Edwardsova křivka s dalšími:

$$x^2+y^2 = 1+dx^2y^2, \quad d \in K \setminus \{0,1\}$$

Proč $d \neq 1$? Protože $1+x^2y^2-x^2-y^2 = (x^2-1)(y^2-1)$

Homogenizace dává $V^2Z^2 + X^2Z^2 = Z^4 + dX^2Y^2$

Pokud $Z=0$ $\quad 0 = dX^2Y^2$, což znamená $X=0$ nebo $Y=0$

TAKŽE BODY V NEKONEČNU EDWARDSOVY KŘIVKY $(1:0:0)$ a $(0:1:0)$

$d = -1$ v reálných číslech $\quad x^2+y^2 = 1 - x^2y^2$

zajímají nás $(\alpha, \beta) \in \mathbb{R}^2$, že $\alpha^2+\beta^2+\alpha^2\beta^2 = 1$

Křivka leží uvnitř jednotkového kruhu. Odtud $\Downarrow$ $0 < \alpha^2+\beta^2 \leq 1$

body $(\pm 1, 0)$ i $(0, \pm 1)$

$\alpha^2+\beta^2+\alpha^2\beta^2 = \alpha^2+\beta^2 \iff \alpha\beta = 0$

Symetrické podle os x i y

$\alpha = \beta \Rightarrow \alpha^4 + 2\alpha^2 - 1 = 0$

$(\alpha^2+1)^2 - 2 \Longrightarrow \alpha^2 = \sqrt{2} - 1$

$|\alpha| \approx 0{,}64 < 0{,}71 \approx \frac{\sqrt{2}}{2}$

$x^2+y^2 = -s^4x^2y^2 + 1$

$d = -s^4$

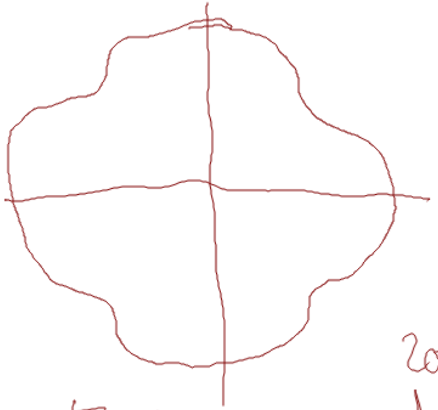
$\rho \longrightarrow \frac{1}{s}\left(\frac{\sqrt{1+s^4} - 1}{s^2}\right)^{1/4}$

ρ (→ 0,64)

$s \longrightarrow \infty$

$\rho \longrightarrow 1/s$

Reálná Edwardsova pro $d<0$ má jednu větev, ta je uzavřená



? Bod v nekonečnu !

Podezřelé: Bod v ∞ pro singulární

Ověříme to.

$$aX^2 + y^2 = 1 + dx^2y^2$$, kde $a, d \in K^*$, $a \neq d$

TWISTED EDWARDS CURVE

zobecněné, přechýlené

$(0:1:0)$ $(1:0:0)$

$$F(X,Y,Z) = dX^2Y^2 + Z^4 - Y^2Z^2 - aX^2Z^2$$

$$\frac{\partial F}{\partial X} = 2X(dY^2 - aZ^2) \quad \frac{\partial F}{\partial Y} = 2Y(dX^2 - Z^2) \quad \frac{\partial F}{\partial Z} = 4Z^3 - 2Z(aX^2 + Y^2)$$

v nevlastních bodech je proj. křivka singulární

$a \neq d$

$dx^2y^2+1=y^2+ax^2$

Parciální derivace

$\frac{\partial f}{\partial x}=2x(dy^2-a)$ $\frac{\partial f}{\partial y}=2y(dx^2-1)$

PRACUJEME ZA PŘEDPOKLADU $\operatorname{char} K \neq 2$

$d\alpha^2\beta^2+1=\beta^2+a\alpha^2$

$\frac{\partial f}{\partial x}(\alpha,\beta)=0$ \ $\frac{\partial f}{\partial y}(\alpha,\beta)=0$	$\beta=0$	$d\alpha^2=1$
$\alpha=0$	✗	$1=0$
$d\beta^2=a$	$0=a$	$\frac{a}{d}+1=\frac{a}{d}+\frac{a}{d} \Rightarrow 1=\frac{a}{d} \Rightarrow a=d$

$d\alpha^2\beta^2=a\alpha^2=\frac{a}{d}$

Zobecněné Edwardsovy křivky hladké ve všech afinních bodech.

