

# Numărul de puncte de pe curbe eliptice

Adrian Manea

GitHub @adimanea/sla/3-criptav/{current,beamer}

510, SLA

Curbe eliptice = obiecte geometrice cu structură algebrică;

Curbe eliptice = obiecte geometrice cu structură algebrică;

Pot fi studiate ca ecuații diofantice (peste  $\mathbb{Q}$ );

Curbe eliptice = obiecte geometrice cu structură algebrică;

Pot fi studiate ca ecuații diofantice (peste  $\mathbb{Q}$ );

Structura algebrică permite operații între soluții;

Curbe eliptice = obiecte geometrice cu structură algebrică;

Pot fi studiate ca ecuații diofantice (peste  $\mathbb{Q}$ );

Structura algebrică permite operații între soluții;

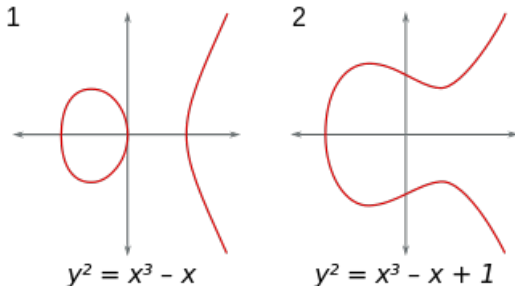
Soluțiile se găsesc greu  $\Rightarrow$  operațiile cu ele sînt destul de sigure criptografic.

# Curbe eliptice

Forma simplă (Weierstrass):  $y^2 = x^3 + ax + b$ ;

# Curbe eliptice

Forma simplă (Weierstrass):  $y^2 = x^3 + ax + b$ ;



Ilustrație: Curbe eliptice [Wikipedia]

**Exemplu:**  $E : y^2 = x^3 + 17$ .



**Exemplu:**  $E : y^2 = x^3 + 17$ .

$$P_1(-2, 3), P_2(-1, 4), P_3(2, 5), P_4(4, 9), P_5(8, 23) \in E.$$

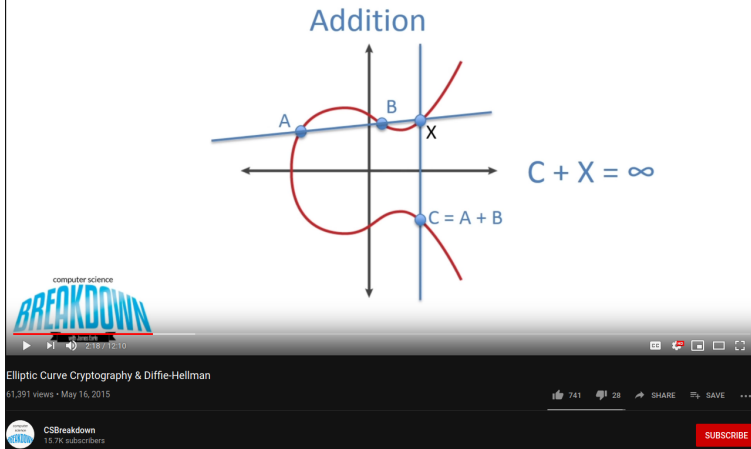
**Exemplu:**  $E : y^2 = x^3 + 17$ .

$$P_1(-2, 3), P_2(-1, 4), P_3(2, 5), P_4(4, 9), P_5(8, 23) \in E.$$

Are loc  $P_5 = -2 \cdot P_1$ ,  $P_4 = P_1 - P_3$ , cu operația următoare:

# Grupul definit de o curbă eliptică

## Elliptic Curve Cryptography



**Ilustrație:** Adunarea punctelor de pe o curbă eliptică [YT @CSBreakdown]

# Numărul de puncte ( $\#E(K)$ )

Depinde de corpul  $K$  peste care este definită curba  $E$ !

# Numărul de puncte ( $\#E(K)$ )

Depinde de corpul  $K$  peste care este definită curba  $E$ !

Exemplu simplu: peste  $\mathbb{F}_5$ ,  $E : y^2 = x^3 + x + 1$ :

# Numărul de puncte ( $\#E(K)$ )

Depinde de corpul  $K$  peste care este definită curba  $E$ !

Exemplu simplu: peste  $\mathbb{F}_5$ ,  $E : y^2 = x^3 + x + 1$ :

$x$	$x^2$	$x^3 + x + 1$	$y$	Puncte
0	0	1	1, 4	$(0, 1), (0, 4)$
1	1	3	$\nexists$	$\nexists$
2	4	1	1, 4	$(2, 1), (2, 4)$
3	4	1	1, 4	$(3, 1), (3, 4)$
4	1	4	2, 3	$(4, 2), (4, 3)$

# Numărul de puncte ( $\#E(K)$ )

Depinde de corpul  $K$  peste care este definită curba  $E$ !

Exemplu simplu: peste  $\mathbb{F}_5$ ,  $E : y^2 = x^3 + x + 1$ :

$x$	$x^2$	$x^3 + x + 1$	$y$	Puncte
0	0	1	1, 4	$(0, 1), (0, 4)$
1	1	3	$\nexists$	$\nexists$
2	4	1	1, 4	$(2, 1), (2, 4)$
3	4	1	1, 4	$(3, 1), (3, 4)$
4	1	4	2, 3	$(4, 2), (4, 3)$

Rezultă  $\#E(\mathbb{F}_5) = 9$ , calculat manual în  $O(5)$  pași.

În general, naiv avem  $\#E(\mathbb{F}_q) \leq 2q + 1$ .

- **Teorema lui Hasse (1924 [E. Artin] – 1933)**  
([Soeten, 2013, Silverman, 2009]):

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



În general, naiv avem  $\#E(\mathbb{F}_q) \leq 2q + 1$ .

- **Teorema lui Hasse (1924 [E. Artin] – 1933)**  
([Soeten, 2013, Silverman, 2009]):

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

- **Baby Step, Giant Step** (pentru log discret)  $\Rightarrow 4\sqrt[4]{q}$ ;

În general, naiv avem  $\#E(\mathbb{F}_q) \leq 2q + 1$ .

- **Teorema lui Hasse (1924 [E. Artin] – 1933)**  
([Soeten, 2013, Silverman, 2009]):

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

- **Baby Step, Giant Step** (pentru log discret)  $\Rightarrow 4\sqrt[4]{q}$ ;
- **Algoritmul Schoof** ([Silverman, 2009])  $\Rightarrow O(\log^8 q) = \text{POLY}$ ;

Pentru  $q \simeq 2^{256}$ , Schoof lucrează cu numere pe 16 kB!

Pentru  $q \simeq 2^{256}$ , Schoof lucrează cu numere pe 16 kB!




Continuare: Elkies, Atkin (cca. 1994) ([Galin, 2007])  $\Rightarrow O(\log^6 q)$ .

Pentru  $q \simeq 2^{256}$ , Schoof lucrează cu numere pe 16 kB!

Continuare: Elkies, Atkin (cca. 1994) ([Galin, 2007])  $\Rightarrow O(\log^6 q)$ .

Folosește unele presupuneri euristice (incl. ipoteza lui Riemann).

# Bibliografie

-  Galin, B. (2007).  
Schoof–Elkies–Atkin algorithm.  
Master's thesis, Stanford University.
-  Silverman, J. (2009).  
*The Arithmetic of Elliptic Curves*.  
Springer.
-  Soeten, M. (2013).  
Hasse's theorem on elliptic curves.  
Master's thesis, Rijkuniversiteit Groningen.