

Kubične krivulje v kriptografiji

Miha Avsec

Ljubljana, 30. marec 2020

Zakaj bi uporabljali kubične krivulje za namene kriptografije?

- Kubične krivulje nam zagotavljajo večjo varnost glede na dolžino uporabljenega ključa.

<i>AES</i>	<i>ECC</i>	<i>RSA</i>
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	15360

- Krajši ključi predstavljajo prednost predvsem v okoljih s slabšo procesorsko močjo in omejenim pomnilnikom (pametne kartice, IoT, ...).

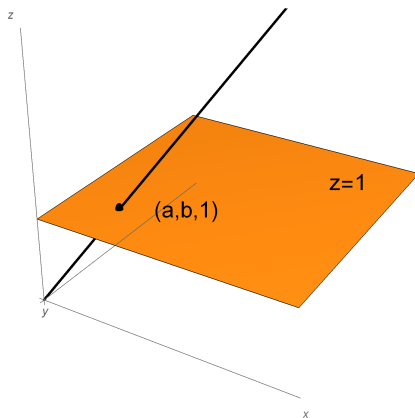
Projektivna ravnina

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

Homogen polinom

Polinom P je *homogen* stopnje d , če velja

$$P(\lambda x, \lambda y, \lambda z) = \lambda^d P(x, y, z) \text{ za vse } \lambda \in \mathbb{F}.$$



Slika: Projektivna ravnina

Algebraična krivulja

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

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

Kubična krivulja

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

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

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

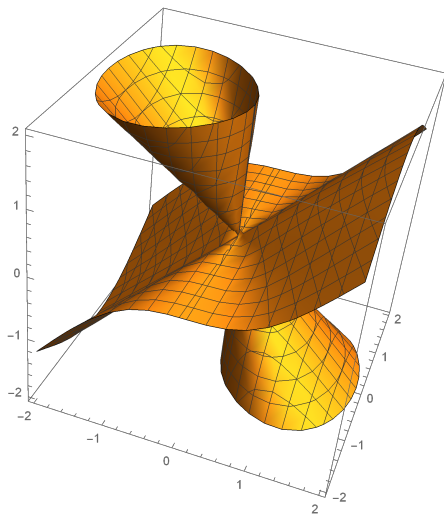
Gladkost

Algebraična krivulja je *gladka*, če nima singularne točke.

Izrek

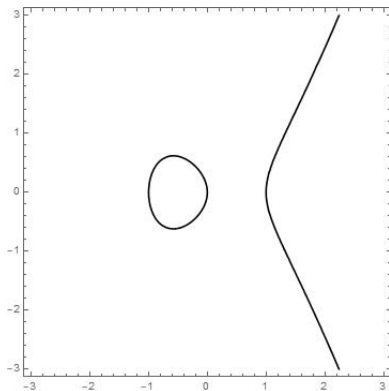
Enačbo gladke kubične krivulje nad algebraično zaprtim poljem lahko zapišemo v Weierstrassovi obliki

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

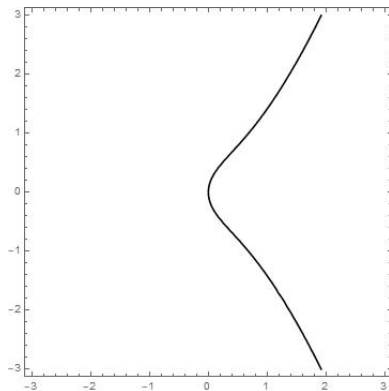


Slika: $y^2z = x^3 - xz^2$

Zgled v projektivni ravnini $z = 1$



Slika: $y^2 = x^3 - x$



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

Za definicijo grupe na kubičnih krivuljah nad \mathbb{C} najprej uvedimo pomožno operacijo

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

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

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

Izrek

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

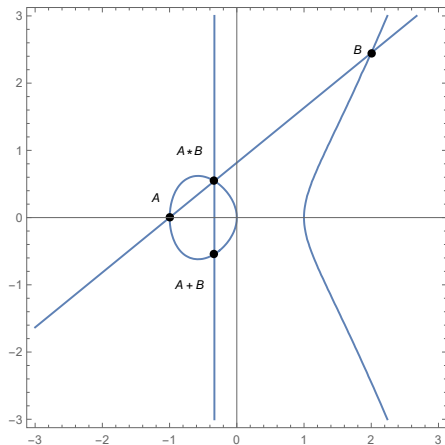
$$\begin{aligned} + : \mathcal{C}_P \times \mathcal{C}_P &\rightarrow \mathcal{C}_P \\ (A, B) &\mapsto (A * B) * O, \end{aligned}$$

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

Opomba

Za kubično krivuljo v Weierstrassovi obliki za točko O ponavadi izberemo tako imenovano točko v neskončnosti, oblike $[0, 1, 0]$, ki jo označimo z ∞ .

