Milivojević, O. i Damjanović, B. (2023). Teoretske pretpostavke za uvod u kriptografiju eliptičnih krivih. *STED Journal, 5*(2), 84-90.

TEORETSKE PRETPOSTAVKE ZA UVOD U KRIPTOGRAFIJU ELIPTIČNIH KRIVIH

Ognjen Milivojević, Boris Damjanović

Panevropski Univerzitet "Apeiron", Fakultet Informacionih Tehnologija, vojvode Pere Krece, 78000 Banja Luka, BiH, ognjenmili1993@gmail.com

STRUČNI RAD

ISSN 2637-2150
e-ISSN 2637-2614
UDK 514.112/.113:316.647.5
DOI 10.7251/STED2302084M
COBISS.RS-ID 13942988

Primljen rad: 03.10.2023.
Prihvaćen rad: 17.11.2023.
Publikovan rad: 29.11.2023.
http://stedj-univerzitetpim.com

Korespodentni autor:
Ognjen Milivojević, Panevropski Univerzitet "Apeiron", Fakultet Informacionih Tehnologija, vojvode Pere Krece, 78000 Banja Luka, BiH, ognjenmili1993@gmail.com

A

čne krive su korištene i u rješavanju jednog od milenijumskih problema, a to je Fermaova poslijednja teorema. Povezane su i sa mnogim hipotezama te problemima u matematici koji tek trebaju biti riješeni. Eliptične krive definisane nad konačnim poljima imaju veliku primjenu u kriptografiji javnog ključa, obzirom da su se pokazale kao grupe koje imaju najbolja svojstva za implementaciju Difi-Helmanovog protokola. U ovom članku dat je pregled teoretskih pretpostavki koje su neophodne za razvoj kriptografskih algoritama koji su zasnovani na kriptografiji eliptične krive, što uključuje definisanje eliptičnih krivih, definisanje osobina aritmetičkih operacija nad eliptičnim krivima koje se koriste u kriptografiji sa posebnim osvrtom na krive definisane nad konačnim poljima.

Ključne riječi: eliptična kriva, Vajerštrasova forma, konačna polja, grupe

UVOD

Eliptične krive se prvi put javljaju u Diofantovom radu u drugom ili trećem vijeku kada je Diofant rješavao jednačinu koja predstavlja eliptičnu krivu i ima sljedeći oblik (Barsagade, & Meshram, 2014):

$$y(a-y) = x^3 - x \qquad (1)$$

Iako se eliptične krive proučavaju i u 8. vijeku, matematičari počinju aktivno da se bave njima nakon što je Fibonači u 11. vijeku rješio problem pronalaženja racionalnog broja r takvog da su (Barsagade, & Meshram, 2014):

$$r^2 - 5 \; i \; r^2 + 5 \qquad (2)$$

racionalni kvadrati. Fibonači je koristio eliptične krive da bi rješio ovaj problem. Poslije su se eliptičnim krivima bavili poznati matematičari kao što su Koši, Ferma i Njutn.

Primjena eliptičnih krivih u kriptografiji se pojavljuje tek 1985. godine kada su N. Kobiltz i V. Miler otkrili da se eliptične krive definisane nad konačnim poljima mogu koristiti u kriptografskim sistemima baziranim na problemu diskretnog algoritma (Barsagade, & Meshram, 2014).

DEFINICIJA ELIPTIČNE KRIVE

U radu je navedeno nekoliko definicija iz projektivne geometrije.

Ako imamo relaciju ekvivalencije, skup svih elemenata koji su u međusobnoj relaciji naziva se klasa ekvivalencije. **Faktor skup** je skup svih klasa relacije ekvivalencije (Halmos, 1960).

Projektivna ravan $\mathbb{P}^2(K)$ je faktor skup relacije ekvivalencije, definisane nad skupom nenultih uređenih trojki (x, y, z) ϵ K^3,

$$(x,y,z) \sim (x',y',z') \Leftrightarrow (\exists t \in K^*)\,(x',y',z') = (tx,ty,tz) \quad (3)$$

(Walker, 2012; Washington, 2008; Milne, 2006).

