Torsionspunkte und Divisionspolynome

Ausarbeitung zum Vortrag des Krypthographyseminars

von

Benjamin Klein

30.05.2011

Betreuer:
Dr. Mohamed Barakat

Technische Universität Kaiserslautern
Fachbereich Mathematik

Inhaltsverzeichnis

1 Grundlagen **3**
1.1 Ein wenig über Gruppen 3
1.2 Ein wenig über elliptische Kurven 3
1.3 Ein wenig über Morphismen 4

2 Torsionspunkte **6**

3 Divisionspolynome **8**

1 Grundlagen

Bevor wir uns dem eigentlichen Themen des Seminarvortrags widmen können, müssen wir zunächst einmal eine Basis schaffen, auf der wir im folgenden aufbauen können. Hierzu werden in diesem Abschnitt die wesentlichen Bausteine behandelt, die zur Behandlung der Torsinonspunkte und der Divisionspolynome notwendig sind. Die Beweise zu den Aussagen finden sich beispielsweise in [$Wash08$] .
Im folgenden sei:

- K *ein Körper*
- $n \in \mathbb{N}$
- $p \in \mathbb{P}$ *Primzahl*

falls dies nicht explizit erwähnt wird.

1.1 Ein wenig über Gruppen

Um das zentrale Theorem dieser Ausarbeitung beweisen zu können, benötigt wir den Hauptsatz über endliche abelsche Gruppen, mit deren Hilfe Gruppen näher untersucht werden können.

Satz 1.1. (*Hauptsatz über endliche abelsche Gruppen*)
Sei G eine endlich erzeugte abelsche Gruppe, dann gilt:

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \tag{1}$$

für $n_1, ..., n_k \in \mathbb{Z}$ und es gilt $n_i | n_{i+1}$ für alle $1 \leq i \leq k-1$.

Bemerkung 1.1. *Berachte, dass in dieser Form des Hauptsatzes, die n_i nicht teilerfremd sind!*

1.2 Ein wenig über elliptische Kurven

Da im folgenden Torsinspunkte, spezielle Punkte einer elliptischen Kurve, näher untersucht werden sollen, muss zunächst einmal klar sein, was man genau unter einer elliptischen Kurve versteht.

Definition 1.1. *Seien $a_1, ..., a_6 \in K$. Man bezeichnet die Gleichung*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

als generalisierte Weierstarss-Gleichung bzgl. $a_1, ..., a_6 \in K$. Die homogene Weisestrass-Gleichung $a_1, ..., a_6 \in K$ lautet:

$$E': \quad y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{3}$$

Die Verschwindungsmenge von E' wird als

$$E(K) := V(E') \subset \mathbb{P}^2_K \tag{4}$$

bezeichnet.

Damit haben wir die Grundlage geschaffen und können nun definieren, was wir unter einer elliptischen Kurve verstehen.

Definition 1.2. *$E(K) \subset \mathbb{P}_k^2$ heißt elliptische Kurve, falls $E(K)$ glatt ist.*

Bemerkung 1.2. *Oftmals können wir uns auf elliptische Kurven der folgenden Form beschränken. Dabei kommte es auf den zugrundeliegenden Körper K an. Für Körper mit Charakteristik ungleich 2 oder 3, lässt sich (2) vereinfachen in*

$$y^2 = x^3 + Ax + B \tag{5}$$

Die elliptische Kurve E ist dann der Graph der Gleichung(5). Diese Form bezeichnet man als Weierstrass-Gleichung. Dabei handelt es sich bei den Koeffizienten $A, B \in K$ um Konstanten.

Bemerkung 1.3. *Die generalisierten Weierstrass-Gleichung stellt eine generellere Form der Weierstrass-Gleichung da, d.h. diese erlaubt uns ein größeres Maß an Flexibilität.*

1.3 Ein wenig über Morphismen

Um unser Ziel, die Untersuchung von Torsionspunkten, zu erreichen werden wir den folgenden Morphismus verwenden.

