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

Maria Petkova
Juli 2005

Abstract

In this paper we represent a reduction and addition algorithm for non hyperelliptic curves of genus 3. Our aim is to give an explicit representation of the group law in the jacobian varieties of curves belonging to the families $y^4 = p_4(x)$ and $y^4 = p_3(x)$. The idea of the algorithm is an extension of the geometric addition of points on elliptic curves. Because of the complexity of the curve structure we work hier with conics instead of chords and tangents as in the genus one case. In the construction of the algorithm we use the so called coordinate form of the divisor. The coordinate form of a divisor is a unique set of three polynomials, which we use for the computations. All computations succeed only with linear algebra knowledges. At the end of the algorithm we need one factorisation so that the result can be defined over a finite extension field. The reduction and addition ist constructed iterativ and can be applied in efficient way to divisors of every degree. [1]

[1] AMS Subject Classification: 11G10, 11T71,14H5, 14H40, 14H45, 14Q05, 14Q20
Key Words: Non hyperelliptic curves of genus 3, Jacobian Varieties, Addition Law

Inhaltsverzeichnis

1 Einführung

In der vorliegenden Arbeit wird ein Reduktions- und Additionsalgorithmus in der Jacobischen Varietät von nicht hyperelliptischen Kurven konstruiert. Mit Hilfe dieser expliziten Darstellung des Gruppengesetzes wird die Jacobische Varietät jeder nicht hyperelliptischen Kurve der Kurvenfamilien $y^4 = p_4(x)$ und $y^4 = p_3(x)$ zu einer abelschen Gruppe, die für kryptographische Zwecke geeignet ist.
Das 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 nicht 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 zugeordnet. 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 fürhyperelliptischen Kurven 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 Reduktions- und Additionsalgorithmus auf nicht hyperelliptischen Kurven

2.1 Nicht hyperelliptische Kurven

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

Definition 2.1 *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 2.2 *Es existieren nicht hyperelliptische Kurven jedes Geschlechtes $g \geq 3$ [Hartshorne].*

Satz 2.3 *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 Quartik. Gilt umgekehrt, dass $X \subset \mathbb{P}^2$ eine nicht singuläre Quartik 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 Quartiken in $\mathbb{P}^2$ und somit nach dem vorigen Satz kanonische Kurven zweier Familien nicht hyperelliptischer Kurven vom Geschlecht 3.

Bemerkung 2.4 *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

$$C': \quad y^4 = x^4 + a_3'x^3 + a_2'x^2 + a_1'x.$$

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

$$C'': \quad u^4 = p_3(w) = w^3 + c_2w^2 + c_1w + c_0$$

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 die Kurve C über $\bar{\mathbb{F}}_q$ definiert, dann hat

$$C: \quad y^4 = p_3(x,z) = x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4$$

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 2.5 *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 2.6 *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 2.7 *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 maximaler 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 2.8 *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 ist somit 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 geometrisch 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 2.9 *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 $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} = 0$.*

Beweis: $(1 \Rightarrow 3)$ Falls q_D eine Gerade ist, dann gilt $a_{11} = a_{02} = 0$ und offensichtlich auch $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} = 0$.
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 $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} = 0$.
$(3 \Rightarrow 2)$ Es gilt $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} = 0$. 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 $q_D(x, y) = a_{02}y^2 + a_{01}y + a_{00} = g_1g_2$ ein Produkt von zwei Geraden.
3. Ist $a_{11} \neq 0$, dann erhalten wir aus $a_{10}^2a_{02} + a_{11}^2a_{00} - a_{11}a_{01}a_{10} = 0$

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

   Beim Einsetzen in q_D bekommen wir

   $$\left(a_{02}y + a_{11}x + a_{01} - \frac{a_{02}a_{10}}{a_{11}}\right)\left(y + \frac{a_{10}}{a_{11}}\right) = g_1g_2.$$

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 2.10 *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 2.11 *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

$$\Phi : Div^{+,i} \to \mathbb{F}_q[x] \times \mathbb{F}_q[x,y] \times \mathbb{F}_q[y], \quad 2 \leq i \leq 4$$

$$\Phi(D) = (u_D(x), q_D(x,y), w_D(y)), \quad mit$$

$$u_D(x) := \prod_{P_i \in supp(D)} (x - x_i)$$

$$w_D(y) := \prod_{P_i \in supp(D)} (y - y_i) \quad und$$

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

die Quadrik durch $P_i \in supp(D)$ grösster 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:

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

Satz 2.12 *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 2.9 erhalten wir dann, dass $q_D(x, y)$ eine Quadrik (oder Gerade) ist mit $a_{11}y_i + a_{10} \neq 0$, 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 2.9 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.

□

2.2 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 *Inverse* eines 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 geschnitten.

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

   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 $D - 4P_\infty$.

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. Insgesamt erhalten wir einen effizienter Reduktionsalgorithmus von kleinerer Komplexität.

