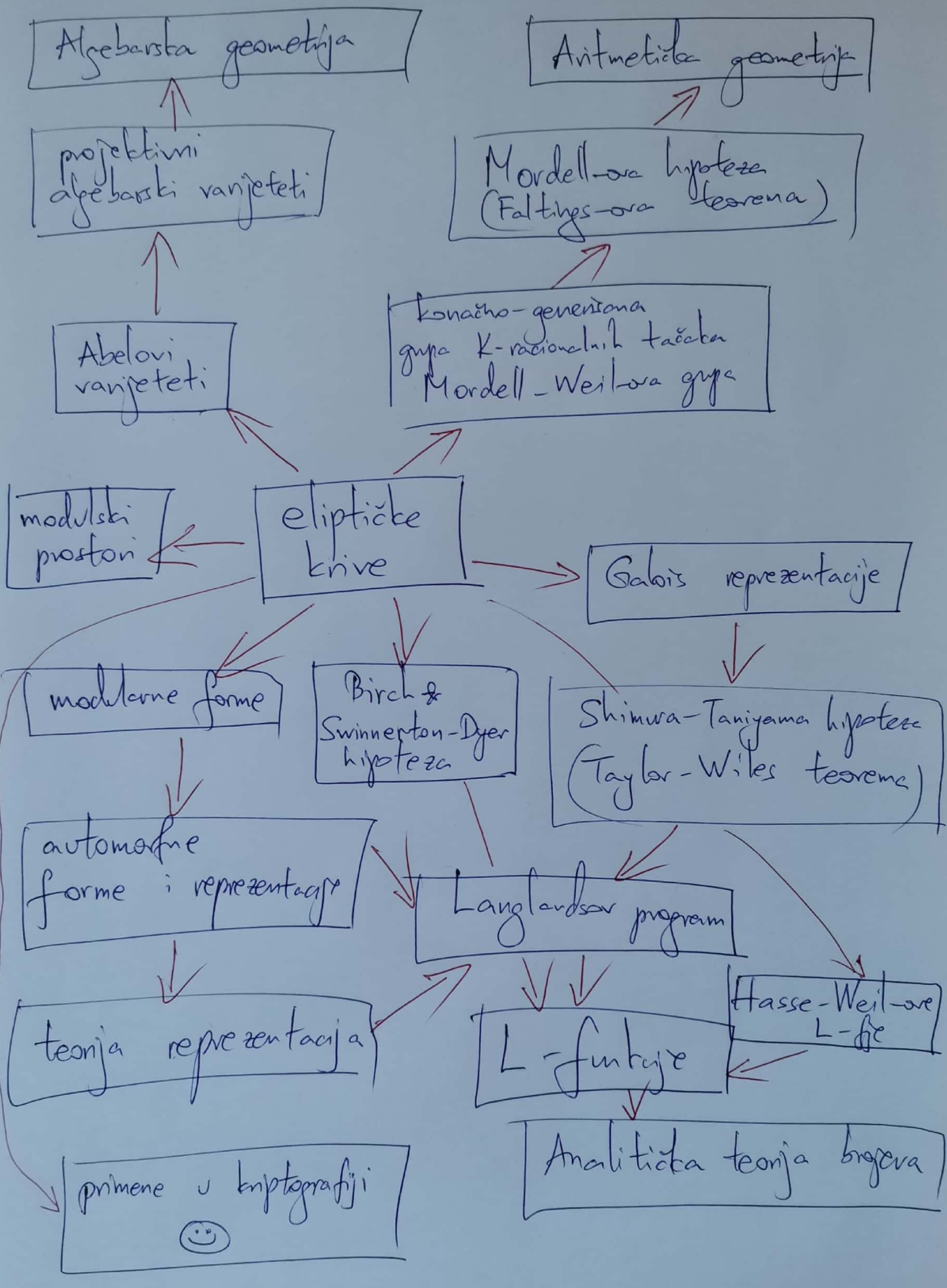
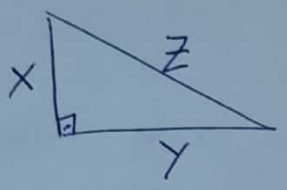