Definition 1.3. *Sei E eine elliptische Kurve über dem algebraischen Abschluss eines Körpers K. So definieren wir den folgenden Endomorphismus:*

$$\alpha_n : E(\overline{K}) \longrightarrow E(\overline{K}); \quad P \longmapsto \alpha_n(P) := n \cdot P \tag{6}$$

Zur näheren Untesuchung benötigen wir jedoch, spezielle Eigenschaften diese Morphismuns bzw. Handwerkszeug, die Thema eines anderen Vortrags sind. Die zentralen Punkte sind im folgenden aufgeführt.

Corollar 1.1. *Sei E eine elliptische Kurve über dem algebraischen Abschluss eines Körpers K. So hat $\alpha_n(x, y)$ die explizite Darstellung:*

$$\alpha_n(x, y) := (R(x), yS(x)) \tag{7}$$

für $R(x)$ und $S(x) \in \mathbb{Q}[x]$.

Um α_n näher klassifizieren zu können, interessieren wir und für dessen Grad. Dies führt zur folgenden Definition.

Definition 1.4. *Sei $\alpha_n(x, y)$ ein Endomorphismus auf einer elliptischen Kurve $E(\overline{K})$. So ist der Grad von α_n definiert als:*

$$deg(\alpha_n) = Max\,\{deg(p(x)), deg(q(x))\} \tag{8}$$

für $R(x) = \frac{p(x)}{q(x)}$ mit $p(x)$ und $q(x)$ teilerfremd.

Definition 1.5. *Der Endomorphismus α_n heißt separabel, falls $R'(x)$ nicht verschwindet.*

Bemerkung 1.4. *Ist α_n separabel, so ist $E[n] = ker\alpha_n$ und es gilt:*

$$deg\alpha_n = \#E[n] \tag{9}$$

Ist α_n nicht separabel, so gilt:

$$deg\alpha_n > \#E[n] \tag{10}$$

Bemerkung 1.5. *Sei E eine elliptische Kurve über dem algebraischen Abschluss eines Körpers K. Betrachten wir den in Definition 1.4 gegebenen Endomorphismus.*

$$\alpha_n : E(\overline{K}) \longrightarrow E(\overline{K}); \quad P \longmapsto \alpha_n(P) := n \cdot P$$

Hat der zugrundeliegende Körper K die Charakteristik $p \in \mathbb{P}$, so lässt sich die Multiplikation mit n und damit $\#E[n]$, mit Hilfe von Definition 1.6 und Bemerkung 1.4 näher klassifizieren. Die Multiplikation mit n ist genau dann separabel, wenn $p \nmid n$.

2 Torsionspunkte

Nachdem in den Grundlagen elliptische Kurven eingeführt wurden, können wir uns speziellen Punkten einer Kurve widmen. Dies führt zur folgenden Definition.

Definition 2.1. *Sei E eine elliptische Kurve über einem Körper K. Die Menge der n-Torsionspunkte ist*

$$E[n] := \{p \in \overline{K} \mid n \cdot P = \infty\} \tag{11}$$

mit $n \in \mathbb{N}$.

Bemerkung 2.1. *Hervorzuheben ist, dass $E[n]$ Punkte aus dem algebraischen Abschluss $\overline{K}$ von K enhält und damit nicht nur Punkte aus $E(K)$.*

Bemerkung 2.2. *Beachte, dass der Punkt ∞ das neutrale Element bezüglich der Gruppenopertion ist.*

Beispiel 2.1. *Sei E eine elliptische Kurve über K mit Charakteristik $\neq 2, 3$. Wir wollen nun die Menge $E[2]$ bestimmen. Dabei können wir*

$$y^2 = x^3 + Ax + B$$

schreiben als

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad mit\ e_1, e_2, e_3 \in \overline{K}$$

Es ist

$$E[2] := \{p \in \overline{K} \mid 2 \cdot P = \infty\}$$

gerade die Punkte, deren y-Wert verschwindet. Diese sind:

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\} \quad \Rightarrow \quad E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Beispiel 2.2. *Sei E eine elliptische Kurve über K mit Charakteristik $= 2$. Wir wollen nun die Menge $E[2]$ bestimmen. Dabei hat die elliptische Kurve die Darstellung:*

