Kryptographie

Torsionspunkte und Divisionspolynome

Benjamin Klein

Technische Universität Kaiserslautern

30.5.2011

Definition

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

$$\alpha_n : E(\overline{K}) \longrightarrow E(\overline{K}); \;\; P \longmapsto \alpha_n(P) := n \cdot P \tag{1}$$

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

Folgerung

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

$$\alpha_n(x,y) := (R(x), yS(x)) \tag{2}$$

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

Definition

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

$$deg(\alpha_n) = Max\{deg(p(x)), deg(q(x))\} \tag{3}$$

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

Satz

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

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \tag{4}$$

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

Definition

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

$$E[n] := \{p \in \overline{K} \mid n \cdot P = \infty\} \tag{5}$$

Beispiel

Sei E eine elliptische Kurve über K mit *Charakteristik* $\neq 2$. 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

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:

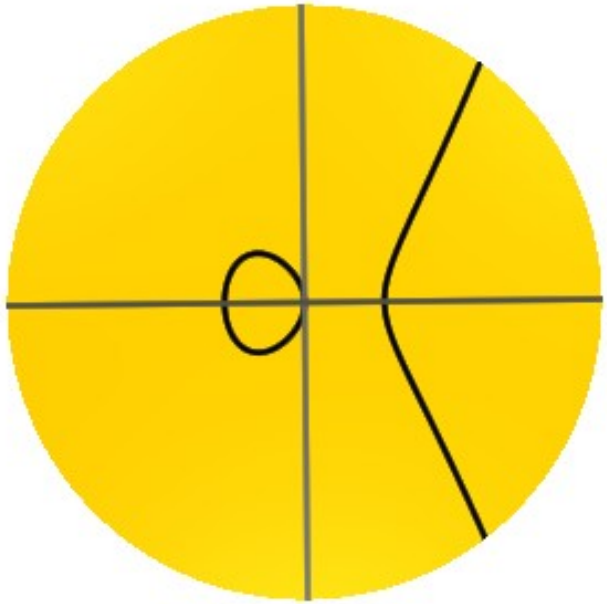
$$E[2] = \{\infty, (0, \sqrt{a_6})\}$$

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

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

Beispiel

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



Theorem

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

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

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

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

Definition

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

$$\psi_0 = 0 \tag{6}$$

$$\psi_1 = 1 \tag{7}$$

$$\psi_2 = 2y \tag{8}$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \tag{9}$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \tag{10}$$

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \tag{11}$$

$$\psi_{2n} = (2y)^{-1}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{12}$$

Lemma

ψ_n ist ein Polynom in $\mathbb{Z}[x, y^2, A, B]$ für n ungerade bzw. in $2y\mathbb{Z}[x, y^2, A, B]$ für n gerade.

Definition

Wir definieren weitere Polynome

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1} \tag{13}$$

$$\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \tag{14}$$

Lemma

Zudem gilt:

$$\phi_n = x^{n^2} + \textit{Term niedriger Ordnung} \tag{15}$$

$$\psi_n^2 = n^2 x^{n^2-1} + \textit{Term niedriger Ordnung} \tag{16}$$

Lemma

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

$$
\begin{aligned}
F(x,z) &= x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z4 \\
G(x,y) &= 4z(x^3 + Axz^2 + Bz^3) \\
f_1(x,y) &= 12x^2z + 16Az^3 \\
g_1(x,z) &= 3x^3 - 5Axz^2 - 27Bz^3 \\
f_2(x,z) &= 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3 \\
g_2(x,z) &= A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 \\
&\quad - 3A^2(A^3 + 8B^2)z^3
\end{aligned}
$$

Dann gilt

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

Folgerung

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:*

$$\alpha_n(P) = n \cdot P = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right) \tag{17}$$

Theorem

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

Theorem

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

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

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

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

Literatur

- Lawrence C. Washington.*Elliptic curves: number theory and cryptography, Chapman and Hall/CRC,2008*
- Mohamed Barakat. *Crypthography: Vorlesungsskript 2010/2011,* `http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf`
- 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`