A se consulta **ghidul FMI**

Lucrare de Licență

Cuciureanu Dragoș-Adrian

Iunie 2023

Cuprins

Rezumat

În această Lucrare de Licență vom aborda tematica ”Rolul algoritmilor geometrici în criptografie”, focusul fiind pus pe curbe eliptice.

Subiectul curbelor eliptice înglobează o mare cantitate de teorie matematică. Scopul acestei lucrări este de a oferi un rezumat concis al conceptelor fundamentale necesare aplicațiilor criptografice.

Acestă lucrare va fi împărțită în două părți: prima va consta într-o sinteză a teoriei, iar cea din urmă va fi o documentație a aplicației suport pe care am realizt-o, ce poate efectua diferite operații pe curbe eliptice, precum adunarea si înmultirea pe $\mathbb{R}$ și pe $\mathbb{F}_p$, dar și crearea a curbe elptice aleatoare peste un anumit câmp finit și prezentarea a diferite informații despre aceasta.

Capturile de ecran din lucrare sunt predominant realizate în aplicația suport creată.

1 Introducere

2 Preliminarii și concepte de bază în Curbe Eliptice

2.1 Curbe Eliptice

Definiţia 2.1. *Fie $\mathbb{K}$ un corp comutativ ($\mathbb{K}$ poate fi corpul numerelor reale $\mathbb{R}$, corpul $\mathbb{F}_p$, unde p este număr prim, sau corpul $\mathbb{F}_{p^k}$, unde p este un număr prim și $k \geq 1$.). Fie $a, b \in \mathbb{K}$ două elemente aparținând de corpul $\mathbb{K}$ și $f(X) = X^3 + aX + b$ un polinom cu coeficienți în $\mathbb{K}$. Acest polinom definește o curbă peste corpul $\mathbb{K}$:*

$$E(\mathbb{K}) = \left\{(X, Y) \in \mathbb{K}^2 : Y^2 = f(X)\right\}$$

Fie x_1, x_2, x_3 rădăcinile polinomului $f(X) = X^3 + aX + b$, atunci discriminantul său este:

$$\begin{aligned}\Delta_E =& \left[(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)\right]^2 \\ =& -4a^3 - 27b^2\end{aligned}$$

Demonstraţie. Fie relațiile lui Viète pentru rădăcini:

$$\begin{aligned}x_1 + x_2 + x_3 &= 0 \\ x_1x_2 + x_2x_3 + x_3x_1 &= a \\ x_1x_2x_3 &= -b\end{aligned}$$

Derivăm $f(X)$ si obținem:

$$f'(X) = 3X^2 + a$$

Introducem rădăcinile x_1, x_2, x_3 în ecuație și cu ajutorul relațiilor lui Viète rezultă:

$$f'(x_1) = (x_1 - x_2)(x_1 - x_3)$$
$$f'(x_2) = (x_2 - x_1)(x_2 - x_3)$$
$$f'(x_3) = (x_3 - x_1)(x_3 - x_2)$$

Realizând produsul ecuațiilor anterioare și înlocuind în relațiile lui Viète obținem discriminantul curbei. □

Pentru a avea o curbă eliptică, toate rădăcinile trebuie sa fie distince una față de celelalte.

Remarca 2.2. *Polinomul f are rădăcini distince una față de celelalte, dacă și numai dacă* $\Delta_E \neq 0$*.*

Definiţia 2.3. *Fie* $F(X,Y) = Y^2 - X^3 - aX - b$ *și punctul* $P(x_0, y_0) \in E(\mathbb{K})$ *un punct de pe curbă. Punctul se numește singular dacă:*

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

Definiţia 2.4. *O curbă* $E(\mathbb{K})$ *cu* $\Delta_E \neq 0$ *nu are puncte singulare.*

Demonstraţie. Presupunem prin absurd că o curbă $E(\mathbb{K})$ cu $\Delta_E \neq 0$ are punct singular $P(x_0, y_0)$. Acesta ar fi soluția derivaleor parțiale ale funcției $F(X,Y) = Y^2 - X^3 - aX - b$. Calculăm derivatele sale parțiale:

$$\frac{\partial F}{\partial x}(x_0, y_0) = 3x_0^2 + a = 0$$
$$\frac{\partial F}{\partial y}(x_0, y_0) = -2y_0 = 0$$

Din a doua ecuație obținem că $y_0 = 0$ și introducem în $Y^2 = X^3 + aX + b$ rezulă că $x_0^3 + ax_0 + b = 0$. Iar din prima ecuație obținem $a = -3x_0^2$ și înlocuind în ecuația obținută anterior avem:

$$\begin{aligned} x_0^3 + ax_0 + b &= 0 \\ x_0^3 - 3x_0^2 x_0 + b &= 0 \\ -2x_0^3 + b &= 0 \\ b &= 2x_0^3 \end{aligned}$$

Aducând in formula discriminantului avem:

$$\begin{aligned} &\Delta_E = -4a^3 - 27b^2 \\ &\Delta_E = -4(-3x_0^2)^3 - 27(2x_0^3)^2 \\ &\Delta_E = 108x_0^6 - 108x_0^3 \\ &\Delta_E = 0 \\ dar &\Delta_E \neq 0 \Rightarrow \perp \end{aligned}$$