Algebarska geometrija
Aritmetička geometrija
projektivni algebarski varijeteti
Mordell-ova hipoteza (Faltings-ova teorema)
Abelovi varijeteti
konačno-generisana grupa K-racionalnih tačaka Mordell-Weil-ova grupa
modulski prostori
eliptičke krive
Galois reprezentacije
modularne forme
Birch & Swinnerton-Dyer hipoteza
Shimura-Taniyama hipoteza (Taylor-Wiles teorema)
automorfne forme i reprezentacije
Langlandsov program
Hasse-Weil-ove L-fje
teorija reprezentacija
L-funkcije
Analitička teorija brojeva
primene u kriptografiji

Problem kongruentnih brojeva

1



$X, Y, Z \in \mathbb{Q}$

$r = Ar(\triangle) = \frac{XY}{2} \in \mathbb{Q}$ – "kongruentan broj"

- Za svako $r \in \mathbb{Q}_{>0}$, $\exists s \in \mathbb{Q}$: $s^2 r \in \mathbb{Z}$ bestkvadratan

$r = \frac{25 \cdot 7}{4 \cdot 3}$, $s = \frac{2 \cdot 3}{5} \longrightarrow s^2 r = 3 \cdot 7$

i $\triangle(sX, sY, sZ)$ ima $Ar(\triangle) = s^2 r$

Dakle, bez gubitka općenitosti, možemo pretp. da je $r = n \in \mathbb{Z}_{>0}$, bestkvadratan cijeli

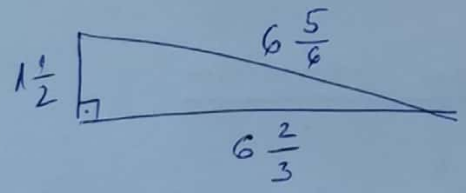
($\leftrightarrow$ svojstvo "r je kongruentan" zavisi samo od kaseta $(\mathbb{Q}^+)^2 \cup \mathbb{Q}^+$ $\mathbb{Q}^+ = (\mathbb{Q}_{>0}, \cdot)$; svaki kaset u $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ sadrži jedinstvenog bestkvadratnog predstavnika)

Primer $3^2 + 4^2 = 5^2$

$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2$,

$n = \frac{3 \cdot 4}{2} = 6$ je kongruentan

$\frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5$ je kongruentan



- 1, 2, 3, 4 nisu, 5, 6, 7 jesu kongruentni ...

Fermat ↑ Euler

Problem Za bestkvadratan $n \in \mathbb{Z}_{>0}$ tražimo rješenja u $\mathbb{Q}^3$ sistema

$$\begin{cases} X^2 + Y^2 = Z^2 \\ \frac{1}{2} XY = n \end{cases}$$

+ možemo fiksirati i poredak tj. pretp. $X < Y < Z$

Tvrd. 1 $n \in \mathbb{Z}_{>0}$ bezkvadratan; $X, Y, Z, x \in \mathbb{Q}_{>0}$, $X < Y < Z$

Imamo 1-1 korespondenciju

$$\left\{ \begin{array}{c} \text{pravougli } \triangle (X,Y,Z) \\ \text{površine } n \end{array} \right\} \longleftrightarrow \left\{ x : \quad x,\ x+n,\ x-n \in (\mathbb{Q}^+)^2 \right\}$$

$$X, Y, Z \longmapsto x := \left(\frac{z}{2}\right)^2$$

$$\left.\begin{array}{l} X := \sqrt{x+n} - \sqrt{x-n} \\ Y := \sqrt{x+n} + \sqrt{x-n} \\ Z := 2\sqrt{x} \end{array}\right\} \longleftarrow x$$

$$(\longrightarrow) \quad \begin{array}{l} X^2 + Y^2 = Z^2 \\ \frac{1}{2} XY = n \end{array} \quad / \cdot 4 \ \Big\uparrow \pm$$

$$(X \pm Y)^2 = Z^2 \pm 4n \quad \longleftrightarrow \quad \left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 \pm n \quad (*)$$

