Ať C ired. proj. planární křivka nad K

(1) $\exists x \in C$, tž. K-rac.

Co to zn., že C je eliptická?

(2) genus = rod = 1

? Co je to rod? GOOD QUESTION!

Vyložit neformálně, co je to rod v případě $K = \mathbb{C}$

Pozn. Přesná definice rodu využívá strukturní vlastnosti kanonických divisorů

$$\sum_P v_P(\sigma) P$$

valuace

$\sigma \in K(C)$ $\forall \sigma$ $\exists$ konečně mnoho míst P že $v_P(\sigma) \neq 0$

Co je to rod, pokud $K = \mathbb{C}$

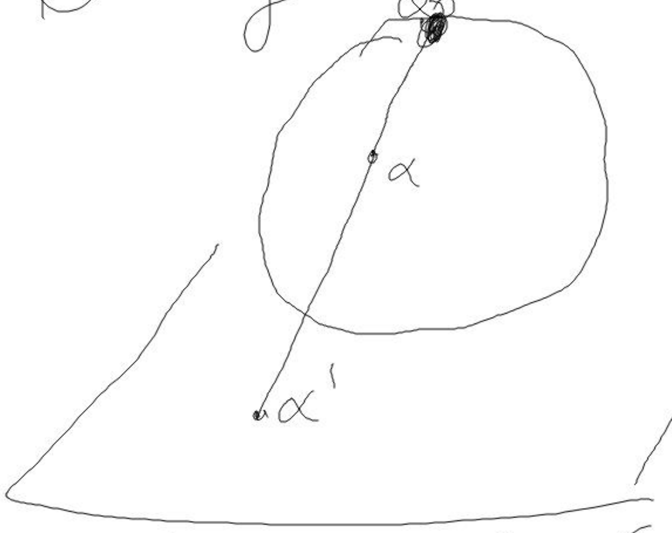
$\mathbb{A}^1(\mathbb{C})$ $\quad$ $\mathbb{P}^1(\mathbb{C})$

euklid. rovina $\mathbb{R}^2$

POVRCH KOULE = SFÉRA

KOULICE

Geometrie křivek nad $\mathbb{C}$



$(1:0) = \infty$

α

α' přímka

STEREOGRAFICKÁ PROJEKCE

Prostorové promítnutí

v $\mathbb{R}^3$ jiné povrchy než koule

kompaktní (v omezené části prostoru)

lok. difeom. kruhu (hladké a bez hranice)

Torus = povrch duše pneumatiky

preclík

spojité deformace

Koule = elipsoid

TOPOLOGICKÝ INVARIANT JE POČET DĚR

Sféra	0	díry
Torus	1	díry
preclík	2	díry

počet děr = genus rod povrchu

Některé 1-rozměrné útvary v $\mathbb{R}^3$ lze
spojitou deformací převést do $\mathbb{R}^2$

Některé dvoj. útvary v $\mathbb{R}^4$ lze spojitou def. převést do $\mathbb{R}^3$

$\mathbb{C}\times\mathbb{C} \longleftrightarrow \mathbb{R}^4$

Křivka nad $\mathbb{C}$ je podmnožina

Pokud C hladká, tak ji lze deformací
umístit do $\mathbb{R}^3$, a tak definovat
její rod (genus)

Křivka rodu 1 nad $\mathbb{C}$

rod C alg. odv. z $K(C)$ dobrá ~~pro~~ domus

Eliptické křivky odpovídají nad $\mathbb{C}$ torům (prstenec)

Struktura el. křivek nad $\mathbb{R}$ o tom vydává svědectví. Řez torem je 1 nebo 2 elipsy.

