UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 2. stopnja

Miha Avsec

# KUBIČNE KRIVULJE V KRIPTOGRAFIJI

Magistrsko delo

Mentor: doc. dr. Anita Buckley
Somentor: pred. mag. Matjaž Praprotnik

Ljubljana, 2019

# Zahvala

Neobvezno. Zahvaljujem se ...

# Kazalo

**Program dela** **vii**

**1 Uvod** **1**

**2 Kubične krivulje** **1**
2.1 Točke na krivulji . . . . . 1
2.2 Struktura grupe na kubičnih krivuljah . . . . . 4

**3 Diffie-Hellmanova izmenjava ključev nad gladkimi kubičnimi krivuljami** **6**
3.1 Index Calculus . . . . . 7

**4 Parjenja** **9**

**5 Integrali po $\omega$-kompleksih** **10**
5.1 Definicija . . . . . 10

**6 Tehnični napotki za pisanje** **10**
6.1 Sklicevanje in citiranje . . . . . 10
6.2 Okrajšave . . . . . 11
6.3 Vstavljanje slik . . . . . 11
6.4 Kako narediti stvarno kazalo . . . . . 12
6.5 Navajanje literature . . . . . 12

**Literatura** **13**

**Stvarno kazalo** **15**

# Program dela

Mentor naj napiše program dela skupaj z osnovno literaturo. Na literaturo se lahko sklicuje kot [7], [4], [**?**], [2].

# Osnovna literatura

Literatura mora biti tukaj posebej samostojno navedena (po pomembnosti) in ne le citirana. V tem razdelku literature ne oštevilčimo po svoje, ampak uporabljamo okolje itemize in ukaz plancite, saj je celotna literatura oštevilčena na koncu.


[7] L. P. Lebedev in M. J. Cloud, *Introduction to Mathematical Elasticity*, World Scientific, Singapur, 2009

[4] M. E. Gurtin, *An Introduction to Continuum Mechanics*, Mathematics in Science and Engineering **158**, Academic Press, New York, 1982

[**?**]

[2] *DRAFT 2016 EU-wide ST templates*, [ogled 3. 8. 2016], dostopno na `http://www.eba.europa.eu/documents/10180/1259315/DRAFT+2016+EU-wide+ST+templates.xlsx`


Podpis mentorja:

## Kubične krivulje v kriptografiji

Povzetek

Tukaj napišemo povzetek vsebine. Sem sodi razlaga vsebine in ne opis tega, kako je delo organizirano.

## English translation of the title

Abstract

An abstract of the work is written here. This includes a short description of the content and not the structure of your work.

**Math. Subj. Class. (2010):** oznake kot 74B05, 65N99, na voljo so na naslovu `http://www.ams.org/msc/msc2010.html?t=65Mxx`

**Ključne besede:** kubična krivulja , kriptografija , ...

**Keywords:** cubic curve , cryptography

# 1 Uvod

Kubične krivulje se v kriptografiji uporabljajo, ker zagotavljajo isto varnost, kot drugi klasični kriptosistemi, pri tem pa potrebujejo manjšo velikost ključa. Ocenjuje se, da je 2048 bitni ključ v RSA algoritmu enako varen kot 224 bitni ključ nad kubičnimi krivuljami. Krajši kluči predstavljajo veliko prednost v okoljih s slabšo procesorsko močjo in/ali omejenim pomnilnikom. Primer take uporabe predstavljajo pametne kartice. Uporaba kubičnih krivulj v namene kriptografije je prvi predlagal Victor S. Miller leta 1985, a so le te v širšo rabo vstopile še le okoli leta 2004.

# 2 Kubične krivulje

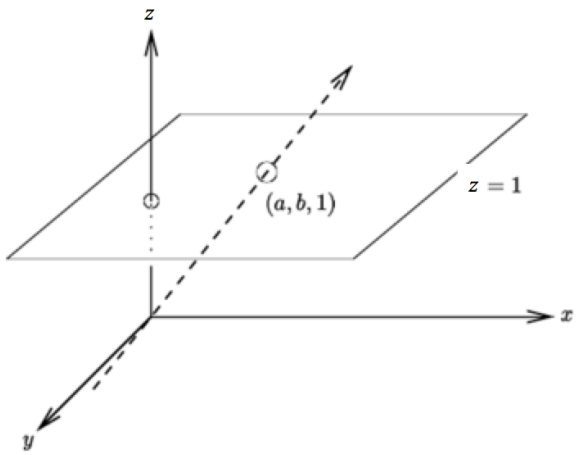
KOPIRANO IZ DIPLOME ALI JE OK????