Primer Za $n = 157$, najjednostavniji racionalni $\triangle$ ima manju katetu

$$X = \frac{411\ 340\ 519\ 227\ 716\ 149\ 383\ 203}{21\ 666\ 555\ 693\ 714\ 761\ 309\ 610}$$

2 Karakterizacija kongruentnih brojeva kubnom jednačinom

Pomnožimo j-ne $(*)$: $\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2$

Dakle, ako je $\triangle(X,Y,Z)$ racionalni pravougli površine n, onda j-na

$$\boxed{u^4 - n^2 = v^2}$$ ima racionalno rešenje $(u, v) = \left(\frac{z}{2}, \frac{X^2 - Y^2}{4}\right)$

Pomnožimo sa u^2:

$$u^6 - n^2u^2 = (uv)^2$$

Smena: $x := u^2 = \left(\frac{z}{2}\right)^2$ (isto kao iz Trat. 1)

$$y := uv = \frac{(x^2-y^2)z}{8}$$

pa imamo i racionalno rešenje kubne jne: (x,y)

$$\boxed{y^2 = x^3 - n^2x} \qquad (1)$$

- Obrnuto, ako imamo racionalnu tačku $(x,y) \in \mathbb{Q}\times\mathbb{Q}$ na kubnoj krivoj (1), da li toj tački odgovara neki pravougli racionalni $\triangle$ površine n?

- Ne baš (ali skoro...)

$(b,a)=1$, $b,a\in\mathbb{Z}$, $(b,n)=1$

Koordinata x mora da bude oblika $x = \frac{b^2}{4a^2} \in (\mathbb{Q}^+)^2$

(Dokaz je elementarno razmatranje sa (primitivnim) Pitagorinim trojkama)

- Ove tačke će imati mnogo lepšu geometrijsku interpretaciju

(1) je primer <u>eliptičke krive</u>

3 Eliptične krive

K - polje ($npr.$ $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$,

$\mathbb{Q}(\zeta_n) = \mathbb{Q} + \mathbb{Q}\zeta + \mathbb{Q}\zeta^2 + \dots + \mathbb{Q}\zeta^{n-1}$, $\zeta_n = e^{2\pi i/n}$, $\zeta^n = 1$

$\mathbb{Q}_p$ - p-adični brojevi

$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots$

$a_0, a_1, \dots \in \{0, 1, 2, \dots, p-1\}$

$\mathbb{R}$, $\mathbb{C}$,

$\mathbb{F}_p$, $\mathbb{F}_p(t)$, $\mathbb{F}_p((t))$, $\dots$)

$\operatorname{char} K \neq 2$

(K nije $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \dots$
$\mathbb{F}_2(t), \dots$)

$f(x) \in K[x]$ kubni polinom koji ima različite korene (u nekom proširenju od K)

$K' \supseteq K$ proširenje polja K

Skup rešenja

$$\{(x, y) \in K' \times K' \mid y^2 = f(x)\}$$

zovemo K'- tačke eliptičke krive $y^2 = f(x)$ (2)

(Kongruentni brojevi $\rightsquigarrow$ racionalne tačke na (1) tj.
$K = K' = \mathbb{Q}$, $f(x) = x^3 - n^2 x$)

• $C: F(x,y)=0$ opšta kriva, $F \in K[x,y]$ polinom

$(x_0, y_0) \in K' \times K'$ tačka na krivoj C

C je <u>glatka</u> u tač. (x_0,y_0) ako $\left(\frac{\partial F}{\partial x}(x_0,y_0), \frac{\partial F}{\partial y}(x_0,y_0)\right) \neq (0,0)$

(parcijalni izvodi su definisani algebarski, tj. postoje i nad $\mathbb{F}_p$, $\mathbb{F}_p(t)$, ...)