Lze očekávat, že proj. eliptické nad $\mathbb{R}$ budou mít 1 nebo 2 větve (uzavřené)

Přesvědčíme se o tom na WK

Weierstraß

ss

$$x_2^2 + x_2 g(x_1) = f(x_1) \qquad f, g \in K[x_1]$$

$\deg(g) \leq 1$

WR zadaná WR (α, β) $\deg(f) = 3$, f monické

R rovnice

$$\beta^2 + \beta g(\alpha_1) = f(\alpha_1)$$

$$x_2^2 + a_1 x_1 x_2 + a_3 x_2 = x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6$$

WR v stand. $b_2 = 4a_2 + a_1^2$, $b_4 = \dots$ $b_6 =$ $b_8 =$

$$\Delta(C) = 8b_4^3 + 9b_2 b_2 b_6 - 27b_6^2 - b_2^2 b_8$$

DISKRIMINANT

C hladká $\iff \Delta(C) \neq 0$

WK $x_2^2 = f(x_1)$ $\mathrm{char}(K) \notin \{2,3\}$

$W(x_1,x_2) = x_2^2 - f(x_1)$ $\mathrm{char}(K) \neq 2$

$C = V_W$ $\frac{\partial W}{\partial x_1} = -f'(x_1)$ $\frac{\partial W}{\partial x_2} = 2x_2$

$(\alpha_1,\alpha_2) \in C$ je singulární? $\Rightarrow \alpha_2 = 0 \Rightarrow f(\alpha_1) = 0$

$\Rightarrow$ $f'(\alpha_1) = 0$

α_1 je vícenásobný kořen

TVRZENÍ C je hladká

$\Longleftrightarrow$ f nemá vícenásobný kořen

Je-li α v.k. f, tak $(\alpha, 0)$ je singularita

Pozn. $x_2^2 = x_1^3 + ax + b$, char$(K) \neq 2$ $\quad 4a^3 + 27b^2 \neq 0 \Leftrightarrow$ HLADKÁ

PWK $\quad x_2^2 x_3 + x_2 x_3 G(x_1, x_3) = F(x_1, x_3)$

homogenizace

$g(x_1) = ax_1 + b$

$G(x_1, x_3) = ax_1 + bx_3$

$(\alpha_1 : \alpha_2 : 0)$ leží na křivce $\Leftrightarrow$ $0 = \alpha_1^3$

JEDINÝ BOD V NEKONEČNU JE $(0:1:0)$

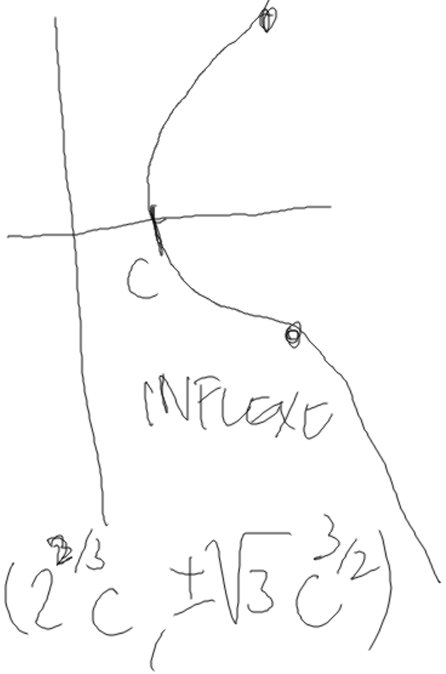
$$\frac{\partial W}{\partial x_3} = x_2^2 + x_2 a x_1 + 2x_2 b x_3 - \frac{\partial F}{\partial x_3} \to 0$$