I $y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \quad mit\ a_6 \neq 0$

II $y^2 + a_3y + x^3 + a_4x + a_6 = 0 \quad mit\ a_3 \neq 0$

Da die Tangente an einem Punkt P vertikal sein muss, gilt dass die partielle Ableitung nach y verschwindet. Daraus ergibt sich aber:

I' $2y + x = 0 \quad mit\ a_6 = 0$

II' $2y + a_3 = 0 \quad mit\ a_3 = 0$

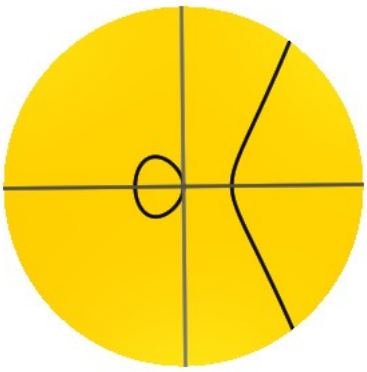
Im Fall I' führt dies zu $y = \sqrt{a_6}$ und damit zu:

$$E[2] = \{\infty, (0, \sqrt{a_6})\}$$

Im Fall II' gilt nach II aber $a_3 \neq 0$, daraus folgt in diesem Fall:

$$E[2] = \{\infty\}$$

Beispiel 2.3. *Betrachten wir die elliptische Kurve gegeben durch* $y^2 = x^3 - x$.



Die 2 Torsionspunkte der gezeichneten Kurve entsprechen gerade den Schnittpunkten der Kurve mit der x-Achse. Also gerade die Punkte, an denen die zugehörigen Tangenten vertikal sind.

Kommen wir nun zur Zentralen Aussage dieser Ausarbeitung, mit deren Hilfe wir Struktur in die Menge der n-Torsionspunkte bringen können.

Theorem 2.1. *Sei* E *eine elliptische Kurve über einem Körper* K *und* $n \in \mathbb{N}$ *eine natürliche Zahl. Ist die* $char(K) = p$ *und* $p \nmid n$ *oder* $char(K) = 0$*, dann gilt*

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$$

Ist die $char(K) = p > 0$ *und* $p \mid n$ *und* $n = p^r n'$ *mit* $p \nmid n'$*. Dann ist*

$$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{oder} \quad E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

3 Divisionspolynome

Bevor wir uns dem Beweis von Theorem 2.1 widmen können, müssen wir zunächst ein wenig Arbeit in die nötigen Grundlagen stecken. Hierzu benötigen wir die Divisionspolynome.

Definition 3.1. *Unter Divisionspolynomen versteht man Polynome der Form* $\psi_n \in \mathbb{Z}[x, y, A, B]$*:*

$$\psi_0 = 0 \tag{12}$$
$$\psi_1 = 1 \tag{13}$$
$$\psi_2 = 2y \tag{14}$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \tag{15}$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \tag{16}$$
$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \tag{17}$$
$$\psi_{2n} = (2y)^{-1}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{18}$$

Lemma 3.1. *ψ_n ist ein Polynom in* $\begin{cases} \mathbb{Z}[x, y^2, A, B], & \text{für } n \text{ ungerade} \\ 2y\mathbb{Z}[x, y^2, A, B], & \text{für } n \text{ gerade} \end{cases}$

Beweis: Beweis, per Induktion nach n.
Aufgrund er Form der Polynome ψ_1 bis ψ_4, ist die Behauptung für $n \leq 4$ korrekt. Sei im nun also $n > 4$. Dann müssen zwei Fälle unterschieden werden, da n gerade und ungerade sein kann.
Sei n nun gerade, so lässt sich n schreiben als $n = 2m$. Da zudem $m > 2$ gilt $2m > m+2$. Damit erfüllen die Polynome aus denen ψ_{2m} zusammengesetzt ist, die Induktionsvoraussetzung.
Für m gerade gilt

