Криптографија
- шести део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

3. - 7. март 2025.

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена
- Зато се у криптосистем обично укључује и хеш алгоритам
  - Алиса примењује хеш алгоритам на поруку пре криптовања, Бобан примењује хеш алгоритам на дешифровану поруку и упоређује добијену вредност са Алисиним резултатом

Интегритет поруке и хеш функције

- Бобан треба да буде сигуран да Алисина порука није успут промењена (случајно или намерно) - интегритет поруке
  - Како је комуникација шифрована, а Цица нема тајни кључ за криптовање: промењена порука може да буде нечитљива.
  - Већи проблем: ако је порука читљива Бобан неће приметити да је промењена
- Зато се у криптосистем обично укључује и хеш алгоритам
  - Алиса примењује хеш алгоритам на поруку пре криптовања, Бобан примењује хеш алгоритам на дешифровану поруку и упоређује добијену вредност са Алисиним резултатом
  - Цица мења шифрат али не може декриптује тај промењени шифрат. Зато не зна како треба да промени Алисину вредност хеш алгоритма

- Хеш функција h има следеће особине
  - h је једносмерна

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције
- хеш функција $h(x, y)$ на улазу има два аргумента фиксиране дужине k и m, при чему је и излаз дужине m

- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције
- хеш функција $h(x, y)$ на улазу има два аргумента фиксиране дужине k и m, при чему је и излаз дужине m
- Улаз хеш алгоритма је порука променљиве дужине, излаз има фиксирану дужину која је обично много мања од дужине улаза улаза

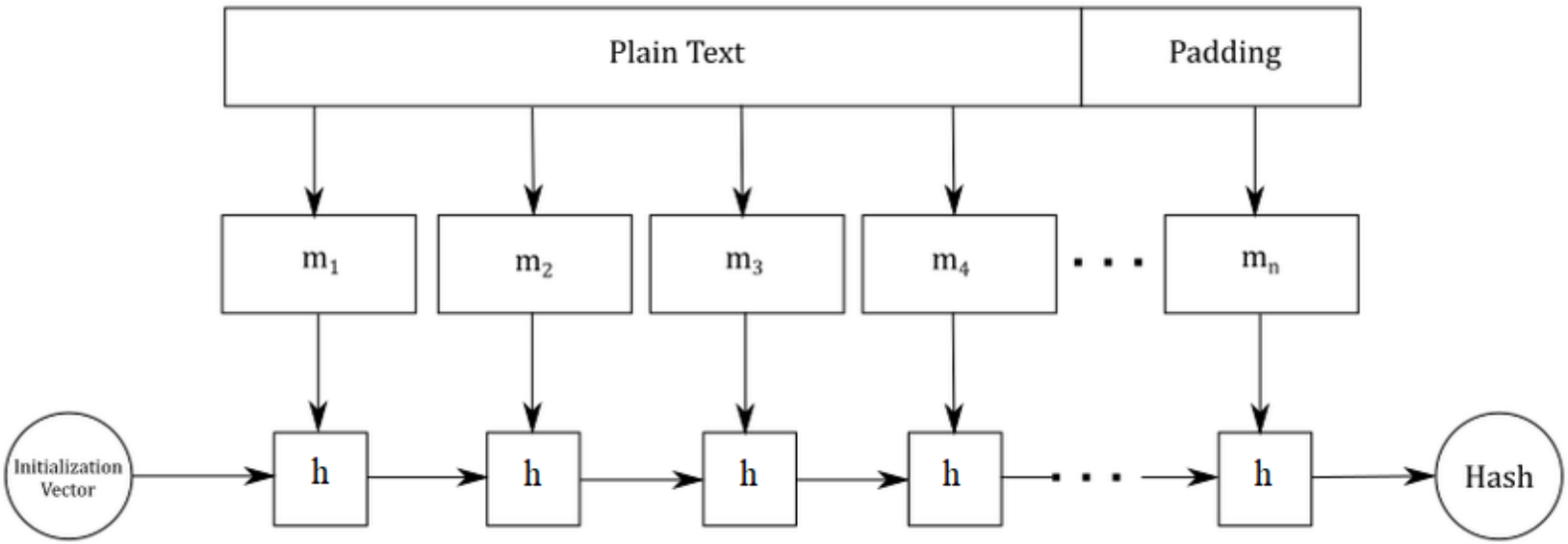
- Хеш функција h има следеће особине
  - h је једносмерна
  - h је отпорна на колизију
    - слаба отпорност: за дато x тешко је одредити $y \neq x$ тд. $h(x) = h(y)$
    - јака отпорност: тешко је одредити различите x, y тд. $h(x) = h(y)$
- хеш алгоритам се састоји од више узастопних примена хеш функције
- хеш функција $h(x, y)$ на улазу има два аргумента фиксиране дужине k и m, при чему је и излаз дужине m
- Улаз хеш алгоритма је порука променљиве дужине, излаз има фиксирану дужину која је обично много мања од дужине улаза улаза
- Најпознатији пример је MD5 алгоритам. Видети: Живковић, Глава 19.1, нећемо улазити у детаље