## 2.1 Točke na krivulji

**Definicija 2.1.**

*Projektivna ravnina* $\mathbb{P}^2$ nad poljem $\mathbb{F}$ je kvocientni prostor $\mathbb{F}^3 - \{0\}/\sim$, kjer je ekvivalenčna relacija podana z $(a, b, c) \sim (\alpha a, \alpha b, \alpha c)$ za vsak $\alpha \in \mathbb{F} \setminus \{0\}$. Točke v $\mathbb{P}^2$ so torej podane s homogenimi koordinatami $[a, b, c] = [\alpha a, \alpha b, \alpha c]$ za vse $\alpha \neq 0$.

Točko projektivne ravnine si lahko predstavljamo kot premico skozi izhodišče, kot prikazuje slika 1.




Slika 1: Točka [a,b,1] v projektivni ravnini.

**Definicija 2.2.**

Polinom $P$ je *homogen* stopnje $d$, če velja $P(\lambda x, \lambda y, \lambda z) = \lambda^d P(x, y, z)$ za vse $\lambda \in \mathbb{F}$.

**Definicija 2.3.**

*Algebraična krivulja*, podana s homogenim polinomom $P$, je množica točk

$$\mathcal{C}_P = \{A \in \mathbb{P}^2, P(A) = 0\}.$$

*Kubična krivulja* je algebraična krivulja, podana s homogenim polinomom stopnje 3. V splošnem je torej oblike

$$a_{300}x^3 + a_{210}x^2y + a_{201}x^2z + a_{120}xy^2 + a_{102}xz^2 + \\ + a_{012}yz^2 + a_{030}y^3 + a_{003}z^3 + a_{111}xyz + a_{021}y^2z = 0,$$

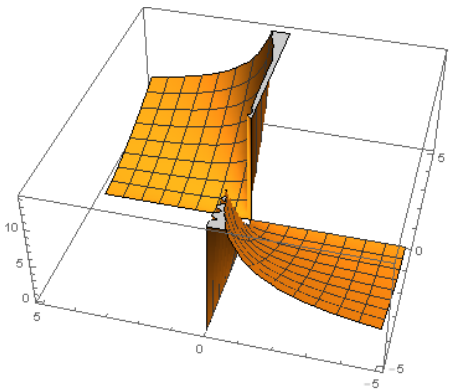
kjer so $a_{ijk} \in \mathbb{F}$. Ta zapis vsebuje 10 koeficientov, vendar se v gladkih primerih lahko polinom poenostavi.

**Definicija 2.4.**
Algebraična krivulja je *gladka*, če nima nobenih samopresečišč ali singularnosti.

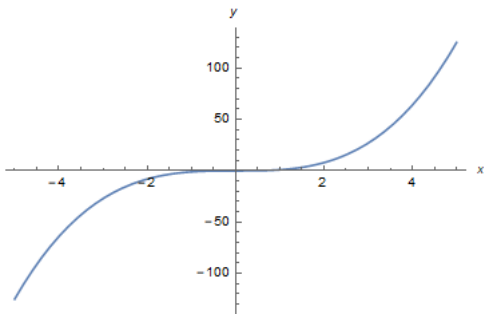
**Izrek 2.5** ([?], Izrek 15.2)**.**
*Gladko kubično krivuljo nad algebraično zaprtim poljem lahko zapišemo v Weierstrassovi obliki*

$$y^2z = x^3 + axz^2 + bz^3.$$

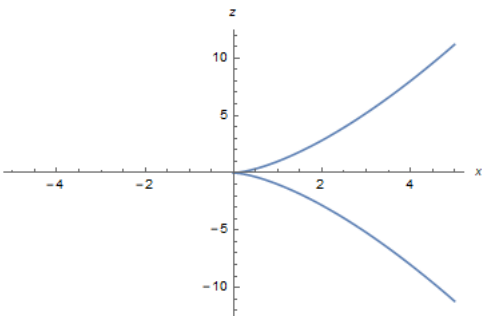
**Primer 2.6.**
Polinom $P(x, y, z) = z^2y - x^3$ je homogen polinom stopnje 3. Rešitve enačbe $z^2y - x^3 = 0$ pa podajajo točke na kubični krivulji.



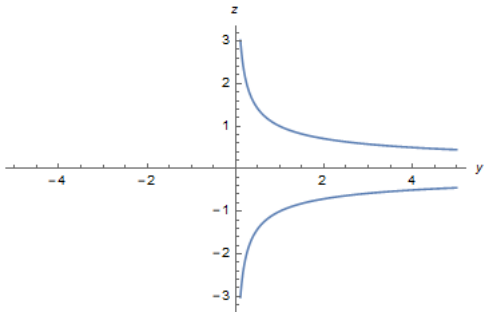
Slika 2: Algebraična krivulja, podana s polinomom $z^2y - x^3$.




Slika 3: Presek algebraične krivulje z ravnino $z = 1$.