Projektivna tačka je (x : y : z) klasa ekvivalenicije tačke (x, y, z) (Walker, 2012; Lawrence, 2008).

Tačke (x : y : 1) se nazivaju Afine tačke i čine Afinu ili Euklidovu ravan $\mathbb{A}^2(K)$ (Walker, 2012; Washington, 2008; Milne, 2006).

Tačke oblika (x : y : 0) se nazivaju tačke u beskonačnosti. One se sastoje od tačaka oblika (x :: 1 :: 0) i tačke (1 : 0 : 0), i formiraju skup $\mathbb{P}^1(K)$ (Lawrence, 2008; Milne, 2006).

Projektivna kriva C_f/K je homogeni polinom $f(x,y,z)$ sa koeficijentima u polju K. Za svako polje koje sadrži K-racionalnu tačku definiše se:

$$C_f(K) = \{\,(x:y:z) \in \mathbb{P}^2(K) \mid f(x,y,z) = 0\,\} \quad (4)$$

Tačka **P je singularna** ako je $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, $\frac{\partial f}{\partial z}$ = 0 (Walker, 2012; Washington, 2008). $C_f(K)$ **je glatka** ako nema nesingularnih tačaka. **Rod krive** je mjera kojom se opisuje kriva, rod krive definiše se sljedećim izrazom:

$$\frac{(n-1)(n-2)}{2} - p \quad (5)$$

gdje je n stepen krive, a p broj singularnih tačaka (Connell, 1999). **Eliptična kriva** nad poljem K je glatka projektovana kriva roda jedan definisana nad poljem K koja sadrži K-racionalnu tačku (Connell, 1999; Marseglia, 2019).

VAJERŠTRASOVA JEDNAČINA

Vajerštrasova jednačina daje skraćenu formu za predstavljanje eliptične krive. Prema njoj, eliptična kriva je skup tačaka koji zadovoljava jednačinu (Marseglia, 2019):

$$y^2 = x^3 + ax + b \quad (6)$$

Pri čemu su koeficijenti a i b i varijable x i y iz nekog polja F koje nije karakteristike 2 ili 3 (Marseglia, 2019). Takođe mora da važi uslov:

$$4a^3 + 27b^2 \neq 0 \quad (7)$$

Karakteristika polja predstavlja najmanji prirodan broj za koji važi da je $n * 1 = 0$ (Gallian, 2021).

Kada je ovaj uslov ispunjen kriva je nesingularna, to nam omogućava da nađemo tangentu krive u bilo kojoj tački (Prynn, 2015). Postoji izomorfizam koji preslikava sve eliptične krive nad poljem K u Vajerštrasovu formu. Za polja karakteristike 2 i 3 važi opštiji oblik (Marseglia, 2019):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (8)$$

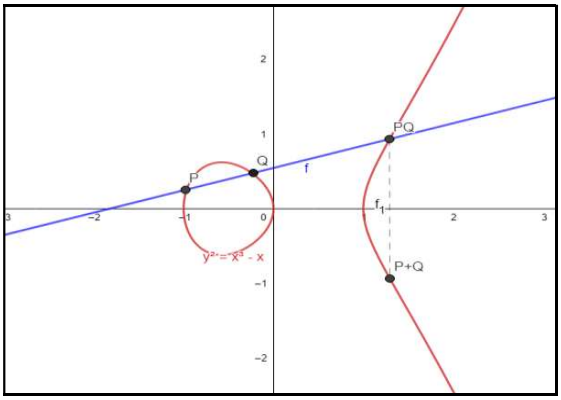
Ako karakteristika polja nije 2 ili 3 tada se ova jednačina pretvara u (kratku) Vajerštrasovu formu.