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m

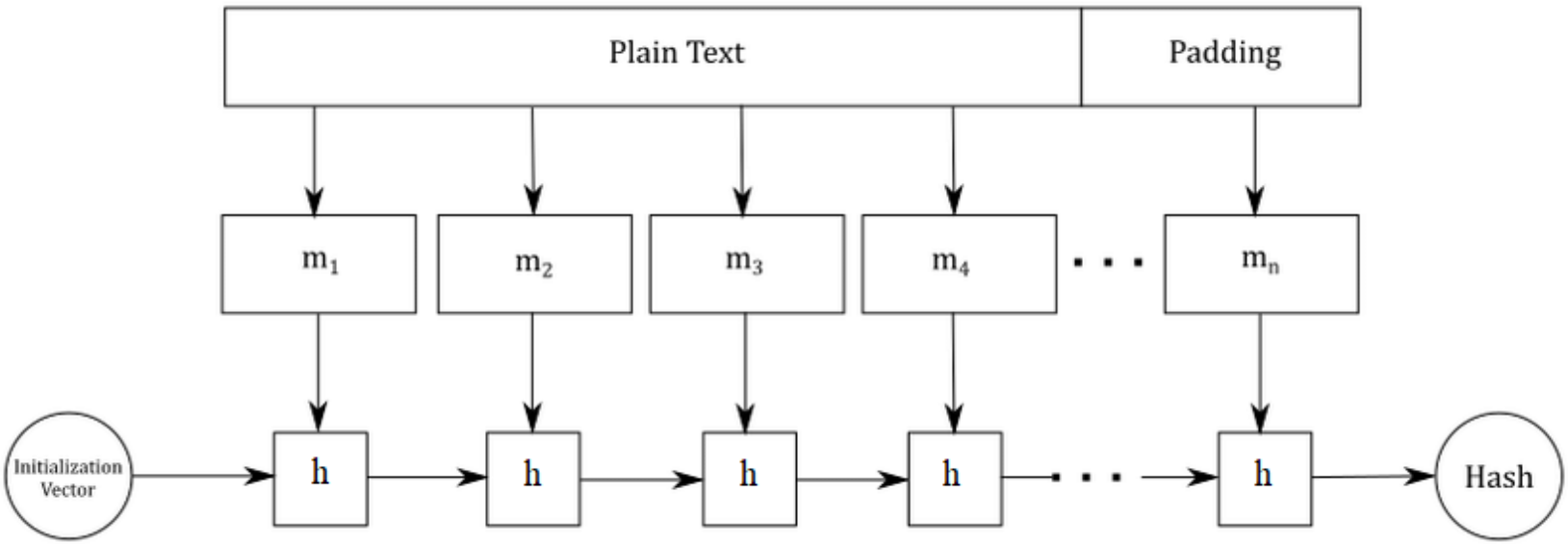
- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h\left(K_0, M_1\right)$

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма

- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма



- Хеш алгоритами се најчешће добијају MD конструкцијом (Меркле-Дамгор):
  - порука се дели на блокове $M_1, M_2, \ldots, M_n$ дужине m
  - изабере се нека иницијална вредност K_0 нпр. $00\ldots0$ и рачуна се $K_1 = h(K_0, M_1)$
  - затим $K_2 = h(K_1, M_2)$, $K_3 = h(K_2, M_3)$, $\ldots$, $K_n = h(K_{n-1}, M_n)$ и K_n ће бити излаз хеш алгоритма



- MAC (message authentication code) је хеш алгоритам који уместо подразумеване иницијалне вредности користи тајни кључ

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца,

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем
  - сертификат - повезује јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише ,,Алиса користи кључ 12345“

Аутентикација

- Бобан мора да буде сигуран да порука коју је добио долази од Алисе (нпр. порука може да буде склапање уговора)
- Аутентикација = процес којим се доказује да порука долази од правог пошиљаоца, обухвата:
  - дигитални потпис - повезује поруку са јавним кључем
  - сертификат - повезује јавни кључ са конкретном особом, то је документ (издат од овлашћеног лица) у коме пише „Алиса користи кључ 12345“
- Имали смо пример дигиталног потписа (код RSA):
  - f_A = Алисина функција криптовања
  - x = вредност коју она треба да потпише (x је изабрао Бобан или је добијено на основу поруке)
  - Алиса рачуна и објављује $f_A^{-1}(x)$. Свако може да провери Алисин потпис јер је f_A јавно, али нико не може да направи њен потпис јер је f_A^{-1} тајно

Пример 1: Дигитални потпис помоћу PCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у PCA

Пример 1: Дигитални потпис помоћу RCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RCA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$

Пример 1: Дигитални потпис помоћу RCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RCA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$

Пример 1: Дигитални потпис помоћу RCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RCA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M

Пример 1: Дигитални потпис помоћу RCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RCA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M
- Цица не може (пре Алисе) да одговори Бобану шта је M

Пример 1: Дигитални потпис помоћу RCA

- Алиса генерише јавни кључ (n, e) и свој тајни кључ d као у RCA
- Бобан генерише (неку насумичну) поруку M и шаље Алиси $M_1 = M^e \bmod n$
- Алиса треба да декриптује M_1 помоћу свог кључа d и врати Бобану $M_2 = M_1^d \bmod n$
- Бобан пореди M_2 са оригиналном поруком M
- Цица не може (пре Алисе) да одговори Бобану шта је M
- Цица ће на крају видети поруку M_2, али не може да је употреби јер Бобан у следећој провери генерише ново M

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у РСА
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у РСА

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у РСА
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у РСА
- $M < n_A, n_B$ кодирана Алисина порука

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у РСА
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у РСА
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у РСА
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у РСА
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2
- Бобан рачуна $M_3 = M_2^{d_B} \bmod n_B$ и $M_4 = M_3^{e_A} \bmod n_A$, и управо M_4 ће бити Алисина порука

Пример 2: Слање поруке + дигитални потпис

Алиса треба да пошаље поруку Бобану, а да Бобан буде сигуран у њен идентитет

- Алиса генерише јавни кључ (n_A, e_A) и тајни кључ d_A као у РСА
- Бобан генерише јавни кључ (n_B, e_B) и тајни кључ d_B као у РСА
- $M < n_A, n_B$ кодирана Алисина порука
- Алиса рачуна $M_1 = M^{d_A} \bmod n_A$ и $M_2 = M_1^{e_B} \bmod n_B$ и шаље Бобану M_2
- Бобан рачуна $M_3 = M_2^{d_B} \bmod n_B$ и $M_4 = M_3^{e_A} \bmod n_A$, и управо M_4 ће бити Алисина порука

Битан је редослед операција (јер се рачуна то различитим модулима):

- $M_3 \equiv_{n_B} M_2^{d_B} \equiv_{n_B} M_1^{e_B d_B} \equiv_{n_B} M_1 \implies M_3 = M_1$
- И слично ће бити $M_4 = M$

```
def main():

    A = RSA()
    B = RSA()

    m  = 207
    m1  = A.decrypt(m)
    m2 = A.encrypt(m1, B.e)
    print("Sifrovano: ", m2)
    m3 = B.decrypt(m2)
    m4 = B.encrypt(m3, A.e)
    print("Desifrovano: ",  m4)
```

- Проблем код Примера 1: потпис не зависи од поруке
  - Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку

- Проблем код Примера 1: потпис не зависи од поруке
  - Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
  - Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор

- Проблем код Примера 1: потпис не зависи од поруке
  - Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
  - Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.