<u>Slučaj:</u> $F(x,y) = y^2 - f(x)$

nije glatka u (x_0,y_0) ako $(-f'(x_0), 2y_0) = (0,0)$.

Ali $\operatorname{char} K \neq 2$, pa $y_0 = 0$ i onda $f(x_0) = f'(x_0) = 0$

što bi značilo da je x_0 <u>višestruki</u> koren f.

Zato pretpostavka da $f(x)$ ima različite korene znači da je eliptička kriva <u>glatka</u> u svakoj svojoj tački.

4 $F(x,y) \in K[x,y]$ polinom

$x^i y^j$ — $i+j$ = "totalni stepen"

totalni stepen n polinoma F = max totalnih stepena monoma.

$\tilde{F}(x,y,z)$ — homogenizacija polinoma F

$\tilde{F}(x,y,z) := z^n F\left(\frac{x}{z}, \frac{y}{z}\right)$ $\qquad F(x,y) = \tilde{F}(x,y,1)$

• <u>Primer:</u> $F(x,y) = y^2 - (x^3 - n^2 x)$

$\tilde{F}(x,y,z) = y^2 z - x^3 + n^2 x z^2$

• za svako $\lambda \in K$ je $\tilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \tilde{F}(x,y,z)$

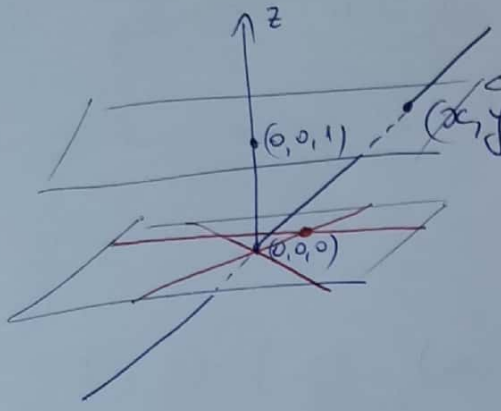
pa ako je $\lambda \neq 0$: $\tilde{F}(\lambda x, \lambda y, \lambda z) = 0 \iff \tilde{F}(x,y,z) = 0$

Specijalno, za $z \neq 0$: $\tilde{F}(x,y,z) = 0 \iff F\left(\frac{x}{z}, \frac{y}{z}\right) = 0$

• Zato definišemo relaciju (ekvivalencije) na $K^3 \setminus \{(0,0,0)\}$:

$(x,y,z) \sim (x',y',z')$ ako $\exists \lambda \in K \setminus \{0\}$ t.d. $(x',y',z') = \lambda(x,y,z)$

② Projektivna ravan $\mathbb{P}^2_K := (K^3 \setminus \{(0,0,0)\}) / \sim$

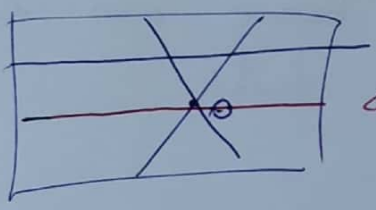


ova ravan predstavlja klase $[(x,y,1)]$ tj. $[(x,y,z)]$ sa $z \neq 0$.

prave u $\{z=0\}$ ravni broz 0 čine "tačke u beskonačnosti"

- to su klase $[(x,y,0)]$; zgodno zove "pravu u beskonačnosti"

Svaka od ovih pravih u xy-ravni ima jedinstven presek sa pravom $\{y=1, z=0\}$



xy-ravan

← osim ove prave tj. klase $[(1,0,0)]$ koja predstavlja "tačku u beskonačnosti"

Dakle možemo da vizualizujemo:

$$\mathbb{P}^2_K = \left(\begin{matrix}\text{obična}\\(\text{afina})\end{matrix} \text{ ravan } [(x,y,1)]\right) \sqcup \left(\begin{matrix}\text{obična}\\(\text{afina})\\\text{prava}\end{matrix} [(x,1,0)]\right) \sqcup \underbrace{[(1,0,0)]}_{\text{tačka u } \infty}$$