Slika 4: Presek algebraične krivulje z ravnino $y = 1$.




Slika 5: Presek algebraične krivulje z ravnino $x = 1$.

Na zgornjih slikah lahko vidimo, kako krivuljo predstavimo v projektivni ravnini, ter njene preseke z različnimi afinimi ravninami.

V nadaljevanju nas bodo zanimale predvsem gladke kubične krivulje v polju $\mathbb{Z}/n\mathbb{Z}$.

**Definicija 2.7.** Za dani števili $a$, $b \in \mathbb{Z}/n\mathbb{Z}$ je *kubična krivulja* nad poljem $\mathbb{Z}/n\mathbb{Z}$ množica točk

$$E_{(a,b)}(\mathbb{Z}/n\mathbb{Z}) = \left\{[x, y, z] \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) : y^2z = x^3 + axz^2 + bz^3\right\}.$$

Drugače povedano, afina kubična krivulja je množica rešitev enačbe

$$y^2 = x^3 + ax + b.$$

Pri čemer upoštevamo zvezo med afinimi in projektivnimi koordinatami točk:

$$(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \Leftrightarrow [x, y, 1] \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}).$$

## 2.2 Struktura grupe na kubičnih krivuljah

Za definicijo grupe na kubičnih krivuljah uvedimo najprej pomožno operacijo

$$* : \mathcal{C}_P \times \mathcal{C}_P \to \mathcal{C}_P,$$

tako da za poljubni točki $A$, $B$ na krivulji velja:

$$A * B = \begin{cases} A & \text{če je } A = B \text{ prevoj,} \\ C & \text{če je } \overline{AB} \cap \mathcal{C}_P = \{A, B, C\}, \\ A & \text{če je } \overline{AB} \text{ tangenta v } A, \text{ ter } A \neq B, \\ B & \text{če je } \overline{AB} \text{ tangenta v } B, \text{ ter } A \neq B, \\ C & \text{če je } A = B \text{ \{in tangenta v A\}} \cap \mathcal{C}_P = \{A, C\}. \end{cases}$$

Intuitivno operacija $*$ vrne tretjo točko v preseku premice skozi $A$ in $B$ in $\mathcal{C}_P$. Poglejmo si še nekaj lastnosti operacije $*$. Dokaze sledečih trditev najdemo v [**?**, Poglavje 17.3].

**Trditev 2.8.**
*Operacija $*$ ima naslednje lastnosti:*

- *komutativnost:* $A * B = B * A$,
- *absorpcija:* $(A * B) * A = B$ ,
- $((A * B) * C) * D = A * ((B * D) * C)$.

**Izrek 2.9.**
*Kubična krivulja ($\mathcal{C}_P$,+) je Abelova grupa za operacijo*

$$\begin{array}{rccc} + : & \mathcal{C}_P \times \mathcal{C}_P & \to & \mathcal{C}_P \\ & (A, B) & \to & (A * B) * O \ , \end{array}$$

*kjer je $O$ poljubna izbrana točka na krivulji $\mathcal{C}_P$.*

*Dokaz.*
S pomočjo trditve 2.8 dokažimo, da je ($\mathcal{C}_P$,+) res Abelova grupa.

- Operacija + je komutativna:

$$A + B = (A * B) * O = (B * A) * O = B + A.$$

- Točka O je nevtralni element:

$$A + O = (A * O) * O = A.$$

- Nasprotni element A definiramo kot $-A = A * (O * O)$ in preverimo:

$$\begin{aligned} A + (-A) &= (A * (A * (O * O))) * O \\ &= (O * O) * O \\ &= O, \end{aligned}$$

kjer smo uporabili absorbcijo.

- Asociativnost $(A+B)+C = A+(B+C)$ dokažemo z računom:

$$\begin{aligned}(A+B)+C &= ((A+B)*C)*O \\ &= (((A*B)*O)*C)*O \\ &= (A*((B*C)*O))*O \\ &= (A*(B+C))*O = A+(B+C). \end{aligned}$$ □

Ta definicija operacije nudi eleganten opis strukture grupe, za numerično računanje pa ni primerna. Možno pa je izpeljati formule, s katerimi lahko eksplicitno izračunamo vsoto dveh točk, v kolikor imamo kubično krivuljo v Weierstrassvi obliki.