- Проблем код Примера 1: потпис не зависи од поруке
  - Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
  - Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.
- Проблем код Примера 2: Потписивање целе поруке M је добро, али споро решење
  - У пракси се обично кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним, па је овај начин неизводљив

- Проблем код Примера 1: потпис не зависи од поруке
  - Цица може да одвоји Алисин потпис и да га подметне на неку другу поруку
  - Нпр. Цица се Бобану представи као Алиса, Бобан шаље Цици x и пита је колико је $f_A^{-1}(x)$. Цица може да започне комуникацију са Алисом и постави јој исто питање са истим x. Цица само проследи Бобану Алисин одговор
- Зато потпис треба везати за поруку M.
- Проблем код Примера 2: Потписивање целе поруке M је добро, али споро решење
  - У пракси се обично кључ и дигитални потпис размењују асиметричним криптосистемом, а порука симетричним, па је овај начин неизводљив
- Зато се најчешће потписује $H(M)$, где је H хеш алгоритам
  - Порука се размењује симетричним криптосистемом, а потпис асиметричним, иде одвојено од поруке али је везан за хеширану поруку

Елиптичке криве

- Многи криптосистеми са јавним кључем (Дифи-Хелман, Меси-Омура, ЕлГамал, ...) имају унапређену верзију која се заснива на елиптичким кривама

Елиптичке криве

- Многи криптосистеми са јавним кључем (Дифи-Хелман, Меси-Омура, ЕлГамал, ...) имају унапређену верзију која се заснива на елиптичким кривама
- Предност: Могуће је постићи исту заштиту са мањим кључем који користи ЕК
  - Пример: 256-битни кључ заснован на елиптичким кривама мења 3072-битни кључ

Елиптичке криве

- Многи криптосистеми са јавним кључем (Дифи-Хелман, Меси-Омура, ЕлГамал, ...) имају унапређену верзију која се заснива на елиптичким кривама
- Предност: Могуће је постићи исту заштиту са мањим кључем који користи ЕК
  - Пример: 256-битни кључ заснован на елиптичким кривама мења 3072-битни кључ
- ЕК се користе у криптоанализи, посебно за напад на RSA. Чак и ако криптосистем не користи ЕК, може бити нападнут алгоритмом који користи ЕК
  - Видели смо: Полардов $(p-1)$-метод факторизације је спор ако n нема прост чинилац p тд. $p-1$ је B-гладак. Са ЕК биће довољно да неки од $p+s$ (за мало s) буде B-гладак

- Елиптичка крива над $\mathbb{R}$ је крива дефинисана једначином

$$E: \ y^2 = x^3 + ax + b,$$

где су $a, b \in \mathbb{R}$ тд. $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$

- Елиптичка крива над $\mathbb{R}$ је крива дефинисана једначином

$$E: \ y^2 = x^3 + ax + b,$$

где су $a, b \in \mathbb{R}$ тд. $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$

- На скуп решења се додаје још једна ,,бесконачно далека“ тачка $\mathcal{O}$, па је

- Елиптичка крива над $\mathbb{R}$ је крива дефинисана једначином

$$E: \ y^2 = x^3 + ax + b,$$

где су $a, b \in \mathbb{R}$ тд. $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$

- На скуп решења се додаје још једна ,,бесконачно далека“ тачка $\mathcal{O}$, па је

Дефиниција

$$E(\mathbb{R}) = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}$$

Sage има имплементиране функције за рад са ЕК

Save Copy Run Sage-10.1

```
E = EllipticCurve([-5, 4])
E
```

```
Elliptic Curve defined by y^2 = x^3 - 5*x + 4 over Rational Field
```

