1; n_i > m_i\}$. Sei jetzt $b' = -h-b+sa'$, für ein $s \in \bar{k}$. Für $P_i = (x_i, y_i) \in C_1{}' \cup C_3$ gilt $b'(x_i) = -h(x_i) - b(x_i) + s(x_i)s'(x_i) = h(x_i) - y_i$. Dann folgt wie in dem Beweis vom Satz 3.25, dass

$$\begin{aligned} div(b'-Y) = &\sum_{P_i \in C_1{}'} 0P_i + \sum_{P_i \in C_1{}'} r_i \tilde{P}_i + \sum_{P_i \in C_3} 0P_i + \sum_{P_i \in C_3} w_i \tilde{P}_i \\ &+ \sum_{P_i \in C_4} z_i P_i - (*)\infty, \end{aligned}$$

wobei $r_i \geq t_i, w_i \geq s_i, w_i = 1$ falls $P_i \in C_3$, und $C_4 = C \setminus (C_1{}' \cup C_3 \cup \{\infty\})$. Letztendlich erhalten wir

$$\begin{aligned} div(a', b') &= \sum_{P_i \in C_1{}'} t_i \tilde{P}_i + \sum_{P_i \in C_3} s_i \tilde{P}_i - (*)\infty \\ &\sim - \sum_{P_i \in C_1{}'} t_i P_i - \sum_{P_i \in C_3} s_i P_i + (*)\infty \\ &= D - div(b-Y), \end{aligned}$$

woraus wir das Gewünschte $D \sim D'$ erhalten.

□

3.3 Beispiele

Wir betrachten die hyperelliptische Kurve $C : y^2 = x^7 + 7x^5 + 11x^3 + 5x$ vom Geschlecht drei über dem Körper $\mathbb{F}_{27}$.

Der Körper $\mathbb{F}_{27}$

0.	0	1.	ζ	2.	ζ^2
3.	ζ^2+2	4.	$\zeta^2+2\zeta+2$	5.	$2\zeta+2$
6.	$2\zeta^2+2\zeta$	7.	ζ^2+1	8.	$\zeta^2+\zeta+2$
9.	$2\zeta^2+2\zeta+2$	10.	$\zeta^2+2\zeta+1$	11.	$\zeta+2$
12.	$\zeta^{+}2\zeta$	13.	2	14.	2ζ
15.	$2\zeta^2$	16.	$2\zeta^2+1$	17.	$2\zeta^2+\zeta+1$
18.	$\zeta+1$	19.	$\zeta^2+\zeta$	20.	$2\zeta^2+2$
21.	$2\zeta^2+2\zeta+1$	22.	$\zeta^2+\zeta+1$	23.	$2\zeta^2+\zeta+2$
24.	$2\zeta+1$	25.	$2\zeta^2+\zeta$	26.	1

Hierbei bezeichnet ζ das Erzeugende von $\mathbb{F}_{27}$. In der folgenden Tabelle sind die Punkte von $C/\mathbb{F}_{27}$ dargestellt.

1.	$(0,0)$	2.	(ζ^2,ζ^7)	3.	(ζ^2,ζ^{20})	4.	(ζ^6,ζ)
5.	(ζ^6,ζ^{14})	6.	(ζ^{10},ζ^{11})	7.	(ζ^{10},ζ^{24})	8.	(ζ^{11},ζ^2)
9.	(ζ^{11},ζ^{15})	10.	(ζ^{12},ζ^{12})	11.	(ζ^{12},ζ^{25})	12.	(ζ^{14},ζ^6)
13.	(ζ^{14},ζ^{19})	14.	(ζ^{17},ζ^2)	15.	(ζ^{17},ζ^{15})	16.	(ζ^{18},ζ^7)
17.	(ζ^{18},ζ^{20})	18.	(ζ^{20},ζ^{12})	19.	(ζ^{20},ζ^{25})	20.	(ζ^{21},ζ^{13})
21.	(ζ^{21},ζ^{26})	22.	(ζ^{22},ζ^2)	23.	(ζ^{22},ζ^{15})	24.	(ζ^{26},ζ)
25.	(ζ^{26},ζ^{14})						

Beispiel 3.32 *Additionalgorithmus*

Seien

$$\begin{aligned} D_1 =& (\zeta^2,\zeta^7) + (\zeta^6,\zeta) + (\zeta^{14},\zeta^6) \\ D_2 =& (\zeta^2,\zeta^{20}) + (\zeta^6,\zeta^{14}) + (\zeta^{18},\zeta^{20}) \end{aligned}$$

gegeben. Die Einfachheit halber werden wir a, b, f statt $a(x), b(x), f(x)$ schreiben. Wir berechnen zuerst die zu D_1, D_2 zugehörige a_i-Polynome:

$$\begin{aligned} a_1 =& (x-\zeta^2)(x-\zeta^6)(x-\zeta^{14}) \\ a_2 =& (x-\zeta^2)(x-\zeta^6)(x-\zeta^{18}) \end{aligned}$$

Es gilt

$$d_1 = ggT(a_1,a_2) = (x-\zeta^2)(x-\zeta^6) = x^2 + \zeta x + \zeta^8 = \zeta^2 a_1 + 2\zeta^2 a_2$$

und

$$e_1 = \zeta^2, e_2 = 2\zeta^2.$$

Für die Polynome b_i erhalten wir

$$\begin{aligned} b_1 &= \zeta^9 x^2 + \zeta^2 x + \zeta \\ b_2 &= \zeta x^2 + \zeta^{10} x + \zeta^{12} \\ b_1 + b_2 &= \zeta^{20} x^2 + \zeta^{21} x + \zeta^2. \end{aligned}$$

Weiterhin gilt

$$d = ggT(d_1, b_1 + b_2) = x^2 + \zeta x + \zeta^8 = d_1$$

und aus $c_1 = \zeta^{13}$ und $c_2 = \zeta^{19}$ erhalten wir:

$$\begin{aligned} s_1 &= c_1 e_1 = \zeta^{15} \\ s_2 &= c_1 e_2 = \zeta^2 \\ s_3 &= c + 2 = \zeta^{19} \end{aligned}$$

Als Nächstes bestimmen wir die Polynome a, b, die zu dem Additionsdivisor $D = D_1 + D_2$ gehören.

$$\begin{aligned} a &= \frac{a_1 a_2}{d^2} = (x - \zeta^{14})(x - \zeta^{18}) = x^2 + \zeta^{13} x + \zeta^6 \\ b &= \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \mod a \\ &= \zeta^{19} x^5 + \zeta^7 x^4 + \zeta^{13} x^3 + \zeta^{24} x^2 + \zeta^6 x + \zeta^{15} \mod a \\ &= \zeta^{13}(x + \zeta^{12}). \end{aligned}$$

Als Ergebnis erhalten wir $D_1 + D_2 = D + div(a, b) = (\zeta^{14}, \zeta^6) + (\zeta^{18}, \zeta^{20})$.

Beispiel 3.33 *Reduktionsalgorithmus*

Sei $D = (\zeta^2, \zeta^7) + (\zeta^6, \zeta) + (\zeta^{14}, \zeta^6) + (\zeta^{18}, \zeta^{20})$. Dann gilt:

$$a = (x - \zeta^2)(x - \zeta^6)(x - \zeta^{14})(x - \zeta^{18}) = x^4 + \zeta^{11} x^3 + \zeta^5 x^2 + \zeta^5 x + \zeta^{14}$$

und

$$b = x^3 + \zeta^{23} x^2 + \zeta^{11} x + \zeta^{20}.$$

Um a' zu bestimmen, müssen wir zuerst $f - b^2$ berechnen.

$$b^2 = x^6 + \zeta^{10} x^5 + \zeta^6 x^4 + \zeta^5 x^3 + \zeta^{15} x^2 + \zeta^{18} x + \zeta^{14}$$

und

$$f - b^2 = x^7 + \zeta^{13} x^6 + \zeta^{15} x^5 + \zeta^{19} x^4 + \zeta^{19} x^3 + \zeta^2 x^2 + x + \zeta.$$

Dann gilt

$$a' = f - b \mod a = x^3 + \zeta^{14} x^2 + x + \zeta^{13}$$

und

$$b' = -b \mod a' = \zeta^{22} x^2 + \zeta^5 x + \zeta^2.$$

Nach Faktorisierung erhalten wir

$$a' = (x - \zeta^{12})^2(x - \zeta^2) = (x - x_1)(x - x_2)(x - x_3)$$

und nach Einsetzen in b' bestimmen wir

$$b'(x_1) = b'(x_2) = \zeta^{25},$$

$$b'(x_3) = \zeta^{20}.$$

Der reduzierte Divisor $D' = div(a', b')$ und $D' \sim D$ ist gleich $(\zeta^2, \zeta^{20}) + 2(\zeta^{12}, \zeta^{25})$.

3.4 Verbesserung

Die folgende Modifizierung des Cantorschen Algorithmus wird in *Hyperelliptic Curves and Cryptography* von M. Jacobson präsentiert. Sei $M(m)$ die Anzahl der notwendigen Operationen in k für die Multiplikation von zwei Polynomen vom höchsten Grad m. Dann hat der erweiterte euklidische Algorithmus eine Komplexität von $O(M(m)logm)$ Operationen in k. D.h. im Fall des Cantorschen Algorithmus erhalten wir für die Komposition zweier reduzierten Divisoren eine Komplexität von $(M(g)log(g))$ und für den Reduktionsalgorithmus $O(gM(g))$ Operationen in K, wobei g bezeichnet hier das Geschlecht der hyperelliptischen Kurve. Mit standarten Algorithmen für die Multiplikation von Polynomen beträgt die Komplexität der Komposition $O(g^2)$ Operationen und dieser der Reduktion $O(g^3)$.
Wir werden zuerst einige Vorschläge zur Verbesserung der Komposition angeben.
Die Komposition lässt sich unter der Beachtung der Rekursivität in der Definition von ggT dreier Polynome und der Fakt, dass a_1, a_2 im allgemein teilerfremd sind, vereinfachen. Seien $D_1 = div(a_1, b_1), D_2 = div(a_2, b_2)$ zwei semireduzierte Divisoren, definiert über k. Wir wollen ein semi-reduzierter Divisor $D = div(a, b)$,der über k definiert ist, ausrechnen. Für den gilt zusätzlich $D \sim D_1 + D_2$ in $Jac(k)$.
Algorithmus:

1. Seien $a_1 = a_2$, dann setze $d_1 = a_1$, $s_1 = 1$. Sonst benutze den halberweiterten euklidischen Algorithmus um $d_1, s_1 \in k[X]$ zu berechnen, so dass $d_1 = ggT(a_1, a_2) = s_1 a_1 + t_1 a_2$, für ein $t_1 \in k[x]$ ist.

2. Ist $deg(d_1) = 0$, dann setze $d_1 = 1, c_1 = d_1^{-1}, c_3 = 0$. Sonst benutze den erweiterten euklidischen Algorithmus um $d, s_2, t_2 \in k[x]$ zu berechnen, so dass $d = ggT(d_1, b_1 + b + 2 + h) = s_2 d_1 + t_2(b_1 + b_2 + h)$ ist. Dann berechne $c_1 = s_1 s_2$ und setze $c_3 = t + 2$.

3. $D = div(a, b)$ ist somit mittels

$$a := \frac{a_1 a_2}{d^2},$$

$$b := \frac{b_1 + (c_1 a_1 (b_2 - b_1) + c_3(f - b_1 h - b_1^2))}{d} \pmod a$$

definiert.

Wir haben in dem ersten Schritt im Fall $a_1 \neq a_2$ nur den halb-erweiterten euklidischen Algorithmus benutzt. Für zufällige semi-reduzierte Divisoren erwarten wir, dass d_1 Konstante ist und es bleibt uns nur c_1, c_2 zu bestimmen.
Als nächstes werden wir die Reduktion vereinfachen. Sei $D = div(a, b)$ ein semi-reduzierter Divisor definiert über k. Wir werden einen Divisor $D' = div(a', b')$ bestimmen, der reduziert ist und gleichzeitig äquivalent zu D.
Am Anfang setzen wir $a_0 = a, b_0 = b$.

1. Berechne $a_1 = (f - hb_0 - b_0^2)/a_0$ und bestimme $q_1, b_1 \in k[x]$, so dass $-h - b = q_1 a_1 + b_1, deg b_1 < deg a_1$ gilt. Sei $div(a_1, b_1)$ ein reduzierter Divisor, d.h. $deg(a_1) \leq g$, dann setzen wir $i = 1$ und vergessen Schritt 2.

2. Für $i \geq 2$ berechnen wir $a_i, b_i, q_1 \in K[X]$, so dass

   $$a_i = a_{i-2} + q_{i-1}(b_{i-1} - b_{i-2})$$

   und

   $$-h - b_{i-1} = q_i a_i + b_i, deg(b_i) < deg(a_1).$$

   Wir rechnen soweit $deg(a_i) \leq g$ für $i \geq 2$.

3. Setze $b' = b_i$ und normiere a_i um a' zu erhalten.

Für ungerade $char(k)$ berechnet der optimisierte Verfahren das Gruppengesetz in $17g^2 + O(g)$ Operationen in k. Die Verdoppelung braucht dann $16g^2 + O(g)$ Operationen. Für $char(k) = 2$ sind die ensprechenden Operationen $14g^2 + O(g)$ bzw. $11g^2 + O(g)$.

3.5 Binäre quadratische Formen

Um die Grundideen im Cantorschen Algorithmus besser erklären zu können, werden wir den Begriff der binären quadratischen Formen einführen.
Bei der Bearbeitung des Kapitels habe ich die Ideen und Konstruktion von *Binary Quadratic Forms* von D. Buell haupsächtlich befolgt.

Definition 3.34 *Seien $a, b, c \in \mathbb{Z}$ drei ganze Zahlen. Dann heißt*

$$(x, y) = ax^2 + bxy + cy^2$$

binäre quadratische Form auf $\mathbb{Z}$.

Zu jeder binären quadratischen Form lassen sich folgende Elemente eindeutig zuordnen:

1. Die Zahl $\Delta_f := b^2 - 4ac$ heißt Diskriminante von f.

2. Die Matrix $M_f := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ heißt Darstellungsmatrix von f.

3. Die Zahl $\tau_f := \frac{-b+\sqrt{\Delta_f}}{2a}$ heißt die zu f gehörige algebraische Zahl.

Weiterhin werden wir für binäre quadratische Formen die folgende Schreibweise verwenden: $f = (a, b, c)$.
Eine solche Form lässt sich offenbar immer als Produkt zweier homogener linearer Funktionen von X, Y darstellen:

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

Die vier Grössen $\alpha, \alpha', \beta, \beta'$ sind natürlich durch (a, b, c) nicht eindeutig bestimmt. Wenn $a \neq 0$, dann lässt sich f z.B. so zerlegen:

$$f(x, y) = \left(\sqrt{a}x + \frac{b + \sqrt{b^2 - 4ac}}{2\sqrt{a}}y)(\sqrt{a}x + \frac{b - \sqrt{b^2 - 4ac}}{2\sqrt{a}}y\right).$$

Definition 3.35 *Zwei binäre quadratische Formen f, g heißen äquivalent bezüglich $SL(2, \mathbb{Z})$ genau dann, wenn $f = Mg$ für eine unimodulare Matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Hierbei ist $g(x_1, y_1)$ eine binäre quadratische Form mit $x = \alpha x_1 + \beta y_1$ und $y = \gamma x_1 + \delta y_1$.*

Satz 3.36 *Äquivalente quadratische Formen haben die gleiche Diskriminante.*

Beweis: Sei

$$\Delta_f = b^2 - 4ac$$

und

$$M_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Es gilt $det M_f = ac - \frac{b^2}{4}$ und somit $\Delta_f = -4 det M_f$. Sei jetzt N eine unimodulare Matrix:

$$N = \begin{pmatrix} m & n \\ p & q \end{pmatrix}, \quad mit \quad mq - np = 1$$

Dann gilt für die zu (a, b, c) äquivalente quadratische Form $g = Nf$.

$$M_g = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} = \begin{pmatrix} m & n \\ p & q \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

Und für die Determinanten erhalten wir

$$det M_g = det N \cdot det M_f = (mq - np) \cdot det M_f = 1 \cdot det M_f \quad oder$$

$$-4 det M_g = -4 det M_f \quad und \quad \Delta_{f'} = \Delta_f.$$

□

Satz 3.37 *Sei Δ die Diskriminante von f und $\Delta > 0$, dann nimmt $f(x, y)$ für geeignete reelle x_0, y_0 sowohl positive wie auch negative Werte an.*
Ist aber $\Delta < 0$, so ist entweder für alle reellen x_0, y_0 der Wert von $f(x_0, y_0) \geq 0$ oder für alle reellen x_0, y_0 gilt $f(x_0, y_0) \leq 0$ und $f(x_0, y_0) = 0$ nur für $x_0 = 0$, $y_0 = 0$.

Beweis: Wir betrachten die Zerlegung

$$af(x, y) = (ax + \frac{b}{2}y) - \frac{D}{4}y^2.$$

Ist nun $D = b^2 - 4ac < 0$, so muss $a \neq 0$ sein und aus der Gleichung folgt $af(x, y) \geq 0$, wobei das Gleichheitszeichen nur für $y = 0$ und $ax + \frac{b}{2}y = 0$ gilt, d.h. $x = y = 0$. Dabei hat $f(x, y)$ stets das Vorzeichen von a, wenn $x^2 + y^2 \neq 0$.
Ist dagegen $D > 0$ und $a \neq 0$, dann ist $af(b, -2a) = -Da < 0$, also nimmt f beide Vorzeichen an und kann offenbar auch für reelle x, y Null sein, ohne dass beide x, y verschwinden.
Ist $D > 0$ und $a = 0$, so zeigt die Gleichung

$$f(x, y) = y(bx + cy)$$

die Richtigkeit der Behauptung.

□

Bemerkung 3.38 *Die Form f ist indefinit, für $\Delta > 0$ und definit für $\Delta < 0$. In letzterem Fall positiv definit, falls $f(x, y) \geq 0$ und negativ definit, falls $f(x, y) \leq 0$.*

3.5.1 Reduktion von binären quadratischen Formen

Definition 3.39 *Eine binäre quadratische Form $f = (a, b, c)$ heißt primitiv, falls $ggT(a, b, c) = 1$.*

Wir betrachten zunächst nur positiv definite Formen und suchen eine kanonische Darstellung für alle positiv definiten binären quadratischen Formen.

