Kryptographie

Die j-Invariante und Endomorphismen

Stephan Hofmann

Technische Universität Kaiserslautern

20.06.2011

Definition

Sei E eine elliptische Kurve in Weierstrassform, d.h. $y^2 = x^3 + Ax + B$ wobei $A, B \in K$ und $char(K) \neq 2, 3$. Dann nennen wir

$$j = j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2} \in K$$

die j-Invariante von E.

Definition

Sei E eine elliptische Kurve in Weierstrassform, d.h. $y^2 = x^3 + Ax + B$ wobei $A, B \in K$ und $char(K) \neq 2, 3$. Dann nennen wir

$$j = j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2} \in K$$

die j-Invariante von E.

Bemerkung

Der Nenner ist das Negative der Diskriminanten von $x^3 + Ax + B$ *und daher ungleich null.*

Satz

Seien $y_1^2 = x_1^3 + A_1 x_1 + B_1$ und $y_2^2 = x_2^3 + A_2 x_2 + B_2$ zwei elliptische Kurven mit j-Invarianten j_1 und j_2. Dann sind die folgenden Aussagen äquivalent:

1. $\exists\, 0 \neq \mu \in \overline{K}$, *sodass* $A_2 = \mu^4 A_1$, $B_2 = \mu^6 B_1$
2. $j_1 = j_2$

Die Substitution $x_2 = \mu^2 x_1$, $y_2 = \mu^3 y_1$ transformiert eine Gleichung in die andere.

Folgerung

Seien E_1 und E_2 zwei elliptische Kurven mit j-Invarianten j_1 und j_2. Die Relation

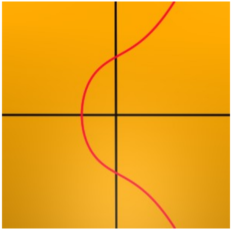
$$E_1 \sim E_2 \;\Leftrightarrow\; j_1 = j_2$$

ist eine Äquivalenzrelation auf der Menge der elliptischen Kurven.
E_1 und E_2 heißen dann $\overline{K}$-äquivalent.

Beispiel

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

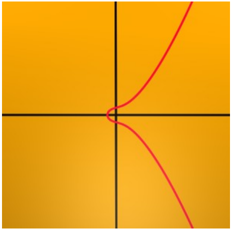
$$j = \frac{55296}{275}$$



Beispiel

$$y^2 = x^3 + \frac{1}{8}x + \frac{3}{64}\ ,\ \mu = 2$$

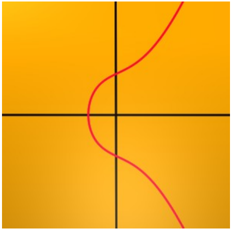
$$j = \frac{55296}{275}$$



Beispiel

$$y^2 = x^3 + \sqrt[4]{2}x + \tfrac{3}{2}\ ,\ \mu = \sqrt[6]{2}$$

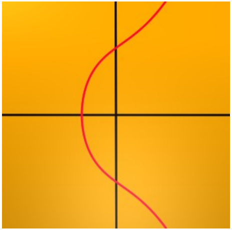
$$j = \tfrac{55296}{275}$$



Beispiel

$$y^2 = x^3 + 3x + 4$$

$$j = \frac{2728}{5}$$



Satz

Es sei $j \neq 0, 1728$. Dann ist j die j-Invariante von

$$y^2 = x^3 + \frac{3j}{1728-j}\,x + \frac{2j}{1728-j} \tag{1}$$

Satz

Es sei $j \neq 0, 1728$. Dann ist j die j-Invariante von

$$y^2 = x^3 + \frac{3j}{1728 - j}\,x + \frac{2j}{1728 - j} \tag{1}$$

Definition

Wir definieren die Standardrepräsentante für $j \neq 0, 1728$ durch (1). Für $j = 0$ sei die Standardrepräsentante durch $y^2 = x^3 + 1$ und für $j = 1728$ durch $y^2 = x^3 + x$ gegeben.