$$\psi_{2m} = \underbrace{(2y)^{-1}}_{\mathbb{Z}[x,y^2,A,B]} \underbrace{\underbrace{\underbrace{\psi_m}_{2y\mathbb{Z}[x,y^2,A,B]}}_{\mathbb{Z}[x,y^2,A,B]} \underbrace{(\underbrace{\psi_{m+2}\psi_{m-1}^2}_{2y\mathbb{Z}[x,y^2,A,B]} - \underbrace{\psi_{m-2}\psi_{m+1}^2}_{2y\mathbb{Z}[x,y^2,A,B]})}_{2y\mathbb{Z}[x,y^2,A,B]}}_{2y\mathbb{Z}[x,y^2,A,B]}$$

Für m ungerade gilt

$$\psi_{2m} = \underbrace{(2y)^{-1}}_{(2y)^{-1}\mathbb{Z}[x,y^2,A,B]} \underbrace{\underbrace{\underbrace{\psi_m}_{\mathbb{Z}[x,y^2,A,B]}}_{\mathbb{Z}[x,y^2,A,B]} \underbrace{(\underbrace{\underbrace{\psi_{m+2}}_{\mathbb{Z}[x,y^2,A,B]}\underbrace{\psi_{m-1}^2}_{4y^2\mathbb{Z}[x,y^2,A,B]}}_{4y^2\mathbb{Z}[x,y^2,A,B]} - \underbrace{\underbrace{\psi_{m-2}}_{\mathbb{Z}[x,y^2,A,B]}\underbrace{\psi_{m+1}^2}_{4y^2\mathbb{Z}[x,y^2,A,B]}}_{4y^2\mathbb{Z}[x,y^2,A,B]})}_{4y^2\mathbb{Z}[x,y^2,A,B]}}_{2y\mathbb{Z}[x,y^2,A,B]}$$

Den Fall für n ungerade zeigt man analog.

□

Definition 3.2. *Wir definieren weitere Polynome*

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1} \tag{19}$$
$$\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{20}$$

Lemma 3.2. *Zudem gilt*

$$\phi_n = x^{n^2} + Term\ niedriger\ Ordnung \tag{21}$$
$$\psi_n^2 = n^2 x^{n^2-1} + Term\ niedriger\ Ordnung \tag{22}$$

Beweis: Beweis per Induktion nach n.

□

Lemma 3.3. *Gegeben sei das Polynom $x^3 + Ax + B$ mit zugehöriger Determinante $\Delta = 4A^3 + 27B^2$ und zudem*

$$F(x,z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4$$
$$G(x,z) = 4z(x^3 + Axz^2 + Bz^3)$$
$$f_1(x,z) = 12x^2z + 16Az^3$$
$$g_1(x,z) = 3x^3 - 5Axz^2 - 27Bz^3$$
$$f_2(x,z) = 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3$$
$$g_2(x,z) = A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^3 + 8B^2)z^3$$

Dann gilt

$$Ff_1 - Gg_1 = 4\Delta z^7 \quad \text{und} \quad Ff_2 + Gg_2 = 4\Delta x^7$$

Beweis: Um die Indentitäten zu bestimmen, muss man die Polynome F(x,1) und G(x,1) näher untersuchen. Diese haben keine gemeinsamen Nullstellen. Damit findet man aber Polynome f_1 und g_1, so dass:

$$F(x,1)f_1(x) - G(x,1)g_1(x) = 1$$

Die erste Identität ergibt sich dann in drei Schritten:

1. *Substitution von x durch $\frac{x}{z}$*
2. *Multiplikation mit z^7 (zur Homogenisierung)*
3. *Multiplikation mit 4Δ (zur Eliminierung der Nenner)*

Die zweite Identität zeigt man analog, mit Vertauschung von x und z.

