Криптографија
- пети део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

12. март 2024.

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 РСА. Чак и ако РСА 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
```

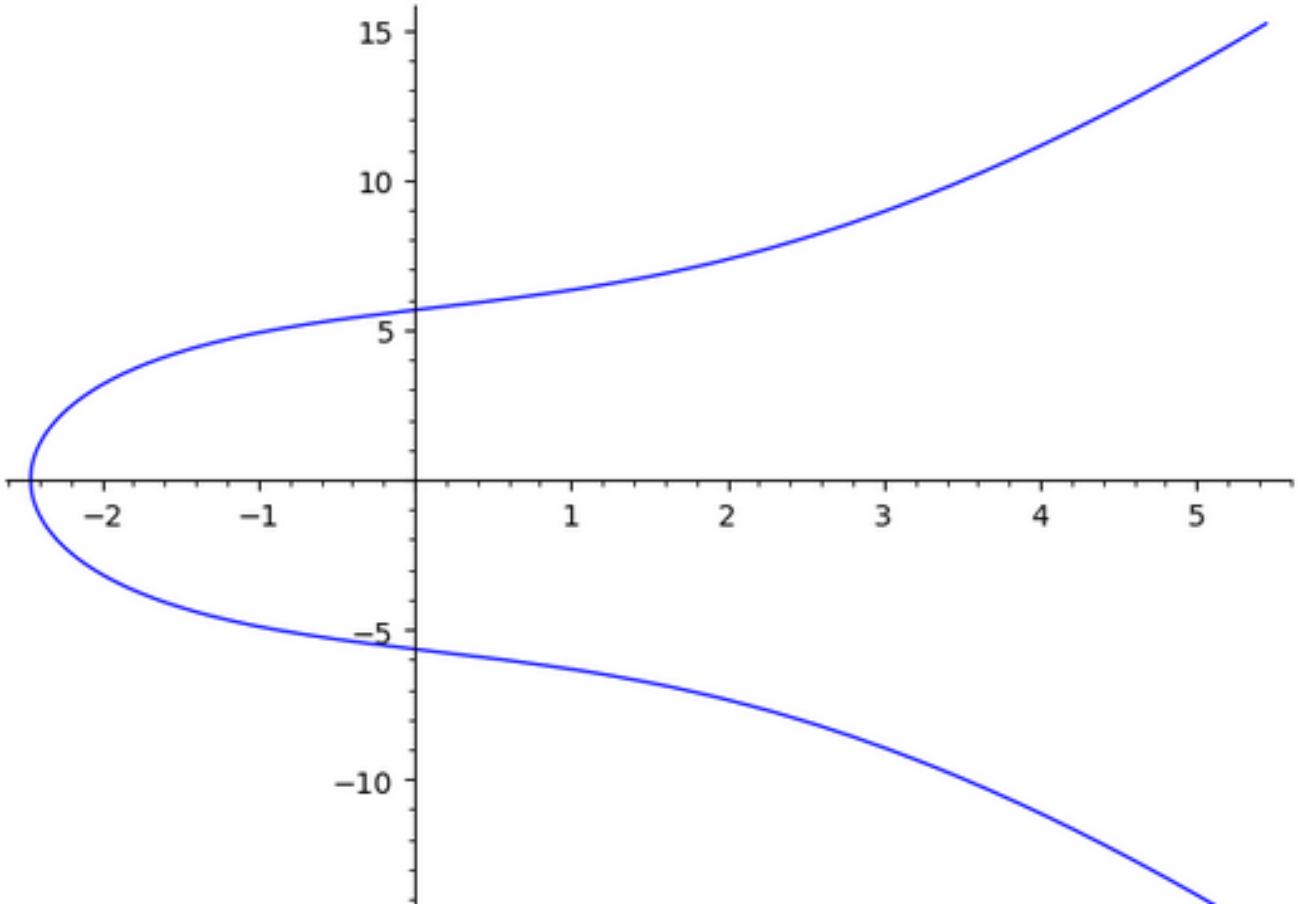