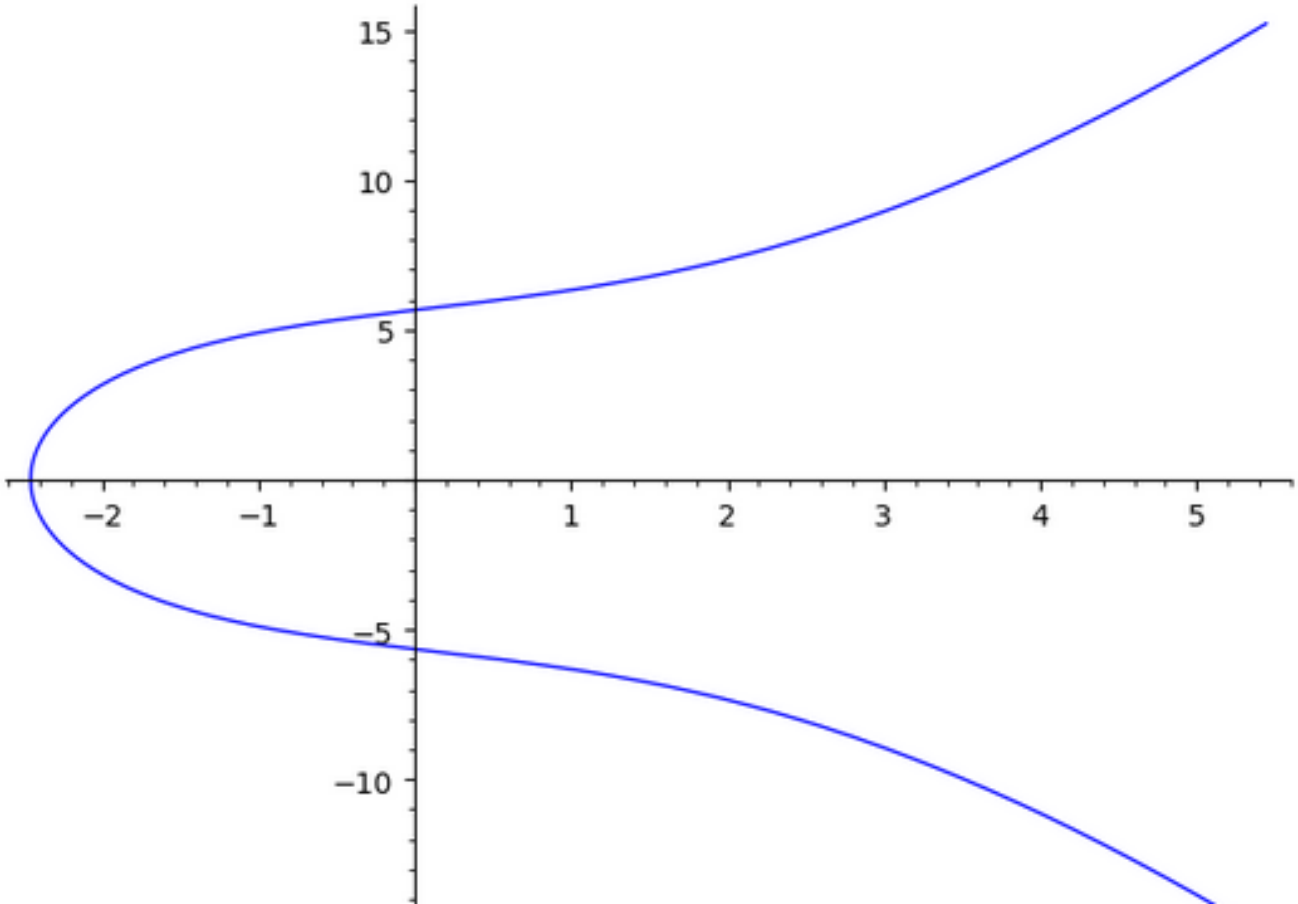
Sage има имплементиране функције за рад са ЕК

Save Copy Run Sage-10.1

```
E = EllipticCurve([-5, 4])
E
```

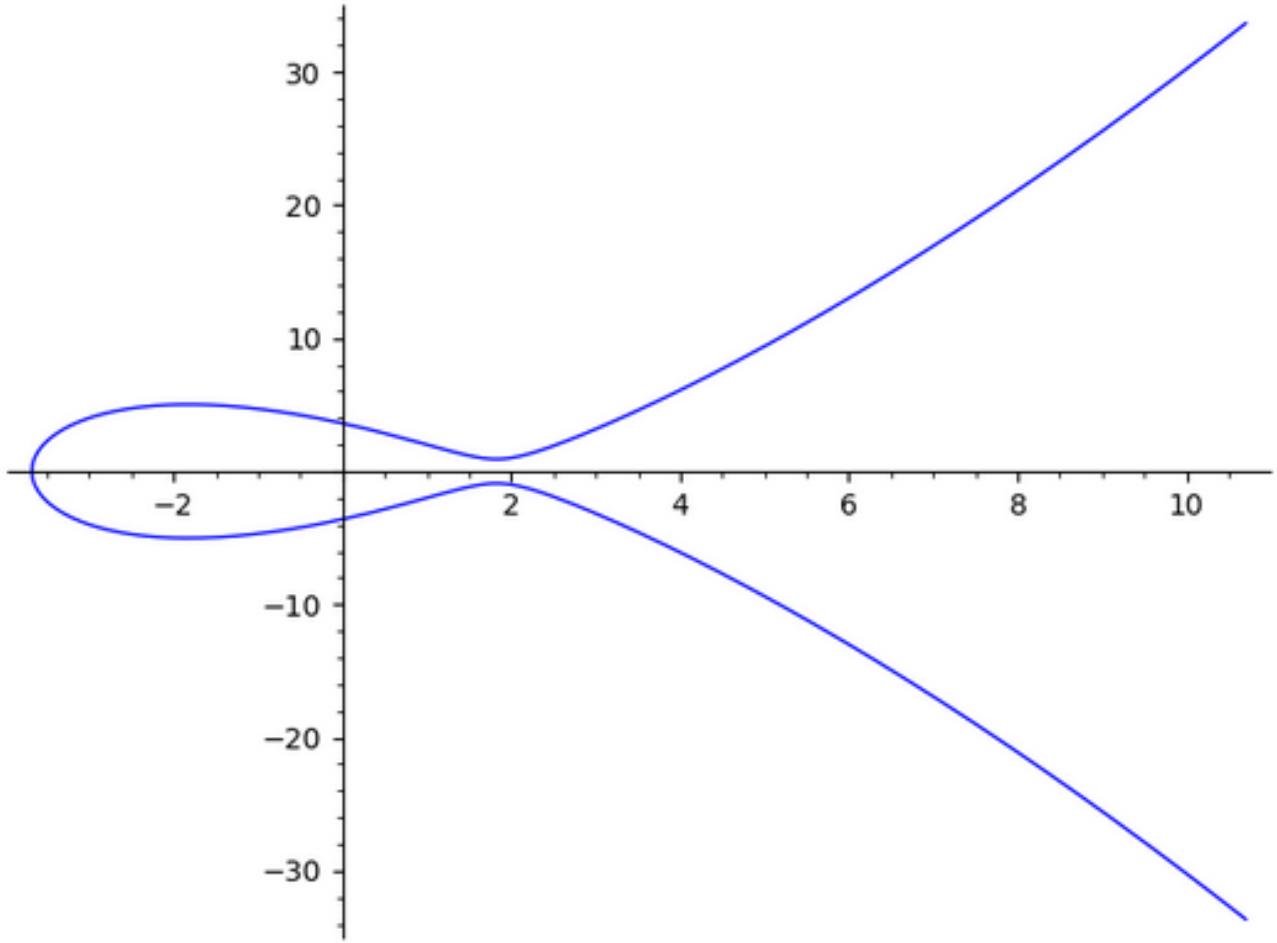
```
Elliptic Curve defined by y^2 = x^3 - 5*x + 4 over Rational Field
```

```
E = EllipticCurve([7, 32])
E.plot()
```