□

Bemerkung 3.1. *Die in Definition 3.1 und 3.2 definierten Polynome bzw. die in Lemma 3.3 gezeigten Identitäten fallen auf den ersten Blick vom Himmel. Letztendlich werden wir diese im Beweis von Theorem 3.1 verwenden, um den Grad von α_n zu bestimmen. Die Form der Polynome ergibt sich eigentlich aus dem Beweis und der im folgenden Corollar beschriebenen explizieten Form des Endomorphismus.*

Corollar 3.1. *Sei P=(x,y) ein Punkt auf der Elliptischen Kurve $E : y^2 = x^3 + Ax + B$ mit $n \in \mathbb{N}$ und $char(K) \neq 2$, so gilt*

$$\alpha_n(P) = n \cdot P = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right) \tag{23}$$

Theorem 3.1. *Sei E eine elliptische Kurve. Dann hat der Endomorphismus α_n den Grad n^2.*

Beweis: Wissen wir, dass $\frac{\phi_n(x)}{\psi_n^2(x)}$ reduziert ist, so sind wir bereits fertig. In diesem Fall haben $\phi_n(x)$ und $\psi_n^2(x)$ keine gemeinsame Nullstellen. Nach Definition 1.4 gilt für den Grad von α_n.

$$deg(\alpha_n) = Max\left\{ deg(\phi_n(x)), deg(\psi_n^2(x)) \right\} = n^2$$

Wir müssen im folgenden also zeigen, dass $\phi_n(x)$ und $\psi_n^2(x)$ reduziert sind. Wir wollen dies per Widerspruchsbeweis tun, indem wir annehmen, dass $\phi_n(x)$ und $\psi_n^2(x)$ nicht reduziert sind und dies zu einem Widerspruch führen.

Sei nun n der kleinste Index, für den $\phi_n(x)$ und $\psi_n^2(x)$ eine gemeinsame Nullstelle haben. Dabei müssen wir wieder zwei Fälle unterscheiden.

Sei n gerade
Da n gerade ist, lässt sich n schreiben als $n = 2m$ mit $m \in \mathbb{N}$. Damit gilt:

$$\begin{aligned} \phi_2(x) &= x\psi_2^2(x) - (\psi_1\psi_3)(x) \\ &= 4xy^2 - (3x_4 + 6Ax^2 + 12Bx - A^2) \\ &= x^4 - 2Ax^2 - 8Bx + A^2 \end{aligned}$$

Die x-Koordinate von $\alpha_{2m}(x,y)$ erhalten wir in zwei Schritten, durch die Multiplikation mit m und anschließend mit 2 und unter der Berücksichtigung, dass

$$\psi_2^2 = 4y^2 = 4(x^3 + Ax + B) \tag{24}$$

wobei hier, die Gleichung der zugrundeliegenden elliptischen Kurve verwendet wurde.

Damit erhalten wir.

$$\begin{aligned}\frac{\phi_{2m}}{\psi_{2m}^2} &= \frac{\phi_2 \frac{\phi_m}{\psi_m^2}}{\psi_2^2 \frac{\phi_m}{\psi_m^2}} \\ &= \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8)}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)} \\ &=: \frac{U}{V}\end{aligned} \tag{25}$$

Lemma 3.3 liefert uns damit die folgenden Identitäten.

$$\begin{aligned}U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) &= 4\psi_m^{14}\Delta \\ U \cdot f_2(\phi_m, \psi_m^2) - V \cdot g_2(\phi_m, \psi_m^2) &= 4\psi_m^{7}\Delta\end{aligned}$$

Dabei ist $\Delta = 4A^3 + 27B^2$. *Zuvor haben wir angenommen, dass* $n = 2m$ *der kleinste Index ist, für den* ϕ_m *und* ψ_m^2 *eine gemeinsame Nullstelle haben. Wenn* U *und* V *nun eine gemeinsame Nullstelle haben, dann auch* ϕ_m *und* ψ_m^2. *Dies ist aufgrund unserer Annahme aber nicht möglich. Also haben* U *und* V *keine gemeinsamen Nullstellen.*