**Lema 2.10** (Seštevanje točk na Weierstrassovi kubični krivulji)**.**
*Naj bo $\mathcal{C}_P$ afina krivulja v Weierstrassovi obliki $y^2 = x^3 + \alpha x^2 + \beta x + \gamma$, ter $O$ prevoj v neskončnosti. Če sta $A_1 = (a_1, b_1)$ in $A_2 = (a_2, b_2)$ točki na afinem delu $\mathcal{C}_P$, potem za $A_3 = A_1 + A_2 = (a_3, b_3)$ velja*

$$\begin{aligned} a_3 &= \lambda^2 - \alpha - a_1 - a_2 \\ b_3 &= -\lambda a_3 - \mu, \end{aligned}$$

*kjer sta*

$$\lambda = \begin{cases} \frac{b_1 - b_2}{a_1 - a_2} & \text{če } a_1 \neq a_2, \\ \frac{3a_1^2 + 2\alpha a_1 + \beta}{2b_1} & \text{sicer}, \end{cases}$$

*ter $\mu = b_1 - \lambda a_1$.*

**Opomba 2.11.** Če krivuljo $\mathcal{C}_P$ predstavimo v projektivni ravnini, torej s homogenim polinomom $yz^2 = x^3 + \alpha x^2 z + \beta x z^2 + \gamma y z^2$ je prevoj $O = [0, 1, 0]$.

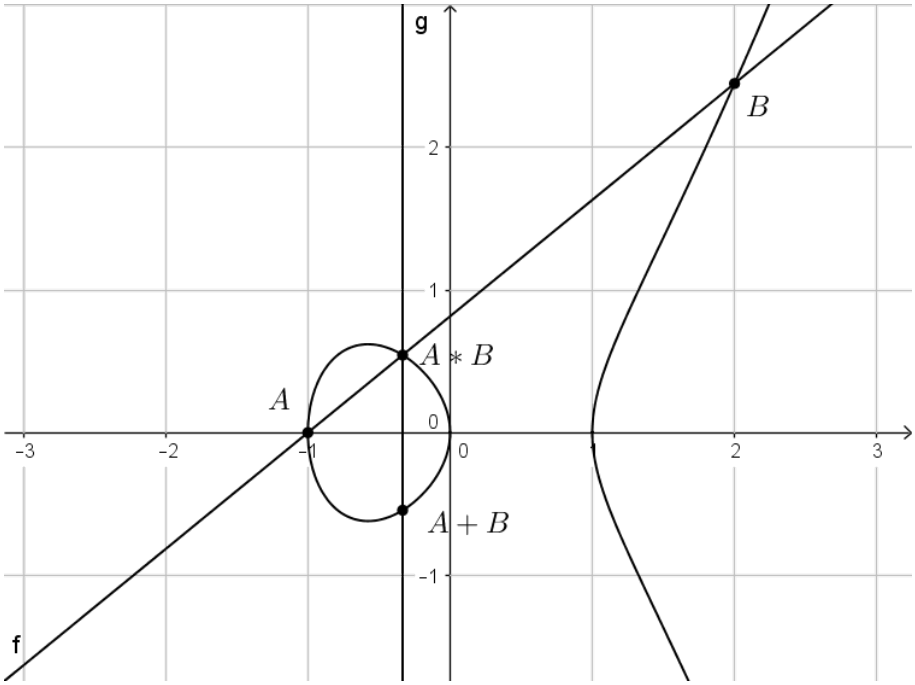
**Primer 2.12.**
Na spodnji sliki je v afini ravnini $y = 1$ prikazano kako grafično seštevamo točke na Weierstrassovi kubiki $yz^2 - x(x-y)(x+y) = 0$. Sešteti želimo točki $A = (-1, 0)$ in $B = (2, \sqrt{6})$.

**Primer 2.13.**
Seštejmo točki $A = (-1, 0), B = (2, \sqrt{6})$ na Weierstrassovi kubični krivulji $yz^2 - x(x-y)(x+y) = 0$ v preseku s projektivno ravnino $y = 1$ še računsko z uporabo zgornje leme 2.10. Prepišimo našo krivuljo najprej v afino obliko iz leme 2.10. Ker smo v ravnini $y = 1$, najprej zamenjajmo vlogi $y$ in $z$.

$$z^2 - x(x-1)(x+1) = 0$$

Dobimo $z^2 = x^3 - x$, torej je $\alpha = 0$, $\beta = -1$ in $\gamma = 0$. Izračunajmo sedaj $\lambda$ in $\mu$, pri čemer upoštevamo prvi predpis, saj sta x-koordinati točk različni:

$$\lambda = \frac{-\sqrt{6}}{-1-2} = \frac{\sqrt{6}}{3},$$




Slika 6: Grafično seštevanje točk na kubični krivulji.

$$\mu = 0 - \frac{\sqrt{6}}{3}(-1) = \frac{\sqrt{6}}{3}.$$

Koordinati vsote $A + B = (x, y)$ sta torej enaki

$$x = \frac{6}{9} - 0 + 1 - 2 = -\frac{1}{3}$$

in

$$z = -\frac{\sqrt{6}}{3}(-\frac{1}{3}) - \frac{\sqrt{6}}{3} = -\frac{2\sqrt{6}}{9} \doteq -0.5443.$$

Iskana točka $A + B \in \mathbb{P}^2$ je torej enaka $[-\frac{1}{3}, 1, -\frac{2\sqrt{6}}{9}]$. Dobljeni rezultat se ujema s točko, ki smo jo dobili z grafičnim seštevanjem.