Grupa nad kubičnimi krivuljami



Slika: Grafično seštevanje točk na kubični krivulji.

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

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

Drugače povedano, afina kubična krivulja je množica rešitev Weierstrassove enačbe

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

pri čemer upoštevamo zvezo med afinimi in projektivnimi koordinatami točk:

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

Definicija

Naj bo E eliptična krivulja nad poljem K , ter naj bo $n \in \mathbb{N}$. Torzijske točke reda n , so točke v množici

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

Izrek

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

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

Zapišimo $n = p^r n'$, kjer p ne deli n' . Če je karakteristika K enaka $p > 0$ in $p \mid n$, potem velja

$$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ ali } E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

Definicija

Naj bo K polje nad katerim je definirana eliptična krivulja E . Endomorfizem na E je homomorfizem $\alpha : E(\overline{K}) \rightarrow E(\overline{K})$, ki je podan z racionalno funkcijo. Torej obstajata racionalni funkciji R_1 in R_2 s koeficienti v \overline{K} za kateri velja

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

za vse $(x, y) \in E(\overline{K})$.

Standardizirana oblika

Endomorfizem α lahko zapišemo v standardizirani obliki

$$\alpha(x, y) = (r_1(x), r_2(x)y), \text{ kjer je } r_1(x) = \frac{p(x)}{q(x)}.$$

Definicija

Stopnja endomorfizma je definirana kot

$$\deg(\alpha) = \begin{cases} \max\{\deg p(x), \deg q(x)\} & \text{če } \alpha \neq 0, \\ 0 & \text{če } \alpha \equiv 0. \end{cases}$$

Definicija

Netrivialni endomorfizem α je separabilen, če je odvod $r_1'(x) \neq 0$.

Naj bo \mathbb{F}_q končno polje z algebraičnim zaprtjem $\overline{\mathbb{F}_q}$ in naj bo

$$\begin{aligned}\phi_q : \overline{\mathbb{F}_q} &\rightarrow \overline{\mathbb{F}_q}, \\ x &\mapsto x^q\end{aligned}$$

Frobeniusova preslikava na \mathbb{F}_q . Če je eliptična krivulja E definirana nad \mathbb{F}_q , potem ϕ_q deluje na točkah E kot:

$$\phi_q(x, y) = (x^q, y^q) \text{ in } \phi_q(\infty) = \infty.$$

Izrek (Hasse)

Naj bo E eliptična krivulja nad končnim poljem \mathbb{F}_q . Potem red $E(\mathbb{F}_q)$ zadošča zvezi

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Trditev

Naj bo $\#E(\mathbb{F}_q) = q + 1 - a$. Zapišimo $X^2 - aX + q = (X - \alpha)(x - \beta)$.
Potem velja

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

za vse $n \geq 1$.

Delitelj

Naj bo K polje in naj bo P točka na krivulji $E(\overline{K})$. Za vsako točko P definirajmo formalen simbol $[P]$. *Delitelj* D na krivulji E je končna linearna kombinacija takih simbolov s celoštevilskimi koeficienti

$$D = \sum_j a_j [P_j], \quad a_j \in \mathbb{Z}.$$

Definicija

Definirajmo *vsoto* in *stopnjo* delitelja kot

$$\text{sum}(\sum_j a_j [P_j]) = \sum_j a_j P_j \in E(\overline{K}),$$

$$\text{deg}(\sum_j a_j [P_j]) = \sum_j a_j \in \mathbb{Z}.$$

Definicija

Naj bo E eliptična krivulja nad poljem K . Funkcija na E je racionalna funkcija

$$f(x, y) \in \overline{K},$$

ki je definirana za vsaj eno točko na $E(\overline{K})$. Funkcija torej zavzame vrednosti v \overline{K} .