Ireducibilita

Ptejme se nejprve zda existují polynomy $u, v \in K[T]$, takže

$f(x,y) = dx^2y^2 + 1 - ax^2 - y^2 = u(x)v(y)$ — možno jen když $\deg(u) = \deg(v) = 2$

$= (u_2x^2 + u_1x + u_0)(v_2y^2 + v_1y + v_0)$

Musí být $u_0v_0 = 1$, takže lineární úpravou můžeme zeskat situaci, kdy $u_0 = 1$, $v_0 = 1$

$(u_2x^2+1)(d^{-1}u_2^{-1}y^2+1) = dx^2y^2 + 1 + du_2^{-1}y^2 + u_2x^2$, $u_2 = a$

$da^{-1} = 1 \Rightarrow a = d$

Pokud $a \neq d$, tak polynomy u a v neexistují.

Proto, pokud se $f(x,y)$ rozkládá $h \cdot g$, tak ~~buď~~ h i g lineární v x nebo ~~buď~~ h i g lineární v y.

Pokud h i g lineární v x, tak že $x^2(dy^2-a) - (y^2-1)$ rozkládá v $K(y)[X]$ $\frac{y^2-1}{dy^2-a}$ je čtverec v $K(y)$

Podobně druhý případ vede na požadavek $\frac{ax^2-1}{dx^2-1}$ ČTVEREC V $F(X)[Y]$ TO JE MOŽNÉ JEN PRO $d=a$

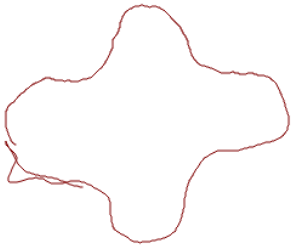
Lze zjistit, že rod (genus) zobecněné Edw. křivky je = 1

Místa stupně 1 tvoří $(E(K), \oplus)$

z hladkosti víme, že každý afinní bod je místo stupně 1

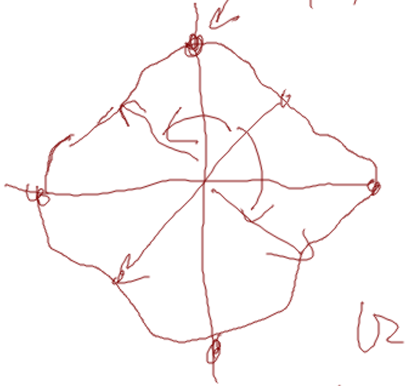
Bod v nekonečnu:
- 2 místa stupně 1
- [illegible] stupně 1
- 1 místo stupně 2

V obou případech body v nekonečnu nezasahují do struktury $(E(K), \oplus)$



Pro zobecněné Edw. křivky je konvence bere jako neutrální prvek bod (0,1)

(0,1) neutrální prvek



VZOREC PRO SČÍTÁNÍ

$$(\alpha_1,\alpha_2)\oplus(\beta_1,\beta_2)=\left(\frac{\alpha_1\beta_2+\alpha_2\beta_1}{1+d\alpha_1\alpha_2\beta_1\beta_2},\frac{\alpha_2\beta_2-a\alpha_1\beta_1}{1-d\alpha_1\alpha_2\beta_1\beta_2}\right)$$

Pokud $d\cdot(\alpha_1,\alpha_2,\beta_1,\beta_2)$ jmenovatele je 1

Vzorec … prvek

$$\alpha\oplus\beta=(\alpha_1\beta_2+\alpha_2\beta_1,\ \alpha_2\beta_2-\alpha_1\beta_1)$$

⊕(0,1) neutr.

⊕(0,−1)

⊕(1,0)

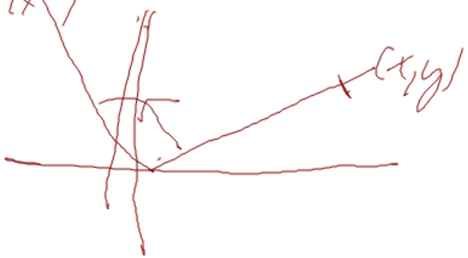
⊕(−1,0)

$\alpha_1=0$, $\alpha_2=\pm1$: $(\pm\beta_1,\pm\beta_2)=\pm\beta$

$\alpha_1=\pm1$, $\alpha_2=0$: $(\pm\beta_2,\mp\beta_1)$

$(x,y)\to(y,-x)$, $(-y,x)$

$(x,-y)$



$$(i\sin\alpha + \cos\alpha)(i\sin\beta + \cos\beta)$$

$$= (i(\sin\alpha\cos\beta + \sin\beta\cos\alpha) + (\cos\alpha\cos\beta - \sin\alpha\sin\beta)$$

$$\frac{\alpha_1\beta_2+\alpha_2\beta_1}{1+d\cdots} \qquad \frac{\alpha_2\beta_2-\alpha_1\beta_1}{1-d\cdots}$$