Definition 3.40 *Eine binäre quadratische Form wird als reduziert bezeichnet, falls $|b| \leq a \leq c$.*

Satz 3.41 *Sei $f = (a, b, c)$ eine reduzierte Form zur Diskriminante $\Delta_f = -D$, $D > 0$, dann gilt $|b| \leq \sqrt{\frac{D}{3}}$.*

Beweis: $4b^2 \leq 4ac = b^2 + D$, woraus folgt $3b^2 \leq D$.

□

Satz 3.42 *Die Anzahl der reduzierten binären quadratischen Formen zur gegebenen Diskriminante ist endlich.*

Beweis: Nach Satz 3.41 gibt es nur endlich viele Möglichkeiten für b und jedes solche b bestimmt nach Faktorisierung eine endliche Menge von Werten für a, c wegen $4ac = b^2 + D$.

□

Satz 3.43 *Jede binäre quadratische Form f zur Diskriminante $-D$ ist äquivalent zu genau einer reduzierten Form derselben Diskriminante.*

Beweis: Sei $f = (a, b, c)$ eine binäre quadratische Form zur Diskriminante $-D$. Ist f nicht reduziert, dann existiert eine ganze Zahl δ mit $|-b + 2c\delta| \leq |c|$. Wir erhalten aus $f = (a, b, c)$ durch die folgende Transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -y' \\ x + \delta y' \end{pmatrix}$$

$$\begin{aligned} ax^2 + bxy + cy^2 &= ay'^2 - by'(x' + \delta y') + c(x' + \delta y')^2 \\ &= cx'^2 + y'x'(-b + 2c\delta) + (c\delta^2 - b\delta + a)y'^2, \end{aligned}$$

dass $f = (a, b, c)$ zu der Form $f' = (a', b', c') = (c, -b + 2c\delta, c\delta^2 - b\delta + a)$ äquivalent ist. Somit haben wir $|b'| \leq a'$ gezeigt.
Falls noch gilt $a' \leq c'$, so ist die Reduktion beendet. Sonst wiederholen wir den Algorithmus. Da wir nur bei der Bedingung $c' < a' = c$ den Prozess fortsetzen können und es gilt $a > 0, c > 0$, wird der Algorithmus nach endlich vielen Schritten enden.

□

Satz 3.44 *Mit Ausnahme von*

1. $(a, b, a) \sim (a, -b, a)$
2. $(a, a, c) \sim (a, -a, c)$

sind keine verschiedenen reduzierten Formen äquivalent.

Beweis: Seien $(a, b, c), (a', b', c')$ äquivalente Formen. Dann gilt:
Es existiert eine unimodulare Matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

mit

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Dies ergibt für die Koeffizienten von $f'(x', y') = a'x'^2 + b'x'y' + cy'^2$

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$$

$$b' = b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta)$$
$$c' = a\beta^2 + b\beta\delta + c\delta^2.$$

Im Fall, dass $a \geq a'$ ist, haben wir $a \geq a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a(\alpha^2 + \gamma^2) + b\alpha\gamma \geq a(\alpha^2 + \gamma^2) - a|\alpha\gamma| \geq a|\alpha\gamma|$ und da α, γ ganze Zahlen sind, erhalten wir nur die folgenden Möglichkeiten für $(\alpha, \gamma) : (0, \pm 1), (\pm 1, 0), (\pm 1, \pm 1)$, wobei die Vorzeichen in den Tupeln unabhängig sind. Der Fall $a' \geq a$ wird analog behandelt.
Wir betrachten dann die folgenden Fälle.

1. $\alpha = \pm 1, \gamma = 0$. Dann gilt $(a, b, c) \sim (a, \delta\alpha b + 2a\beta, *) = (a, b + 2a\beta, *)$, wegen $\alpha\delta = 1$ und $*$ lässt sich aus der Determinante ablesen. Aus $|b| \leq a$ und $|b \pm 2ab| \leq a$ folgt $\beta = 0$ und die beiden Formen sind identisch, oder $\beta = \pm 1$ und es gilt $(a, a, c) \sim (a, -a, c)$.

2. Sei $\alpha = 0, \gamma = \pm 1$. Dann ist $(a, b, c) \sim (c, -b \pm 2cd, *)$. Aus $|b| \leq a < c$ für die beiden mittleren Koeffizienten folgt $\delta = 0, -1, 1$.
Sei $\delta = 0$, dann sind (a, b, c) und $(c, -b, a)$ beide reduziert, was zu $a = c$ führt und somit ist $(a, b, c) \sim (a, -b, a)$.
Ist $\delta = \pm 1$, dann haben wir $(a, c, c) \sim (c, -c, a)$, aber wegen $a \leq c$ und $c \leq a$ gilt $(a, a, a) \sim (a, -a, a)$.

3. $\alpha = \pm 1, \gamma = \pm 1$
Hier haben wir $a \geq a' \geq a|\alpha\gamma| = a$ und es folgt $a = a' = a \pm b + c$. Damit erhalten wir $(a', b', c') = (a, b, \pm b)$ und weil die Form reduziert ist, muss gelten $a = \pm b$. Die reduzierten äquivalenten Formen sind (a, a, a) und $(a, -a, a)$.

□

Somit erhalten wir den folgenden Satz:

Satz 3.45 *Jede binäre quadratische Form zur Diskriminante $-D < 0$ ist äquivalent zu genau einer reduzierten Formen unter Berücksichtigung der oberen beiden Ausnahmen.*

Als Nächstes betrachten wir indefinite Formen, d.h. $\Delta_f = D, D > 0$. Wir wollen wieder zu jeder Äquivalenzklasse eine kanonische Form konstruieren. In diesem Fall aber liegen mehrere reduzierte Formen in einer Klasse.

Definition 3.46 *Eine indefinite binäre quadratische Form heißt reduziert, falls $0 < b < \sqrt{D}$ und $\sqrt{D} - b < 2|a| < \sqrt{D} + b$ gilt.*

Satz 3.47 *Falls (a, b, c) eine reduzierte binäre quadratische Form ist, dann gilt:*

$$\sqrt{D} - b < 2|c| < \sqrt{D} + b.$$

Beweis: $b^2 = 4ac + D$ und somit erhalten wir

$$(\sqrt{D} - b)(\sqrt{D} + b) = -4ac = (2|a|)(2|c|).$$

Da aber $0 < b < \sqrt{D}$ und $\sqrt{D} - b < \sqrt{D} + b$ und wir uns in der Situation $xy = zw$ mit $x < z < y$ befinden, erhalten wir $x < w < y$ und somit auch die Behauptung.

□

Satz 3.48 *Wie bei positiv definiten quadratischen Formen, ist die Anzahl der reduzierten binären quadratischen Formen zur gegebenen Diskriminante endlich.*

Beweis: Die Anzahl der Werte von b ist nach Satz 3.47 endlich und somit auch die Anzahl der verschiedenen Faktorisierungen von $4ac = b^2 - D$. Aus diesen Beobachtungen folgt die Behauptung des Satzes.

□

Satz 3.49 *Jede indefinite Form ist äquivalent zur reduzierten Form derselben Diskriminante.*

Beweis: Wir betrachten den folgenden Reduktionsalgorithmus:
Sei (a, b, c) eine nicht reduzierte Form. Dann existiert ein eindeutiges δ, so dass $\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D}$ und wir erhalten nach Transformation analog zu positiven binären quadratischen Formen:

$$(a, b, c) \sim (c, -b + 2c\delta, a - b\delta + c\delta^2)$$

Ist $|a - b\delta + c\delta^2| < |c|$, so wiederholen wir den Schritt. Wie bei den definiten Formen endet das Prozes nach endlich vielen Schritten, wobei wir eine Form (a, b, c) mit $|a| \leq |c|$ und $\sqrt{D} - 2|a| < b < \sqrt{D}$ gefunden haben. Dann gilt $\sqrt{D} - b < 2|a|$. Aus $|\sqrt{D} - b||\sqrt{D} + b| = 4|a||c|$ erhalten wir $|\sqrt{D} + b| > 2|c|$, woraus $|\sqrt{D} + b| > 2|c| > 2|a| > \sqrt{D} - b$ folgt. Wegen $|\sqrt{D} + b| > \sqrt{D} - b$ gilt, dass $b > 0$ und $0 < b < \sqrt{D}$ und dass (a, b, c) reduziert ist.

□

Definition 3.50 *Zwei reduzierte Formen $(a, b, a'), (a', b', c')$ gleicher Diskriminante heißen benachbart, falls $b + b' \equiv 0 \pmod{2a'}$.*

Satz 3.51 *Die Menge der reduzierten Formen zur vorgegebenen Diskriminante lässt sich in Zyklen von benachbarten Formen unterteilen.*

Beweis: Sei (a, b, c) eine beliebige reduzierte Form. (c, b', c') sei eine zu (a, b, c) und (c', b'', c'') eine zu (c, b', c') benachbarte Form. Wir konstruieren rekursiv zu der vorherigen benachbarten Formen. Da die Menge der reduzierten Formen

endlich ist, muss auch die Folge nacheinander benachbarter Formen zurück auf die ursprüngliche Form führen. Eine solche Folge von reduzierten Formen nennen wir Zyklus. Falls es keine weiteren reduzierten Formen gibt, dann ist der Prozess beendet. Sonst wählen wir eine noch nicht verwendete Form und wiederholen ihn.
Da die nacheinander benachbarten Formen äquivalent unter der Transformation

$$\begin{pmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a} \end{pmatrix}$$

sind und jede Äquivalenzrelation transitiv ist, folgt, dass die Formen in jedem Zyklus äquivalent untereinander sind.

□

Satz 3.52 *Zwei reduzierte Formen sind äquivalent genau dann, wenn sie in dem gleichen Zyklus liegen.*

Beweis: [Buell]

□

3.5.2 Kompositionsalgorithmus für binäre quadratische Formen

In diesem Teil werden wir eine Operation, die sogenannte Komposition, auf der Menge der binären quadratischen Formen zu gegebener Diskriminante definieren. Mit Hilfe der Komposition wird diese Menge zu einer abelschen Gruppe. Die Struktur und Existenz der Gruppe wurde zuerst von Gauß entdeckt und studiert in seinem Werk *Disquisitiones Arithmeticae.*

Satz 3.53 *Seien $f_1 = (a_1, b_1, c_1)$ und $f_2 = (a_2, b_2, c_3)$ zwei binäre quadratische Formen der Diskriminante Δ. Es werden $\beta = \frac{(b_1+b_2)}{2}$ und $n = ggT(a_1, a_2, \beta)$ definiert und die Zahlen t, u, v so gewählt, dass $a_1 t + a_2 u + \beta v = n$. Seien weiterhin*

$$A = \frac{a_1 a_2}{n^2}$$

und

$$B = \frac{a_1 b_2 t + a_2 b_1 u + v(b_1 b_2 + \Delta)/2}{n}$$

gegeben. Dann ist B Lösung von

$$\frac{a_1 B}{n} \equiv \frac{a_1 b_2}{n} \pmod{2A}$$
$$\frac{a_2 B}{n} \equiv \frac{a_2 b_1}{n} \pmod{2A}$$
$$\frac{\beta B}{n} \equiv \frac{b_1 b_2 + \Delta}{2n} \pmod{2A}$$

und die Form $(\frac{a_1 a_2}{n^2}, B, \frac{B^2-\Delta}{4A})$ ist die Komposition von f_1 und f_2 [Buell].

Beweis: Aus $\Delta = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$ erhalten wir

$$\frac{(b_1+b_2)}{2}\frac{(b_1-b_2)}{2} = a_1c_1 - a_2c_2$$

oder äquivalent dazu

$$\frac{(b_1+b_2)}{2n}\frac{(b_1-b_2)}{2} = \frac{a_1c_1}{n} - \frac{a_2c_2}{n}.$$

Daraus folgt, dass jeder gemeinsame Faktor von $\frac{a_1}{n}$ und $\frac{a_2}{n}$ auch $\frac{(b_1-b_2)}{2}$ teilt und das Kongruenzsystem

$$B \equiv \frac{b_1}{2} \mod \frac{a_1}{n}$$

$$B \equiv \frac{b_2}{2} \mod \frac{a_2}{n}$$

eine Lösung hat. Die Zahlen, welche die erste Kongruenz erfüllen, sind $b_1 + \delta_1\frac{a_1}{n}$. Dies ist eine Lösung der zweiten Kongruenz genau dann, wenn $\frac{b_1-b_2}{2} \equiv -\delta_1\frac{a_1}{n} \mod \frac{a_2}{n}$ lösbar ist. Dies gilt, falls $ggT(\frac{a_1}{n},\frac{a_2}{n})|\frac{(b_1-b_2)}{2}$, was vorausgesetzt war. Nach entsprechender Multiplikation erhalten wir, dass B die folgenden Kongruenzen erfüllt:

$$\frac{a_2B}{n} \equiv \frac{a_2b_1}{n} \mod \frac{a_1a_2}{n^2}$$

$$\frac{a_1B}{n} \equiv \frac{a_1b_2}{n} \mod \frac{a_1a_2}{n^2}$$

Es bleibt zu zeigen, dass B Lösung der dritten Kongruenz ist. Dafür betrachten wir

$$\begin{aligned}\frac{b_1b_2+\Delta}{2n} &= \frac{b_1b_2+b_1^2-4a_1c_1}{2n}\\ &= \frac{b_1a_2}{a_2n}\frac{(b_1+b_2)}{2} - \frac{2a_1a_2}{n}\frac{c_1}{a_2}\end{aligned}$$

Es folgt

$$\begin{aligned}\frac{b_1b_2+\Delta}{2n} &\equiv \frac{b_1a_2}{a_2n}\frac{(b_1+b_2)}{2} \mod \frac{2a_1a_2}{n^2}, \quad a_2 = nk\\ &\equiv \frac{Ba_2}{n}\frac{1}{a_2}\frac{(b_1+b_2)}{2} \mod \frac{2a_1a_2}{n^2}\\ &\equiv \frac{B\beta}{n} \mod \frac{2a_1a_2}{n^2}.\end{aligned}$$

Sei

$$B = \frac{a_1b_2t + a_2b_1u + \frac{(b_1b_2+\Delta)}{2}}{n},$$

dann ist B Lösung des gegebenen Kongruenzsystems.
Weiterhin gilt für die binären quadratischen Formen f_1, f_2

$$\begin{aligned} f_1 f_2 &= (a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2)(a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2) \\ &= (AX^2 + BXY + CY^2) \end{aligned}$$

unter der Berücksichtigung der Transformation

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} n & \frac{(b_2-B)n}{2a_2} & \frac{(b_1-B)n}{2a_1} & \frac{(b_1b_2+\Delta-B(b_1+b_2))n}{4a_1a_2} \\ 0 & \frac{a_1}{n} & \frac{a_2}{n} & \frac{b_1+b_2}{2n} \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}.$$

□

Satz 3.54 *Seien f_1, f_2 und f_3, f_4 zwei Paare von binären Formen gleicher Diskriminante, mit $ggT(a_1, a_2, \frac{b_1+b_2}{2}) = 1$ und $ggT(a_3, a_4, \frac{b_3+b_4}{2}) = 1$, für die gilt $f_1 \sim f_3$ und $f_2 \sim f_4$. Dann folgt*

$$f_1 \circ f_2 \sim f_3 \circ f_4.$$

Hierbei bezeichnet $f_1 \circ f_2$ die in dem vorigen Satz definierte Komposition der binären Formen f_1, f_2 mit gleicher Diskriminante.

Beweis: [Buell]

□

Dieser Satz zeigt, dass die durch die Komposition von quadratischen Formetimmte Klasse nur von den Äquivalenzklassen der jeweiligen Formen abhängt. Es gilt noch:

$$(1, b_1, c_1) \circ (a_2, b_2, c_2) \sim (a_2, b_2, c_2)$$
$$(a, b, c) \circ (a, -b, c) \sim (a, b, c) \circ (c, b, a) \sim (ac, b, 1)$$

Satz 3.55 *Die Gruppe der Äquivalenzklassen binärer quadratischer Formen zu gegebener Diskriminante Δ bildet unter der Komposition von Formen eine endliche abelsche Gruppe. Die Identität der Gruppe ist die Form $(1, 0, \Delta)$ und die inverse Form ist $(a, -b, c)$.*

3.6 Die Idee des Cantorschen Algorithmus

Der Cantorsche Algorithmus, *Computing in the Jacobian of a Hyperelliptic Curve* D. Cantor, 1994, ist derzeit das effizienteste Verfahren für Reduktion und Addition in den Jacobischen Varietäten von hyperelliptischen Kurven beliebigen Geschlechtes. Der ist eine neue Methode, die sich wesentlich von der geometrischen Addition von Punkten elliptischer Kurven unterscheidet. Auf diese Weise eignen sich auch hyperelliptische Kurven höheren Grades für kryptographische Zwecke. Im praktischer Hinsicht interessant sind nur Kurven vom Geschlecht

$g(C) = 2$ oder 3, da für die anderen Werte von $g(C)$ erfolgrei-chen Angriffsalgorithmen bekannt sind. Mittels Cantorsches Algorithmus lassen sich auch hyperelliptische Kurven in kryptographische Verfahren wie El Gamal, Schnorr oder Diffie-Hellman implementieren. Die höhere Sicherheit dieser Methoden beruht auf dem Problem des diskreten Logarithmus. Die Suche nach neuen Kurven, geeignet für die Kryptographie, entspricht eigentlich der Suche nach neuen abelschen Gruppen, in denen das Diskrete-Logarithmus-Problem schwer zu lösen ist. Eine große Menge solcher Gruppen lässt sich unter den Jacobischen Varietäten algebraischer Kurven finden. Deswegen sind Algorithmen wie der Cantorsche von großer Bedeutung, da sie eine explizite Darstellung der Gruppenoperation ermöglichen.
Die Konstruktion des Cantorschen Algorithmus beruht auf zwei großen Ideen. Die erste davon ist die Darstellung jedes Divisors mittels Koordinatenfunktionen. Die zweite Idee ist die Übertragung der schon bekannten Gausschen Reduktion und Komposition binärer quadratischer Formen auf die Menge der Koordinatenfunktionen.
Die Anwendung von Koordinatenfunktionen ist eigentlich eine alte, aber nicht häufig benutzte Idee. Die Korrespondenz zwischen den Divisoren D und Tripeln (a, b, c) von Polynomialfunktionen in $\mathfrak{L}(D)$ transformiert die Divisoren in Punkte einer Varietät, für welche die Koeffizienten von (a, b, c) Koordinaten sind. Diese Konstruktion wird explizit in *Tata Lectures on Theta II* von Mumford erläutert.
Mumford betrachtet eine hyperelliptische Kurve $C : y^2 = f(x)$ und definiert die Menge der zugelassenen Divisoren vom Grad r als

$$Div_0^{+,r}(C) := \{D \in Div^{+,r}(C) | D = \sum_{i=1}^{r} P_i, P_i \neq P_\infty \quad P_i \neq \iota P_j\},$$

wobei ι die kanonische Involution bezeichnet. Dann werden zu jedem Divisor $D \in Div_0^{+,r}$drei Polynome assoziiert:

1. $a(x) = \prod_{i=1}^{r}(x - x_i)$
2. $b(x) = \sum_{i=1}^{r} y_i \frac{\prod_{i \neq j}(x - x_i)}{\prod_{i \neq j}(x_i - x_j)}$, für verschiedene P_i
3. $c(x)$ mit $f(x) - b(x)^2 = a(x)c(x)$.