$\square$

Exemplul 2.5. *Exemple de curbe care au $\Delta_E = 0$ (au puncte singulare):*

$$E1 : Y^2 = X^3 \; varful\; de\; coordonate\; (0, 0)\; este\; punct\; de\; inflexiune$$

$$E2 : Y^2 = (X + 1)^2(X - 2) = X^3 - 3x - 2\; punctul\; de\; coordonate\; (-1, 0)$$

$$este\; izolat$$

Definiţia 2.6. *Fie $\mathbb{K}$ un corp comutativ ($\mathbb{K}$ poate fi corpul numerelor reale $\mathbb{R}$, corpul*

$\mathbb{F}_p$, unde p este număr prim, sau corpul $\mathbb{F}_{p^k}$, unde p este un număr prim și $k \geq 1$.). Fie $a, b \in \mathbb{K}$ două elemente aparținând de corpul $\mathbb{K}$ și $f(X) = X^3 + aX + b$ un polinom cu coeficienți în $\mathbb{K}$. Acest polinom definește o curbă peste corpul $\mathbb{K}$:

$$E(\mathbb{K}) = \left\{(X, Y) \in \mathbb{K}^2 : Y^2 = f(X)\right\} \cup \infty$$
$$cu\ \Delta_E \neq 0$$

Pe scurt, putem spune că o curbă elitpică este totalitatea soluțiilor cu ecuația cu $\Delta_E \neq 0$ de forma:

$$E : Y^2 = X^3 + aX + b$$

Ecuațiile de această natură se cheamă ecuații *Weierstrass*.

Exemplul 2.7. *Exemple de curbe eliptice:*

$$E1 : Y^2 = X^3 - 6X + 6$$
$$E2 : Y^2 = X^3 + 3X - 1$$

Așa arată exemplele ilustrate:

2.2 Adunarea punctelor pe Curbe Eliptice

Una dintre proprietățile remarcabile ale curbelor eliptice este capacitate de a „aduna” în mod natural două puncte pe o curbă eliptică pentru a genera un al treilea punct. Înconjurăm cuvântul „aduna” între ghilimele, deoarece descriem o operație care reunește două puncte într-un mod asemănător cu adunarea (este comutativă, asociativă și există o identitate), dar destul de diferită în alte aspecte. Geometria este cel mai natural mod de a reprezenta operația de ”adunare” pe curbe eliptice.

Fie două puncte de pe curba eliptică E: $P(x_1, y_1)$ $și$ $Q(x_2, y_2)$. Trasăm dreapta ce trece prin cele 2 puncte. Cum curba eliptică este determinată de un polinom de gradul 3, dreapta desenată ca interesecta curba eliptică E în exact 3 puncte (nu este nevoie ca acestea să fie dintincte). Vom nota al treilea punct din intersecție cu $R(x_3, y_3)$, realizăm reflecția sa față de axa OX (cruba eliptică E este simetrică față de axa OX) adică, din punct de vedere numeric înmulțim coordonata a doua a punctului R cu -1, acest punct va fi notat cu R’ și va avea coordonatele $(x_3, -y_3)$.

Punctul R’ este rezultatul ”adunării” între punctele P si Q. Pentru a nu confunda acestă operație cu adunarea naturala o vom nota cu:

$$P \oplus Q = R'$$

Exemplul 2.8. *Fie curba eliptică E de ecuație:*

$$E : Y^2 = X^3 - 7X + 10 \tag{1}$$

Și punctele $P(1, 2)$ *și* $Q(3, 4)$ *de pe E. Calculăm ecuația dreptei L ce inter-*

sectează punctele cu ajutorul pantei:

$$
\begin{aligned}
&m = \frac{y_2 - y_1}{x_2 - x_1} \\
&m = \frac{4-2}{3-1} = 1 \\
&L : Y - y_1 = m(X - x_1) \\
&L : Y - 2 = 1(X - 1) \\
&L : Y = X + 1
\end{aligned}
\tag{2}
$$

Pentru a determina R' calculăm toate punctele de intersecție dintre dreapta L si curba eliptică E, substituind ecuația lui L (2) în ecuția lui E (1):

$$
\begin{aligned}
(X+1)^2 &= X^3 - 7X + 10 \\
X^2 + 2X + 1 &= X^3 - 7X + 10 \\
X^3 - X^2 - 9X + 9 = 0
\end{aligned}
\tag{3}
$$

Cum ecuția rezultată la (3) este de gradul 3, o să aibă exact 3 rădăcini. Cum punctele $P(1,2)$ *și* $Q(3,4)$ *sunt si pe dreaptă si pe curbă, înseamnă că 1 și 3 sunt rădăcini, deci ne rămâne de găsit doar a 3-a rădăcină (descompunem în factori):*

$$
\begin{aligned}
X^3 - X^2 - 9X + 9 &= (X-3)(X-1)(X+3) \\
(X-3)(X-1)(X+3) = 0
\end{aligned}
$$