# 3 Diffie-Hellmanova izmenjava ključev nad gladkimi kubičnimi krivuljami

Diffe-Hellmanova izmenjava ključev je postopek, pri katerem se dve osebi npr. Alenka in Boris dogovorita za skrivni ključ na takšen način, da tudi v primeru ko njun pogovor posluša tretji nepovabljeni gost npr. Ciril le ta iz pogovora ne more rekonstruirati ključa za katerega sta se tekom pogovora dogovorila Alenka in Boris.

**Algoritem 1** Diffie-Hellmanova izmenjava ključev.

1. Alenka in Boris se dogovorita za elitpično krivuljo $E$ nad končnim obsegom $\mathbb{F}q$, ter za točko $P \in E(\mathbb{F}_q)$.
2. Alenka se odloči za skrivno število $a \in \mathbb{N}$, in izračuna $P_a = aP$, ter to pošlje Borisu.
3. Boris se odloči za skrivno število $b \in \mathbb{N}$, in izračuna $P_b = bP$, ter to pošlje Alenki.
4. Alenka izračuna $aP_b = abP$.
5. Boris izračuna $bP_a = baP$.

Kot sam ključ bi lahko na koncu Alenka in Boris uporabila npr. zadnjih 256 bitov x-koordinate točke $abP$. Tu se zanašamo na to, da je iz $E, \mathbb{F}q, P, P_a, P_b$ težko izračunati $baP$. Zelo veliko pa je tu odvisno od same izbire krivulje E.

To nas privede do t. i. problema diskretnega logaritma.

**Definicija 3.1.** Naj bosta $a, b \in \mathbb{N}$, ter naj bo p praštevilo. Iščemo število k tako, da bo

$$a^k \equiv b \pmod{p}.$$

**Trditev 3.2.** *Če lahko rešimo problem diskretnega logaritma, potem smo rešili tudi problem Diffie-Hellmanove izmenjave ključev. Povedano drugače velja*

$$DL \Rightarrow DH.$$

*Dokaz.* Problem Diffie-Hellmanove izmenjave ključev lahko enostavno prevedemo na problem diskretnega logaritma na sledeč način:

- Vzemi $aP$ in izračunaj $a$ tako, da rešiš problem diskretnega logaritma.
- Izračunaj $a(bP)$.

□

## 3.1 Index Calculus

Naj bo $p$ praštevilo in naj bo $g$ generator ciklične grupe $\mathbb{F}_p^\times$. Naj $L(h)$ označuje vrednost, za katero velja

$$g^{L(h)} \equiv h \pmod{p}.$$

Iz definicije $L(h)$ sledi, da velja

$$L(h_1 h_2) = L(h_1) + L(h_2) \pmod{p}.$$

Idejo napada na problem diskretnega logaritma v taki grupi najlažje vidimo na primeru.

**Primer 3.3.** Naj bo $p = 1217$ in $g = 3$. Rešiti hočemo $3^k \equiv 37 \mod 1217$. Izberimo si bazo praštevil $\{2, 3, 5, 7, 11, 13\}$. Pri tem upoštevamo, da bo večja baza pomenila več računanja a hkrati lažjo pot do odgovora. Išemo $x$-e tako, da bo

$$3^x \equiv \pm\text{produktu praštevil iz baze} \mod 1217.$$

Ob iskanju takih $x$ najdemo naslednje enakosti:

$$\begin{aligned}
3^1 &\equiv 3 \pmod{1217} \\
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \pmod{1217} \\
3^{25} &\equiv 5^3 \pmod{1217} \\
3^{30} &\equiv -2 \cdot 5^2 \pmod{1217} \\
3^{54} &\equiv -5 \cdot 11 \pmod{1217} \\
3^{87} &\equiv 13 \pmod{1217}
\end{aligned}$$

Z večjo bazo bi v tem primeru lažje našli take enačbe, a bi jih hkrati potrebovali več. Z uporabo malega Fermatovega izreka, velja

$$3^{1216} \equiv 1 \equiv (-1)^2 \mod 1217,$$

od koder sledi $L(-1) \equiv 608 \mod 1216$. Če enačbe sedaj zapišemo z uporabo $L(h)$, dobimo

$$\begin{aligned}
1 &\equiv L(3) \pmod{1216} \\
24 &\equiv 608 + 2L(2) + L(7) + L(13) \pmod{1216} \\
25 &\equiv 3L(5) \pmod{1216} \\
30 &\equiv 608 + L(2) + 2L(5) \pmod{1216} \\
54 &\equiv 608 + L(5) + L(11) \pmod{1216} \\
87 &\equiv L(13) \pmod{1216}
\end{aligned}$$