Dabei bezeichnen $(x_i, y_i), i = 1, ..., r$ die Koordinaten der Punkte P_i aus $supp(D)$. Es lassen sich die folgenden Eigenschaften nachweisen:

1. $b(x) \in k[x]$, k der Grundkörper, ist das eindeutige Polynom mit $degb(x) < dega(x)$ und $b(x_i) = y_i, i - 1, ..., r$.
2. $a(x)|(f(x) - b(x)^2)$

Das Tripel (a, b, c) heißt Repräsentation eines Punktes der Varietät $Div_0^{+r}(C)$. Andersseits existiert zu vorgegebenen drei Polynomen mit den oben aufgezählten Eigenschaften ein eindeutiger Divisor $D \in Div_0^{+r}(C)$. Wir erhalten somit eine bijektive Korrespondenz

$$\{D \in Div_0^{+r}(C)\} \Leftrightarrow \{(a,b,c) \in k[x] \times k[x] \times k[x] \quad wie \quad oben \quad definiert\}$$

Wenn wir diese Konstruktion des Tripels (a,b,c) mit dem im den Cantorschen Algorithmus angegebenen (a,b) vergleichen, sehen wir, dass es sich hier um ein und dieselbe Konstruktion handelt. Die Existenz von c wird in dem Verfahren von D. Cantor durch die Bedingung $a(x)|f(x) - b(x)^2$ äquivalent ersetzt. Entsprechend ist das Interpolationspolynom $b(x)$ nur durch seine Charakteristiken angegeben und nicht in Lagrangescher Form. Somit werden auch bei dem Cantorschen Algorithmus die Divisoren $D \in Div_0^{+,r}(C)$ zu Punkten einer Varietät mit Koordinaten die Koeffizienten von (a,b,c).
Diese Korrespondenz liegt nicht nur dem in diesem Kapitel beschriebenen Algorithmus zu Grunde. In *Efficient Reduction on the Jacobian Variety of Picard Curves* J. Estrada, 1998, werden auf eineindeutige Weise jedem zugelassenen Divisor drei Polynomialfunktionen zugeordnet. Die gleiche hilfreiche Konstruktion habe ich bei der Definition des Reduktions- und Additionsalgorithmus für nicht hyperelliptische Kurven in dem lezten Kapitel befolgt.
Nachdem jeder Divisor D mittels Polynomialtripels (a,b,c) dargestellt wird, werden die Reduktions- und Additionsalgorithmen ensprechend der bekannten Verfahren für binäre quadratische Formen konstruiert.
Seien $f_1 = (a_1, b_1, c_1)$ und $f_2 = (a_2, b_2, c_2)$ zwei binäre quadratische Formen mit ganzen Koeffizienten und Diskriminante $\Delta = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$. In seinem Algorithmus betrachtet Cantor die Divisoren $D_1 = div(a_1(x), b_1(x))$ und $D_2 = div(a_2(x), b_2(x))$, welche den angegebenen Formen f_1, f_2 entsprechen. Hierbei wird das Polynom $c_i = \frac{b_i(x)^2 - f(x)}{4a_i(x)}$ nur formal eingeführt. Als Analogon für die Diskriminante Δ wird $f(x) \in k[x]$ betrachtet. Bei der Konstruktion des Additionsalgorithmus verwendet Cantor die Kompositionsformel für die binären quadratischen Formen f_1, f_2.

Komposition von BQF	**Cantorscher Algorithmus Addition**
$f_1 \circ f_2 = (A,B,C)$	$D_1 + D_2 = (A(x), B(x))$
$A = \frac{a_1 a_2}{n^2}$	$A(x) = \frac{a_1(x)a_2(x)}{n^2}$
$B = \frac{a_1 b_2 t + a_2 b_1 u + (b_1 b_2 + \Delta)v}{n}$	$B(x) = \frac{a_1(x)b_2(x)t + a_2(x)b_1(x)u + (b_1(x)b_2(x)+f)v}{n}$
$C = \frac{B^2 - \Delta}{4A}$	
$n = ggT(a_1, a_2, b_1 + b_2)$	$n = ggT(a_1(x), a_2(x), b_1(x) + b_2(x))$
$n = a_1 t + a_2 u + (b_1 + b_2)v$	$n = a_1(x)t + a_2(x)u + (b_1(x) + b_2(x))v$

Wir sehen, dass es sich hier um eine formale Übertragung der Kompositionsformel auf die Koordinatendarstellung der Divisoren handelt. Anders sieht es bei dem Reduktionsalgorithmus aus. In beiden Fällen wird das gleiche Ziel verfolgt, aber diesmal mit anderen Mitteln. Die Reduktion von positiv definiten binären quadratischen Formen erfolgt in $\mathbb{Z}$ und der Zweck hierbei ist die Verkleinerung von b, so dass $|b| \leq |a| \leq |c|$ erreicht wird. Dies geschieht, indem von b eine geeignete Zahl δc subtrahiert wird. Somit erhalten wir eine Verminderung bezüglich der Betragnorm. Anders sieht es bei dem Cantorschen Algorithmus aus. In diesem Fall wird die Reduktion im Ring $k[x]$ durchgeführt. Das Ziel ist wiederum eine Verkleinerung aber diesmal von $deg(D)$. Wir mini-mieren den Grad von D, indem wir $deg(a(x)) = deg(D)$ reduzieren. Das erfolgt entsprechend durch Polynomdivision. Bei der Subtraktion und bei der Polynomdivision müssen bestimmte Bedingungen beachtet werden. In dem zahlentheoretischen Fall ist dies $a|b^2 - \Delta$ und in dem funktionentheoretischen $a(x)|f(x) - b(x)^2 = N(b(x) - y)$. Wir sehen, dass die Diskriminantenbedingung durch eine Normenbedingung ersetzt wird.
In der folgenden Tabelle wird ein Vergleich zwischen den beiden Reduktionsalgorithmen dargestellt:

Gausssche Reduktion für quadratische Formen	**Cantorscher Algorithmus Reduktion**
Algorithmus	**Algorithmus**
0. Ist $\|c\| \leq \|a\|$ dann $a \leftrightarrow c$, $b' = -b$ $(a^*, b^*, c^*) = (c, -b, a)$	
1. während $\|a^*\| \leq \|c^*\|$ $\delta := [\frac{-b^*}{2c^*}]$ $b' = b^* - 2c^*\delta$ $a' = a^* + \delta(b' + \delta c^*)$	1. während $deg(a(x)) > g$ $b(x)' = -b(x) \mod a'(x)$ $a'(x) = \frac{f(x)-b(x)^2}{a}$
2. Ist $\|c'\| \leq \|a'\|$, dann $a = a', b = b', c = c'$ und gehe zu 1.	2. Ist $deg(a(x)) > g(C)$, dann $a(x) = a'(x), b(x) = b'(x)$ und gehe zu 1.
	3. Normierung von $a'(x)$
Ausgabe	**Ausgabe**
$(a', b', c') = (c, -b + 2c\delta, a - b\delta + c\delta^2)$	$div(a'(x), b'(x)) \sim div(a(x), b(x))$
$(a, b, c) \sim (a', b', c')$ unter	
$T = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$	
Diskriminantenbedingung	**Normbedingung**
$a \| b^2 - \Delta$	$a(x) \| b(x)^2 - f(x)$
Auswirkung der Determinantenbedingung auf Subtraktion	**Auswirkung der Normbedingung auf Polynomendivision**
$a' = c, b' = -b + 2acd$ der Faktor $2c\delta$ wird um $a' \| b'^2 - \Delta$ zu erreichen	$a'(x) = \frac{f(x)-b(x)^2}{a(x)} \in k[x]$,da $a(x) \| b(x)^2 - f(x)$ damit gilt $a'(x) \| bi(x)^2 - f(x)$
Verkleinerung von $\|b\|$	**Verkleinerung von** $deg(a(x))$
Austausch $a \leftrightarrow c$	**Kein Austausch** $c(x)$ wird nur formal betrachtet

In seinem Algorithmus hat Cantor die Idee der Gaussschen Reduktion für positive binäre quadratische Formen übernommen und entsprechend der Polynomeneigenschaften implementiert. Dabei ist eine effiziente Methode mit praktischer Anwendung entstanden.

In diesem Kapitel wurde ein Reduktions- und Additionsalgorithmus in der jacobischen Varietät von nicht hyperelliptischen Kurvenfamilien vom Geschlecht 3 definiert. Die Idee hierfür ist eine Fortsetzung der geometrischen Addition von Punkten einer elliptischen Kurve [Koblitz] oder einer hyperelliptischen Kurve vom Geschlecht 2 [Lauter]. Die entsprechende arithmetische Reduktion erfolgt mit Hilfe des eingeführten Koordinatensystems wie in den *Thata Lectures on Theta II* von Mamford. Der Reduktionsalgorithmus ist von kleinerer Komplexität, da höchstens lineare $4 \times 4-$Gleichungssysteme zu lösen sind, und lässt sich mittels symbolischer Sprachen wie MAPLE IX einfach implementieren. Bei der Konstruktion des Algorithmus bin ich ausgegangen, von dem Reduktionsalgorithmus für Picard Kurven, dargestellt in *Efficient Reduction on the Jacobian Variety of Picard Curves* von J. Estrada.

4 Reduktions- und Additionsalgorithmus auf nicht hyperelliptischen Kurven

4.1 Nicht hyperelliptische Kurven

Aus Kapitel 1 wissen wir, dass jede Kurve C vom Geschlecht $g > 1$, für die eine Abbildung $f : C \to \mathbb{P}^1$ vom Grad 2 existiert, hyperelliptisch heißt. Im Bezug auf diese Definition können wir jetzt nicht hyperelliptische Kurven definieren.

Definition 4.1 *Sei C eine Kurve vom Geschlecht $g > 1$. Dann heißt C nicht hyperelliptisch, falls keine Abbildung $f : C \to \mathbb{P}^1$ vom Grad 2 existiert.*

Bemerkung 4.2 *Es existieren nicht hyperelliptische Kurven jedes Geschlechtes $g \geq 3$ [Hartshorne].*

Satz 4.3 *Sei C eine nicht hyperelliptische Kurve vom Geschlecht $g \geq 3$. Dann ist die kanonische Abbildung $\varphi : C \to \mathbb{P}^{g-1}$ eine Einbettung. Die Kurve $\varphi(C) \subset \mathbb{P}^{g-1}$ heißt die kanonische Kurve von C und ist vom Grad $2g - 2$.*
Im Fall $g = 3$ ist $\varphi(C) \subset \mathbb{P}^2$ eine nicht singuläre Quadrik. Gilt umgekehrt, dass $X \subset \mathbb{P}^2$ eine nicht singuläre Quadrik ist, dann ist $X = \varphi(C)$ die kanonische Kurve einer nicht hyperelliptischen Kurve vom Geschlecht 3. [Hartshorne]

Sei $\mathbb{F}_q$ ein endlicher Körper der $char(\mathbb{F}_q) \neq 2$ und $\bar{\mathbb{F}}_q$ sein algebraischer Abschluss. Weiterhin werden wir die folgenden glatten Kurvenfamilien betrachten:

$$\begin{aligned} A: &\quad y^4 = p_4(x,z) = x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \\ B: &\quad y^4 = p_3(x,z) = x^3z + b_2x^2z^2 + b_1xz^3 + b_0z^4 \end{aligned}$$

Die Kurven aus A und B sind Quadriken in $\mathbb{P}^2$ und somit nach dem vorigen Satz kanonische Kurven zweier Familien nicht hyperelliptischer Kurven vom Geschlecht 3.

Bemerkung 4.4 *Nach der Plückerformel für glatte Kurven in $\mathbb{P}^2$ gilt:*

$$g(C) = \frac{(degC - 1)(degC - 2)}{2} = \frac{3 \cdot 2}{2} = 3, C \in A, B$$

Sei jetzt C eine Kurve aus der Familie A. Dann ist

$$C: \quad y^4 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

die affine Darstellung von C. Nach Translation erhalten wir die äquivalente Kurve

$$C': \quad y^4 = x^4 + a'_3x^3 + a'_2x^2 + a'_1x.$$

C' lässt sich birational zu der Kurve C'' transformieren:

$$C'' : \quad \frac{y^4}{x^4} = 1 + a'_3 \frac{1}{x} + a'_2 \frac{1}{x^2} + a'_1 \frac{1}{x^3}$$

$$u := \frac{y}{x}, v := \frac{1}{x}$$

$$C'' : \quad u^4 = a''_1 v^3 + a''_2 v^2 + a''_3 v + 1.$$

Die letzte Kurvengleichung ist nach Normierung in die Gleichung

$$C'' : \quad u^4 = p_3(w) = w^3 + c_2 w^2 + c_1 w + c_0$$

überführbar. Somit ist jede glatte Kurve aus Familie A birational äquivalent zu einer Kurve aus Familie B. Auf Grund dessen, werden wir von nun an nur Kurven aus der Kurvenfamilie B betrachten.
Ist $\mathbb{F}_q = \bar{\mathbb{F}}_q$, dann hat die Kurve

$$C : \quad y^4 = p_3(x, z) = x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4$$

vier Verzweigungspunkte $V_1, ..., V_4$ bezüglich der Überlagerung

$$\pi : C \to \mathbb{P}^1$$

$$(x : y : z) \mapsto x.$$

Es gilt $V_i = (v_i : 0 : 1)$, $i = 1, 2, 3$, wobei v_i die Nullstellen von $p_3(x)$ sind und $V_4 = P_\infty = (1 : 0 : 0)$ der unendliche Punkt von C.
Sei jetzt ϱ eine primitive vierte Einheitswurzel. Dann lässt sich der folgende Automorphismus von C definieren:

$$\sigma : C \to C$$

$$(x : y : z) \mapsto (x : \varrho y : z),$$

wobei gilt

$$\sigma^4 = id_C.$$

Definition 4.5 *Zwei Punkte $P_1, P_2 \in C$ heißen konjugiert, falls $P_1 = \sigma(P_2)$ oder $P_1 = \sigma^2(P_2)$ oder $P_1 = \sigma^3(P_2)$.*

Die letzten Punkte spielen eine wichtige Rolle in dem Reduktionsalgorithmus.

Definition 4.6 *Sei D ein effektiver Divisor vom Grad ≥ 3. D heißt kollinear, falls es drei Punkte $P_1, P_2, P_3 \in supp(D)$ gibt, so dass eine Gerade g existiert mit $(g)_0 \geq P_1 + P_2 + P_3$. Sonst heißt D generischer Divisor.*

Definition 4.7 *Ein affiner, effektiver Divisor D heißt semireduziert, falls kein Punkt $P \in supp(D)$ existiert, so dass $D \geq P + \sigma P + \sigma^2 P + \sigma^3 P$. D wird reduziert genannt, falls zusätzlich $deg(D) \leq g$ gilt, mit $g = g(C)$.*

Wir bezeichnen mit

$$\begin{aligned} Div^{+,i} = & \{D \in Div(C); \\ & D \quad \mathbb{F}_q - rational, \quad effektiv, \quad semireduziert \quad vom \quad Grad \quad i\} \end{aligned}$$

die Menge der effektiven semireduzierten Divisoren vom Grad i. Desweiteren führen wir die folgenden Begriffe ein:
Sei $f \in \mathbb{F}_q[x,y]$. Wir nennen den Term $a_{i_*,j_*}x^{i_*}y^{j_*}$ Hauptterm von f, falls

$$\nu_{P_\infty}(f) := min_{i,j}\nu_{P_\infty}(a_{i,j}x^iy^j) = \nu_{P_\infty}(a_{i_*,j_*}x^{i_*}y^{j_*})$$

gilt. Für eine Polynomialfunktion f, die zu dem Funktionenkörper von C gehört definieren wir

$$deg_{P_\infty}(f) := deg_{P_\infty}\left(\sum_{i,j} a_{i,j}x^iy^j\right) = max_{i,j}(4i+3j).$$

Wir berücksichtigen dabei $\nu_{P_\infty}(x) = -4$ und $\nu_{P_\infty}(y) = -3$.
Sei jetzt $D \in Div(C)$ ein Divisor vom Grad i, wobei i die Werte 2, 3 oder 4 annimmt. Wir assoziieren zu jedem Divisor D eine Quadrik $q_D(x,y) = a_{20}x^2 + a_{10}x + a_{11}xy + a_{01}y + a_{02}y^2 + a_{00}$ von minimaler Bewertung in P_∞. Es soll weiterhin gelten $(q_D(x,y))_0 \geq D$ und der Koeffizient des Hauptterms von q_D ist gleich eins. Nach dem folgenden Satz existiert eine solche Quadrik immer.