GEOMERIJSKA INTERPRETACIJA SABIRANJA

Ako imamo dvije različite tačke na eliptičnoj krivoj P i Q , crtajući pravu kroz te dvije tačke dobijamo tačku presjeka sa eliptičnom krivom PQ (Slika 1.). Preslikavajući PQ u odnosu na x osu dobijamo P + Q (Muyinda, 2009). Ako bi pravu i krivu predstavili preko odgovarajućih jednačina:

$$\begin{array}{c} y^2 = x^3 - ax + b \\ y = kx + d \\ \hline (kx + d)^2 = x^3 - ax + b \end{array} \qquad (9)$$

rješavanjem sistema te dvije jednačine dobijemo skup presječnih tačaka. Vidimo da se skup tačaka presjeka krive i prave može predstaviti kao skup rješenja polinoma trećeg stepena.

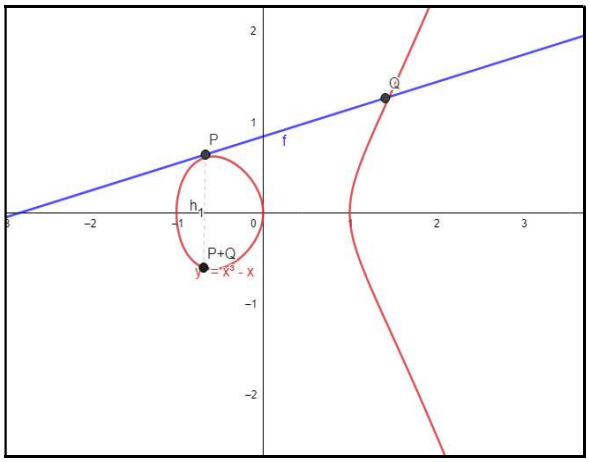


Slika 1. Sabiranje tačaka na eliptičnoj krivoj

Polinom trećeg stepena može imati: Tri realna rješenja, sva tri različita (postoje tri različite tačke presjeka). Tačno dva ista (postoje dvije tačke presjeka); Jedna tačka predstavlja dodirnu tačku tangente i krive, dok je druga presjek te tangente sa krivom. Sva tri ista (postoji tačno jedna tačka presjeka), to je moguće samo u slučaju ako to rješenje tj. tačka prestavlja dodirnu tačku tangente koje je zapravo vertikalna prava tj. prava koja je normalna na x osu. Tri kompleksna rješenja (prava i kriva se ne sijeku).

Dva kompleksna i jedno realno (postoji jedna tačka presjeka).

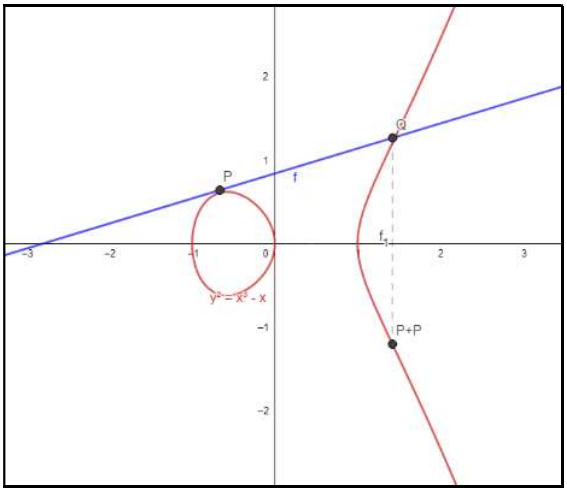
Ako bi postojala samo jedna tačka presjeka onda ta tačka mora da predstavlja dodirnu tačku tangente, gdje je tangenta normalna na x osu, što znači da postoje bar dvije različite tačke koje predstavljaju rješenja polinoma trećeg stepena. Prema tome treće rješenje polinoma mora biti realan broj. Rješenje može biti realno i različito od oba ili realno i isto kao jedno od dva prethodno spomenuta. Ako imamo slučaj kada su sve tri tačke različite, zbir tačaka P i Q se definiše kao refleksija tačke PQ u odnosu na x osu, pri čemu je PQ treća tačka presjeka prave i krive. Ako imamo slučaj da postoje dva ista i jedno različito (P,P,Q) rješenje, onda će ponovljeno rješenje predstavljati dodirnu tačku tangente u odnosu na krivu i zbir predstavlja refleksiju tačke P u odnosu na x osu (Slika 2) (Atticus, 2019; Gordon, 2022). Prethodno je definisano sabiranje za svake dvije različite tačke. U slučaju da sabiramo tačku samu sa sobom onda se povuče tangenta iz te tačke. Tačka PP čini presjek sa krivom, refleksijom te tačke u odnosu na x osu dobijemo zbir (Gordon, 2022).