dosazení $(0:1:0)$ dá $1^2 = 1$

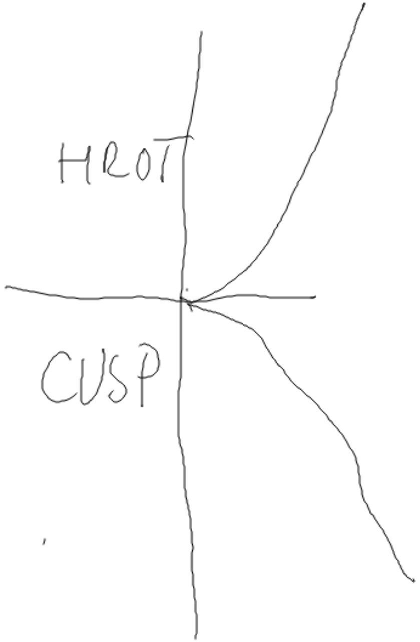
KŘIVKA JE HLADKÁ v $(0:1:0)$

$x_2^2 = x_1^3 - c^3$

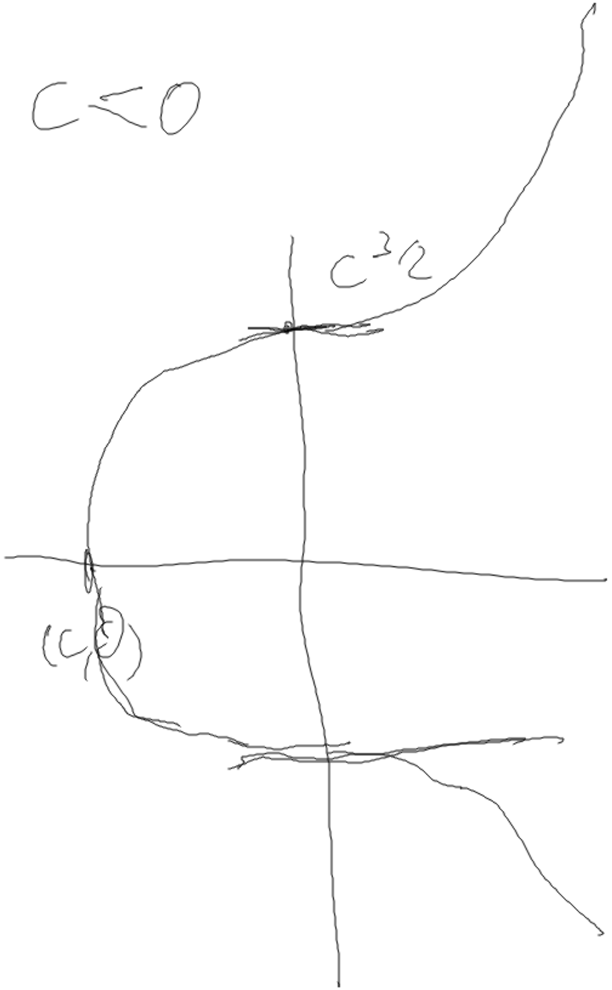
$c > 0$



$c = 0$



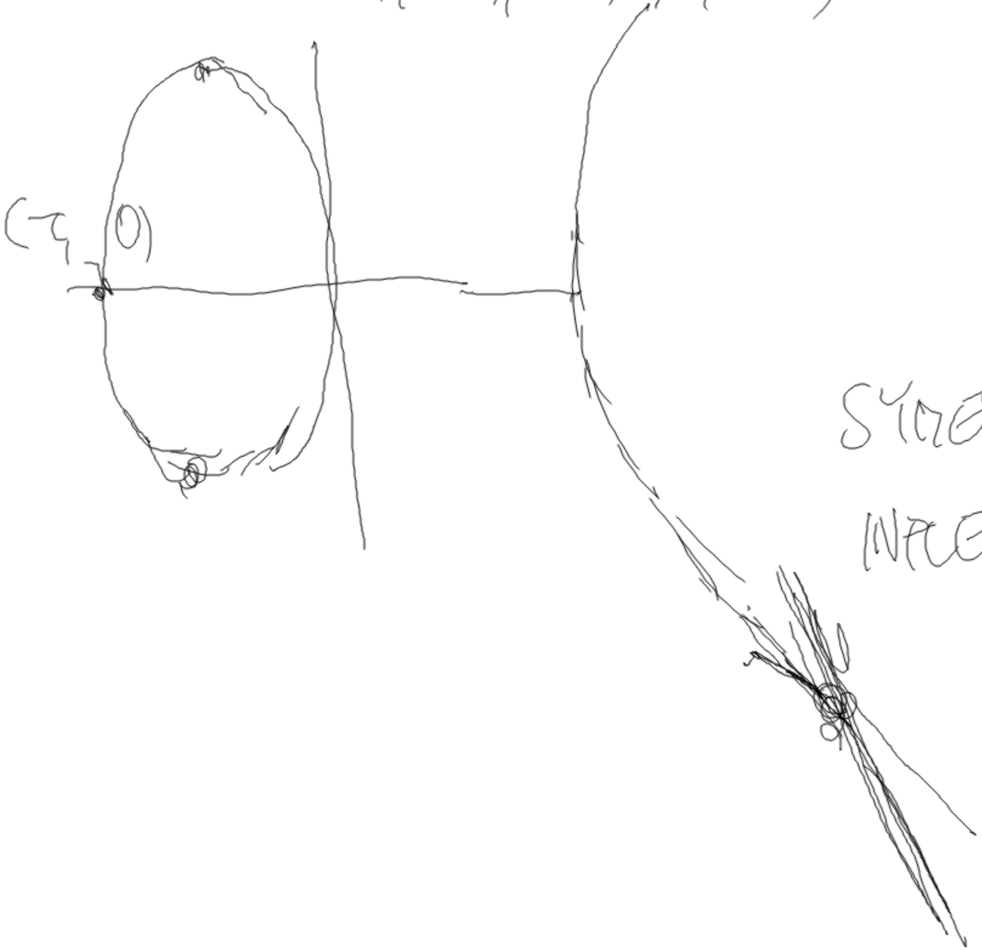
$c < 0$



řez torem

$$x_2^2 = x_1^3 - c^2 x_1$$
$$= x_1(x_1 - c)(x_1 + c)$$

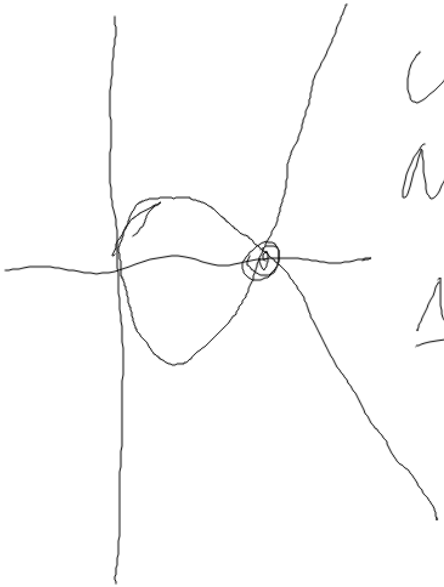
$c > 0$



SYMETRICKY

INFLEXE NA TODE

$$x_2^2 = x_1(x_1 - 1)^2$$



UZEL

NODE

NOD

Co je to grupa eliptické křivky

Lze definovat v řeči divisorů formální suma $\sum a_P P$

DIVISORY LZE SČÍTAT — grupa F

P umístěk(C)

$a_P \neq 0$ je v $< \infty$ případech

$a_P \in \mathbb{Z}$

$\deg(\sum a_P P) = \sum a_P \deg(P)$

divisory stupně 0 tvoří podgrupu

Podgrupu označíme B

Hlavní divisory také tvoří podgrupu.