Satz 4.8 *Sei $D \in Div(C)$ mit $2 \leq deg(D) \leq 4$, dann gilt:*

1. *Sei $deg(D) = 2$, dann folgt $a_{02} = a_{11} = a_{20} = 0$.*
2. *Sei $deg(D) = 3$, dann folgt $a_{11} = a_{20} = 0$ und $\nu_{P_\infty}(q_D) = -6$.*
3. *Sei $deg(D) = 4$, dann folgt $a_{20} = 0$ und $\nu_{P_\infty}(q_D) = -7$.*

Beweis: Wir betrachten die folgenden Fälle:

1. $deg(D) = 2$: Es existiert immer eine Gerade durch zwei Punkte. Diese Gerade hat auch den kleinsten Grad in P_∞ und istsomit gleich q_D. Wir erhalten $a_{02} = a_{11} = a_{20} = 0$.
2. $deg(D) = 3$: Durch drei nicht kollineare Punkte verläuft stets eine Quadrik, welche die unendlich ferne Gerade in einem Punkt P_∞ tangiert. Affin geo-
metrisch bedeutet, dass eine Parabel durch die drei Punkte existiert, deren Symmetrie-Achse parallel zu $\vec{OX}$ ist und welche die unendlich ferne Gerade in $(1:0:0)$ tangiert. Aus $P_\infty = (1:0:0) \in q_D$ erhalten wir $a_{20} = 0$ und nach Ausrechnen der Ableitungen bekommen wir zusätzlich $a_{11} = 0$. Somit gilt $\nu_{P_\infty} = -6$.

3. $deg(D) = 4$: Es lässt sich nur eine Quadrik durch vier Punkte zeichnen, welche die unendlich ferne Gerade in einem Punkt berührt. Aus $P_\infty = (1 : 0 : 0) \in q_D$ folgt $a_{20} = 0$ und $\nu_{P_\infty}(q_D) = -7$.

□

Von nun an können wir annehmen, dass $a_{20} = 0$ und dass q_D die folgende Form für jeden Divisor $D \in Div(C)$ hat:

$$q_D(x, y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}.$$

Lemma 4.9 *D sei ein Divisor in $Div(C)$ mit $3 \leq deg(D) \leq 4$. Dann sind die folgenden Aussagen äquivalent:*

1. *$q_D(x, y)$ ist linear oder zerfällt in lineare Faktoren.*
2. *$D + P_\infty$ ist kollinear.*
3. *$q_D(x, y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$ mit $a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a_{10} = 0$.*

Beweis: ($1 \Rightarrow 3$) Falls q_D eine Gerade ist, dann gilt $a_{11} = a_{02} = 0$ und offensichtlich auch $a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a_{10} = 0$.
Ist aber $deg(q_D) = 2$, dann zerfällt q_D in lineare Faktoren. Das ist äquivalent zu:

$$4 \cdot det \begin{pmatrix} 0 & \frac{a_{11}}{2} & \frac{a_{10}}{2} \\ \frac{a_{11}}{2} & a_{02} & \frac{a_{01}}{2} \\ \frac{a_{10}}{2} & \frac{a_{01}}{2} & a_{00} \end{pmatrix} = 0$$

Nach Ausrechnen erhalten wir für die obige Determinante das gewünschte $a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a_{10} = 0$.
($3 \Rightarrow 2$) Es gilt $a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a_{10} = 0$. Dann betrachten wir die folgenden Fälle:

1. Ist $a_{11} = a_{02} = 0$, dann ist $q_D(x, y) = a_{10}x + a_{01}y + a_{00}$ eine Gerade.
2. Ist $a_{11} = a_{10} = 0$, dann ist $q_D(x, y) = a_{02}y^2 + a_{01}y + a_{00} = g_1 g_2$ ein Produkt von zwei Geraden.
3. Ist $a_{11} \neq 0$, dann erhalten wir aus $a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a_{10} = 0$

   $$\frac{a_{10}a_{02}}{a_{11}} + \frac{a_{11}a_{00}}{a_{10}} = a_{01}.$$

   Beim Einsetzen in q_D bekommen wir

   $$\left(a_{02}y + a_{11}x + a_{01} - \frac{a_{02}a_{10}}{a_{11}}\right)\left(y + \frac{a_{10}}{a_{11}}\right) = g_1 g_2.$$

In jedem der Fälle ist q_D ein Produkt von Geraden. Ist $D \in Div^{+,4}(C)$, dann enthält $D + P_\infty$ fünf Punkte. Mindestens drei davon müssen zu einer Geraden gehören. Ist $D \in Div^{+,3}(C)$, dann gilt das gleiche diesmal aber für $D + 2P_\infty$.
($2 \Rightarrow 1$) Gilt nach dem Satz von Bezout.

□

Lemma 4.10 *Sei $D \in Div(C)$ mit $2 \leq deg(D) \leq 4$ und q_D sei die zu D assoziierte Quadrik. Gilt für die Punkte $P, \sigma P, \sigma^2 P \in q_D$, dann gilt dies auch für $\sigma^3 P$.*

Beweis: $q_D(x,y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$.
Wir setzen die Koordinaten von $P, \sigma P, \sigma^2 P, \sigma^3 P$ in die Gleichung von q_D ein:

$$\begin{aligned}
A: &\quad a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00} = 0 \\
B: &\quad a_{02}\varrho^2 y^2 + a_{01}\varrho y + a_{11}x\varrho y + a_{10}x + a_{00} = 0 \\
C: &\quad a_{02}y^2 + a_{01}\varrho^2 y + a_{11}x\varrho^2 y + a_{10}x + a_{00} = 0 \\
D: &\quad a_{02}\varrho^2 y^2 + a_{01}\varrho^3 y + a_{11}x\varrho^3 y + a_{10}x + a_{00} = c,
\end{aligned}$$

wobei c eine Konstante ist. Nach Substrahieren erhalten wir:

$$\begin{aligned}
D - B: &\quad a_{11}xy(\varrho^3 - \varrho) + a_{01}y(\varrho^3 - \varrho) = c \\
C - A: &\quad a_{11}xy(\varrho^2 - 1) + a_{01}y(\varrho^2 - 1) = 0
\end{aligned}$$

Damit bekommen wir

$$D - B: \quad \varrho(a_{11}xy(\varrho^2 - 1) + a_{01}y(\varrho^2 - 1)) = \varrho(A - C) = 0.$$

Daraus folgt, dass $c = 0$ und $\sigma^3 P$ ein Punkt der Quadrik q_D ist, was zu zeigen war.

□

Lemma 4.11 *Hat $y^4 - p_3(x) = 0$ drei verschiedene Nullstellen, dann können die Punkte $P_1 = (x_1, y), P_2 = (x_2, y)$ und $P_3 = (x_3, y)$ nicht gleichzeitig zu einer irreduziblen Quadrik gehören, die von x abhängig ist.*

Beweis: Sei $q = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$ mit $a_{11}y + a_{10} \neq 0$. Dann erhalten wir für x den eindeutigen Wert $x = -\frac{a_{02}y^2 + a_{01}y + a_{00}}{a_{11}y + a_{10}}$. Somit müssen die Werte von x_1, x_2, x_3 zusammenfallen.

□

Weiterhin betrachten wir die Abbildung

$$\begin{aligned} \Phi : Div^{+,i} &\to \mathbb{F}_q[x] \times \mathbb{F}_q[x,y] \times \mathbb{F}_q[y], \quad 2 \le i \le 4 \\ \Phi(D) &= (u_D(x), q_D(x,y), w_D(y)), \quad mit \\ u_D(x) &:= \prod_{P_i \in supp(D)} (x - x_i) \\ w_D(y) &:= \prod_{P_i \in supp(D)} (y - y_i) \quad und \\ q_D &:= a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}, \end{aligned}$$

die Quadrik durch $P_i \in supp(D)$ kleinster Bewertung in P_∞ mit normiertem Hauptkoeffizient.
Wir betrachten die folgenden Divisoren:

$$\begin{aligned} D_1 &= (x_1 : y_1 : 1) + (x_2 : y_1 : 1) + (x_3 : y_2 : 1) \\ D_2 &= (x_1 : y_1 : 1) + (x_3 : y_1 : 1) + (x_2 : y_2 : 1) \\ D_3 &= (x_1 : y_1 : 1) + (x_2 : y_1 : 1) + (x_3 : y_2 : 1) + (x_1 : y_2 : 1) \\ D_4 &= (x_1 : y_1 : 1) + (x_3 : y_1 : 1) + (x_2 : y_2 : 1) + (x_1 : y_1 : 1), \end{aligned}$$

wobei x_1, x_2, x_3 die verschiedenen Nullstellen von $p_3(x) = y_1^4$ und $y_1 = \varrho^k y_2, k = 1, 2, 3$ sind. In diesem Fall gilt $\Phi(D_1) = \Phi(D_2)$ und analog $\Phi(D_3) = \Phi(D_4)$, d.h. die Divisoren haben das gleiche Bild unter Φ. Deswegen betrachten wir die folgende Menge:

$$\begin{aligned} \cup_{i=2}^4 Div_0^{+,i}(C) := \{D \in Div^{+,i}(C); & D \in Div^{+,2}, D \ne (x_1, y_1) + (x_2, y_1), \\ & D \in Div^{+,3}, D \ne (x_1, y_1) + (x_2, y_1) + (x_3, y_3), \\ & mit \quad y_1 \ne y_3 \\ & D \in Div^{+,4}, D \ne P_1 + P_2 + P_3 + P_4 \quad mit \\ & y_{P_1} = y_{P_2} = y_{P_3}, y_{P_1} \ne y_{P_2} \quad oder \\ & y_{P_1} = y_{P_2}, y_{P_3} = y_{P_4}, y_{P_1} \ne y_{P_2}\} \end{aligned}$$

Satz 4.12 *Sei $\bar{\mathbb{F}}_q$ der algebraische Abschluss von $\mathbb{F}_q$. Dann ist*

$$\Phi : \cup_{i=2}^4 D_0^{+,i}(C/\bar{\mathbb{F}}_q) \to \Phi(\cup_{i=2}^4 D_0^{+,i}(C/\bar{\mathbb{F}}_q))$$

eine Bijektion.

Beweis:

1. Sei $D \in Div_0^{+,2}, Div_0^{+,3}, Div_0^{+,4}$ und sei $D + P_\infty$ generisch. Nach Lemma 4.9 erhalten wir dann, dass $q_D(x,y)$ eine Quadrik (oder Gerade) ist mit $a_{11}y_i + a_{10} \ne 0$, wobei y_i die $y-$Koordinaten von $P_i \in supp(D)$bezeichnen. Wir erhalten die $y-$Koordinaten der Punkte $P_i \in supp(D)$ nach Faktorisierung von $w_D(y)$. Durch Einsetzen bestimmen wir eindeutig die entsprechenden $x-$Koordinaten.

2. Sei $D = P_1+P_2+P_3+P_4$, mit P_1, P_2, P_3 kollinear und $P_4 \neq \sigma^i(P_j), \quad i,j = 1,2,3$. Dann gilt $q_D(x,y) = g_1(x,y)(y-y_4)$, wobei $(g_1)_0 \geq P_1 + P_2 + P_3$, $g_1 = ax + by + c, a \neq 0$. Nach Faktorisierung von $w_D(y)$ und Einsetzen in $g_1(x,y)$ bekommen wir die $y-$ und die entsprechenden $x-$Koordinaten von P_1, P_2, P_3. Die $x-$Koordinate von P_4 lässt sich als Nullstelle des linearen Polynoms
$$p = \frac{u_D(x)}{(x-x_1)(x-x_2)(x-x_3)}$$
gewinnen.

   Der Fall $q_D(x,y) = g_1g_2 = ay^2 + by + c = (y-y_1)(y-y_2), y_1 \neq y_2$ ist nach der Definition der betrachteten Divisoren nicht zugelassen.
   Das gleiche gilt, falls $deg(D) = 2,3$.

3. Sei jetzt D generisch, aber $D + P_\infty$ sei kollinear. Nach Lemma 4.9 zerfällt $q_D(x,y)$ in lineare Faktoren. $D = P_1 + P_2 + P_3 + P_4$ ist aber generisch und somit dürfen keine drei Punkte zu der gleichen Geraden gehören, d.h. o.B.d.A. $P_1, P_2 \in g_1(x,y)$ und $P_3, P_4 \notin g_1(x,y)$ mit $q_D(x,y) = g_1(x,y)(y-y_3)$.
   Durch $(y-y_3) = 0$ ist $y = y_3$ eindeutig bestimmt. Es bleiben die Möglichkeiten $P_3 = (x_3, y_3)$ und $P_4 = (x_4, y_3)$, wobei x_3, x_4 Nullstellen von $y_3^4 = p_3(x)$ sind.
   Die y-Koordinaten von P_1, P_2 lassen sich als Nullstellen von
$$p = \frac{w_D(y)}{(y-y_3)^2}$$
ermitteln. Nach Einsetzen in $g_1(x,y)$ erhalten wir die Werte x_1, x_2. Danach bestimmen wir die restliche $x-$Koordinaten x_3, x_4 als Nullstellen des Polynoms
$$p = \frac{u_D(x)}{(x-x_1)(x-x_2)}.$$
   Wie in 2) ist der Fall $g_1(x,y) \in \mathbb{F}_q[y]$ unmöglich.

Somit haben wir bewiesen, dass wir aus $\bar{D} = (u_D, q_D, w_D)$ auf eindeutige Weise den Divisor D rekonstruieren können.
Die Surjektivität ist klar.

$\square$

4.2 Reduktionalgorithmus in der jakobischen Varietät von $y^4 = p_3(x,z) = x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$

In diesem Teil werden wir einen Reduktionsalgorithmus für effektive Divisoren in der jakobischen Varietät von $y^4 = p_3(x,z) = x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$ vorstellen. Die Idee dabei ist eine Fortsetzung der geometrischen Addition von

Punkten elliptischer Kurven. Da wir in diesem Fall eine Kurvenfamilie vom Geschlecht 3 haben und somit eine wesentlich kompliziertere Struktur, können wir nicht wie in dem bekannten Fall mit Sekanten oder Tangenten arbeiten. Wir werden mit Hilfe von zwei Quadriken zuerst den Grad unseres Divisors verkleinern und danach das Ïnverseëines Zwischendivisors bestimmen. Dabei müssen wir die folgende Aufgabe lösen:

Problem: Gegeben sei ein affiner effektiver Divisor $D \in Div(C)$. Unter affiner Divisor verstehen wir einen Divisor D mit $P_\infty \notin supp(D)$. Unser Ziel ist es einen äquivalenten effektiven Divisor D' zu finden mit $deg(D') \leq 3$ und $D - deg(D)P_\infty \sim D' - deg(D')P_\infty$.

Reduktionsalgorithmus: Sei $D = P_1 + P_2 + P_3 + P_4 \in Div(C)$ ein affiner Divisor. Dann betrachten wir die folgenden Fälle:

1. D sei kollinear. Dann ist D ein kanonischer Divisor, d.h. Schnittdivisoren einer Geraden mit C [Estrada] und $D - 4P_\infty \sim 0$.

2. Sonst müssen wir die Interpolationsquadrik von $D - 4P_\infty$ bestimmen. Nach dem Satz von Bezout wird C von q_D in höchstens noch drei Punkten.

$$(q_D) = P_1 + P_2 + P_3 + P_4 + Q_1 + Q_2 + Q_3 - 7P_\infty$$

oder

$$(q_D) = (D - 4P_\infty) + (D' - 3P_\infty), \quad D' = Q_1 + Q_2 + Q_3$$

und

$$D - 4P_\infty \sim -(D' - 3P_\infty).$$

Jetzt müssen wir das Inverse von D' bestimmen. Dafür berechnen wir die Interpolationsquadrik von $D' + 2P_\infty$. Nach dem Satz von Bezout schneidet $q_{D'}$ die Kurve C in höchstens noch drei Punkten. Dann gilt

$$(q_{D'}) = Q_1 + Q_2 + Q_3 + T_1 + T_2 + T_3 - 6P_\infty$$

äquivalent zu

$$(q_{D'}) = (D' - 3P_\infty) + (D'' - 3P_\infty), \quad D'' = T_1 + T_2 + T_3$$

und

$$D' - 3P_\infty \sim -(D'' - 3P_\infty).$$

Wir erhalten somit

$$D - 4P_\infty \sim D'' - 3P_\infty.$$

$D'' - 3P_\infty$ heißt die Reduktion von $D - 4P_\infty$.

4.2 Reduktionalgorithmus in der jakobischen Varietät von $y^4 = p_3(x,z) = x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$

Sei jetzt $D \in Div(C)$ ein effektiver Divisor vom Grad $deg(D) > 4$. Dann lässt sich D darstellen als $D = D_0 + E_0 + E_1 + ... + E_{N-1}$. E_i sind effektive Divisoren, zusammengestellt aus den restlichen Punkten $P_i \in supp(D)$, so dass $deg(D_{3j}) = 4$ erreicht wird, und $deg(D_0) = 4$. Wir können den oben beschriebenen Reduktionalgorithmus zuerst auf D_0 anwenden. Somit erhalten wir an Stelle von D_0 zwei Divisoren D_1, D_2, welche den oben definierten D', D'' entsprechen und D_2 ist die Reduktion von D_0. Damit haben wir durch äquivalente Umformungen den Grad von D verkleinert. Wir wenden die gleiche Prozedur auf den neuen Divisor. An Stelle von D_0 reduzieren wir diesmal zuerst $D_2 + E_0$ mit $deg(D_2 + E_0) = 4$.
Wir setzen diese Reduktion iterativ fort bis wir einen reduzierten Divisor D_{3N+2} bekommen. Innerhalb der Iteration erhalten wir eine Kette von Divisoren:

$$D_0, D_1, D_2, D_3, ..., D_{3j}, D_{3j+1}, D_{3j+2}, ..., D_{3N}, D_{3N+1}, D_{3N+2}.$$

Je drei davon $(D_{3j}, D_{3j+1}, D_{3j+2})$ entsprechen genau einem Reduktions- und somit auch Iterationsschritt.

$$D_{3j} := D_{3(j-1)+2} + E_{(j-1)}, \quad j = 1, ..., N$$
$$D_{3j} - 4P_\infty \sim -(D_{3j+1} - deg(D_{3j+1})P_\infty) \sim D_{3j+2} - deg(D_{3j+2})P_\infty$$

mit $0 \leq deg(D_{3j+1}),\ deg(D_{3j+2}) \leq 3$, $deg(D_{3j}) = 4$ und $deg(E_{(j-1)}) = 4 - deg(D_{3j+2})$.
Nach Durchlaufen der Iterationskette erhalten wir

$$D - deg(D)P_\infty \sim D_{3N+2} - deg(D_{3N+2})P_\infty,$$

d.h. D_{3N+2} ist die Reduktion von D.
Sind die Divisoren $D_j, \quad j = 1, ..., 3N+2$ in $Div_0^{+,i}(C), \quad i = 2,3,4$, dann können wir ihre Koordinaten $\bar{D}_j = (u_{D_j}, q_{D_j}, w_{D_j})$ ausrechnen. Demnach erhalten wir für die oben definierte Folge die Koordinatendarstelung:

$$\bar{D}_0, \bar{D}_1, \bar{D}_2, \bar{D}_3, ..., \bar{D}_{3j}, \bar{D}_{3j+1}, \bar{D}_{3j+2}, ..., \bar{D}_{3N}, \bar{D}_{3N+1}, \bar{D}_{3N+2}.$$

Als Nächstes wollen wir die einzelnen Schritte, bei der Berechnung der oben definierten Iterationsfolge beschreiben. Unser Ziel dabei wird D_j, oder falls $D \in Div_0(C)$ $\bar{D}_j$, auszurechnen. Bei jedem der Rekursionsschritte werden wir höchstens ein 4×4 lineares Gleichungssystem ausrechnen müssen. Es werden keine Faktorisierungen durchgeführt. Insgesamt erhalten wir einen effizienter Reduktionsalgorithmus von kleinerer Komplexität.