Slika 2. Sabiranje tačke na Eliptičnoj krivoj – dvije različite tačke presjeka

U slučaju da se radi o tački koja ima horizontalnu tangentu tj. tangentu paralelnu sa x osom onda ne postoji druga tačka presjeka već refleksijom te tačke u odnosu na

x osu dobijemo zbir. U slučaju eliptične krive, zbog simetrije u odnosu na x osu, to je moguće samo za tačke na x osi koje se refleksijom u odnosu na x osu slikaju same u sebe (Slika 3) (Gordon, 2022).



Slika 3: Sabiranje tačke same sa sobom na eliptičnoj krivoj

FORMULA ZA SABIRANJE DVIJE TAČKE NA ELIPTIČNOJ KRIVOJ

Ako imamo dvije tačke na eliptičnoj krivoj $P(x_1, y_1)\ i\ Q(x_2, y_2)$. Koeficijent pravca prave koja sadrži tačke P i Q se može izraziti na sljedeći način (Atticus, 2019; Prynn, 2015; Koblitz, Menezes, & Vanstone 2000):

$$k = \frac{y_2 - y_1}{x_2 - x_1} \tag{10}$$

U slučaju da su tačke P i Q jednake tj. ako sabiramo tačku P samu sa sobom onda je koeficijent pravca prave zapravo koeficijent pravca tangente u tački P. Koeficijent određujemo izvodom krive u tački x_1

$$\begin{aligned} 2yy'(x) &= 3{x_1}^2 + a \ / : 2y \\ k = y'(x_1) &= \frac{3{x_1}^2 + a}{2y_1} \end{aligned} \tag{11}$$

Treću tačku presjeka možemo dobiti rješavajući sistem (Atticus, 2019):

$$\begin{aligned} y^2 &= x^3 + ax + b \\ y &= kx + n \end{aligned} \tag{12}$$

Ako uvrstimo $y = kx + n$ u jednačinu krive dobijemo polinom trećeg stepena

$$\begin{aligned} (kx + n)^2 &= x^3 + ax + b \\ x^3 - k^2x^2 + (a - 2n)x + (b - n^2) &= 0 \end{aligned} \tag{13}$$

Primjenom Vijetovih formula možemo da izrazimo treću tačku presjeka PQ preko koordinata tačaka P i Q .

$$\begin{aligned} x_1 + x_2 + x_3 &= k^2 \\ PQ &= (k^2 - x_1 - x_2, k^3 - k(x_1 + x_2) + (y_1 - kx_1)) \end{aligned} \tag{14}$$

Konačno zbir tačaka P i Q dobijemo refleksijom tačke PQ u odnosu na x osu.

$$P + Q = (k^2 - x_1 - x_2, -k^3 + k(x_1 + x_2) + (kx_1 - y_1))$$

$$k = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \frac{3{x_1}^2 + a}{2y_1}, & P = Q \end{cases} \quad \text{(Koblitz,2000)} \tag{15}$$

OSOBINE SABIRANJA TAČAKA NA ELIPTIČNOJ KRIVOJ

Zatvorenost: Sabiranjem tačaka na krivoj dobijamo takođe tačku na krivoj zbog same definicije sabiranja dvije tačke, prema tome eliptična kriva je zatvorena za sabiranje (Prynn, 2015).