Satz

Es sei $j \neq 0, 1728$. Dann ist j die j-Invariante von

$$y^2 = x^3 + \frac{3j}{1728-j}\,x + \frac{2j}{1728-j} \tag{1}$$

Definition

Wir definieren die Standardrepräsentante für $j \neq 0, 1728$ durch (1). Für $j = 0$ sei die Standardrepräsentante durch $y^2 = x^3 + 1$ und für $j = 1728$ durch $y^2 = x^3 + x$ gegeben.

Folgerung

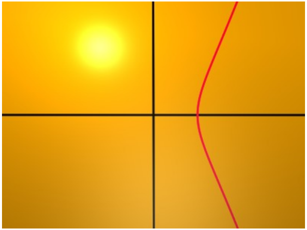
Es gibt eine Bijektion

$$K \leftrightarrow \left\{\overline{K}\text{ Äquivalenzklassen elliptischer Kurven über } K\right\}$$

Beispiel

$$j = -1000$$

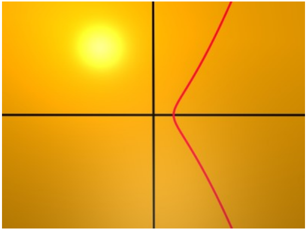
$$y^2 = x^3 + \frac{3*(-1000)}{1728-(-1000)}\,x + \frac{2*(-1000)}{1728-(-1000)}$$



Beispiel

$$j = -100$$

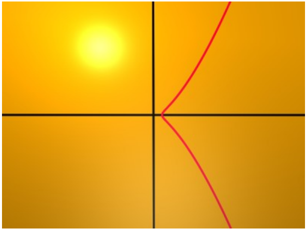
$$y^2 = x^3 + \frac{3*(-100)}{1728-(-100)}\,x + \frac{2*(-100)}{1728-(-100)}$$



Beispiel

$$j = -10$$

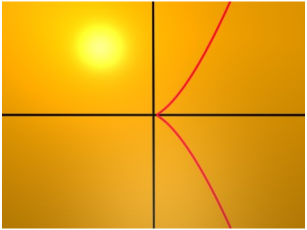
$$y^2 = x^3 + \frac{3*(-10)}{1728-(-10)}\,x + \frac{2*(-10)}{1728-(-10)}$$



Beispiel

$$j = -1$$

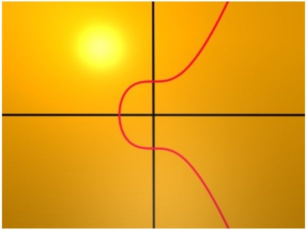
$$y^2 = x^3 + \frac{3*(-1)}{1728-(-1)}\,x + \frac{2*(-1)}{1728-(-1)}$$



Beispiel

$$j = 0$$

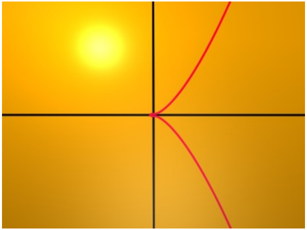
$$y^2 = x^3 + 1$$



Beispiel

$$j = 1$$

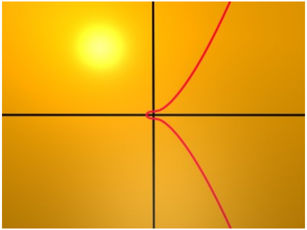
$$y^2 = x^3 + \frac{3*1}{1728-1}\, x + \frac{2*1}{1728-1}$$



Beispiel

$$j = 10$$

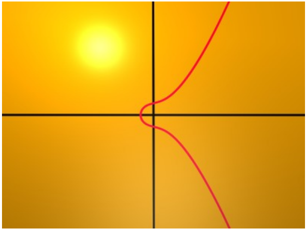
$$y^2 = x^3 + \frac{3*10}{1728-10}\,x + \frac{2*10}{1728-10}$$