Satz 4.13 *Sei $\bar{D}_{3j+1}$ gegeben, dann lässt sich $\bar{D}_{3j+2}$ wie folgt bestimmen:*

$$\begin{aligned} q_{3j+2} &= q_{3j+1} \\ u_{3j+2} &= \left(\frac{R_y(q_{3j+1}, C)}{u_{3j+1}}\right)^* \\ w_{3j+2} &= \left(\frac{R_x(q_{3j+1}, C)}{w_{3j+1}}\right)^*. \end{aligned}$$

Hierbei bezeichnen $q_{3j+1}, u_{3j+1}, w_{3j+1}$ die Koordinaten von D_{3j+1}. Das gleiche gilt für die Koordinaten von D_{3j+2}. $()^*$ bedeutet, dass der betroffene Term normiert wird. Falls q_{3j+1} unabhängig von x ist, gilt

$$w_{3j+2} = w_{3j+1}.$$

Beweis: Die Gleichheiten für u_{3j+1} und w_{3j+2} sind nach der geometrischen Konstruktion klar.
Es bleibt zu zeigen:

$$q_{3j+2} = q_{3j+1}.$$

Nach Konstruktion gilt $deg(D_{3j+1}) < deg(D_{3j}) = 4$ und falls $deg(q_{3j}) > 1$ ist, gilt wegen $deg_{P_\infty}(q_{3j}) > deg_{P_\infty}(q_{3j+1})$ $\nu_{P_\infty}(q_{3j+1}) \geq -6$ und $deg(D_{3j+1}) > 1$.

1. $deg(w_{3j+1}) = 3$. Dann sind die Punkte in $supp(D_{3j+1})$ nicht kollinear (Beweis durch Annahme des Gegenteils). Es gilt $deg(q_{3j+1}) = 2$, d.h. $y^2 \in q_{3j+1}$ und $\nu_{P_\infty}(q_{3j+1}) = -6$. $q_{3j+1} = Q_1 + Q_2 + Q_3 + T_1 + T_2 + T_3 - 6P_\infty$ mit $D_{3j+1} = Q_1 + Q_2 + Q_3 - 3P_\infty$ und $D_{3j+2} = T_1 + T_2 + T_3 - 3P_\infty$ und es gilt $q_{3j+2} = q_{3j+1}$.

2. $deg(w_{3j+1}) = 2$. D_{3j+1} besteht nur aus zwei Punkten. Dann enthält die Quadrik kleinster Bewertung in P_∞, gleichzeitig D_{3j+1} und D_{3j+2}. D.h. $w_{3j+2} = w_{3j+1}$. ($q_{3j+1} = Q_1 + Q_2 + T_1 + T_2 - 4P_\infty$).

□

Satz 4.14 *Sei $D_{3j} \in Div^{+,4}$, dann lassen sich die folgenden Koordinatendarstellungen der Divisoren explizit bestimmen:*

1. *$\bar{D}_{3j}$, falls $D_{3j} \in Div_0^{+,4}$.*

2. *$\bar{D}_{3j+1}$ und $\bar{D}_{3j+2}$, falls $D_{3j} \notin Div_0^{+,4}$.*

Beweis:

1. $D_{3j} \in Div_0^{+,4}$ und $q_{3j}(x, y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$. Wir bestimmen u_{3j} und w_{3j} wie im Satz 4.13. Da der Hauptkoeffizient von q_{3j} normiert ist, müssen wir nur noch die restlichen vier Koeffizienten bestimmen. Diese erhalten wir als Lösung des linearen Gleichungssystems

$$q_{3j}(P_i) = 0, \quad i = 1, 2, 3, 4, \quad D_{3j} = P_1 + P_2 + P_3 + P_4.$$

2. $D_{3j} \notin Div_0^{+,4}$ und es gilt $D = P_1 + P_2 + P_3 + P_4$ mit

   (a) $P_1 = (x_1, y_1), P_2 = (x_2, y_1), P_3 = (x_3, y_1), P_4 = (x_4, y_2)$ mit $y_1 \neq y_2$ oder

   (b) $P_1 = (x_1, y_1), P_2 = (x_2, y_1), P_3 = (x_3, y_2), P_4 = (x_4, y_2)$ mit $y_1 \neq y_2$.

(a) Nach geometrische Konstruktion besteht die Quadrik q_{3j} aus zwei Geraden $g_1 = (y - y_1)$ und g_2 die Gerade durch P_4, P_∞. Unter der Berücksichtigung der Bewertung von q_{3j} in P_∞ erhalten wir, dass die beiden Geraden einen gemeinsamen Punkt P_∞ haben. Somit enthält der Schnitt von g_1, g_2 und C noch zwei gemeinsamen Punkte. Da $P_\infty \in g_1$ und jede Gerade maximal vier Schnittpunkte mit C haben kann, erhalten wir $Q_1, Q_2 \in g_2$. Es gilt $y_{Q_1} = y_{Q_2} = y_2$ und x_{Q_i} sind die Nullstellen von
$$p = \frac{Res_y(C, g_2)}{(x - x_4)}.$$
Die Quadrik q_{3j+1} von $D_{3j+1} = Q_1 + Q_2$ ist gleich die Gerade durch Q_1, Q_2. Da $q_{3j+1} = q_{3j+2}$ gilt, erhalten wir $D_{3j+2} = P_4$.

(b) Wir untersuchen jetzt den zweiten Fall. Hierbei gilt $q_{3j} = g_1g_2 = (y-y_1)(y-y_2)$ und die beiden Geraden haben P_∞ als gemeinsammen Punkt. D.h. in dem Durchschnitt von $(g_1 \cap C) \cup (g_2 \cap C)$ bleiben noch zwei weitere Punkte Q_1, Q_2. Es gilt $y_{Q_1} = y_1$ und $y_{Q_2} = y_2$. Die entsprechenden $x-$Koordinaten erhalten wir als Nullstellen von:
$$p = \frac{Res_y(g_1, C)}{(x - x_1)(x - x_2)} \quad bzw. \quad p = \frac{Res_y(g_2, C)}{(x - x_3)(x - x_4)}.$$
Die Quadrik q_{3j+1} von dem Divisor $D_{3j+1} = Q_1 + Q_2$ ist gleich die Gerade durch Q_1 und Q_2. Der Divisor $D_{3j+2} = T_1 + T_2$ besteht aus den anderen zwei Schnittpunkten von q_{3j+1} und C.

□

Satz 4.15 *$\bar{D}_{3j} = (u_{3j}, q_{3j}, w_{3j})$ seien die Koordinaten von $D_{3j} \in Div_0^{+,4}(C)$. Dann können wir die Divisoren bzw. die Koordinaten in einer der folgenden Fälle explizit angeben.*

1. *$\bar{D}_{3j+1} = (u_{3j+1}, q_{3j+1}, w_{3j+1})$ und $\bar{D}_{3j+2} = (u_{3j+2}, q_{3j+2}, w_{3j+2})$, mit q_{3j+1} bzw. q_{3j+2}.*
2. *Wir können D_{3j+2} explizit ausrechnen.*

Beweis:

1. Sei $q_{3j}(x,y)$ linear. Dann sind die Punkte in $supp(D_{3j})$ kollinear und aus $D_{3j} - 4P_\infty \sim 0$ folgt $D_{3j+2} = 0$.

2. Sei $q_{3j}(x,y)$ eine Quadrik, die nicht in lineare Faktoren zerfällt, d.h. $q_{3j}(x,y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$ mit $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} \neq 0$.
   Wir berechnen u_{3j+1}, w_{3j+1} nach Satz 4.13.
   Um $q_{3j+1}(x,y) = b_{02}y^2 + b_{01}y + b_{10}x + b_{00}$ zu bestimmen, müssen wir ein 4×4 lineares Gleichungssystem lösen. Zu beachten ist, dass wegen

$deg_{P\infty}(q_{3j}) > deg_{P\infty}(q_{3j+1})$ $b_{11} = 0$ gilt und wir müssen nur die vier Koeffizienten b_{02}, b_{01}, b_{10} und b_{00} berechnen.
Es gilt

$$R_x(q_{3j}, q_{3j+1}) = \lambda w_{3j+1}, \lambda \neq 0$$

und

$$\begin{aligned} R_x(q_{3j}, q_{3j+1}) = &- b_{10}a_{02}y^2 - b_{10}a_{01}y - b_{10}a_{00} + b_{02}y^3a_{11} + b_{02}a_{10}y^2 \\ &+ b_{01}a_{11}y^2 + b_{01}a_{10}y + b_{00}a_{11}y + b_{00}a_{10} \\ \lambda w_{3j+1} = \ & s_3y^3 + s_2y^2 + s_1y + s_0. \end{aligned}$$

Nach Koeffizientenvergleich erhalten wir das folgende Gleichungssystem:

$$\begin{pmatrix} a_{11} & 0 & 0 & 0 \\ a_{10} & a_{11} & -a_{02} & 0 \\ 0 & a_{10} & -a_{01} & a_{11} \\ 0 & 0 & -a_{00} & a_{10} \end{pmatrix} \begin{pmatrix} b_{02} \\ b_{01} \\ b_{10} \\ b_{00} \end{pmatrix} = \begin{pmatrix} s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix}$$

Die Determinante der Matrix ist $-a_{11}(a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10})$. Sie ist nach Voraussetzung ungleich Null. Somit bekommen wir eine eindeutige Lösung für die Koeffizienten von q_{3j+1}. Durch die Auswahl von λ lässt sich q_{3j+1} zusätzlich normieren.

3. $q_{3j}(x,y)$ ist eine Quadrik, die in lineare Faktoren zerfällt.

$$q_{3j}(x,y) = g_1(x,y)(y+\frac{a_{10}}{a_{11}}) = (a_{02}y+a_{11}x+a_{01}-\frac{a_{02}a_{10}}{a_{11}})(y+\frac{a_{10}}{a_{11}}), a_{11} \neq 0$$

(Nach dem Satz 4.12 ist die andere Faktorisierung, d.h. $g_1(x,y)$ unabhängig von x nicht zugelassen.)

   (a) Sei $(y + \frac{a_{10}}{a_{11}})^2 | w_{3j}$. Dann ist $D_{3j} = P_1 + P_2 + P_3 + P_4$ mit $P_3 = (x_3, y_3), P_4 = (x_4, y_3)$ mit $y_3 = -\frac{a_{10}}{a_{11}}$ und x_3, x_4 Nullstellen von $y_3^4 = p_3(x)$. Unser Ziel hierbei ist, $\bar{D}_{3j+1}$ zu bestimmen.
   Wir berechnen nach Satz 4.13 u_{3j+1}, w_{3j+1}. Offensichtlich können wir q_{3j+1} nicht wie im Fall 2) mittels Lösung von linearem Gleichungssystem erhalten.
   $y_3 = -\frac{a_{10}}{a_{11}}$ und wir bekommen x_3, x_4 als Nullstellen von

$$p = \frac{u_{3j}}{ggT(R_y(g_1, C), u_{3j})},$$

   falls $deg(ggT(R_y(g_1, C), u_{3j})) = 2$. Ist $deg(ggT(R_y(g_1, C), u_{3j})) = 3$, dann gehört P_3 oder P_4 zu $g_1(x,y)$ und durch Einsetzen in g_1 erhalten wir die verbliebene $x-$Koordinate.

      i. Sei jetzt einer der Punkte $P_3, P_4 \in g_1$, und o.B.d.A. gilt es $P_4 \in g_1$. Daraus folgt, dass D_{3j} kollinear ist. Jede Quadrik, die D_{3j}

enthält besteht aus Geraden, wobei $P_1, P_2, P_4 \in g_1$ und $P_3 \in g_2$. Aus der Kurvengleichung von q_{3j} können wir $\nu_{P_\infty}(q_{3j}) = -7$ ablesen. Daraus folgt, dass es noch drei zusätzliche Punkte in dem Durchsnitt $q_{3j} \cap C$ gibt. Jede Gerade hat maximal vier Schnittpunkte mit C, d.h. höchstens ein Punkt von D_{3j+1} kann zu g_1 gehören. Sei M der vierte Schnittpunkt von g_1 mit C und entsprechend der geometrischen Konstruktion ist $M \in supp(D_{3j+1})$. Dann lässt sich die $y-$Koordinate von M als Nullstelle des linearen Polynoms

$$p = \frac{Res_x(C, g_1)}{(y-y_1)(y-y_2)(y-y_4)}$$

bestimmen. Die $x-$Koordinate erhalten wir nach Einsetzen in g_1.
Seien Q_1, Q_2 die andere zwei Punkte mit $Q_1, Q_2 \in g_2$. Es gilt $y_{Q_i} = y_3$ und die entsprechenden $x-$Koordinaten erhalten wir als Nullstellen von

$$p = \frac{Res_y(C, g_2)}{(x-x_3)}.$$

$D_{3j+1} = Q_1 + Q_2 + M$ und die Quadrik q_{3j+1} besteht aus den Geraden g_2 durch Q_1, Q_2 und g_1' durch M, P_∞. D_{3j+2} ist gleich $T_1 + T_2 + P_3$. P_3 ist der restliche Punkt in $C \cap g_2$ und T_1, T_2 sind die anderen zwei Punkte in dem Durchschnitt $C \cap g_1'$. Die $y-$Koordinaten von T_1, T_2 sind die Nullstellen von

$$p = \frac{Res_x(C, g_1')}{(y-y_M)}$$

und die entsprechenden x_{T_i} bestimmen wir nach Einsetzen.

ii. Seien $P_1, P_2 \in g_1$ und $P_3, P_4 \in g_2$. $P_3 = (x_3, y_3), P_4 = (x_4, y_3)$, mit $y_3 = -\frac{a_{10}}{a_{11}}$. Sei $P_5 = (x_5, y_3) \in C$ der letzte Punkt von C mit $y_{P_5} = y_3$ und $x-$Koordinate x_5 Nullstelle von $y_3^4 = p_3(x)$. Auf Grund der Singularitätenfreiheit von C gilt $x_3 \neq x_4 \neq x_5$. Seien Q_1, Q_2 die anderen Schnittpunkte von C und g_1, dann definieren wir $D_{3j+1} = P_5 + Q_1 + Q_2$ ein. Die $y-$Koordinaten y_{Q_1}, y_{Q_2} lassen sich als Nullstellen von

$$p = \frac{R_x(g_1, C)}{(y-y_1)(y-y_2)}$$

berechnen. Nach Einsetzen in g_1 erhalten wir die ensprechenden $x-$Werte. Jetzt können wir leicht die Koordinaten $(u_{3j+1}, q_{3j+1}, w_{3j}+1)$ von D_{3j+1} bestimmen und nach Satz 4.13 auch die von D_{3j+2}.

(b) Falls $(y + \frac{a_{10}}{a_{11}})^2 \nmid w_{3j}$, dann ist $D_{3j} = P_1 + P_2 + P_3 + P_4$ mit $P_1, P_2, P_3 \in g_1$ kollinear. M sei der vierte Schnittpunkt von C und g_1. Seien

$Q_1, Q_2 \in g_2$ die Punkte mit $x-$Koordinaten x_{Q_i} die andere zwei Nullstellen von $y_4^4 = p_3(x)$. Dann ist wie in Fall a) $D_{3j+1} = Q_1 + Q_2 + M$. Jetzt bleibt nur, die Koordinaten von M, Q_1, Q_2 zu berechnen. Wir wissen, dass $y_4 = -\frac{a_{10}}{a_{11}}$ ist und bestimmen zunächst y_M als Nullstelle von

$$p = \frac{R_x(g_1, C)(y + \frac{a_{10}}{a_{11}})}{w_{3j}}.$$

Falls g_1 abhängig von y ist, dann lässt sich x_M durch Einsetzen ausrechnen und x_4 ist die Nullstelle des linearen Polynoms

$$p = \frac{u_{3j}(x - x_M)}{R_y(g_1, C)}.$$

x_{Q_1} bzw. x_{Q_2} erhalten wir als Nullstellen des Polynoms zweiten Grades

$$p = \frac{y_4^4 - p_3(x)}{x - x_4}.$$

Ist aber x_M die einzige Lösung von $g_1 = 0$, dann ist x_4 die Lösung von

$$\frac{u_{3j}}{(x - x_M)^3} = 0.$$

Die Werte von x_{Q_1} bzw. x_{Q_2} lassen sich wie im vorigen Fall ausrechnen. Danach können wir, analog zu ii) $\bar{D}_{3j+1}$ und $\bar{D}_{3j+2}$ bestimmen.

□

Satz 4.16 *Gegeben sind $\bar{D}_{3j+1}, \bar{D}_{3j+2}$. Dann bestimmen wir zuerst E_j und danach können wir genau einen der folgenden Fälle ausrechnen:*

(a) $D_{3(j+1)}$ explizit bestimmen.
(b) $\bar{D}_{3(j+1)}$ explizit bestimmen.