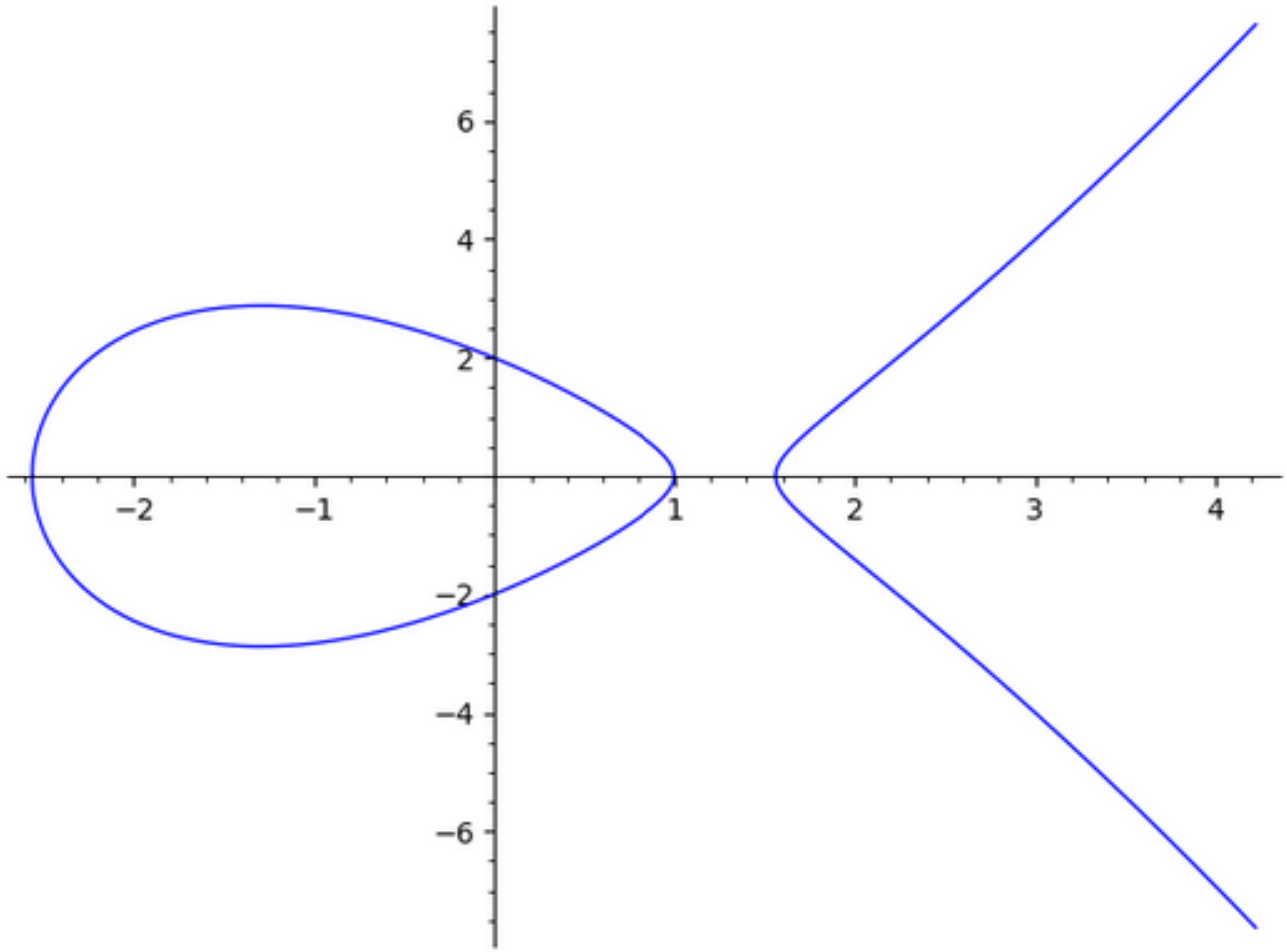


Save Copy Run SageMath 10.1

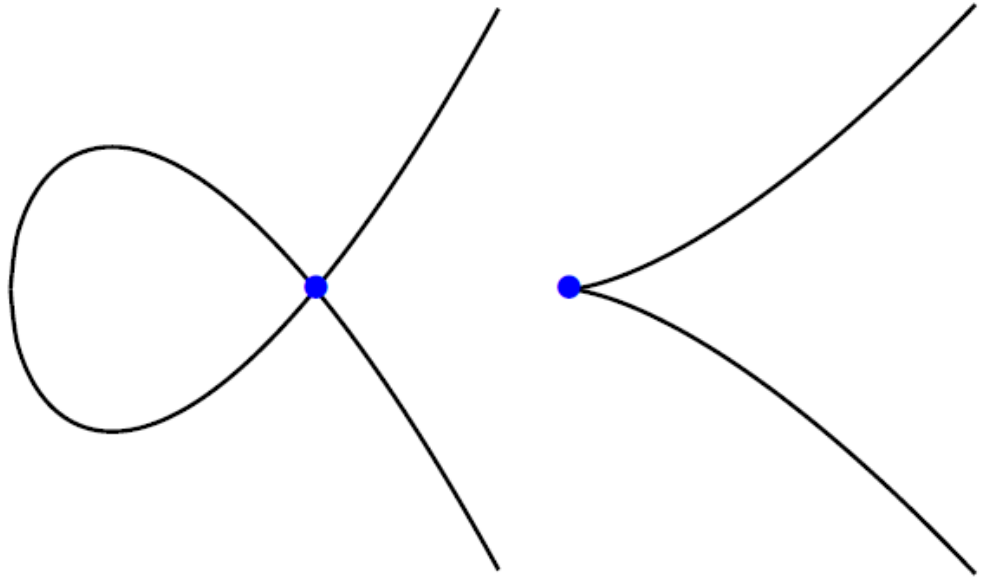
```
E = EllipticCurve([-10, 13])
E.plot()
```



```
E = EllipticCurve([-5, 4])
E.plot()
```