Trditev

Naj bo P točka na krivulji E . Potem obstaja funkcija u_P , kateri rečemo uniformizator, z lastnostjo $u_P(P) = 0$, za katero velja, da lahko vsako funkcijo $f(x, y)$ nad E zapišemo kot

$$f = u_P^r g, \text{ za nek } r \in \mathbb{Z}, \text{ kjer } g(P) \neq 0 \text{ in } \frac{1}{g(P)} \neq 0.$$

Definicija

Številu r iz trditve rečemo red funkcije f v točki P in ga označimo z $\text{ord}_P(f)$.

Definicija

Naj bo f funkcija nad E , ki ni identično enaka 0. Definirajmo delitelj funkcije f kot

$$\text{div}(f) = \sum_{P \in E(\overline{K})} \text{ord}_P(f)[P] \in \text{Div}(E).$$

Definicija

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

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

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

Izrek

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

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

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

Lzrek (nadaljevanje)

- e_n je neizrojena v obeh spremenljivkah. To pomeni, $e_n(S, T) = 1$ za vse $T \in E[n]$ natanko tedaj, ko je $S = \infty$.
- $e_n(T, T) = 1$ za vse $T \in E[n]$.
- $e_n(T, S) = e_n(S, T)^{-1}$ za vse $S, T \in E[n]$.
- $e_n(\rho S, \rho T) = \rho(e_n(S, T))$ za vse avtomorfizme ρ na \bar{K} , za katere je ρ identiteta na koeficientih enačbe za E .
- $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ za vse separabilne endomorfizme α polja E .

Izrek

Naj bo E eliptična krivulja in naj bosta $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ ne ničelni točki na E .

- ① Označimo z λ naklon premice, ki povezuje točki P , Q . V primeru, da sta ti točki enaki, λ predstavlja naklon tangente v točki. Če je premica navpična ($x_P = x_Q$), potem privzamemo, da je $\lambda = \infty$. Definirajmo funkcijo $g_{P,Q}$ na sledeči način:

$$g_{P,Q} = \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2} & \text{če } \lambda \neq \infty, \\ x - x_P & \text{sicer.} \end{cases}$$

Potem velja

$$\text{div}(g_{P,Q}) = [P] + [Q] - [P + Q] - [\infty].$$

Izrek (nadaljevanje)

❶ (Millerjev algoritem) Naj bo $m \geq 1$. Zapišimo m v binarnem kot

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \dots + m_{n-1} \cdot 2^{n-1},$$

kjer so $m_i \in \{0, 1\}$ in $m_{n-1} \neq 0$. Potem algoritem 1 vrne funkcijo f_P , za katero velja

$$\operatorname{div}(f_P) = m[P] - [mP] - (m-1)[\infty].$$

Algoritem 1 Millerjev algoritem

```
1: Vhod: število  $m$  podano v binarnem zapisu, točka  $P$  na eliptični krivulji
2: Izhod: funkcija  $f_P$ 
3:  $T = P, f = 1$ 
4: for  $i = n - 2 : 0$  do
5:      $f = f^2 \cdot g_{T,T}$ 
6:      $T = 2T$ 
7:     if  $m_i = 1$  then
8:          $f = f \cdot g_{T,P}$ 
9:          $T = T + P$ 
10:    end if
11: end for
```

Diffie-Hellmanova izmenjava ključev nad eliptičnimi krivuljami

- 1 Alenka in Boris se dogovorita za eliptično krivuljo E nad končnim obsegom \mathbb{F}_q , ter za točko $P \in E(\mathbb{F}_q)$.
- 2 Alenka se naključno odloči za skrivno število $a \in \mathbb{N}$, in izračuna $P_a = aP$, ter to pošlje Borisu. Pri tem red točke P ne sme biti enak a .
- 3 Boris se naključno odloči za skrivno število $b \in \mathbb{N}$, in izračuna $P_b = bP$, ter to pošlje Alenki. Pri tem red točke P ne sme biti enak b .
- 4 Alenka izračuna $aP_b = abP$.
- 5 Boris izračuna $bP_a = baP$.
- 6 Skupni ključ je abP .