Beweis: Unsere Strategie hier ist, zuerst $\bar{D}_{3(j+1)}$ zu berechnen. Falls das nicht möglich ist, werden wir zu dem anderen Fall übergehen. $u_{3(j+1)}, w_{3(j+1)}$ lassen sich wie folgt ausrechnen:

$$u_{3(j+1)} = u_{3j+2} \prod_{P_i \in supp(E_j)} (x - x_i)$$

$$w_{3(j+1)} = w_{3j+2} \prod_{P_i \in supp(E_j)} (y - y_i)$$

Wir werden versuchen, $q_{3(j+1)}$ aus dem folgenden linearen System zu bestimmen:

$$q_{3(j+1)}(P_i) = 0, \quad P_i \in supp(E_j)$$
$$R_x(q_{3j+2}, q_{3(j+1)}) = \lambda w_{3j+2}, \quad \lambda \neq 0.$$

Dafür betrachten wir die folgenden Fälle:

(a) Sei $q_{3j+2}(x,y) = b_{01}y + b_{00}$ linear. Dieser Fall trifft nur, falls $D_{3j+2} = P$. D.h. $E_j = P_{01} + P_{02} + P_{03}$ und wir bestimmen $u_{3(j+1)}$ bzw. $w_{3(j+1)}$ wie oben vorgegeben. Da der Hauptkoeffizient von $q_{3(j+1)}$ gleich eins ist, brauchen wir nur die restliche vier Koeffizienten zu bestimmen. Dies erfolgt nach dem Lösen des folgenden linearen Gleichungssystems:

$$q_{3(j+1)}(P) = 0$$
$$q_{3(j+1)}(P_{0i}) = 0, i = 1,2,3.$$

(b) $q_{3j+2}(x,y) = b_{01}y + b_{10}x + b_{00}$ ist linear. Nach den vorigen Sätzen lässt sich zeigen, dass $b_{10} \neq 0$ und $deg(D_{3j+2}) = 2$ ist. Dann ist $E_j = P_{01} + P_{02}$, $q_{3(j+1)} = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$ und das obige Gleichungssystem bekommt die folgende Form:

i. $P_{01} = P_{02} = (x,y)$

$$\begin{pmatrix} -b_{10} & 0 & b_{01} & 0 & 0 \\ 0 & -b_{10} & b_{00} & b_{01} & 0 \\ 0 & 0 & 0 & b_{00} & -b_{10} \\ 2y & 1 & x+y & 1 & 0 \\ y^2 & y & xy & x & 1 \end{pmatrix} \begin{pmatrix} a_{02} \\ a_{01} \\ a_{11} \\ a_{10} \\ a_{00} \end{pmatrix} = \begin{pmatrix} s_2 \\ s_1 \\ s_0 \\ 0 \\ 0 \end{pmatrix}.$$

Dabei benutzen wir, dass

$$\begin{aligned} R_x(q_{3j+2}, q_{3(j+1)}) = &- b_{10}a_{02}y^2 - b_{10}a_{01}y - b_{10}a_{00} + b_{01}a_{11}y^2 \\ &+ b_{01}a_{10}y + b_{00}a_{11}y + b_{00}a_{10} \end{aligned}$$

und

$$\lambda w_{3j+2} = s_2y^2 + s_1y + s_0.$$

Die Determinante des obigen Systems ist $2b_{10}(b_{01}y + b_{10}x + b_{00}) = 2b_{10}q_{3j+2}(P_{01})$.

ii. $P_{01} \neq P_{02}$. Dann ist das linare Gleichungssystem

$$\begin{pmatrix} -b_{10} & 0 & b_{01} & 0 & 0 \\ 0 & -b_{10} & b_{00} & b_{01} & 0 \\ 0 & 0 & 0 & b_{00} & -b_{10} \\ y_1^2 & y_1 & x_1y_1 & x_1 & 1 \\ y_2^2 & y_2 & x_2y_2 & x_2 & 1 \end{pmatrix} \begin{pmatrix} a_{02} \\ a_{01} \\ a_{11} \\ a_{10} \\ a_{00} \end{pmatrix} = \begin{pmatrix} s_2 \\ s_1 \\ s_0 \\ 0 \\ 0 \end{pmatrix}$$

und die Determinante ist $-b_{10}(y_1 - y_2)(b_{01}y_1 + b_{10}x_1 + b_{00})(b_{01}y_2 + b_{10}x_2 + b_{00})$.

Bezüglich der Determinante müssen wir die folgenden Fälle betrachten:

A. Sei $w_{3j+2}(P_{01}) = 0$ oder $w_{3j+2}(P_{02}) = 0$. Aus $deg(D_{3j+2}) = 2$ erhalten wir $deg(w_{3j+2}) = 2$. Da wir aus $P_{01} \in q_{3j+2}$ bzw.

$P_{02} \in q_{3j+2}$ den einen Wert y_{0i}, der in w_{3j+2} vorkommt kennen, können wir den zweiten ohne Faktorisierung ausrechnen. Die entsprechenden $x-$Werte bestimmen wir nach Einsetzen. Somit erhalten wir D_{3j+2} explizit und wegen $D_{3(j+1)} = D_{3j+2} + P_{01} + P_{02}$, wissen wir auch $D_{3(j+1)}$. Darauf können wir Satz 4.14 anwenden.

B. Sei $q_{3j+2}(P_{01}) = 0$ und $w_{3j+1}(P_{01}) = 0$ (oder $q_{3j+2}(P_{02}) = 0$ und $w_{3j+1}(P_{02}) = 0$). Aus $q_{3j+1} = q_{3j+2}$ und $w_{3j+1}(P_{01}) = 0$ folgt $P_{01} \in D_{3j+1}$. $P_{01} \in q_{3j+2}$ und wie in dem vorigen Fall ist q_{3j+2} eine Gerade, daraus folgt, dass $D_{3(j+1)} = D_{3j+2}+E_j$ kollinear ist. Wir können daher den vierten Schnittpunkt M von C und q_{3j+2} bestimmen. x_M ist Nullstelle von

$$p = \frac{R_y(C, q_{3j+2})}{u_{3j}(x - x_{P_{01}})}$$

und durch Einsetzen in q_{3j+2} erhalten wir auch y_M.
Wir kennen die Koordinaten von P_{01} und M und können mittels

$$p = \frac{R_x(C, q_{3j+2})}{(x - x_{P_{01}})(x - x_M)}$$

die $x-$Koordinaten von Q_1 und $Q_2 \in supp(D_{3j+2})$ ausrechnen. Durch Einsetzen erhalten wir wieder die entsprechenden $y-$Koordinaten. Somit kennen wir D_{3j+2} explizit und mit ihm auch $D_{3(j+1)} = D_{3j+2} + E_j$.

C. Sei $P_{01} = \sigma P_{02}$. Dann lässt sich $q_{3(j+1)}$ als $(x - x_{01})q_{3j+2}$ schreiben.

D. Sonst ist $q_{3j+2}(P_{01}) \neq 0$ und $q_{3j+2}(P_{02}) \neq 0$ und das lineare Gleichungssystem eindeutig lösbar.
Zuletzt wird darauf aufmerksam gemacht, dass der Hauptkoeffizient von $q_{3(j+1)}$ gleich eins ist, deswegen brauchen wir nur ein 4×4 Gleichungssystem zu lösen:

(c) Sei jetzt $q_{3j+2} = b_{02}y^2 + b_{01}y + b_{10}x + b_{00}, b_{02} \neq 0$. Wegen $deg(q_{3j+1}) > deg(q_{3j+2})$ gilt $b_{11} = 0$. In diesem Fall ist $E_j = P_{01}$. Wir berechnen $u_{3(j+1)}, w_{3(j+1)}$ wie am Anfang des Satzes angegeben war. Um die Interpolationsquadrik zu bestimmen,müssen wir dieses Mal das folgende Gleichungssystem lösen:

$$\begin{pmatrix} 0 & 0 & b_{02} & 0 & 0 \\ -b_{10} & 0 & b_{01} & b_{02} & 0 \\ 0 & -b_{10} & b_{00} & b_{01} & 0 \\ 0 & 0 & 0 & b_{00} & -b_{10} \\ y^2 & y & xy & x & 1 \end{pmatrix} \begin{pmatrix} a_{02} \\ a_{01} \\ a_{11} \\ a_{10} \\ a_{00} \end{pmatrix} = \begin{pmatrix} s_3 \\ s_2 \\ s_1 \\ s_0 \\ 0 \end{pmatrix}.$$

Die Resultante beträgt diesmal:

$$\begin{aligned} R_x(q_{3j+2}, q_{3(j+1)}) = &- b_{10}a_{02}y^2 - b_{10}a_{01}y - b_{10}a_{00} + b_{02}a_{11}y^3 \\ &+ b_{02}a_{10}y^2 + b_{01}a_{11}y^2 + b_{01}a10y + b_{00}a_{11}y \\ &+ b_{00}a_{10} \end{aligned}$$

und die Determinante ist $2b_{10}b_{02}q_{3j+2}(P_{01})$.
Bezüglich des Wertes der Determinante betrachten wir die folgenden Fälle:

i. Sei $q_{3j+2}(P_{01}) \neq 0$. Dann hat das Gleichungssystem eine eindeutige Lösung.
ii. Sei $q_{3j+2}(P_{01}) = 0$ und $w_{3j+1}(P_{01}) = 0$. Wegen $q_{3j+1} = q_{3j+2}$ gilt $P_{01} \in supp(D_{3j+1})$ und $q_{3(j+1)} = q_{3j+2}$.
iii. Sei $q_{3j+2}(P_{01}) = 0$ und $w_{3j+2}(P_{01}) = 0$. Dann gilt $P_{01} \in D_{3j+2}$. In diesem Fall betrachten wir das folgende Gleichungssystem:

$$\begin{aligned} q_{3(j+1)}(P_{01}) &= 0, \quad 2. \quad \textit{Ordnung} \\ \frac{R_x(q_{3j+2}, q_{3(j+1)})}{y - y_{01})} &= \lambda(\frac{w_{3j+2}}{y - y_{01}}), \quad \lambda \neq 0 \end{aligned}$$

Dabei ist

$$\begin{aligned} R_x(q_{3j+2}, q_{3(j+1)}) = &- b_{10}a_{02}y^2 - b_{10}a_{01}y - b_{10}a_{00} + b_{02}a_{11}y^3 \\ &+ b_{02}a_{10}y^3 + b_{01}a_{11}y^2 + b_{01}a_{10}y + b_{00}a_{11}y \\ &+ b_{00}a_{10}. \end{aligned}$$

Nach der Division durch $(y - y_{01})$ erhalten wir:

$$\begin{aligned} \frac{R_x(q_{3j+2}, q_{3(j+1)})}{(y - y_{01})} &= b_{02}a_{11}y^2 + (b_{01} + y_{01}b_{02})a_{11}y + b_{02}a_{10}y \\ &\quad - b_{10}a_{02}y + (b_{00} + y_{01}b_{01} + y_{01}^2b_{02})a_{11} \\ &\quad + (b_{01} + y_{01}b_{02})a_{10} - b_{10}a_{01} - y_{01}b_{10}a_{02}, \\ \lambda\left(\frac{w_{3j+2}}{y - y_{01}}\right) &= s_2y^2 + s_1y + s_0. \end{aligned}$$

Nach Koefizientenvergleich ist die Matrix des zugehörigen Gleichungssystems:

$$\begin{pmatrix} 0 & 0 & b_{02} & 0 & 0 \\ -b_{10} & 0 & b_{01} + y_{01}b_{02} & b_{02} & 0 \\ -y_{01}b_{10} & -b_{10} & b_{02}y_{01}^2 + b_{01}y_{01} + b_{00} & b_{01} + b_{02}y_{01} & 0 \\ y_{01}^2 & y_{01} & x_{01}y_{01} & x_{01} & 1 \\ 2y_{01} & 1 & x_{01} + y_{01} & 1 & 0 \end{pmatrix}$$

Diese Matrix hat die Determinante $-b_{02}b_{10}(2y_{01}b_{02} + b_{01} + b_{01})$. Der letzte Ausdruck ist aber genau die Summe der partiellen Ableitungen von q_{3j+2}. Da $y_{01} \in q_{3j+2}$ gilt, ist $(2y_{01}b_{02} + b_{01} + b_{01}) =$

0 genau dann, wenn P_{01} zweifache Nullstelle von $q_{3j+2} = 0$ ist.

A. Hat die Quadrik q_{3j+2} zweifache Nullstelle P_{01}, dann ist wegen $deg(w_{3j+2}) = 3$

$$p = \frac{w_{3j+2}}{(y - y_{01})^2}$$

ein lineares Polynom. Somit können wir die $y-$Koordinate des anderen Punktes P_{02} in $supp(D_{3j+2})$ ohne Faktorisierung bestimmen. Wir erhalten $D_{3(j+1)} = 3P_{01} + P_{02}$ und wenden darauf wieder Satz 4.14 an.

B. Für den Fall, dass P_{01} kein Verzweigungspunkt ist, ist die Determinante des Gleichungssystems ungleich Null und wir können es eindeutig lösen.
Hierbei müssen wir ein $4 \times 4-$ Gleichungssystem lösen, da der Hauptkoeffizient von $q_{3(j+1)} = 1$ ist und wir müssen praktisch nur vier Koeffizienten bestimmen.

□

Im jeden Schritt des Algorithmus wird höchstens ein lineares Gleichungssystem mit 4×4 Darstellungsmatrix gelöst und Polynome vom Grad 3 faktorisiert. Diese Polynome kommen aus den Formeln:

$$w_{D_{j+1}} = \frac{R_x(C, q_{D_j})}{w_{Dj}}$$

und

$$u_{D_{j+1}} = \frac{R_x(C, q_{D_j})}{u_{Dj}}$$

In gewissen Fällen tretten als Nullstellen der Polynomen auf, Elemente einer endlichen Erweiterung des Grundkörpers $\mathbb{F}_q$.

Beispiel 4.17

C sei durch die Gleichung $y^4 = x^3 - 1$ definiert und $\mathbb{F}_q = \mathbb{F}_{27}$.

1.	(ζ^4, ζ)	2.	(ζ^4, ζ^{14})	3.	(ζ^5, ζ^5)	4.	(ζ^5, ζ^{18})
5.	(ζ^7, ζ^8)	6.	(ζ^7, ζ^{21})	7.	(ζ^8, ζ^{10})	8.	(ζ^8, ζ^{23})
9.	(ζ^{10}, ζ^9)	10.	(ζ^{10}, ζ^{22})	11.	(ζ^{11}, ζ^7)	12.	(ζ^{11}, ζ^{20})
13.	(ζ^{12}, ζ^3)	14.	(ζ^{12}, ζ^{16})	15.	(ζ^{13}, ζ^{13})	16.	(ζ^{13}, ζ^{26})
17.	(ζ^{15}, ζ^2)	18.	(ζ^{15}, ζ^{15})	19.	(ζ^{19}, ζ^6)	20.	(ζ^{19}, ζ^{19})
21.	(ζ^{20}, ζ^{12})	22.	(ζ^{20}, ζ^{25})	23.	(ζ^{21}, ζ^{11})	24.	(ζ^{21}, ζ^{24})
25.	(ζ^{24}, ζ^4)	26.	(ζ^{24}, ζ^{12})	27.	$(1, 0)$	28.	$(0, 1)$

Die obige Tabele enthält die Punkten von C über $\mathbb{F}_{27}$.
Wir betrachten den Divisor $D = P_1 + P_2 + P_3 + P_4$ mit

$$\begin{aligned} P_1 &= (\zeta^4, \zeta) &&= (\zeta^2 + 2\zeta + 2, \zeta), \\ P_2 &= (\zeta^5, \zeta^5) &&= (2\zeta + 2, 2\zeta + 2), \\ P_3 &= (\zeta^7, \zeta^8) &&= (\zeta^2 + 1, \zeta^2 + \zeta + 2) \quad \textit{und} \\ P_4 &= (\zeta^{13}, \zeta^{13}) &&= (2, 2). \end{aligned}$$

Um $q_D(x,y) = a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00}$ zu bestimmen, müssen wir das folgende Gleichungssystem lösen:

$$\begin{pmatrix} \zeta^2 & \zeta & 2\zeta + 2 & \zeta^2 + 2\zeta + 2 & 1 \\ \zeta^2 + 2\zeta + 1 & 2\zeta + 2 & \zeta^2 + 2\zeta + 1 & 2\zeta + 2 & 1 \\ 2\zeta^2 + 1 & \zeta^2 + \zeta + 2 & 2\zeta^2 & \zeta^2 + 1 & 1 \\ 1 & 2 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_{02} \\ a_{01} \\ a_{11} \\ a_{10} \\ a_{00} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Wir erhalten als Lösunng

$$(a_{02}, a_{01}, a_{11}, a_{10}, a_{00}) = ((\zeta^2 + 2)t, (\zeta^2 + \zeta + 1)t, \zeta t, 2t, t)$$

und nach Normieren des Hauptkoeffizient a_{11}

$$(a_{02}, a_{01}, a_{11}, a_{10}, a_{00}) = (\zeta^2, (2\zeta^2 + 2\zeta + 1), 1, (\zeta^2 + 2\zeta), (2\zeta^2 + \zeta)).$$

Die Quadrik von D hat die folgende Form

$$q_D(x,y) = \zeta^2 y^2 + (2\zeta^2 + 2\zeta + 1)y + xy + (\zeta^2 + 2\zeta)x + (2\zeta^2 + \zeta).$$

Wir mssen jetz überprüfen, ob q_D in lineare Faktoren zerfählt. Dafür berechnen wir den folgenden Ausdruck:

$$a_{10}^2 a_{02} + a_{11}^2 a_{00} - a_{11}a_{01}a10 = 1 + 2\zeta^2 + \zeta - \zeta^2 - 1 = \zeta^2 + \zeta \neq 0$$

Daraus folgt, dass q_D unzerlegbar ist.
Als nächstes wollen wir D_1 bestimmen. Dafür bestimmen wir u_{D_1} und w_{D_1} nach Satz 4.13:

$$u_{D_1} = \frac{R_y(C, q_D)}{u_D}$$
$$w_{D_1} = \frac{R_x(C, q_D)}{w_D}$$

Wobei es gilt:

$$\begin{aligned} R_y &= 2x^7 + (2\zeta^2 + \zeta + 1)x^6 + (2\zeta^2 + 2\zeta + 1)x^5 + (2\zeta^2 + \zeta + 1)x^4 + 2\zeta x^3 \\ &\quad + (\zeta^2 + \zeta + 2)x^2 + (\zeta^2 + 2\zeta)x + \zeta^2 + 2, \\ R_x &= 2y^7 + (\zeta^2 + \zeta)y^6 + (2\zeta^2 + \zeta + 2)y^4 + 2\zeta y^3 \end{aligned}$$