Sčítání na Edwardsově křivce lze „aproximovat“

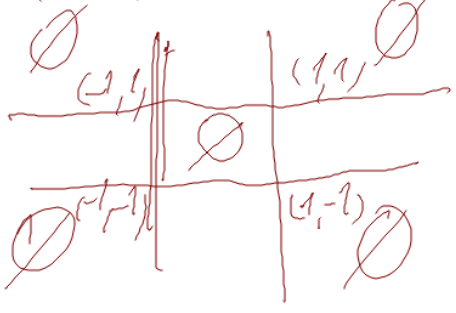
a komplexním násobením na jednotkové kružnici po výměně os x a y (přesněji: po otočení o 90°)

Jak wygląda Edwardsova krivka E: $x^2+y^2=1+dx^2y^2$
reálná
pokud $d>1$

$A\in(\alpha,\beta)\in E$ $\quad \alpha=0 \Rightarrow \beta=\pm 1$
$\beta=0 \Rightarrow \alpha=\pm 1$

Pokud
$0<|\alpha|\leq 1$ $\Rightarrow 1+d\alpha^2\beta^2-\alpha^2-\beta^2 > 1+\alpha^2\beta^2-\alpha^2-\beta^2$
$0<|\beta|\leq 1$ ZÁPORNÝ ROZDÍL $=(1-\alpha^2)(1-\beta^2)\geq 0$

$|\alpha|\geq 1,\ |\beta|\geq 1$ $\quad 1+d\alpha^2\beta^2-\alpha^2-\beta^2 > (1-\alpha^2)(1-\beta^2)\geq 0$




$y^2 = \frac{x^2-1}{dx-1}$
dárek 2 místo
dárek 2 místo

Biracionálně ekvivalentní křivky
mají izomorfní funkční tělesa

Pokud jsou rodu 1, tak mají navzájem izomorfní
grupy sčítání, protože tyto grupy se dají
definovat pomocí funkčních těles

Vypadá třída biracionální ekvivalence

<u>2 kroky</u>

1. krok racionální zobrazení
2. krok vzájemně inverzní rac. zobrazení

Racionální zobrazení nad K. Ať C_1, C_2 planární ireducibilní afinní křivky

Pro $\rho : C_1 \to C_2$ existují $r_1, r_2 \in K(x_1, x_2)$ $\quad r_i = \frac{a_i}{b_i}$

že pro nekonečně mnoho $\alpha \in C_1$ je $b_1(\alpha) \neq 0$
$b_2(\alpha) \neq 0$

a současně $(r_1(\alpha), r_2(\alpha)) \in C_2$

Pozad ~~toto~~ platí tak

(1) kdykoliv $b_1(\alpha) \neq 0$, $b_2(\alpha) \neq 0$ tak $(r_1(\alpha), r_2(\alpha)) = \rho(\alpha) \in C_2$

(2) existuje jen konečně mnoho $\alpha \in C_1$, že $b_1(\alpha) = 0$
nebo $b_2(\alpha) = 0$

Rac. zobrazení je definováno skoro všude

Pozn.

(r_1, r_2) je reprezentant ρ

ρ může mít více reprezentantů

2 reprezentanti se shodují ve všech, kde jsou oba definovány.

Biracionalna ekvivalenca krivulj

C_1 in C_2 nadalje zaporedoma, ne

$\exists\ \varphi: C_1 \to C_2$ $\quad \sigma: C_2 \to C_1$ racionalni obratna, ne

$\sigma\varphi(x) = x$ skoraj vsude (za vsako točko $x \in C_1$ razen morda končno mnogih)

in $\varphi\sigma(y) = y$ za skoraj vsako točko $y \in C_2$ (razen morda končno mnogih)

Biracionalna ekvivalenca afinih krivulj

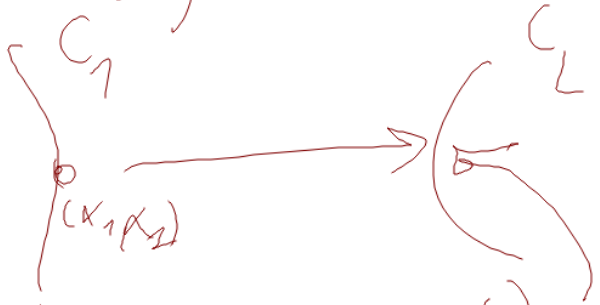
Definicija podobna ekvivalenci projektivnih krivulj

a zgornja $\cong$ funkcijskih teles.