Definicija

Naj bo G grupa, kjer njeno operacijo označimo z \circ . Naj bosta $a, b \in G$. Naj b^k označuje

$$b^k = \underbrace{b \circ b \circ \dots \circ b}_{k\text{-krat}}.$$

Število $k \in \mathbb{N}$, ki reši enačbo

$$b^k = a$$

imenujemo diskretni logaritem elementa a pri osnovi b .

Problem Diffie-Hellmanove izmenjave ključev lahko prevedemo na problem diskretnega logaritma na sledeč način

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

Velja torej:

$$DL \Rightarrow DH$$

MOV napad uporabi Weilovo parjenje, da pretvori problem diskretnega logaritma iz $E(\mathbb{F}_q)$ v problem diskretnega logaritma nad $\mathbb{F}_{q^m}^\times$. Nato pa diskretni logaritem nad novim poljem napademo s pomočjo algoritma izračun indeksa. To deluje če velikost polja \mathbb{F}_{q^m} ni dosti večja od velikosti polja \mathbb{F}_q . Postopek napada sledi poteku dokaza naslednje trditve.

Trditev

Naj bo E eliptična krivulja nad \mathbb{F}_q . Naj bosta $P, Q \in E(\mathbb{F}_q)$, ter naj bo N red točke P . Predpostavimo, da velja $\gcd(N, q) = 1$. Potem obstaja tako število k , da velja $Q = kP$ natanko tedaj ko $NQ = \infty$ in $e_N(P, Q) = 1$.

Izberi m tako, da

$$E[N] \subset E(\mathbb{F}_{q^m}).$$

Ker imajo vse točke $E[N]$ koordinate v $\overline{\mathbb{F}_q} = \bigcup_{j \geq 1} \mathbb{F}_{q^j}$ tak m obstaja. Prav tako je μ_N v \mathbb{F}_{q^m} .

- 1 Izberi točko $T \in E(\mathbb{F}_{q^m})$.
- 2 Izračunaj red M točke T .
- 3 Naj bo $d = \gcd(M, N)$ in naj bo $T_1 = (M/d)T$. Potem ima T_1 red, ki deli N , torej je $T_1 \in E[N]$.
- 4 Izračunaj $\zeta_1 = e_N(P, T_1)$ in $\zeta_2 = e_N(Q, T_1)$. Tu sta ζ_1 in ζ_2 v $\mu_d \subset \mathbb{F}_{q^m}^\times$.
- 5 Reši problem diskretnega logaritma $\zeta_2 = \zeta_1^k$ v $\mathbb{F}_{q^m}^\times$. To nam da k mod d .
- 6 Ponovi za različne točke T dokler ni k določen.

Definicija

Krivulji E nad poljem \mathbb{F}_q , za katero velja

$$\#E(\mathbb{F}_q) = q,$$

rečemo anomalna krivulja.

Trditev

Naj bo E eliptična krivulja nad \mathbb{F}_p in naj bosta $P, Q \in E(\mathbb{F}_p)$.

Predpostavimo še, da je krivulja E oblike $y^2 = x^3 + ax + b$. Potem obstajajo cela števila $a', b', x_1, x_2, y_1, y_2$ in eliptična krivulja E' podana z

$$y^2 = x^3 + a'x + b',$$

ter točke $P' = (x_1, y_1), Q' = (x_2, y_2) \in E'(\mathbb{Q})$. Za ta števila velja

$$a \equiv a', \quad b \equiv b', \quad P \equiv P', \quad Q \equiv Q' \pmod{p}.$$

Algoritem 2 Napad na anomalne krivulje

Vhod: Točki P, Q nad eliptično krivuljo E .

Izhod: diskretni logaritem k .

- 1 Razširi E, P, Q nad \mathbb{Z} , kot v trditvi 11.
- 2 Izračunaj $P'_2 = (p-1)P' \equiv (x', y') \pmod{p^2}$.
- 3 Izračunaj $Q'_2 = (p-1)Q' \equiv (x'', y'') \pmod{p^2}$.
- 4 Izračunaj

$$m_1 = p \frac{y' - y_1}{x' - x_1}, \quad m_2 = p \frac{y'' - y_2}{x'' - x_2}.$$

- 5 Če $v_p(m_2) < 0$ ali $v_p(m_1) < 0$ poizkusi na drugi krivulji E' . V nasprotnem primeru je $k \equiv m_1/m_2 \pmod{p}$.
-