Тачка $\mathcal{O}$ се не види



Singular curve $y^2 = x^3 - 3x + 2$ over $\mathbb{R}$.

Singular curve $y^2 = x^3$ over $\mathbb{R}$.

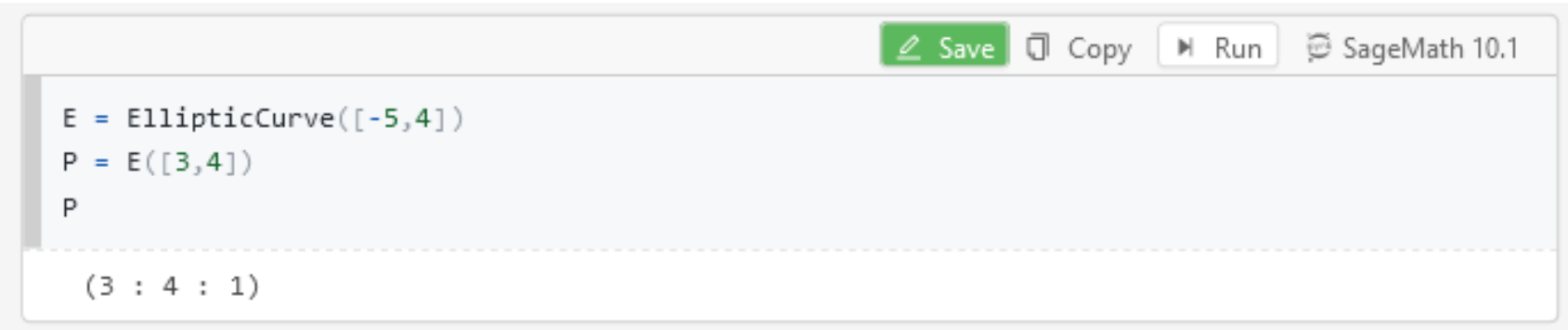
Нису елиптичке криве јер је $\Delta = 0$

- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \left(\mathbb{R}^3 \setminus \{(0,0,0)\}\right) / \sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$

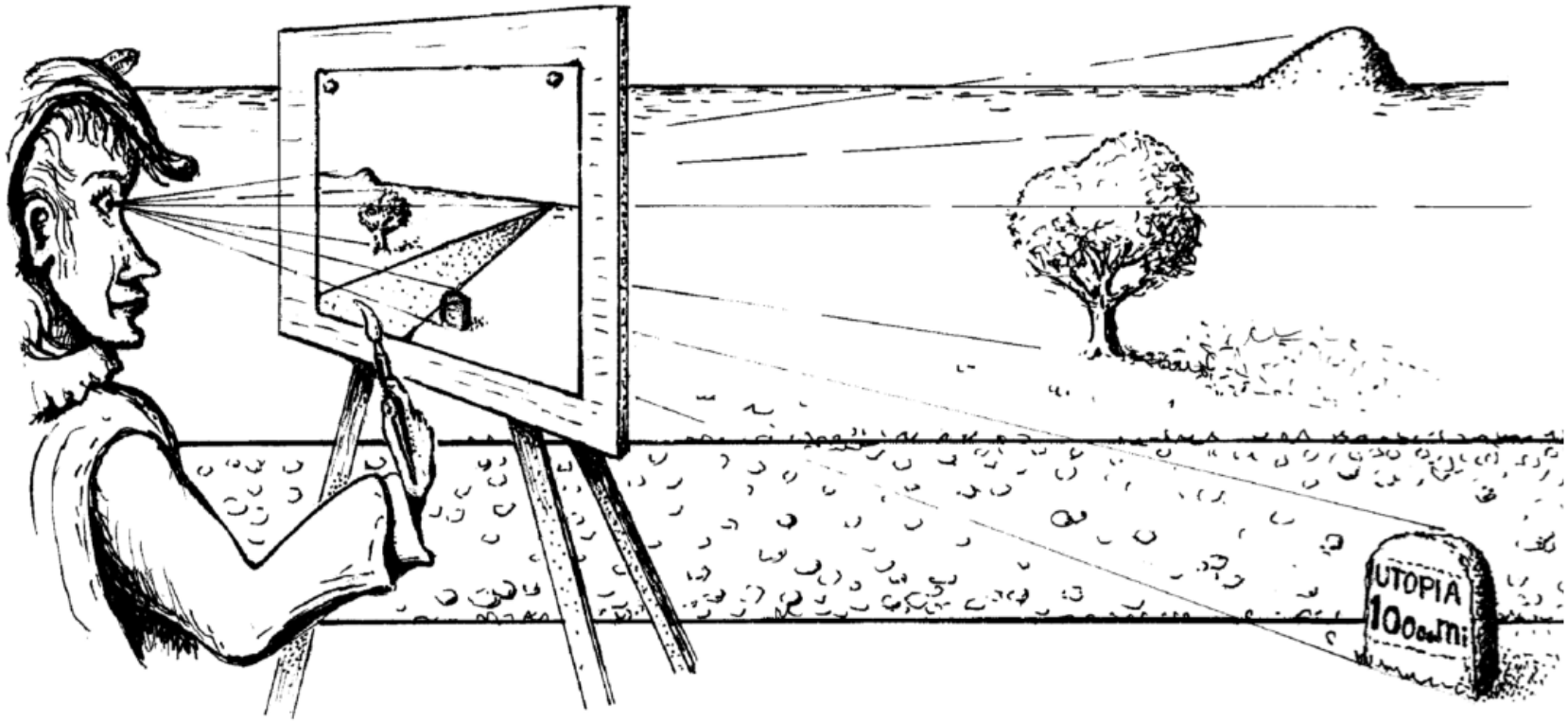
- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \big(\mathbb{R}^3 \setminus \{(0,0,0)\}\big)\big/ \sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$
- Ако је $Z \neq 0$ имамо $(X,Y,Z) \sim \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$ што је реална раван
- и имамо неки ,,додатак“ када је $Z = 0$

- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \big(\mathbb{R}^3 \setminus \{(0,0,0)\}\big)/\sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$
- Ако је $Z \neq 0$ имамо $(X,Y,Z) \sim \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$ што је реална раван
- и имамо неки ,,додатак“ када је $Z = 0$
- Тада је крива $E(\mathbb{R})$ задата са $Y^2Z = X^3 + aXZ^2 + bZ^3$ при чему $(x,y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right) \leftrightarrow \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$ и $(0,1,0) \leftrightarrow \mathcal{O}$

- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \left(\mathbb{R}^3 \setminus \{(0,0,0)\}\right) / \sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$
- Ако је $Z \neq 0$ имамо $(X,Y,Z) \sim \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$ што је реална раван
- и имамо неки ,,додатак“ када је $Z = 0$
- Тада је крива $E(\mathbb{R})$ задата са $Y^2Z = X^3 + aXZ^2 + bZ^3$ при чему $(x,y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right) \leftrightarrow \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$ и $(0,1,0) \leftrightarrow \mathcal{O}$



Sage рачуна у пројективним координатама



- Око = координатни почетак
- Све тачке са праве кроз око (у 3Д) се на слици (2Д) виде као једна иста тачка

Операције на елиптичкој кривој $E(\mathbb{R})$

- За $P = (x, y) \in E(\mathbb{R})$ дефинишемо $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$

Операције на елиптичкој кривој $E(\mathbb{R})$

- За $P = (x, y) \in E(\mathbb{R})$ дефинишемо $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$
- За $P, Q \in E(\mathbb{R})$ дефинишемо сабирање $P \oplus Q$:
  1. ако је $P = \mathcal{O}$: $\mathcal{O} \oplus Q = Q$
  2. ако је $Q = \mathcal{O}$: $P \oplus \mathcal{O} = P$
  3. ако је $Q = \ominus P \neq \mathcal{O}$: $P \oplus Q = \mathcal{O}$
  4. ако је $P, Q \neq \mathcal{O},\ Q \neq P, \ominus P$: повучемо праву l кроз P и Q
     - 4.1 или l сече ЕК у још тачно једној тачки R $(\neq P, Q)$
     - 4.2 или је l тангентна на ЕК у једној од тачака P и Q, означимо је са R

     тада је $P \oplus Q = \ominus R$
  5. ако је $P = Q \neq \mathcal{O}, \ominus P$: повучемо тангенту l на ЕК у тачки P, она ће пресећи ЕК у још тачно једној тачки R (различитој од P). Тада је $2P = P \oplus P = \ominus R$

Операције на елиптичкој кривој $E(\mathbb{R})$

- За $P = (x, y) \in E(\mathbb{R})$ дефинишемо $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$
- За $P, Q \in E(\mathbb{R})$ дефинишемо сабирање $P \oplus Q$:
  1. ако је $P = \mathcal{O}$: $\mathcal{O} \oplus Q = Q$
  2. ако је $Q = \mathcal{O}$: $P \oplus \mathcal{O} = P$
  3. ако је $Q = \ominus P \neq \mathcal{O}$: $P \oplus Q = \mathcal{O}$
  4. ако је $P, Q \neq \mathcal{O},\ Q \neq P, \ominus P$: повучемо праву l кроз P и Q
     - 4.1 или l сече ЕК у још тачно једној тачки R $(\neq P, Q)$
     - 4.2 или је l тангентна на ЕК у једној од тачака P и Q, означимо је са R

     тада је $P \oplus Q = \ominus R$
  5. ако је $P = Q \neq \mathcal{O}, \ominus P$: повучемо тангенту l на ЕК у тачки P, она ће пресећи ЕК у још тачно једној тачки R (различитој од P). Тада је $2P = P \oplus P = \ominus R$
- Случај 4.1 је најважнији, све остало су неки гранични случајеви тога

Теорема (Групни закон на ЕК)

$(E(\mathbb{R}), \oplus, \ominus, \mathcal{O})$ је Абелова група.

Теорема (Групни закон на ЕК)

$(E(\mathbb{R}), \oplus, \ominus, \mathcal{O})$ је Абелова група.