Daraus folgt, dass die restliche drei Punkte, die zu dem Schnitt $C \cap q_D$ gehören, die folgende Form haben:

$$Q_1 = (x_1, 0), Q_2 = (x_2, 0), Q_3 = (x_3, 0), \quad x_i^3 = 0, \quad i = 1, 2, 3$$

$$D_1 = Q_1 + Q_2 + Q_3$$

Hierbei müssen wir zu der Erweiterung $\mathbb{F}_{27}(\xi)$, mit $\xi^3 = 1$, übergehen. Als nächstes wollen wir q_{D_1}, die Quadrik von $Q_1 + Q_2 + Q_3 + 2P_\infty$ bestimmen. Sie hat dreifache Nullstelle in $(1, 0)$. Wir erhalten, dass $q_{D_1} = y^2 + 2xy + y$ ist.
Es bleibt nur noch D_2 zu berechnen. Nach Satz 4.13 gilt

$$u_{D_2} = \frac{R_y(q_{D_1}, C)}{u_D} = (x-1)^2(x-2),$$

$$w_{D_2} = \frac{R_x(q_{D_1}, C)}{w_D} = y^2(y-1),$$

und nach Einsetzen in $q_{D_1} = q_{D_2}$ erhalten wir den reduzierten Divisor:

$$D_2 = 2(1,0) + (2,1) = 2(1,0) + (\zeta^{13}, \zeta^{26})$$

4.3 Additionsalgorithmus

Nachdem wir den Reduktionsalgorithmus eingeführt haben, können wir die Divisoren formal addieren. Der entstandene Divisor vom Grad ≥ 4 wird danach reduziert.
Eine andere Möglichkeit, im Sinne der Punktaddition auf elliptischen Kurven, ist die geometrische Konstruktion des Additionsdivisors. Dieses Verfahren ist in *Fast Arithmetic on Jacobians of Picard Curves* angegeben. In diesem Artikel wird darauf hingewiesen, dass der Additionalgorithmus sich auch für nicht hyperelliptischen Kurven eignet. Im Fall von nicht hyperelliptischen Kurven werden die Sekanten und Tangenten mit Quadriken und Kubiken ersetzt. Seien D_1, D_2 zwei reduzierte Divisoren. Nach dem Satz von Riemann-Roch existiert immer eine Kubik q, die durch die Punkte P_i, Q_i mit $P_i \in supp(D_1), Q_i \in supp(D_2)$.
Die, in diesem Kapitel, eingeführte Reduktions- und Additionsalgorithmen bieten eine elegante Möglichkeit Punkten in den Jacobischen Varietäten von nicht hyperelliptischen Kurven vom Geschlecht 3 zu addieren. Die Grundidee ist eine Fortsetzung der geometrischen Addition von Punkten auf elliptischen Kurven. Diese Konstruktion lässt sich leider nicht auf hyperelliptischen Kurven vom Geschlecht 3 übertragen, auf Grund des höheren Grades der Kurvenfamilie.

Wir erhalten einen effizienten Algorithmus, wobei in jedem Rekursionsschritt höhstens ein 4×4 lineares Gleichungssystem gelöst wird und zwei Polynome 3. Grades faktorisiert werden. Die bei der Faktorisierung entstandenen Werte, gehören im schlimsten Fall zu einer endlichen Erweiterung des Grundkörpers $\mathbb{F}_q$.
Die Grundidee des Algorithmus ist die eindeutige Darstellung jedes Divisors D als Tupel von sogenannten Koordinatenfunktionen (u_D, w_D, q_D). Diese Darstellung wird zum ersten mal von D. Mumford in *Thata Lectures on Theta II* für hyperelliptischen Kurven verwendet. Sie ist auch der Grundstein des Cantorschen Algorithmus für hyperelliptischen Kurven.
Mit Hilfe der definierten Algorithmen wird ermöglicht explizite Berechnungen in den Jakobischen Varietäten einiger nicht hyperelliptischen Kurvenfamilien vom Geschlecht 3 durchzuführen. Somit erhalten wir weitere wichtige Kurvenfamilien, die für kryptographischen Zwecken geeignet sind.

5 Anhang Äquivalenz zwischen binären quadratischen Formen und Moduln quadratischer Ordnungen

In der vorliegenden Arbeit ist eine praktische Anwendung der Eigenschaften der binären quadratischen Formen über $\mathbb{Z}$ dargestellt. Häufig werden binäre quadratische Formen bei der Bestimmung der Klassenzahl h_k eines Zahlkörpers k gebraucht. Mit Hilfe der bijektiven Korrespondenz zwischen der Klassengruppe von k und der Gruppe der eigentlich äquivalenten Formen lassen sich elegantere Algorithmen für die Berechnung von h_k konstruieren [Paulus].
R sei ein Hauptidealring und $k = Quot(R)$ der Quotientenkörper von R. l/k sei eine endliche und separable Erweiterung vom Grad n und $\{\sigma_1, ..., \sigma n\}$ seien die $k-$isomorphen Einbettungen von l in $\bar{l}$, einem algebraischen Abschluß von l.
Wir wollen zuerst an einige Grundbegriffe erinnern.
$Tr_{l/k}(x) := \sum_{i=1}^{n} \sigma_i(x)$, heißt die *Spur* von $x \in l$ und
$N_{l/k}(x) := \prod_{i=1}^{n} \sigma_i(x)$ die *Norm* von x.
Für je n beliebige Elemente $\{e_1, ..., e_n\}$ von l bezeichnet

$$d_{l/k}(e_1, ..., e_n) := det(Tr_{l/k}(e_i e_j)_{i,j}) = det(\sigma_i(e_j)_{i,j})^2$$

die Diskriminante von $\{e_1, ..., e_n\}$.
Unter $\mathcal{M}_k$ werden wir die Menge der endlich erzeugten $R-$Moduln in k verstehen. Sie sind von großer Bedeutung für die Algebra und Zahlentheorie. Mit Hilfe der Äquivalenz zwischen Moduln quadratischer Ordnungen und binären quadratischen Formen, die wir später einführen werden, werden die Eigenschaften der quadratischen Formen für die Berechnung der Klassenzahl verwendet. Auf diese Weise erhalten wir eine elegante Methode für die Bestimmung der Klassenzahl.

Definition 5.1 *Die Menge* $\mathcal{O}(\mathfrak{m}) := \{\lambda \in k \mid \lambda\mathfrak{m} \subset \mathfrak{m}\}$ *mit* $\mathfrak{m} \in \mathcal{M}_k \setminus \{0\}$ *fest gewählt heißt die Ordnung von* $\mathfrak{m}$.

Lemma 5.2 *Es lassen sich die folgenden Eigenschaften der Ordnung* $\mathcal{O}(\mathfrak{m})$ *nachweisen.*

(a) $\mathcal{O}(\mathfrak{m}$ *ist ein Ring mit Eins-Element.*

(b) $\mathcal{O}(\mathfrak{m})$ *ist in den Ringen der ganzen Zahlen von* k $\mathcal{O}_k$ *enthalten.*

(c) $\mathcal{O}(\mathfrak{m})$ *ist ein endlich erzeugter* $R-$*Modul.*

Beweis: $\mathcal{O}(\mathfrak{m})$ ist offensichtlich abgeschlossen bezüglich der Addition, Subtraktion, Multiplikation und enthält das Eins-Element von k.

Sei $\lambda \in k$ mit $\lambda\mathfrak{m} \subset \mathfrak{m}$ und $(b_1, ..., b_n)$ eine Basis von $\mathfrak{m}$. Dann lassen sich die Zahlen $\lambda b_i, i = 1, ..., n$ als $R-$lineare Kombinationen der Basis darstellen:

$$\lambda b_i = \sum_{i=1}^{n} a_{i,j} b_j, \quad a_{i,j} \in R.$$

Für die Determinante von $(\lambda E_n - (a_{i,j})_{i,j})$ erhalten wir

$$det(\lambda E_n - (a_{i,j})_{i,j}) = 0.$$

Somit entsteht eine normierte Gleichung für λ mit Koeffizienten aus R, was äquivalent zu $\lambda \in \mathcal{O}_k$ ist. Daraus folgt $\mathcal{O}(\mathfrak{m}) \subset \mathcal{O}_k$.
Sei jetzt $\mu \neq 0, \mu \in \mathfrak{m}$. Dann gilt

$$\mathcal{O}(\mathfrak{m})\mu \subset \mathcal{O}(\mathfrak{m})\mathfrak{m} \subset \mathfrak{m}$$

oder äquivalent dazu $\mathcal{O}(\mathfrak{m}) \subset \mu^{-1}\mathfrak{m}$. Daraus lässt sich schliessen, dass $\mathcal{O}(\mathfrak{m})$ ein endlich erzeugter $R-$Modul ist.

$\square$

Sei jetzt k ein quadratischer Zahlkörper, d.h. $k = \mathbb{Q}(\sqrt{d})$. Wir betrachten weiterhin die Ordnungen von k, genannt quadratische Ordnungen, wobei unser Ziel sein wird, eine Äquivalenz zwischen Moduln in quadratischen Ordnungen und binären quadratischen Formen nachzuweisen. Dafür werden wir zuerst zeigen, dass die Menge der Moduln einer quadratischen Ordnung in k eine multiplikative Gruppe bildet. Danach werden wir eine Äquivalenzrelation auf dieser Menge definieren. Bei der Konstruktion des Anhangs werden wir von dem Buch *Zahlenrtheorie* von H. Koch ausgehen.

Satz 5.3 *Jeder Modul $\mathfrak{m}$ in k hat eine Basis der Form (B, Bj) mit $B \in \mathbb{Q}, j \in k$. Die Zahl B ist durch $\mathfrak{m}$ eindeutig bestimmt.*

Beweis: Da k ein quadratischer Körper ist, lässt sich jeder Modul $\mathfrak{m}$ als $\mathfrak{m} = (\alpha, \beta)$ darstellen, $\alpha, \beta \in k$. Es existieren $k_1, k_2 \in \mathbb{Q}$ mit

$$1 = k_1\alpha + k_2\beta$$

und es existiert eine ganze Zahl B mit $u := Bk_1$ und $v := Bk_2$ ganz und teilerfremd. Seien r, s zwei ganze rationale Zahlen, für die $us - vr = 1$ gilt. Wir definieren

$$j := \frac{r\alpha + s\beta}{B}.$$

Wegen

$$\begin{aligned} B &= B(k_1\alpha + k_2\beta) = u\alpha + v\beta \quad \textit{und} \\ Bj &= r\alpha + s\beta \end{aligned}$$

gilt $B, Bj \in \mathfrak{m}$. Somit erhalten wir ein lineares Gleichungssystem für α, β mit ganzen Koeffizienten und Determinante $us - rv = 1$.
B ist durch $\mathfrak{m}$ eindeutig bestimmt, da die in $\mathfrak{m}$ enthaltenen ganzen rationalen Zahlen die ganzen Vielfachen von B sind.

□

k sei quadratische algebraische Erweiterung und $j \in k$. Daraus folgt, dass j Nullstelle eines Polynoms zweiten Grades mit rationalen Koefizienten ist:

$$P_1 = y^2 - \frac{2r\alpha}{B} + \frac{r\alpha)^2 - (s\beta)^2}{B^2}.$$

Nach entsprechender Multiplikation erhalten wir, dass j Nullstelle eines Polynoms mit ganzen Koeffizienten ist:

$$P_2 = ay^2 + by + c.$$

Damit die Koeffizienten eindeutig bestimmt sind, verlangen wir zusätzlich $a > 0$ und $ggT(a, b, c) = 1$.
$aj \in \mathcal{O}_k$ ist eine ganze algebraische Zahl und lässt sich darstellen als

$$aj = k_1 + k_2\sqrt{d}, k_1, k_2 \in \mathbb{Z}.$$

Wir nennen ein Element j zulässig, falls $k_2 > 0$ gilt. Gegebenenfalls erhalten wir ein solches Element durch Übergang zu $-j$.

Satz 5.4 *Die Ordnung von $\mathfrak{m} = (B, Bj)$ ist $\mathcal{O}(\mathfrak{m}) = (1, aj) = (1, k_2\sqrt{d})$ und j und $\mathcal{O}(\mathfrak{m})$ haben die gleiche Diskriminante.*

Beweis: Sei $\alpha \in k \setminus \{0\}$. Dann haben die Moduln $\mathfrak{m}$ und $\alpha\mathfrak{m}$ die gleiche Ordnung und es reicht, nur $\mathcal{O}(\mathfrak{m}) = (1, aj)$ zu betrachten.
Es gilt offensichtlich $aj \in \mathcal{O}(\mathfrak{m})$ und somit auch $(1, aj) \subset \mathcal{O}(\mathfrak{m})$. Es bleibt damit nur $\mathcal{O}(\mathfrak{m}) \subset (1, aj)$ zu zeigen.
Sei $\delta \in \mathcal{O}(\mathfrak{m})$ ein Element der Ordnung. Dann gilt $\delta \in \mathfrak{m}$ und $j\delta \in \mathfrak{m}$.
Wegen $\mathcal{O}(\mathfrak{m}) \subset \mathcal{O}_k$ besitzt δ die Darstellung $\delta = k_1 + k_2 j$ mit $k_1, k_2 \in \mathbb{Z}$. Damit $j\delta \in \mathfrak{m}$ erfüllt ist, muss zusätzlich noch $k_2 j \in \mathfrak{m}$ gelten. Aus $aj^2 + bj + c = 0$ erhalten wir $k_2 j^2 = k_2 \frac{bj+c}{a}$. Da aber a, b, c teilerfremd sind, muss $a|k_2$ gelten, woraus $\delta \in (1, aj)$ folgt.
Um die zweite Behauptung beweisen zu können, müssen wir die Diskriminante von j definieren als die Zahl $d(j) = b^2 - 4ac$.
Die Diskriminante der Ordnung $\mathcal{O}(\mathfrak{m})$ ist gleich *det* $\begin{pmatrix} 1 & 1 \\ aj & a\bar{j} \end{pmatrix} = b^2 - 4ac$ und somit gleich jener von j. Hierbei bezeichnet $\bar{j}$ die zu j konjugierte Zahl.

□

Als Nächstes wollen wir zeigen, dass die Menge aller Moduln zu gegebener Ordnung eine multiplikative Gruppe bildet. Dafür werden wir zuerst einige Begriffe definieren.
Aus der Definition der Norm eines Ideals erhalten wir den Begriff Norm eines Moduls.

Definition 5.5 *Sei $\mathfrak{m} = (\alpha, \beta)$ ein beliebiger Modul und $\mathcal{O}(\mathfrak{m}) = (\alpha_1, \beta_1)$ seine Ordnung. Unter der Norm von $\mathfrak{m}$ verstehen wir die Zahl $N(\mathfrak{m}) = |detA|$, wobei A die Übergangsmatrix von (α_1, β_1) zu (α, β) ist. Die Norm ist unabhängig von der Wahl der Basen.*

Bemerkung 5.6 *Im Fall $\mathfrak{m} = (B, Bj)$ und $\mathcal{O}(\mathfrak{m}) = (1, aj)$ hat A die Form*

$$A = \begin{pmatrix} B & 0 \\ 0 & \frac{B}{a} \end{pmatrix}$$

und es gilt $N(\mathfrak{m}) = \frac{B^2}{a}$.

Definition 5.7 $\bar{\mathfrak{m}} := \{\bar{a} \mid a \in \mathfrak{m}\}$ *heißt zu $\mathfrak{m}$ konjugiertes Modul. $\bar{\mathfrak{m}}$ hat die gleiche Ordnung und Norm wie $\mathfrak{m}$.*

Satz 5.8 *Die Menge $\mathcal{M}(\mathcal{O})$ der Moduln zu gegebener Ordnung $\mathcal{O}$ bilden eine multiplikative Gruppe.*

Beweis: Seien $\mathfrak{m}$ und $\mathfrak{m}_1$ zwei Moduln der Ordnung $\mathcal{O}$. Dann gilt wegen

$$\begin{aligned} \mathfrak{m}\bar{\mathfrak{m}} = (B, Bj)(B, B\bar{j}) &= B^2(1, j, \bar{j}, j\bar{j}) \\ = \frac{B^2}{a}(a, aj, b, c) &= \frac{B^2}{a}(1, aj) = \frac{B^2}{a}\mathcal{O}(\mathfrak{m}), \end{aligned}$$

dass

$$\mathfrak{m}\bar{\mathfrak{m}} = N(\mathfrak{m})\mathcal{O}(\mathfrak{m}).$$

Aus $\mathfrak{m}\bar{\mathfrak{m}}_1 = \bar{\mathfrak{m}}\bar{\mathfrak{m}}_1$ und dem soeben Gezeigtem lässt sich noch schließen, dass
$N(\mathfrak{m}\mathfrak{m}_1)\mathcal{O}(\mathfrak{m}\mathfrak{m}d_1) = \mathfrak{m}\mathfrak{m}_1\bar{\mathfrak{m}}\bar{\mathfrak{m}}_1 = \mathfrak{m}\bar{\mathfrak{m}}\mathfrak{m}_1\bar{\mathfrak{m}}_1 = N(\mathfrak{m})N(\mathfrak{m})\mathcal{O}$
und folglich auch $\mathcal{O}(\mathfrak{m}\mathfrak{m}_1) = \mathcal{O}$ und $N(\mathfrak{m}\mathfrak{m}_1) = N(\mathfrak{m})N(\mathfrak{m}_1)$.
Wegen $\mathcal{O}(\mathfrak{m}\mathfrak{m}_1) = \mathcal{O}$ ist $\mathcal{M}(\mathcal{O})$ bezüglich der Modulnmultiplikation abgeschlossen.
Sei $\mathfrak{n} = \frac{\bar{\mathfrak{m}}}{N(\mathfrak{m})}$ ein Modul, dann gilt $\mathfrak{n}\mathfrak{m} = \frac{\mathfrak{m}\bar{\mathfrak{m}}}{N(\mathfrak{m})} = \mathcal{O}(\mathfrak{m})$ oder $\mathfrak{n}$ ist das Inverse von $\mathfrak{m}$.