Unser Ziel wird es nun sein zu zeigen, dass $U = \phi_{2m}$ *bzw.* $V = \psi_{2m}^2$ *ist. Aus (25) wissen wir aber bereits.*

$$\phi_{2m} \mid U \qquad und \qquad \psi_{2m}^2 \mid V$$

Zudem kann man zeigen dass U *von der folgenden Form ist.*

$$U = x^{4m^2} + Term\ niedriger\ Ordnung \tag{26}$$

Ein Vergleich mit Lemma 3.2 liefert damit aber die Gleichheit, da U *und* ϕ_m *den gleichen Leitterm haben*

$$U = \phi_{2m} \tag{27}$$

Dies impliziert aber auch, dass

$$V = \psi_{2m}^2 \tag{28}$$

Damit haben aber nun ϕ_n *und* ψ_n^2, *für* n *gerade, keine gemeinsamen Nullstellen. Woraus folgt, dass der Grad von* α_n *gerade* n^2 *ist.*

Sei n ungerade
In diesem Fall können wir n *schreiben als* $n = 2m + 1$ *für* $m \in \mathbb{N}$. *Nehmen wir an, dass* r *eine gemeinsame Nullstelle von* ϕ_n *und* ψ_n^2 *ist. Damit gilt aber*

$$\psi_{n+1}\psi_{n-1}(r) = 0 \tag{29}$$

Da nach Definition 3.2 gerade

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

gilt und $\psi_{n+1}\psi_{n-1}$ ein Polynom in x ist. Aus (29) folgt aber direkt, dass $\psi_{n+1}(r) = 0$ oder $\psi_{n-1}(r) = 0$ damit ist aber auch $\psi^2_{n+\delta}(r) = 0$ wobei entweder $\delta = 1$ oder $\delta = -1$ ist. Dabei ist zu beachten, dass ψ^2_{n+1} und ψ^2_{n-1} Polynome in x sind.
Da n aber in diesem Fall ungerade ist, sind ψ_n und $\psi_{n+2\delta}$ Polynome in x und wir erhlaten, da $\psi^2_n(r) = 0$ ist.

$$(\psi_n\psi_{n+2\delta})^2(r) = (\psi^2_n\psi^2_{n+2\delta})(r) = 0 \tag{30}$$

Im weiteren erhalten wir, dass $\phi_{n+\delta}(r) = 0$ ist, da

$$\phi_{n+\delta} = x\psi^2_{n+\delta} - \psi_n\psi_{n+2\delta} \tag{31}$$

ist. Damit haben aber $\phi_{n+\delta}$ und $\psi^2_{n+\delta}$ eine gemeinsame Nullstelle, wobei $n+\delta$ hier gerade ist. In diesem Fall haben wir zuvor aber gezeigt, dass wenn ϕ_{2m} und ψ^2_{2m} gemeinsame Nullstellen haben, dann haben auch ϕ_m und ψ^2_m gemeinsame Nullstellen.
Im betrachteten Fall können wir dies auf $2m = n + \delta$ anwenden. Mit der zu Beginn getroffenen Wahl von n (n ist kleinster Index so dass....) erhalten wir

$$\frac{n+\delta}{2} \geq n \tag{32}$$

Dies impliziet aber gerade, dass $n = 1$ ist. Jedoch haben aber $\phi_1 = x$ und $\psi^2_1 = 1$ keine gemeinsamen Nullstellen. Damit haben wir also einen Widerspruch!

Daraus folgt aber gerade, dass für n ungerade α_n Grad n^2 hat.

□

Nun haben wir alle Werkzeuge beisammen um Theorem 2.1 zu beweisen.

Beweis von Theorem 2.1:
Wir wollen im folgenden die möglichen Fälle näher betrachten.