Satz 2.13 *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 $|\nu_{P_\infty}(q_{3j})| > |\nu_{P_\infty}(q_{3j+1})|$ $\nu_{P_\infty}(q_{3j+1}) \geq -6$ 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 2.14 *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 2.13. 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:

$$p = \frac{Res_y(g_1, C)}{(x-x_1)(x-x_2)} \quad bzw. \quad q = \frac{Res_y(g_2, C)}{(x-x_3)(x-x_4)}.$$

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, $u_{3j+1} = p.q$, $w_{3j+1} = (y-y_1)(y-y_2)$. Der Divisor $D_{3j+2} = T_1+T_2$ besteht aus den anderen zwei Schnittpunkten von q_{3j+1} und C.

□

Satz 2.15 *$\bar{D}_{3j} = (u_{3j}, q_{3j}, w_{3j})$ 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 $\bar{D}_{3j+2} = (u_{3j+2}, q_{3j+2}, w_{3j+2})$,*
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 2.13.
   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 $|\nu_{P\infty}(q_{3j})| > |\nu_{P\infty}(q_{3j+1})|$ $b_{11} = 0$ 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
   $$\begin{aligned} R_x(q_{3j}, q_{3j+1}) = &- b_{10}a_{02}y^2 - b_{10}a_{01}y - b_{10}a_{00} + b_{02}y^3a_{11} + b_{02}a_{10}y^2 \\ &+ b_{01}a_{11}y^2 + b_{01}a_{10}y + b_{00}a_{11}y + b_{00}a_{10} \\ \lambda w_{3j+1} = &\quad s_3y^3 + s_2y^2 + s_1y + s_0. \end{aligned}$$
   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 2.12 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 2.13 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

$$p = \frac{Res_x(C, g_1)(y - y_3)}{w_{3j}}$$

      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 $Q_2 = P_4$ und $y_{Q_1} = y_3$. Die $x-$Koordinaten von P_3, P_4, Q_1 erhalten wir als Nullstellen von $y_3^4 = p_3(x)$. Alle Nullstellen dieser Gleichung sind verschiedene und zwei davon teilen u_{3j}. Diese die

u_{3j} nicht teilt ist x_{Q_1}. Eine der restlichen Nullstellen (y_3, x_i) ist Nullstelle von g_1 und x_i entspricht somit x_4.
Die Quadrik q_{3j+1} besteht demnach aus den Geraden g_2 und die Gerade durch M und P_∞ und ist gleich q_{3j+2}. Der reduzierte Divisor D_2 ist gleich $D_2 = T_1 + T_2 + P_3$, wobei T_1, T_2 die restlichen zwei Punkten in dem Durchschnitt $M\bar{P}_\infty \cap C$ und es gilt

$$u_{3j+2} = (x - x_3)\frac{Res_y(M\bar{P}_\infty, C)}{x - x_M}$$

$$w_{3j+2} = (y - y_3)\frac{Res_x(M\bar{P}_\infty, C)}{y - y_M}.$$

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, dabei ist möglich $Q_1 = P_5$. Die $y-$Koordinaten y_{Q_1}, y_{Q_2} lassen sich als Nullstellen von

$$p = \frac{R_x(g_1, C)(y - y_3)}{w_{3j}}$$

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 2.13 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 $D_{3j+1} = Q_1 + Q_2 + M$, wobei wie im Fall a) ist möglich $M = Q_1$. 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

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

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. Die Quadrik q_{3j+1} ist gleich die Vereinigung der Geraden g_2 und $M\bar{P}_\infty$.

$$u_{3j+1} = (x - x_M)q,$$
$$w_{3j+1} = (y - y_M)(y + \frac{a_{10}}{a_{11}})^2.$$

Danach können wir, analog zu ii) $\bar{D}_{3j+2}$ bestimmen.

□

Satz 2.16 *Gegeben sind $\bar{D}_{3j+1}, \bar{D}_{3j+2}$. Dann bestimmen wir zuerst E_j und danach können wir 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 mit $b_{10} \neq 0$ und $deg(D_{3j+2}) = 2$. 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 2.14 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 $y_{P_{01}} = y_{P_{02}}$. Dann lässt sich $q_{3(j+1)}$ als $(y - y_{01})q_{3j+2}$ 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 $|\nu_{P_\infty}(q_{3j+1})| > |\nu_{P_\infty}(q_{3j+2})|$ 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:

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

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 2.14 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 $4\times4-$ 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 2.17

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

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

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

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

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 2.13:

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

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 2.13 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:

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

2.3 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.

3 Danksagung

Dieser Artikel ist als Teil meiner Diplomarbeit von 2004 an der Mathematische Institut von Humboldt Universität zu Berlin entstanden. Ich möchte meinem Betreuer Prof. Dr. R.-P. Holzapfel meinen grossen Dank für seine hochwertige Beratung und stetige Unterstützung aussprechen. Ich möchte mich auch bei Prof. J. Estrada Sarlabous von Instituto De Cibernetica , Mathematica Y Fisica, Havanna, Kuba herzlich für seine zahlreiche Hinweise und ständige Hilfe bedanken.

4 Literatur

Literatur

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

[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

[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

[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

[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

[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