$\square$

Wie bei Idealen lässt sich auf der Gruppe der Moduln von Ordnung $\mathcal{O}$ eine Äquivalenzrelation definieren.

Definition 5.9 *Zwei Moduln $\mathfrak{m}_1, \mathfrak{m}_2 \in \mathcal{M}(\mathcal{O})$ heißen ähnlich, falls eine Zahl $\alpha \in k$ existiert mit $\mathfrak{m}_2 = \alpha\mathfrak{m}_1$.*
Gilt zusätzlich $N(\alpha) > 0$, dann heißen $\mathfrak{m}_1, \mathfrak{m}_2$ ähnlich im engeren Sinne.

$Cl(\mathcal{O}) = \mathcal{M}(\mathcal{O})/\{\alpha\mathcal{O} | \alpha \in k^*\}$ heißt die *Klassengruppe von $\mathcal{O}$* und $Cl_0(\mathcal{O}) = \mathcal{M}(\mathcal{O})/\{\alpha\mathcal{O} | \alpha \in k^*, N(\alpha) > 0\}$ heißt die *Klassengruppe* im engeren Sinne.
Es ist leicht zu überprüfen, dass beide Relationen Äquivalenzrelationen sind. Desweiteren lässt sich noch zeigen, dass bei negativer Körperdiskriminante d alle Normen positiv sind und die Klassengruppe und die Klassengruppe im engeren Sinne übereinstimmen. Ist aber $d > 0$, dann existieren Zahlen $\alpha \in k$ mit $N(\alpha) > 0$ und $\beta \in k$ mit $N(\beta) < 0$. In diesem Fall betrachten wir den Ring der Einheiten von k. Die Multiplikation mit Einheit erhält den Moduln. Daraus folgt, falls es eine Einheit $\varepsilon \in k$ mit $N(\varepsilon) = -1$ existiert, dann sind alle ähnliche Moduln auch ähnlich im engeren Sinne, aufgrund $(\alpha) = (\varepsilon\alpha)$ und die Norm einer der Zahlen α und $\varepsilon\alpha$ positiv ist. Ist das aber nicht der Fall, dann zerfällt jede Äquivalenzklasse in zwei Äquivalenklassen im engeren Sinne.

Satz 5.10 *Es gilt:*

(a) Sei $k = \mathbb{Q}(\sqrt{d})$ und $d < 0$, dann stimmen die Äquivalenzrelationen überein.

(b) Gilt $d > 0$ und es existiert eine Lösung von

$$k_1^2 - dk_2^2 = -4,$$

dann fallen die beiden Äquivalenzrelationen wieder zusammen.

(c) Falls $d > 0$, aber keine Lösung der obigen Gleichung existiert, dann enthält die Klassengruppe die Untergruppe der Quadrate der Klassengruppe im engeren Sinne [Buell].

Seien $\mathfrak{m}_1 = (1, j_1)$ und $\mathfrak{m}_2 = (1, j_2)$ zwei Moduln der Ordnung $\mathcal{O}$. Dann lässt sich eine Beziehung zwischen den Zahlen j_1, j_2 feststellen.

Satz 5.11 *Seien $\mathfrak{m}_1 = (1, j_1)$ und $\mathfrak{m}_2 = (1, j_2)$ zwei Moduln der Ordnung $\mathcal{O}$ und $j_1 = k_1 + k_2\sqrt{d}, j_2 = k_3 + k_4\sqrt{d}$ mit $k_2, k_4 > 0$. $\mathfrak{m}_1$ und $\mathfrak{m}_2$ sind ähnlich im engeren Sinne genau dann, wenn eine Matrix $A = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in SL_2(\mathbb{Z})$ mit*

$$j_2 = \frac{kj_1 + l}{mj_1 + n}$$

existiert.

Beweis: Seien $(a, j_1), (1, j_2)$ ähnlich im engeren Sinne. Dann existiert $\alpha \in k^*$ mit $N(\alpha) > 0$ und eine Matrix $A = \begin{pmatrix} k & l \\ m & n \end{pmatrix}$ mit $det(A) = \pm 1$ und

$$\begin{pmatrix} j_2 \\ 1 \end{pmatrix} = A \begin{pmatrix} \alpha j_1 \\ \alpha \end{pmatrix}.$$

Da die Multiplikation und die Konjugation mit einander verträglich sind, lässt sich folgern

$$\begin{pmatrix} j_2 & \bar{j}_2 \\ 1 & 1 \end{pmatrix} = A \begin{pmatrix} \alpha j_1 & \bar{\alpha}\bar{j}_1 \\ \alpha & \bar{\alpha} \end{pmatrix}$$

und $j_2 - \bar{j}_2 = detAN(\alpha)(j_1 - \bar{j}_1)$.
Die Zahlen j_1, j_2 waren als zulässiig vorausgesetzt, woraus folgt $det(A) = 1$ und $A \in SL_2(\mathbb{Z})$. Aus $\begin{pmatrix} j_2 \\ 1 \end{pmatrix} = A \begin{pmatrix} \alpha j_1 \\ \alpha \end{pmatrix}$ folgt auch

$$j_2 = \frac{kj_1 + l}{mj_1 + n}.$$

Existiere umgekehrt eine Matrix $A \in SL_2(\mathbb{Z})$ wie in der Behauptung. Dann gilt $\mathfrak{m}_2 = \frac{\mathfrak{m}_1}{mj_1+n}$ und aus $j_2 - \bar{j}_2 = detAN(\alpha)(j_1 - \bar{j}_1)$ folgt

$$N\left(\frac{1}{mj_1 + n}\right) > 0$$

.

□

Am Schluss wollen wir noch die bijektive Korrespondenz zwischen der Klassengruppe im engeren Sinne $Cl_0(\mathcal{O})$ und der Gruppe der eigentlich äquivalenten binären quadratischen Formen zeigen. Dafür sei $j = k_1 + k_2\sqrt{d}, k_2 > 0$. Wir ordnen j einerseits die Klasse des Moduls $(1, j)$ und anderseits die Klasse der eigentlich äquivalenten Formen zu:

$$\begin{aligned} F_j(x,y) &= \frac{1}{N(\mathfrak{m})}(x - jy)(x - \bar{j}y) = a(x^2 - (j + \bar{j})xy + j\bar{j}y^2) \\ &= a(x^2 + \frac{b}{a}xy + \frac{c}{a}y^2) = ax^2 + bxy + cy^2. \end{aligned}$$

Somit hat F_j ganzzahlige Koeffizienten und wegen $ggT(a, b, c) = 1$ ist F_j auch primitiv.

Satz 5.12 *Sei $\mathcal{O}$ eine Ordnung in k. Dann ist*

$$\Phi : Cl_0(\mathcal{O}) \to \mathcal{K}$$

eine Bijektion. Hierbei bezeichnet $\mathcal{K}$ die Gruppe der Klassen äquivalenter binärer quadratischer Formen. Im Fall $d(\mathcal{O}) < 0$ werden nur die positiv definiten Formen berücksichtigt.

Beweis: Seien j_1, j_2 zwei zulässige Zahlen und $\mathfrak{m}_1 = (1, j_1), \mathfrak{m}_2 = (1, j_2)$ zwei Moduln ähnlich im engeren Sinne. Dann existiert Matrix $A = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in SL_2(\mathbb{Z})$ und $j_2 = \frac{kj_1+l}{mj_1+n}$. Nach dem vorigen Satz gilt $\mathfrak{m}_1 = \alpha \mathfrak{m}_2$ mit $\alpha = \frac{1}{mj_1+n}$.
Für die entsprechenden quadratischen Formen gilt

$$\begin{aligned} F_{j_2}(x,y) &= \frac{1}{N(\mathfrak{m}_2)}(x - j_2 y)(x - \bar{j}_2 y) \\ &= \frac{((my_1+n)x - (kj_1+l)y)(((m\bar{j}_1+n)x - (k\bar{j}_1+l)y)}{N(\mathfrak{m}_2)N(mj_1+n))} \\ &= \frac{(x_2 - j_1 y_2)(x_2 - \bar{j}_1 y_2)}{N(\mathfrak{m}_1)}, \end{aligned}$$

wobei

$$A^{-1}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} n & -l \\ -m & k \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} nx - ly \\ -mx + ky \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Somit sind auch die Formen F_{j_1} und F_{j_2} äquivalent.
Bei der Zuordnung $\mathfrak{m} \to F_j$ werden nach Satz 5.3 alle Modulnklassen berücksichtigt.
Ist umgekehrt eine Klasse von Formen vorgegeben, die im Fall $d(k) < 0$ positiv definit ist, dann existiert darunter eine Form

$$F(x,y) = ax^2 + bxy + cy^2 \quad a > 0.$$

j sei die zulässige Nullstelle von $ax^2 + bx + c$. Dann lässt sich F in der Form

$$F(x,y) = a(x - jy)(x - \bar{j}y)$$

darstellen. Somit ist $F = F_j$ und der Satz ist bewiesen.

□

Die gezeigte Bijektion zwischen der Klassengruppe und der Gruppe der Klassen eigentlich äquivalenter binärer quadratischer Formen bietet eine Möglichkeit die Klassenzahl $Cl_0(\mathcal{O})$ zu bestimmen. Somit wird ein wesentlich kompliziertres Problem auf die elegante Theorie der quadratischen Formen mit ganzzahligen Koeffizienten zurückgeführt. Eine Verallgemeinerung der gerade gezeigten Korrespondenz auf quadratische Formen mit Koeffizienten im beliebigen Hauptidealring wird in *Ein Algorithmus zur Berechnung der Klassengruppe quadratischer Ordnungen über Hauptidealring* S. Paulus, 1996, dargestellt. Diese bietet die Möglichkeit, die Klassenzahl einer wesentlich größeren Menge von Gruppen zu bestimmen. Zusätzlich wird auch die Theorie der quadratischen Formen, z.B. Reduktionsalgorithmen, auf den allgemeinen Fall von Hauptidealringen erweitert.

5 Anhang
Äquivalenz zwischen binären quadratischen Formen und Moduln quadratischer Ordnungen

Die klassische Theorie der binären quadratischen Formen, zum ersten Mal ausführlich dargestellt in dem Gaußschen *Disquisitiones Arithmeticae*, 1801, bietet einerseits eine elegante Methode, die Klassenzahl von Moduln- bzw. Idealgruppen über Hauptidealringen zu bestimmen. Anderseits haben wir, innerhalb der vorliegenden Arbeit gesehen, dass sich mit Hilfe der bekannten Eigenschaften von quadratischen Formen, effiziente Algorithmen für Addition und Reduktion in der Jakobischen Varietät hyperelliptischer Kurven konstruieren lassen. Diese Algorithmen erlauben die Implementierung einer großen Klasse von Kurven in kryptographischen Verfahren. Das führt zu größerer Vielfachheit der Wahl der Basisgruppe für kryptographische Algorithmen wie El Gamal, Schnorr, Diffie-Hellman und somit zu komplizierteren Diskrete-Logarithmus-Problemen. Letzter garantiert eine höhere kryptographische Sicherheit bei der Datenübertragung und im Umgang im Internet oder allgemein im täglichen Leben.

Literatur

[Buell] Buell, D. A. *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer-Verlag, 1989

[Cantor] Cantor, D. *Computing in the Jacobian of a Hyperelliptic Curve*, Mathematics of Computation, Volume 48, Nummer 177, Januar 1994, Seiten 95-101

[Cassels1] Cassels, J. W. S., Flynn, E. V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996

[Cassels2] Cassels, J. W. S. *Rational Quadratic Forms*, Academic Press, 1978

[Choie] Choie, Y., Jeong, E. *Isomorphism Classes of Elliptic and Hyperelliptic Curves over Finite Fields* $\mathbb{F}_{(2g+1)^n}$, Department of Mathematics, Pohang University of Science and Technology, Pohang, 790-784, Korea

[Cohen] Cohen, H. *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993

[Estrada1] Estrada, J., Reinaldo, E., Piñero, J. *On the Jacobian Varieties of Picard Curves: Explicit Addition Law and Algebraic Structure*, Humboldt Universität zu Berlin, Institut für Mathematik, Preprint: 95-5, 1995

[Estrada2] Estarada, J. Cherdieu, J., Reinaldo, E. *Efficient Reduction on the Jacobian Variety of Picard Curves*, Coding Theory, Crypthography and Related Areas, Proceedings of the ICCC-98, Buchmann, J., Hohold, T., Stichtenoth, H., Tagia-Reallas, H., (Her), Springer-Verlag, 1998, Seiten 13-28

[Estrada3] Estrada, J. Cherdieu, J., Reinaldo, E., Holzapfel, R.-P. *The Emergency of Picard Jacobians in Cryptograohy*, Proceedings IV IT-LA, 2001, Seiten 266-275

[Estrada4] Estrada, J., Blache, R., Cherdieu, J.*Some Computational Aspects of Jacobians of Curves in the Family* $y^3 = \gamma x^5 + \delta$ *over* $\mathbb{F}_p$, Humboldt Universität zu Berlin, Institut für Mathematik, Preprint: 2004-2, 2004

[Encinas] Encinas, L., Menezes, A., Masque, J. em Isomorphism Classes of Genus-2 Hyperelliptic Curves over Finite Fields, www.citeseer.ist.psu.edu/445362.html, 2000

[Flon] Flon, S., Oyono, R. *Fast Arithmetic on Jacobians of Picard Curves*, www.citeseer.ist.psu.edu/flon03fast.html, 2003

[Griffits1] Griffits, P., Harris, J. *Principles of Algebraic Geometry*, A Wiley-Interscience Publication, 1994

[Griffits2] Griffits, P *Introduction to Algebraic Curves*, American Mathematical Society, 1989

[Harris] Harris, J., Morrison, I. *Moduli of Curves*, Springer-Verlag, 1998

[Hartshorne] Hartshorne, R. *Algebraic Geometry*, Springer-Verlag, 1977

[Hecke] Hecke, E. *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, 1954

[Jacobson] Jacobson, M., Menezes, A., Stein, A. *Hyperelliptic Curves and Crypthography*, www.citeseer.ist.psu.edu/menezes04hyperelliptic.html, 2004

[Koblitz] Koblitz, N. *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998

[Koch] Koch, H. *Zahlentheory*, Vieweg, 1997

[Lauter] Lauter, K. *The Equivalence of Geometric and Algebraic Group Laws for Jacobians of Genus 2 Curves*, Contemporary Mathematics, Volume 324, 2003

[Liu] Liu, Qing *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002

[Lockhart] Lockhart, P. *On the Discriminant of a Hyperelliptic Curve*, Transactions of the American Mathematical Society, Volume 342, Nummer 2, April 1994

[Menezes] Menezes, A., Wu, Y., Zuccherato, R. *An elementary Introduction to Hyperelliptic Curves*, Technical Report CORR 96-19, Department of C&O), University of Waterloo, Ontario, Canada, November 1996

[Miranda] Miranda, R. *Algebraic Curves and Riemann Surfaces*, American Mathematical Society, 1995

[Mumford1] Mumford, D. *Tata Lectures on Theta II*, Birkhäuser, 1984

[Mumford2] Mumford, D. *Curves and Their Jacobiams*, Ann Arbor, The University of Michigan Press, 1975

[Paulus] Paulus, S. M. *Ein Algorithmus zur Berechnung der Klassengruppe quadratischer Ordnungen über Hauptidealringe*, Dissertation, Universität Essen, 1996

[Rose] Rose, H. E. *A Course in Number Theory*, Oxford University Press, 1994

[Stepanov] Stepanov, S. *Codes on Algebraic Curves*, Kluwer Academic/ Plenum Publishers, 1999

[Stichtenoth] Stichtenoth, H. *Algebraic Function Fields and Codes*, Springer-Verlag, 1993

6 Selbständigkeitserklärung

Erklärung

Ich erkläre, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angeferligt habe.

Berlin, Oktober, 2004

Maria Petkova

7 Thesen

In der vorliegenden Arbeit wurden Reduktions- und Additionsalgorithmen für die Jacobischen Varietäten von den nicht hyperelliptischen Kurvenfamilien, vom Geschlecht 3

$$y^4 = p_4(x,z) = x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$$
$$y^4 = p_3(x,y) = x^3z + b_2x^2z^2 + b_1xz^3 + b_0z^4$$

über einem endlichen Körper $\mathbb{F}_q$ konstruiert.

(a) In $Div^{+,i}(C/\mathbb{F}_q)$ wurden bestimmte Divisoren ausgezeichnet ($Div_0^{+,i}(C/\mathbb{F}_q)$).

(b) Den Divisoren $D \in \mathrm{Div}_0^{+,i}(C/\mathbb{F}_q)$ wurden auf eine eindeutige Weise Tripeln von Polynomialfunktionen (u_D, q_D, w_D) zugeordnet.

(c) Die Divisorenoperationen werden auf Polynomenoperationen reduziert.

(d) Reduktionsalgorithmus (geometrische Version)

  i. Sei $D \in Div^{+,4}(C/\mathbb{F}_q)$ ein Divisor mit $deg(D) = 4$, und q_D die dazugehörige Interpolationsquadrik. Mit Hilfe von q_D konstruieren wir einen Divisor D', so dass

  $$(q_D) = (D - 4P_\infty) + (D' - 3P_\infty).$$

  Sei $q_{D'}$ die Interpolationsquadrik von D', dann konstruieren wir den Divisor D'' mit

  $$(q_{D'}) = (D' - 3P_\infty) + (D'' - 3P_\infty)$$

  und es gilt

  $$D - 4P_\infty \sim D'' - 3P_\infty,$$

  wobei D'' reduziert ist.

  ii. Rekursive Fortsetzung der Reduktion auf Divisoren höheres Grades.

(e) Reduktionsalgorithmus
Sei $D \in Div(C)$ effektiver Divisor mit $deg(D) > 3$, dann lässt sich D als $D = D_0 + E_0 + E_1 + ... + E_n$ darstellen, wobei E_i effektive Divisoren sind.

  i. Betrachte D_0

    A. Falls $D_0 \in Div_0(C)$ konstruiere $\bar{D}_0$ und berechne $\bar{D}_1$ und $\bar{D}_2$ oder D_2 explizit.

    B. Falls $D_0 \notin Div_0(C)$ konstruiere $\bar{D}_1$ und $\bar{D}_2$.

  ii. Nach 4.16 bestimme D_3 oder $\bar{D}_3$, setze $D_3 = D_0$ und gehe zu i)