Od tod bobimo $L(2) = 216, L(11) = 1059, L(7) = 113, L(5) = 819, L(13) = 87, L(3) = 1$. Sedaj poračunamo za različne $j$ vrednost $3^j * 37$, dokler ne dobimo $3^j * 37 \equiv$ produktu elementov iz baze. Pri vrednosti $j = 16$ dobimo

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}.$$

Iščemo $L(37)$, iz definicije $L$ pa velja

$$3^{L(37)} \equiv 37 \pmod{1217} \equiv 2^3 \cdot 7 \cdot 11 \cdot 3^{-16} \pmod{1217}.$$

Če sedaj namesto baze vstavimo primerne $L$ dobimo

$$3^{L(37)} \equiv 3^{3L(2)} \cdot 3^{L(7)} \cdot 3^{L(11)} \cdot 3^{-16L(3)} \pmod{1217}.$$

$L(37)$ lahko sedaj zapišemo kot

$$L(37) \equiv 3L(2) + L(7) + L(11) - 16L(3) \pmod{1216} \equiv 588 \pmod{1216}.$$

Torej je naš iskani $k = 588$.

# 4 Parjenja

Parjenja imajo pomembno vlogo pri napadih na problem diskretnega logaritma nad gladkimi kubičnimi krivuljami.

**Definicija 4.1.** *Eliptična* krivulja je gladka kubična krivulja.

**Definicija 4.2.** Naj bo $E$ eliptična krivulja nad poljem $K$, ter naj bo $n \in \mathbb{N}$. *Torizjske točke* so množica

$$E[n] = \{P \in E(\overline{K}) | nP = \infty\}.$$

**Izrek 4.3.** *Naj bo $E$ eliptična krivulja nad poljem $K$ in naj bo $n \in \mathbb{N}$. Če karakteristika polja $K$ ne deli $n$, ali je enaka $0$ potem*

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

*Dokaz.* Se ne vem kako bo napisan □

**Definicija 4.4.** Definirajmo *deliteljski polinom* $\gamma_m \in \mathbb{Z}[x, y, A, B]$ kot,

$$\begin{aligned}
\gamma_0 &= 0 \\
\gamma_1 &= 1 \\
\gamma_2 &= 2y \\
\gamma_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\gamma_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\gamma_{2m+1} &= \gamma_{m+2}\gamma_m^3 - \gamma_{m-1}\gamma_{m+1}^3 \text{za } m \geq 2 \\
\gamma_{2m} &= (2y)^{-1}\gamma_m(\gamma_{m+2}\gamma_{m-1}^2 - \gamma_{m-2}\gamma_{m+1}^2) \text{za } m \geq 3
\end{aligned}$$

**Lema 4.5.** *$\gamma_n$ je element $\mathbb{Z}[x, y^2, A, B]$, za vse lihe $n$. Za sode $n$ pa je $\gamma_n$ element $2y\mathbb{Z}[x, y^2, A, B]$.*

*Dokaz.* Dokažimo to s pomočjo indukcije. Za $n \leq 4$ lema očitno velja. Obravnavajmo primera, ko je $n = 2m$ in $n = 2m + 1$ za nek $m \in \mathbb{N}$.

- n=2m Indukcijska predpostavka je v tem primeru, da lema velja za vse $n < 2m$. Predpostavimo lahko, da je $2m > 4$, saj vemo da lema velja za $n \leq 4$, torej velja $m > 2$. Potem velja $2m > m + 2$, kar pomeni, da vsi polinomi v definiciji $\gamma_{2m}$ zadoščajo indukcijski predpostavki. Če je $m$ sodo število ,potem se $\gamma m, \gamma m + 2, \gamma m - 2$ nahajajo v $2y\mathbb{Z}[x, y^2, A, B]$. Od tod pa sledi, da je tudi $\gamma_{2m} \in 2y\mathbb{Z}[x, y^2, A, B]$. Če je $m$ lih, potem sta $\gamma m - 1, \gamma m + 1 \in 2y\mathbb{Z}[x, y^2, A, B]$. To pa pomeni, da je tudi $\gamma_{2m} \in 2y\mathbb{Z}[x, y^2, A, B]$.

- n=2m+1 Primer obravnavamo podobno kot $n = 2m$.

□

**Definicija 4.6.** Naj bo $K$ polje in naj bo $n \in \mathbb{N}$ tak, da karakteristika $K$ ne deli $n$.

$$\mu_n = \{x \in \overline{K} | x^n = 1\}$$

je *grupa n-tih korenov enote* grupe $\overline{K}$.