Neutralni element: Da bi se na eliptičnoj krivoj formirala aditivna grupa potrebno je dodati neutralni element. Zato se eliptičnoj krivoj dodaje tačka u beskonačnosti koja predstavlja neutralni element. O je tačka u beskonačnosti pravih normalnih na x osu. Kako je eliptičnoj kriva simetrična u odnosu na x osu treća tačka presjeka je tačka –P koja predstavlja tačku simetričnu tački P u odnosu na x osu (Knapp, 1992; Washington, 2008).

$$P + O = O(PO) = -PO = P \quad (16)$$

(Husemoller, 1987)

Prema tome vidimo da tačka O predstavlja neutralni element.

Suprotni element (Knapp, 1992):

$$P + (-P) = O(P(-P)) = OO = O \quad (17)$$

Iz prethodne jednakosti vidimo da je tačka –P inverzni element tačke P (Washington, 2008).

Asocijativnost: Asocijativnost važi, a može se provjeriti direktno iz formule za računanje zbira.

$$(P + Q) + R = P + (Q + R) \quad (18)$$

Komutativnost:

$$P + Q = O(PQ) = O(QP) = Q + P \quad (19)$$

Komutativnost važi jer je $PQ = QP$ prava kroz dvije tačke i jedinstvena je, te dobijamo istu treću tačku presjeka za PQ i QP.

Kako važi zatvorenost, asocijativnost te postoje neutralni i suprotni element i važi komutativnost eliptičnoj kriva čini Abelovu grupu. Sve ove osobine važe nad proizvoljnim poljem K (Washington, 2008; Prynn, 2015).

ELIPTIČNA KRIVA NAD KONAČNIM POLJEM

U kriptografiji se koriste samo eliptične krive nad konačnim poljima.

Prilično dobru procjenu broja elemenata u grupi eliptičnih krivih daje Heseova (H.Hasse) teorema: Ako je Fp konačno polje sa p elemenata i E eliptičnoj kriva nad poljem Fp i neka je $\#E$ red eliptične krive, onda iz Heseove teoreme dobijamo sljedeću procjenu za red grupe:

$$|\#E - (p + 1)| \leq 2\sqrt{p} \quad (20)$$

Hoffstein, 2006).

Red eliptične krive možemo računati sljedećom jednakošću:

$$\#E = (p + 1) - t,\ t \in (-2\sqrt{p}, 2\sqrt{p}) \quad (21)$$

Gdje je t Frobeniusov trag.

Postoje neki posebni slučajevi kod eliptičnih krivih koje je poželjno izbjeći jer se kod njih mogu kreirati efikasni napadi, takve krive su anomalne i supersingularne.

Anomalna kriva je kriva kod koje je Frobeniusov trag jednak 1, tj. $|E| = |F_p| = p$ (Wiener, & Zuccherto, 1998).

Supersingularne krive su krive kod kojih karakteristika polja dijeli Frobeniusov trag (Wiener, & Zuccherto, 1998).

ZAKLJUČAK

Svojstva koja ima grupa eliptičnih krivih nad konačnim poljima čine rješavanje problema diskretnog logaritma izuzetno teškim dok je implementacija multiplikacije elementa samog sa sobom je relativno jednostavna. Zbog ove osobine, eliptične krive su veoma pogodne za implementaciju Difi-Helmanovog protokola. Kroz Difi-Helmanov protokol i algoritam za digitalno potpisivanje, kriptografija eliptične krive obezbjeđuje efektivan mehanizam za provjeru integriteta podataka, sigurnu razmjena podataka, kao i distribuciju privatnih ključeva i autentifikaciju.