Beispiel

$$j = 100$$

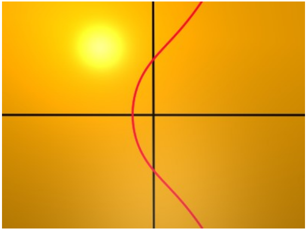
$$y^2 = x^3 + \frac{3*100}{1728-100}\,x + \frac{2*100}{1728-100}$$



Beispiel

$$j = 1000$$

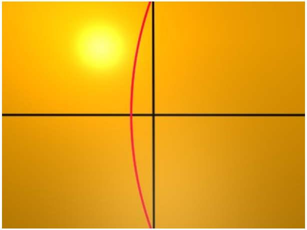
$$y^2 = x^3 + \frac{3*1000}{1728-1000}\,x + \frac{2*1000}{1728-1000}$$



Beispiel

$$j = 1500$$

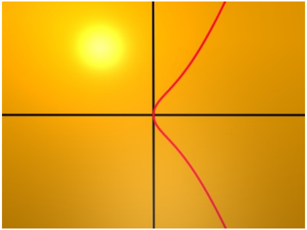
$$y^2 = x^3 + \frac{3*1500}{1728-1500}\,x + \frac{2*1500}{1728-1500}$$



Beispiel

$$j = 1728$$

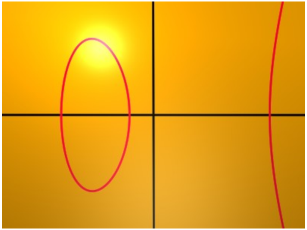
$$y^2 = x^3 + x$$



Beispiel

$$j = 2500$$

$$y^2 = x^3 + \frac{3*2500}{1728-2500}\,x + \frac{2*2500}{1728-2500}$$



Definition

Unter einem Endomorphismus verstehen wir eine Abbildung

$$\alpha : E(\overline{K}) \to E(\overline{K})$$

sodass $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$
und es existieren rationale Funktionen $R_1(x,y), R_2(x,y)$ mit Koeffizienten in $\overline{K}$, sodass

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)) \quad \forall (x,y) \in E(\overline{K})$$

Definition

Unter einem Endomorphismus verstehen wir eine Abbildung

$$\alpha : E(\overline{K}) \to E(\overline{K})$$

sodass $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$
und es existieren rationale Funktionen $R_1(x,y), R_2(x,y)$ mit Koeffizienten in $\overline{K}$, sodass

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)) \quad \forall (x,y) \in E(\overline{K})$$

Bemerkung

Es gilt immer $\alpha(\infty) = \infty$. Wir notieren den trivialen Endomorphismus, der jeden Punkt auf ∞ abbildet, durch $\alpha = 0$ und nehmen an, dass von jetzt an $\alpha \neq 0$.

Beispiel

Sei E gegeben durch $y^2 = x^3 + Ax + B$ und sei $\alpha(P) = 2P$.
α ist ein Homomorphismus und $\alpha(x,y) = (R_1(x,y), R_2(x,y))$ mit

$$R_1(x,y) = m^2 - 2x$$
$$R_2(x,y) = m(3x - m^2) - y$$

wobei $m = \left(\frac{3x^2+A}{2y}\right)$
Also ist α sogar ein Endomorphismus.

Lemma

Sei $\alpha : E(\overline{K}) \to E(\overline{K})$ ein Endomorphismus und E in Weierstrassform gegeben. Dann existieren rationale Funktionen $r_1(x), r_2(x)$ sodass

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, r_2(x)y\right) \tag{2}$$

wobei $p(x)$ und $q(x)$ teilerfremde Polynome sind.