**Trditev 4.7.** *Naj bo $E$ eliptična krivulja definirana nad poljem $K$, in naj bo $n \in \mathbb{N}$. Predpostavimo, da karakteristika polja $K$ ne deli $n$. Potem obstaja* Weilovo parjenje

$$e_n : E[n] \times E[n] \to \mu_n,$$

*za katerega velja:*

- *$e_n$ je bilinearna v obeh spremenljivkah*

  $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

  *in*

  $$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

  *za vse $S, S_1, S_2, T, T_1, T_2 \in E[n]$.*

# 5 Integrali po $\omega$-kompleksih

## 5.1 Definicija

**Definicija 5.1.** Neskončno zaporedje kompleksnih števil, označeno z $\omega = (\omega_1, \omega_2, \ldots)$, se imenuje *$\omega$-kompleks*.[1]

Črni blok zgoraj je tam namenoma. Označuje, da LaTeX ni znal vrstice prelomiti pravilno in vas na to opozarja. Preoblikujte stavek ali mu pomagajte deliti problematično besedo z ukazom `\hyphenation{an-ti-ko-mu-ta-ti-ven}` v preambuli.

**Trditev 5.2** (Znano ime ali avtor)**.** *Obstaja vsaj en $\omega$-kompleks.*

*Dokaz.* Naštejmo nekaj primerov:

$$\omega = (0, 0, 0, \ldots), \tag{5.1}$$
$$\omega = (1, i, -1, -i, 1, \ldots),$$
$$\omega = (0, 1, 2, 3, \ldots).$$

□

# 6 Tehnični napotki za pisanje

## 6.1 Sklicevanje in citiranje

Za sklice uporabljamo `\ref`, za sklice na enačbe `\eqref`, za citate `\cite`. Pri sklicevanju in citiranju sklicano številko povežemo s prejšnjo besedo z nedeljivim presledkom ~, kot npr. `iz trditve~\ref{trd:obstoj-omega} vidimo`.

**Primer 6.1.** Zaporedje (5.1) iz dokaza trditve 5.2 na strani 10 lahko najdemo tudi v Spletni enciklopediji zaporedij [13]. Citiramo lahko tudi bolj natančno [7, trditev 2.1, str. 23].

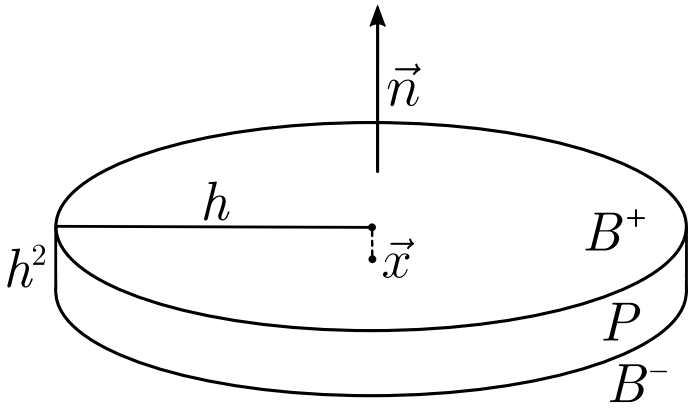
[1] To ime je izmišljeno.

## 6.2 Okrajšave

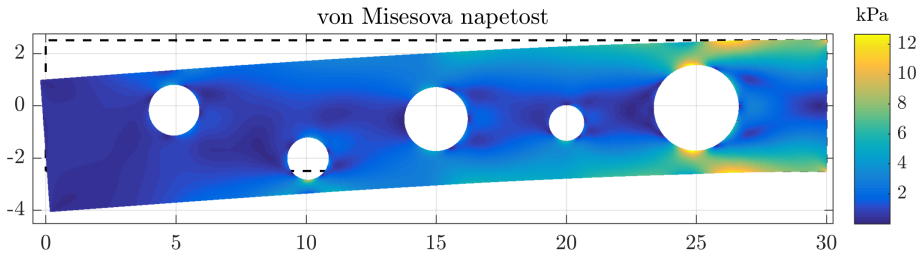
Pri uporabi okrajšav LaTeX za piko vstavi predolg presledek, kot npr. tukaj. Zato se za vsako piko, ki ni konec stavka doda presledek običajne širine z ukazom \␣, kot npr. tukaj. Primerjaj z okrajšavo zgoraj za razliko.