Sage има имплементиране функције за рад са ЕК

Save Copy Run Sage-10.1

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

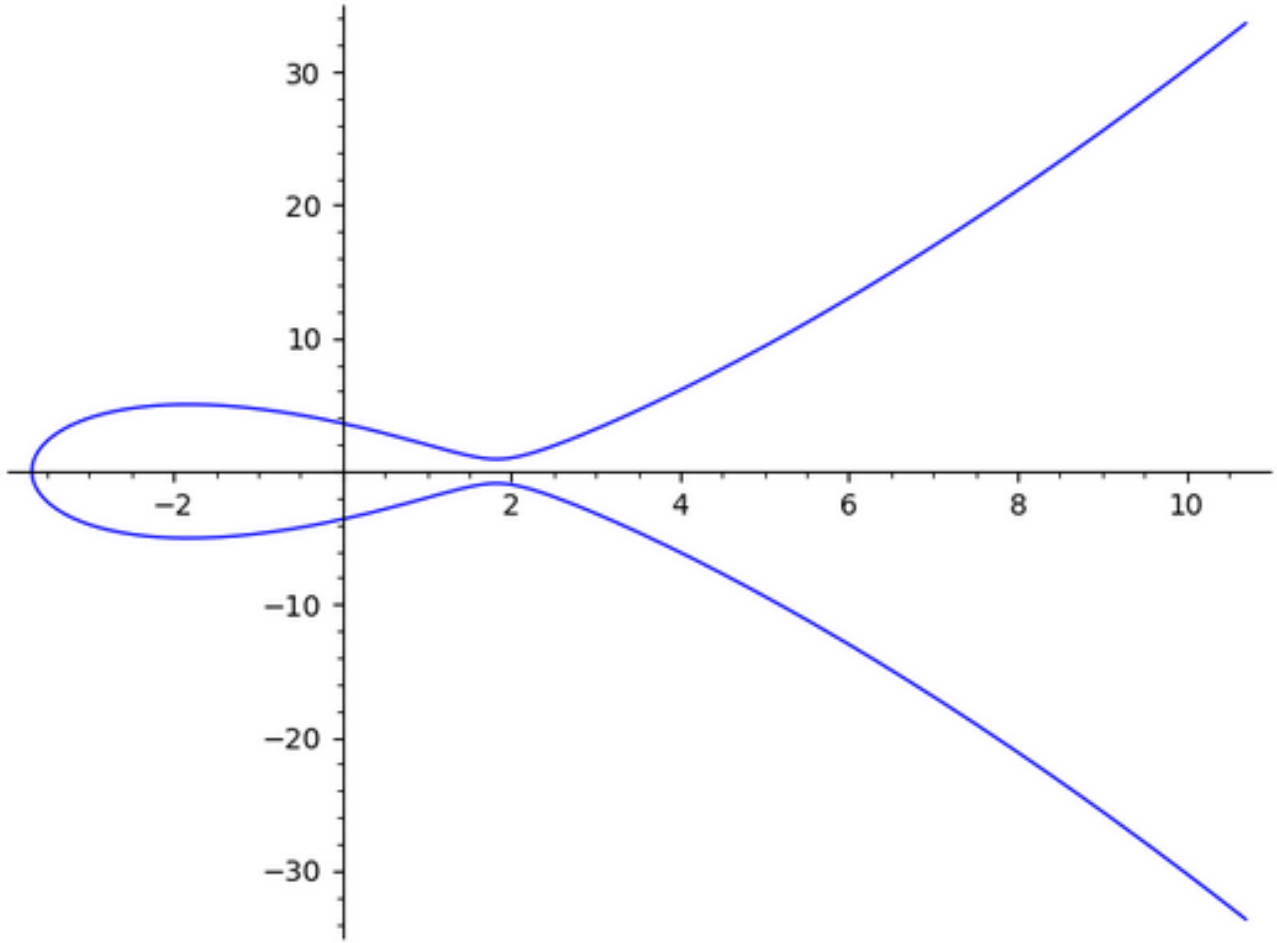
```
Elliptic Curve defined by y^2 = x^3 - 5*x + 4 over Rational Field