Din descompunerea în factori determinăm că a treia rădăcină este -3, aceasta fiind și componenta R_x*, acum calculăm componeneta* R_y *din ecuția dreptei de la* *punctul (2):*

$$\begin{aligned} Y &= X + 1 \\ &= (-3) + 1 = -2 \end{aligned}$$

Astfel obținem punctul R(-3, -2), tot ce rămâne de făcut pentru a obține rezultatul căutat este să reflectăm componenta R_y și obținem $R'(-3, 2)$, prin urmare:

$$P \oplus Q = (-3, 2)$$

Acesta este cazul general de adunare a două puncted de pe o curbă eliptică. Însă există și câteva cazuri particulare, fie punctul $P(x, y)$, $P' = -P = (x, -y)$ și punctul $O(\infty, \infty)$:

(i) $P \oplus P$ adunarea unui punct cu el însuși

(ii) $P \oplus P'$ adunarea unui punct cu inversul său

(iii) $P \oplus O$ adunarea unui punct cu infinit

Începem cu primul caz particular, pentru a realiza $P \oplus P$ dreapta L va fi tangenta la E, astfel dreapta intersectează curba eliptică tot în 3 puncte, doar ca 2 dintre acestea sunt P (putem să facem o paralelă cum un polinom ca $(x-1)^2$ are 2 rădăcini, chiar dacă acestea sunt identice). Al 3-lea punct va fi R și apoi calculăm R' la fel ca mai sus.

Exemplul 2.9. *Considerăm aceeași curbă eliptică E și $P(1, 2)$ de la (1) și calculăm $P \oplus P$:*

Determinăm panta lui E prin diferențiere în (1):

$$2Y\frac{dY}{dX} = 3X^2 - 7$$
$$\frac{dY}{dX} = \frac{3X^2 - 7}{2Y}$$

Calculăm panta lui E în P substituind P în ecuție și obținem panta $m = \dfrac{-4}{4} = -1$. *Astfel tangenta la E în P este:*

$$\begin{aligned} L &: Y - y_1 = m(X - x_1) \\ L &: Y - 2 = -1(X - 1) \\ L &: Y = -X + 3 \end{aligned} \tag{4}$$

Analog ca la adunarea generală, determiăm R' calculând toate punctele de intersecție dintre dreapta L si curba eliptică E, substituind ecuația lui L (4) în ecuția lui E (1):

$$\begin{gathered} (-X+3)^2 = X^3 - 7X + 10 \\ X^2 - 6X + 9 = X^3 - 7X + 10 \\ X^3 - X^2 - X + 1 = 0 \\ (X-1)^2(X+1) = 0 \end{gathered} \tag{5}$$

Observăm din descompunere ca rădăcinile sunt: -1, 1 și 1 (de remarcat că rădăcina 1, mai exact componenta P_x apare de două ori). Cea de-a treia rădăcină este componenta R_x, pe care o introducem în ecuația de la (4) și obținem $R(-1, 4)$, *respectiv* $R'(-1,-4)$*:*

$$P \oplus P = (-1,-4)$$

2.3 Curbe Eliptice în Criptografie

3 Preliminarii si concepte de baza

Definiţia 3.1. *Spunem ca* $X : \Omega \to \mathrm{R}$ *e o variabila aleatoare daca...*

Conform Definiţiei 3.1, avem ca...

Remarca 3.2. *(i) Mentionam ca problema dezbatuta aici poate fi studiata si intr-un cadru mai general, ...*

(ii) Daca se renunta la ipoteza 2, atunci rezultatul nu mai este valabil, pentru ca ...

4 Rezultate principale

Propoziţia 4.1. *Avem ca*

$$\lim_n X_n = x. \tag{6}$$

Demonstraţie. Fie... □

Conform Propoziţiei 4.1, mai precis relatiei (6), deducem ca...

4.1 Subsectiune

Rezultatul principal al acestei sectiuni este urmatorul; vezi, de exemplu, (1), Teorema 2.13.

Teorema 4.2. *Daca* $(X_n)_{n\geq 1}$ *variabile aleatoare reale iid, de medie* 0 *si variatie* 1*, atunci*

$$\frac{X_1 + \cdots X_n}{\sqrt{n}} \underset{n}{\Longrightarrow} N(0,1). \tag{7}$$

Demonstraţie. Fie... □

4.2 Subsectiune

Teorema 4.3. *Urmatoarele afirmatii sunt echivalente:*

(i) $\dfrac{X_1 + \cdots X_n}{\sqrt{n}} \underset{n}{\Longrightarrow} N(0,1)$

(ii) $\lim_n \mathbb{P}\left(\left|\dfrac{X_1 + \cdots X_n}{\sqrt{n}}\right| > x\right) = F(x)$*, unde* F *este ...*

Demonstraţie. Fie... □

4.3 Subsectiune

5 Aplicaţii

Problema supermarketurilor. In acest paragraf suntem interesati de urmatoarea situatie: bla bla

Bibliografie

[1] L. Beznea, I. Cîmpean, Quasimartingales associated to Markov processes, Trans. Amer. Math. Soc., 370, 7761-7787 (2018).