Každá krivka rodu 1, ktorá má aspoň 1 K-rac. bod je birac. ekv. nad K nejakej WK nad K

Musíme definovať racionálne zobrazenie Edw. krivky na WK

Pokud pro 2 konvex K-diferencovatelné křivky platí



$$(x_1, y_1) \rightsquigarrow (\lambda_{11} x_1 + \lambda_{12} x_2 + \mu_1,\ \lambda_{21} x_1 + \lambda_{22} x_2 + \mu_2)$$

je všech WK pro K-diferencovatelné Γ_K,
ale pouze γ_1 $\exists$ f konvexní, že WK $y^2 = f(x)$
$f'(\xi)$ je ~~dobře~~ dvojec

Zobecněné EDW křivky jsou birac. ekvivalentní MK

Věta Ať $a, d \in K^*$ takové, že $a \neq d$.

Ať $A = \dfrac{2(a+d)}{a-d}$, $B = \dfrac{4}{a-d}$. Pak $A \neq \pm 2$.

Každé $(A,B) \in K \times K^*$, $A \neq 2$, existují $a, d \in K^*$, že $a \neq d$, a toto platí)

Zobecněná Edw. křivka $1 + dx^2y^2 = ax^2 + y^2$ je biracionálně ekvivalentní MK $By^2 = x^3 + Ax^2 + x$

Příslušná rac. zobrazení jsou

$E \to M \qquad (x,y) \mapsto \left(\dfrac{1+y}{1-y}, \dfrac{1+y}{x(1-y)}\right)$

$M \to E \qquad (x,y) \mapsto \left(\dfrac{x}{y}, \dfrac{x-1}{x+1}\right)$

Lemma E.4

↓

Věta E.7

Pokud $u = \frac{1+y}{1-y}$ $v = \frac{1+y}{x(1-y)}$, tak

$x = \frac{u}{v}$, $u(1-y) = 1+y \implies y = \frac{u-1}{u+1}$

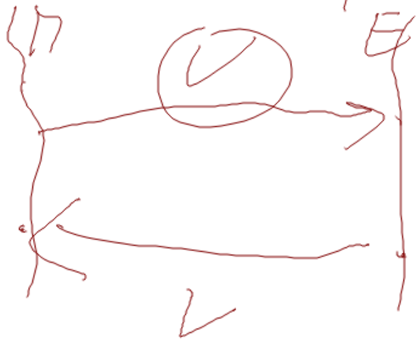
$u-1 = uy + y$

To ukazuje, že

$(x,y) \longmapsto \left(\frac{1+y}{1-y}, \frac{1+y}{x(1-y)}\right)$ má „inverzní" zobrazení

$(u,v) \longmapsto \left(\frac{u}{v}, \frac{u-1}{u+1}\right)$

↑ na skoro všude (což pro [illegible] dle def. rac. zobrazení „nevadí")



Ať $By^2 = x^3 + Ax^2 + x$ $\quad a = \frac{A+2}{B}$ $\quad d = \frac{A-2}{B}$

Pokud (x,y) leží na $\mathcal{K}$, pak (u,v) leží na

kvadrice $1 + du^2v^2 = au^2 + v^2$ $\quad u = \frac{x}{y}$ $\quad v = \frac{x-1}{x+1}$

$$1 + \frac{(A-2)}{B}\frac{x^2}{y^2}\underbrace{\frac{(x-1)^2}{(x+1)^2}}_{x^3+Ax^2+x} \overset{?}{=} \frac{A+2}{B}\frac{x^2}{y^2} + \frac{(x-1)^2}{(x+1)^2}$$

$$(x^2+Ax+1)(x+1)^2 + (A-2)x(x-1)^2 \overset{?}{=} (A+2)x(x+1)^2 + (x^2+Ax+1)(x-1)^2$$

$$(x^2+Ax+1)4x = Ax(4x) + 2x\underbrace{((x+1)^2+(x-1)^2)}_{2x^2+2}$$

$4x(x^2+1)$ $\qquad$ $4x(x^2+1)$

$$(a,d) \longmapsto \left(\frac{2(a+d)}{a-d}, \frac{4}{a-d}\right) \qquad a,d \neq 0 \quad a \neq d$$

$$(A,B) \longmapsto \left(\frac{A+2}{B}, \frac{A-2}{B}\right) \qquad B \neq 0 \quad A \neq \pm 2$$

$$\frac{2(a+d)}{a-d} = 2 \iff d = 0$$

$$= 2 \iff a = 0$$

$$a = \frac{A+2}{B}$$

$$d = \frac{A-2}{B}$$

$$a+d = \frac{2A}{B} \qquad a-d = \frac{4}{B}$$