```

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

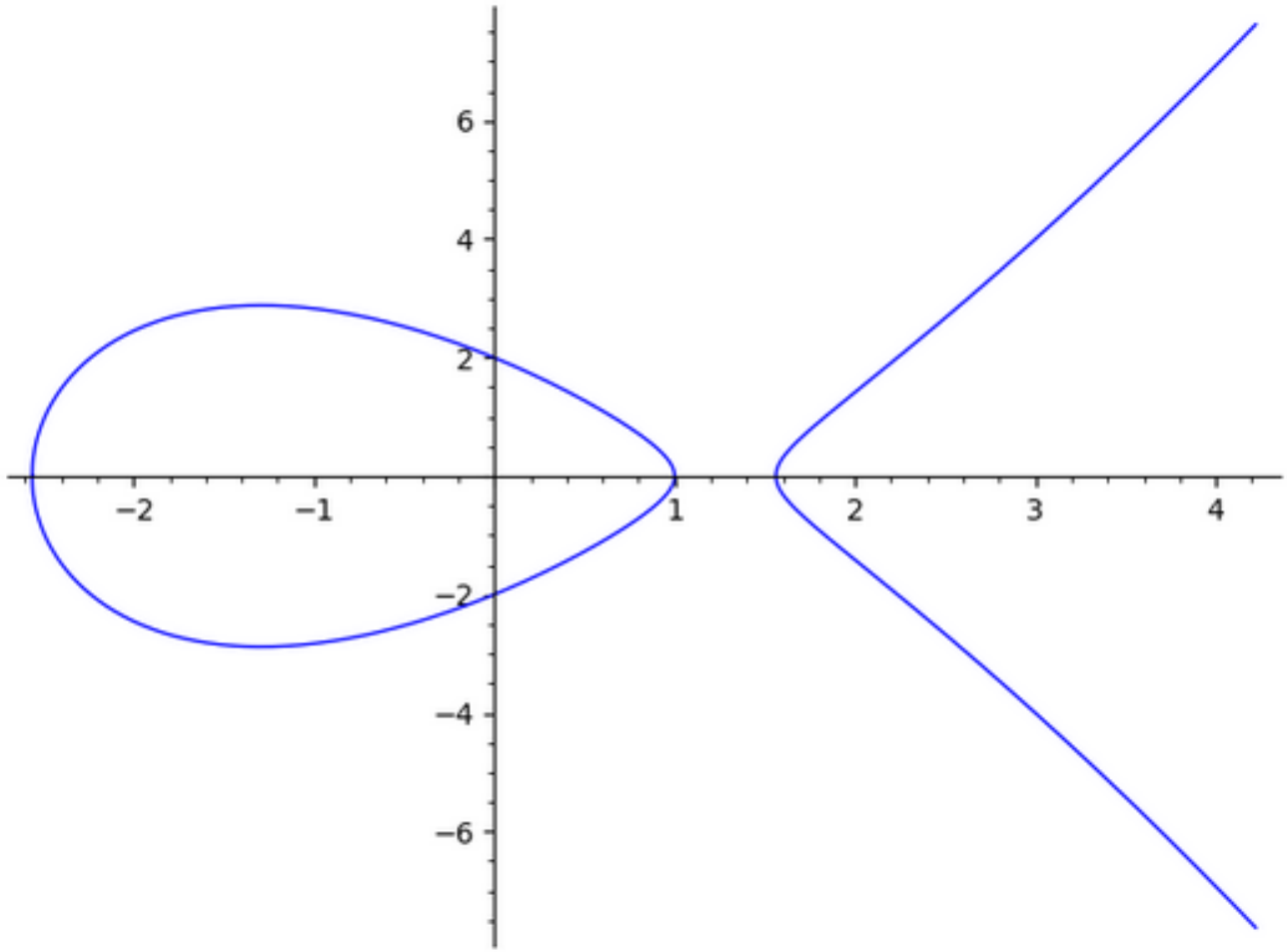


Save Copy Run SageMath 10.1

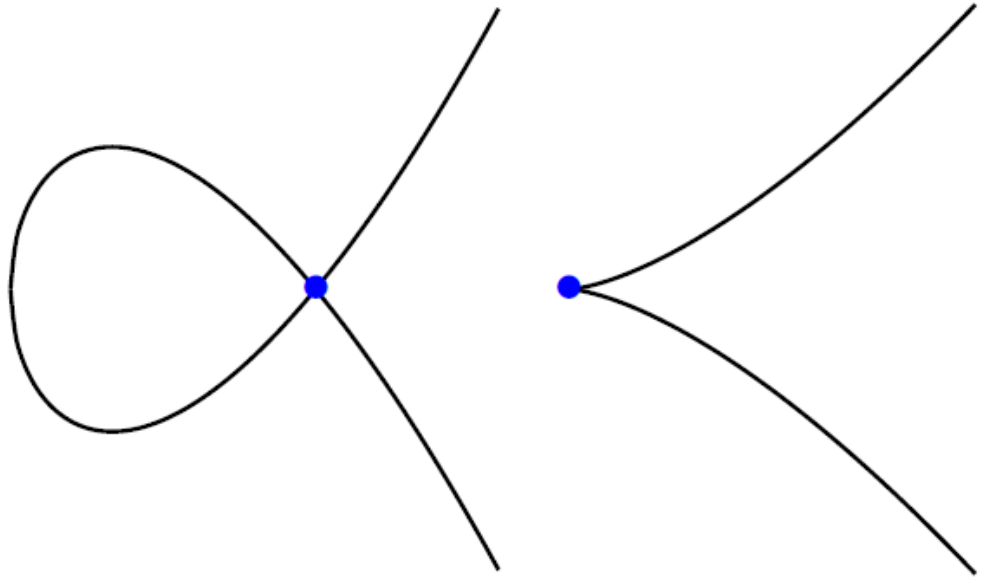
```
E = EllipticCurve([-10, 13])
E.plot()
```



```