$\underline{char(K) = p \nmid n}$
Aus Corollar 1.1 erhalten wir eine explizite Darstellung für $\alpha_n(x, y) := (R(x), yS(x))$. Es gilt mit Lemma 3.2 und Corollar 3.1 aber gerade

$$R(x) = \frac{x^{n^2} + \cdots}{n^2x^{n^2-1} + \ldots} \tag{33}$$

und damit, dass der Zähler von $R'(x) = n^2x^{n^2-2} + \cdots \neq 0$ ist. Damit ist nach Definition 1.5 die Multiplikation mit n aber gerade separabel. Aus Bemerkung 1.4 folgt damit für α_n aber direkt

$$deg\alpha_n = \#E[n]$$

Damit hat nach Theorem 3.1 der Kern von α_n, $ker\alpha_n = E[n]$, die Orndung n^2. Mit Satz 1.1 erhalten wir eine Zerlegung von $E[n]$.

$$E[n] \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

wobei $n_1|n_2|\cdots|n_k$. Ist nun $l \in \mathbb{P}$ mit $l \mid n_i \quad \forall i$, dann ist $E[l] \subseteq E[n]$ und hat Ordnung l^k. Zudem haben wir gezeigt, dass $E[l]$ die Ordnung l^2 hat. Damit ist aber $k = 2$ und wir erhalten, da $n_2 \mid n$ ist, dass $n^2 = \#E[n] = n_1 n_2$. Daraus folgt aber, dass $n_1 = n_2 = n$. Somit haben wir die Behauptung für den Fall $char(K) = p \nmid n$ gezeigt.

$\underline{char(K) = p|n}$
Um diesen Fall näher zu betrachten bestimmen wir die Menge der p-Torsionspunkte $E[p]$. Hier ist zu beachten, dass die Multiplikation mit p nicht separabel ist. Dies ergibt sich aus Bemerkung 1.5. Damit wissen wir aber nach Bemerkung 1.4, dass

$$\#E[p] < p^2$$

Jedes Element von $E[p]$ hat aber gerade die Ordnung 1 oder p, da $E[p]$ nur die Ordnung 1 oder p haben kann. Falls $E[p]$ trivial ist, so ist dies natürlich auch $E[p^k] \quad \forall k$ und wir sind fertig. Betrachten wir nun also den Fall dass die Ordnung von $E[p] = p$ ist. Wir müssen nun zeigen, dass

$$E[p^k] \cong \mathbb{Z}_{p^k}$$

Zunächst wissen wir einmal, dass $E[p^k]$ zyklisch ist. Nehmen wir nun einmal an, dass $E[p^k]$ die Ordnung p^j hat, für $j < k$. Da α_p surjektiv ist wissen wir aber

$$\exists\, Q \quad : \quad pQ = P \tag{34}$$

Damit wissen wir aber $p^j Q = p^{j-1} P \neq \infty$ und somit $p^{j+1} Q = p^j P = \infty$. D.h. Q hat die Ordnung p^{j+1}. Wir können so aber induktiv zeigen, dass für alle k Punkte existieren, die Ordnung p^k haben. Daraus folgt aber direkt, dass $E[p^k]$ zyklisch mit Ordnung p^k ist.

Schreiben wir $n = p^r n'$ mit $r \geq 0$ und $p \nmid n'$, so ist

$$E[n] \cong E[n'] \oplus E[p^r]$$

nun gilt aber zudem, dass $p \nmid n'$. Im ersten Fall ($char(K) = p \nmid n$) haben wir aber gesehen, dass

$$E[n'] \cong \mathbb{Z}[n'] \oplus \mathbb{Z}[n']$$

Der chinesischen Restsatz liefert uns zudem

$$\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \cong \mathbb{Z}_{n'p^r} \cong \mathbb{Z}_n \tag{35}$$

so dass, für den Fall $E[p^r] \cong 0$ oder $E[p^r] \cong \mathbb{Z}_{p^r}$ dies letztendlich bedeutet, dass

$$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{oder} \quad E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

□

Literatur

[Wash08] Lawrence C. Washington. *Elliptic curves: number theory and cryptography, Chapman and Hall/ CRC,2008*

[Ba2011] Mohamed Barakat. *Crypthography: Vorlesungsskript 2010/2011,* `http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf`

[Ma2009] Thomas Markwig. *Theorie und Visualisierung algebraischer Kurven und Flächen: Fortbildung für Mathematiklehrer 2009,* `http://www.mathematik.uni-kl.de/~keilen/download/Lehre/EMWS08/fortbildung.pdf`