## 6.3 Vstavljanje slik

Sliko vstavimo v plavajočem okolju `figure`. Plavajoča okolja *plavajo* po tekstu, in jih lahko postavimo na vrh strani z opcijskim parametrom '`t`', na lokacijo, kjer je v kodi s '`h`', in če to ne deluje, potem pa lahko rečete LaTeXu, da ga *res* želite tukaj, kjer ste napisali, s '`h!`'. Lepo je da so vstavljene slike vektorske (recimo `.pdf` ali `.eps` ali `.svg`) ali pa `.png` visoke resolucije (več kot 300 dpi). Pod vsako sliko je napis in na vsako sliko se skličemo v besedilu. Primer vektorske slike je na sliki 7. Vektorsko sliko prepoznate tako, da močno zoomate v sliko, in še vedno ostane gladka. Več informacij je na voljo na `https://en.wikibooks.org/wiki/LaTeX/Floats,_Figures_and_Captions`. Če so slike bitne, kot na primer slika 8, poskrbite, da so v dovolj visoki resoluciji.




Slika 7: Primer vektorske slike z oznakami v enaki pisavi, kot jo uporablja LaTeX. Narejena je s programom Inkscape, LaTeX oznake so importane v Inkscape iz pomožnega PDF.




Slika 8: Primer bitne slike, izvožene iz Matlaba. Poskrbite, da so slike v dovolj visoki resoluciji in da ne vsebujejo prosojnih elementov (to zahteva PDF/A-1b format).

## 6.4 Kako narediti stvarno kazalo

Dodate ukaze `\index{polje}` na besede, kjer je pojavijo, kot tukaj. Več o stvarnih kazalih je na voljo na `https://en.wikibooks.org/wiki/LaTeX/Indexing`.

## 6.5 Navajanje literature

Članke citiramo z uporabo `\cite{label}`, `\cite[text]{label}` ali pa več naenkrat s `\cite\{label1, label2}`. Tudi tukaj predhodno besedo in citat povežemo z nedeljivim presledkom ~. Na primer [1, 8], ali pa [6], ali pa [14, str. 12], [11, enačba (2.3)]. Vnosi iz `.bib` datoteke, ki niso citirani, se ne prikažejo v seznamu literature, zato jih tukaj citiram. [15], [3], [12], [9], [5], [2], [10].

# Literatura


[1] Y. Chen, J. Lee in A. Eskandarian, *Meshless Methods in Solid Mechanics*, Springer, New York, 2006.

[2] *DRAFT 2016 EU-wide ST templates*, [ogled 3. 8. 2016], dostopno na `http://www.eba.europa.eu/documents/10180/1259315/DRAFT+2016+EU-wide+ST+templates.xlsx`.

[3] R. Gregorič, *Stopničeni E-∞ kolobarji in Proj v algebraični spektralni geometriji*, magistsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2017.

[4] M. E. Gurtin, *An Introduction to Continuum Mechanics*, Mathematics in Science and Engineering **158**, Academic Press, New York, 1982.

[5] E. A. Kearsley in J. Fong, *Linearly independent sets of isotropic Cartesian tensors of ranks up to eight*, J. Res. Natl Bureau of Standards Part B: Math. Sci. B **79** (1975) 49–58, doi: 10.6028/jres.079b.005.

[6] A. M. Kibriya in E. Frank, *An Empirical Comparison of Exact Nearest Neighbour Algorithms*, v: Knowledge Discovery in Databases: PKDD 2007: 11th European Conference on Principles and Practice of Knowledge Discovery in Databases, Warsaw, Poland, September 17-21, 2007. Proceedings (ur. J. N. Kok in dr.), Springer, Berlin, Heidelberg, str. 140–151, doi: 10.1007/978-3-540-74976-9_16.

[7] L. P. Lebedev in M. J. Cloud, *Introduction to Mathematical Elasticity*, World Scientific, Singapur, 2009.

[8] G.-R. Liu in Y. Gu, *A point interpolation method for two-dimensional solids*, Int. J. Numer. Methods Eng. **50**(4) (2001) 937–951.

[9] *n-sphere*, [ogled 21. 8. 2017], dostopno na `https://en.wikipedia.org/wiki/N-sphere`.

[10] *Nürnberger Tand*, [ogled 23. 1. 2018], dostopno na `https://www.nuernbergwiki.de/index.php/N%C3%BCrnberger_Tand#Geschichte`.

[11] K. Pereira in dr., *On the convergence of stresses in fretting fatigue*, Materials **9**(8) (2016), doi: 10.3390/ma9080639.

[12] J. Slak, *Induktivni in koinduktivni tipi*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2015.

[13] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, Sequence A005043*, [ogled 9. 7. 2016], dostopno na `http://oeis.org/A005043`.

[14] R. Trobec in G. Kosec, *Parallel scientific computing: theory, algorithms, and applications of mesh based and meshless methods*, SpringerBriefs in Computer Science, Springer, New York, 2015.

[15] V. Vene, *Categorical programming with inductive and coinductive types*, doktorska disertacija, Univerza v Tartuju, 2000.

# Stvarno kazalo

tukaj, 12