Гледано у пројективном простору $\mathbb{RP}^2$:

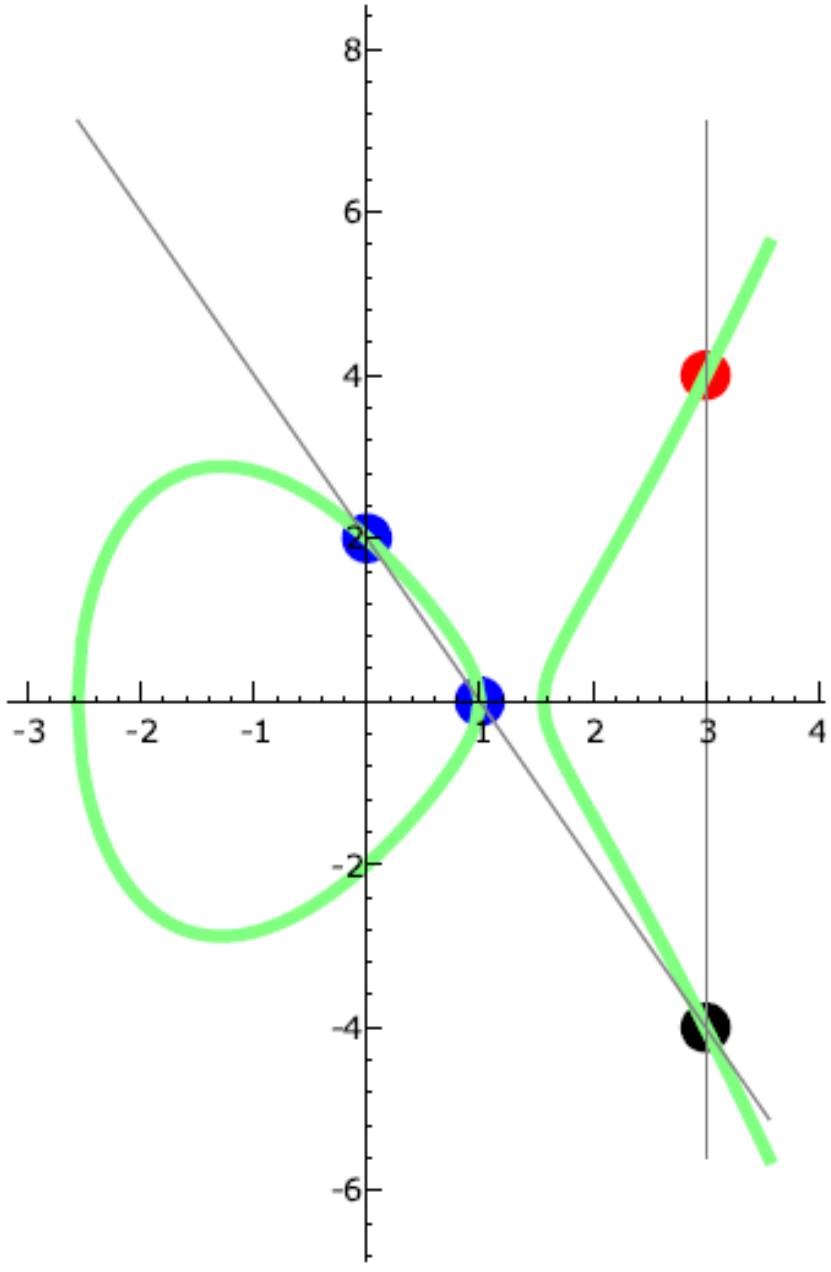
- ЕК $E(\mathbb{R})$ је допуњена тачком $\mathcal{O} = (0, 1, 0)$
- права l је исто допуњена бесконачно далеком тачком $(x, y, 0)$ која не мора бити $\mathcal{O}$

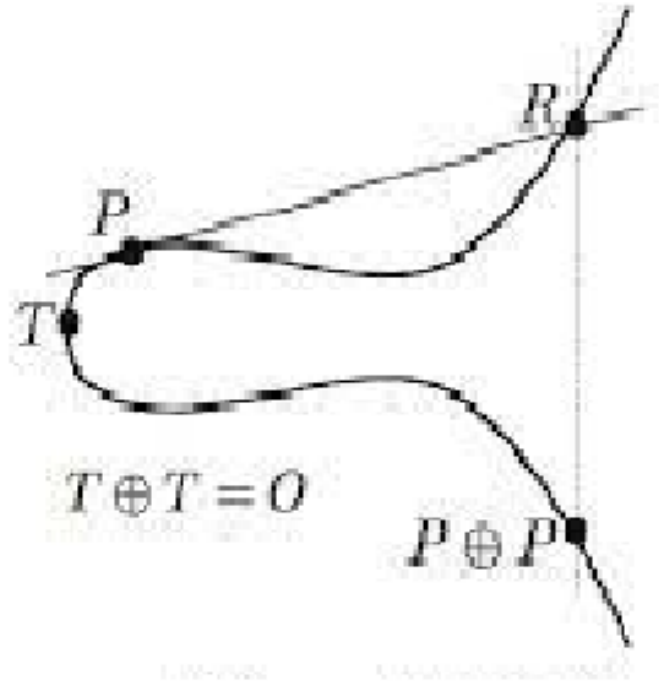
Теорема (Групни закон на ЕК)

$(E(\mathbb{R}), \oplus, \ominus, \mathcal{O})$ је Абелова група.

Гледано у пројективном простору $\mathbb{RP}^2$:

- ЕК $E(\mathbb{R})$ је допуњена тачком $\mathcal{O} = (0, 1, 0)$
- права l је исто допуњена бесконачно далеком тачком $(x, y, 0)$ која не мора бити $\mathcal{O}$
- Тада се $E(\mathbb{R})$ и l секу у тачно 3 (не обавезно различите) тачке $P, Q, R \in \mathbb{RP}^2$ тд. $P \oplus Q \oplus R = \mathcal{O}$





$(1,0) \oplus (0,2) = (3,4)$ on
$y^2 = x^3 - 5x + 4$

У 4. и 5. случају дефиниције $\oplus$ можемо да изведемо једначину праве l и затим нађемо њен пресек (заједничко решење) са елиптичком кривом. Ако су $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ добијамо $P \oplus Q = (x_3, y_3)$ где је

За P ≠ Q

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2; \\ y_3 = -y_1 + \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{cases}$$

За P = Q

$$\begin{cases} x_3 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1; \\ y_3 = -y_1 + \left(\dfrac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{cases}$$

($x_1 \neq x_2$ у 4. случају и $y_1 \neq 0$ у 5.)