Označme ji A

B/A

Platí pro každou projektivní hlad. křivku C

Závisí jen na struktuře divisorů

F vhodná místy   B/A   vyjadřuje δ, G

B stupeň 0   A schází

A kladný div.   rod = 0, tak A = B

C proj. hl. křivka hladká ve všech K-racionálních bodech

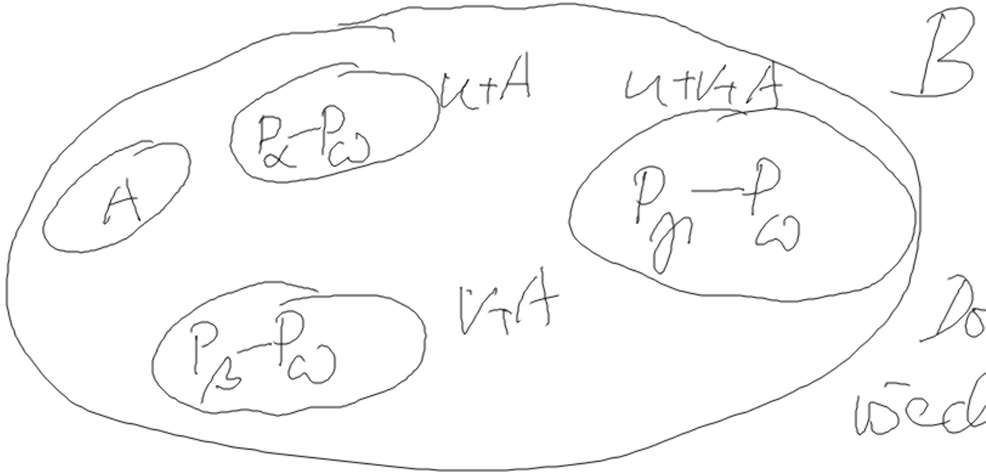
Každé místo stupně 1 lze asociovat právě s 1

Je-li ten bod α, místo P_α K-rac. bodem

Vybereme nějaký pevný K-rac bod ω

<u>Platí</u>   Každý prvek B/A obsahuje právě jeden divisor tvaru $P_\alpha - P_\omega$

α je K-rac.



$u, v \in B$

B/A strukt. grupy

$\gamma = \alpha \oplus \beta$

Dostáváme grupu $C(K)$ všech K-rac. bodů křivky C

$C(K) \cong B/A$

rozkl. třída

$\alpha \longmapsto P_\alpha - P_\omega$

Definice $\oplus$ závisí na volbě ω

Výpočetní vzorce pro $\oplus$ mohou být komplikované, může být potřeba více různých předpisů závislých na poměrech a vlastnostech α, β $\quad \alpha = \beta$ $\quad \alpha \neq \beta$

NĚKDY SE PODAŘÍ JEN JEDINÁ (uzavřená) FORMULE

Aplikace eliptických křivek

podgru

$|E(K)|$

ECC elliptic curve cryptography

Dnes se typicky řeší užití křivek nad $\mathbb{F}_p$, p velké prvočíslo.

? $\mathbb{F}_{2^n}$ nezkoumané, protože krypt. obtížnost DLP

DLP pro tělesa malých charakteristik menší složitost GOLOGLU

Dostaneme-li zápis křivky C (polynom) tak z toho nelze odvodit

$\boxed{\text{URČIT ŘÁD } |C(K)| \text{ JE PRVOTNÍ ALG. CÍL}}$

$$|C(K)| = \#\ K\text{-rac. bodů}$$

ZNÁME INTERVAL, KDE $|C(K)|$ LEŽÍ, ALE CHOVÁ SE NÁHODNĚ

Z CHARAKTERU EL. KŘIVEK PLYNE, ŽE $C(K)$ MUSÍ MÍT VELKOU CYKLICKOU PODGRUPU PRVOČÍSELNÝC ŘÁD

Parametrem pro ECC

tedy je (C, P) kde C je křivka, P její bod

P je řádu prvočísla

$P = \alpha$

$$[p]\alpha = \underbrace{\alpha \oplus \dots \oplus \alpha}_{p} = \mathcal{O} = \infty$$

Odolnost ECC proti útokům je především otázka odolnosti vůči obecným útokům na DLP

Výhod – klíče výrazně kratší

Nevýhoda – kvantové počítače (ECDSA)

Efektivita výpočtu

isogenie supersingulárních křivek

Kromě použití pro šifry, se el. křivky dají použít
pro budování pseudonáhodných
pro faktorizaci čísel

<u>Pozn.</u> NFS je nejlepší ale potřebuje
spoustu pomocných faktorizací.
K tomu použít Lenstrův alg. faktorizace
pomocí eliptických křivek
Ten je nejlepší pro čísla délky
~ 200 bitů a prvočísla
~ 40 bitů