LITERATURA

Atticus, K. (2019). *Elliptic Curves in Cryptography.* Retrieved June 23, 2023 from https://atticuskuhn.github.io/papers/atticus-ec.pdf

Barsagade, M. W., & Meshram, S. (2014). Overview of history of elliptic curves and its use in cryptography. *International Journal of Scientific & Engineering Research*, *5*(4), 467-471.

Milivojević, O. i Damjanović, B. (2023). Teoretske pretpostavke za uvod u kriptografiju eliptičnih krivih. *STED Journal, 5*(2), 84-90.

Connell, I. (1999). *Elliptic curve handbook.* McGill University.

Gallian, J. (2021). *Contemporary abstract algebra*. Chapman and Hall/CRC.

Gordon, S. (2022). *Cryptography Study Notes.* School of Engineering and Technology.

Halmos, P. R. (1960). *Naive set theory*. van Nostrand.

Husemoller., D. (1987). *Elliptic Curves.* New York: Springer Verlag.

Hoffstein, J. P. (2006). *An Introduction to Mathematical Cryptography.* University of Wyoming.

Knapp, A. W. (1992). *Elliptic curves* (Vol. 40). Princeton University Press.

Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, codes and cryptography*, *19*, 173-193.

Washington C. L. (2008). *Elliptic curves: number theory and cryptography*. CRC press.

Marseglia, S. (2019). *Elliptic Curves over Finite Fields.* Utrecht: Utrecht University.

Milne, S. (2006). *Elliptic curves.* Book Surge Publishers.

Muyinda, N. (2009). Elliptic curve cryptography. *African Institute for Mathematical Sciences (AIMS)*.

Prynn, T. (2015). *A Gentle Introduction to Elliptic Curve.* Retrieved June 21, 2023 from https://www.tannerprynn.com/docs/eccreport.pdf

Walker, J. L. (2012). *Codes and Curves.* American Mathematical Society.

Wiener, M. J., & Zuccherto, R. J. (1998). Faster attacks on elliptic curve cryptosystems. In *Proceedings 5th Annual International Workshop, Selected Areas in Cryptography: SAC'98.* Ontario, Canada: Kingston.

Milivojević, O. i Damjanović, B. (2023). Teoretske pretpostavke za uvod u kriptografiju eliptičnih krivih. *STED Journal, 5*(2), 84-90.

THEORETICAL ASSUMPTIONS FOR AN INTRODUCTION TO ELLIPTIC CURVE CRYPTOGRAPHY

Ognjen Milivojević, Boris Damjanović

Pan-European University "Apeiron", Faculty for Information Technologies, vojvode Pere Krece, 78000 Banja Luka, Bosnia and Herzegovina, ognjenmili1993@gmail.com

PROFESSIONAL PAPER

ISSN 2637-2150
e-ISSN 2637-2614
UDC 514.112/.113:316.647.5
DOI 10.7251/STED2302084M
COBISS.RS-ID 13942988

Paper Submited: 03.10.2023.
Paper Accepted: 17.11.2023.
Paper Published: 29.11.2023.
http://stedj-univerzitetpim.com

Corresponding Author:
Ognjen Milivojević, Pan-European University "Apeiron", Faculty for Information Technologies, vojvode Pere Krece, 78000 Banja Luka, Bosnia and Herzegovina, ognjenmili1993@gmail.com

ABSTRACT

Understanding elliptic curves contributed to solving mathematical problems in number theory that had been unsolved for centuries. Elliptic curves were also used in solving one of the millennial problems, which is Fermat's last theorem. They are also connected with many hypotheses and problems in mathematics that have yet to be solved. Elliptic curves defined over finite fields are widely used in public key cryptography, since they have proven to be groups that have the best properties for implementing the Diffie-Hellman protocol. This article provides an overview of the theoretical assumptions that are necessary for the development of cryptographic algorithms based on elliptic curve cryptography, which includes defining elliptic curves, defining the properties of arithmetic operations on elliptic curves used in cryptography with reference to curves defined over finite fields.

Keywords: elliptic curve, Weierstrass form, finite fields, groups