Lemma

Sei $\alpha : E(\overline{K}) \to E(\overline{K})$ ein Endomorphismus und E in Weierstrassform gegeben. Dann existieren rationale Funktionen $r_1(x), r_2(x)$ sodass

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, r_2(x)y\right) \tag{2}$$

wobei $p(x)$ und $q(x)$ teilerfremde Polynome sind.

Definition

Wir definieren den Grad eines Endomorphismus α durch

$$deg(\alpha) := max\{deg(p(x)), deg(q(x))\}$$

wobei p und q die Polynome aus (2) sind.

Definition

Wir nennen einen Endomorphismus separabel, wenn $r_1'(x) \neq 0$, wobei $r_1(x)$ die rationale Funktion aus (2) ist.

Definition

Wir nennen einen Endomorphismus separabel, wenn $r_1'(x) \neq 0$, wobei $r_1(x)$ die rationale Funktion aus (2) ist.

Lemma

- $r_1'(x) \neq 0 \Leftrightarrow p'(x) \neq 0$ *oder* $q'(x) \neq 0$
- *Falls char(K)=0 haben alle nichtkonstanten Polynome eine Ableitung ungleich null.*
- *Falls char(K)=p haben alle Polynome der Form* $f(x^p)$ *eine Ableitung gleich null.*

Beispiel

Sei $\alpha(P) = 2P$. Dann ist $R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x$. Mit $y^2 = x^3 + Ax + B$ folgt dass:

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

Damit ist $deg(\alpha) = 4$.
Außerdem ist $q'(x) = 4(3x^2 + A) \neq 0$, auch falls $char(K) = 3$ da $A = 0$ nicht auftreten darf, und somit ist α separabel.

Definition

Sei E eine elliptische Kurve über $\mathbf{F}_q$. Wir definieren die Frobenius Abbildung durch

$$\phi_q(x,y) := (x^q, y^q).$$

Definition

Sei E eine elliptische Kurve über $\mathbf{F}_q$. Wir definieren die Frobenius Abbildung durch

$$\phi_q(x,y) := (x^q, y^q).$$

Lemma

ϕ_q ist ein Endomorphismus. Es gilt $deg(\phi_q) = q$ und ϕ_q ist nicht separabel.

Satz

Sei $\alpha \neq 0$ ein Endomorphismus. Dann gilt:

1. *Falls α separabel $\Rightarrow deg(\alpha) = |ker(\alpha)|$*
2. *Falls α nicht separabel $\Rightarrow deg(\alpha) > |ker(\alpha)|$*

Satz

Sei E eine elliptische Kurve über K und $0 \neq \alpha$ ein Endomorphismus von E.
Dann ist $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektiv.

Lemma

Seien $\alpha_1, \alpha_2, \alpha_3$ Endomorphismen einer elliptischen Kurve E und $\alpha_1 + \alpha_2 = \alpha_3$. Schreibe

$$\alpha_j(x,y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x)) \;\; \forall j = 1,2,3$$

Falls Konstanten c_{α_1} und c_{α_2} existieren, sodass:

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1} \; , \; \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}$$

Dann gilt:

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}$$

Proposition

Sei E eine elliptische Kurve über einem Körper K und $0 \neq n \in \mathbb{Z}$. Sei die Multiplikation mit n auf E gegeben durch:

$$n(x,y) = (R_n(x), yS_n(x)) \ \ \forall (x,y) \in E(\overline{K})$$

wobei R_n und S_n rationale Funktionen sind. Dann gilt:

$$\frac{R_n'(x)}{S_n(x)} = n.$$

Somit ist die Multiplikation mit n genau dann separabel, wenn gilt $p \nmid n$ wobei $p = char(K)$.

Proposition

Sei E eine elliptische Kurve über dem Körper $\mathbf{F}_q$, wobei $q = p^n$, $p \in \mathbb{P}$, $n \in \mathbb{N}$ und seien $0 \neq r, s \in \mathbb{Z}$. Dann ist der Endomorphismus

$$r\phi_q + s$$

separabel, genau dann wenn $p \nmid s$.