$\mathbb{P}^2_K$ – projektivna ravan

$\mathbb{P}^1_K$ – projektivna prava u ∞

• I opšte, n-dim. projektivni prostor $\mathbb{P}^n_K = (K^{n+1} \setminus \{(0,\dots,0)\}) / \sim$ se može vizualizovati kao

$$\mathbb{P}^n_K = \mathbb{A}^n_K \sqcup \mathbb{P}^{n-1}_K$$

$\mathbb{A}^n_K$ – afini n-dim prostor

$\mathbb{P}^{n-1}_K$ ← $(n-1)$-dim. "proj. prostor u ∞"

• Vratimo se na jednačinu

$$\boxed{\tilde{F}(x,y,z)=0}$$

ali sada u projektivnoj ravni $\mathbb{P}_K^2$

gde je $\tilde{F}$ homogeni polinom.

- Rešenja sa $z \neq 0$, tj. tačke $[(x,y,1)]$ za koje je $\tilde{F}(x,y,1)=0$ odgovaraju rešenjima $F(x,y)=0$

- Preostala rešenja, za koje je $z=0$, pripadaju pravoj u ∞.

• Skup svih rešenja

$$\left\{ [(x,y,z)] \in \mathbb{P}_K^2 \;:\; \tilde{F}(x,y,z)=0 \right\} \subseteq \mathbb{P}_K^2$$

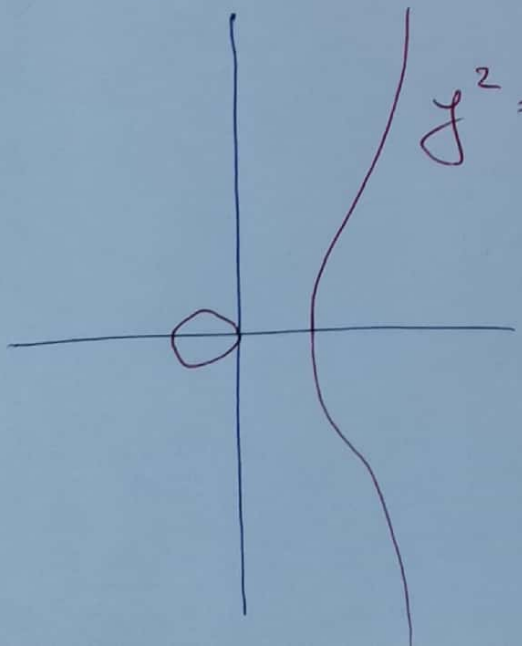
zovemo "projektivno kompletiranje" krive $\{(x,y) \in K \times K \mid F(x,y)=0\}$.

• Primer: $F(x,y) = y^2 - x^3 + n^2 x$

$$\tilde{F}(x,y,z) = y^2 z - x^3 + n^2 x z^2$$

Tačke u ∞ na ovoj eliptičkoj krivoj su oblika $[(x,y,0)]$ za koje je $0 = \tilde{F}(x,y,0) = -x^3$ tj. $x=0$.

Dakle postoji samo 1 tačka u ∞: $[(0,1,0)]$



slika realnih tačaka

- Svaka točka projektivne ravni $\mathbb{P}^2_K$ ima okolinu koja izgleda kao afina ravan, pa sva lokalna svojstva, možemo ispitivati u takvim afinim okolinama.

Npr. točku $[(0,1,0)]$ u ∞ eliptičke krive

$$y^2z - x^3 + n^2xz^2 = 0$$

možemo promatrati u ravni $\{[(x,1,z)]\}$ u kojoj krivu ima afinu jednadžbu

$$z - x^3 + n^2xz^2 = 0$$

(Ova jna dođe sve točke eliptičke krive, osim onih oblika $[(x,0,z)]$ a takvih je samo 3:

$[(0,0,1)]$
$[(n,0,1)]$
$[(-n,0,1)]$

} to su "točke u ∞" ako razmišljamo u xz-koordinatama)