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 $\mathbb{R}$.

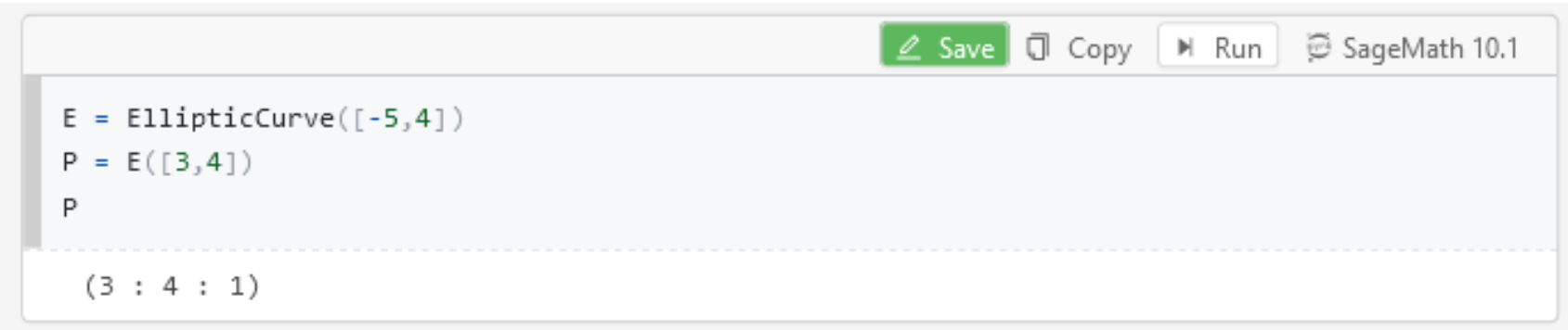
Нису елиптичке криве јер је $\Delta = 0$

- $E(\mathbb{R})$ 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 $\lambda \in \mathbb{R} \setminus \{0\}$

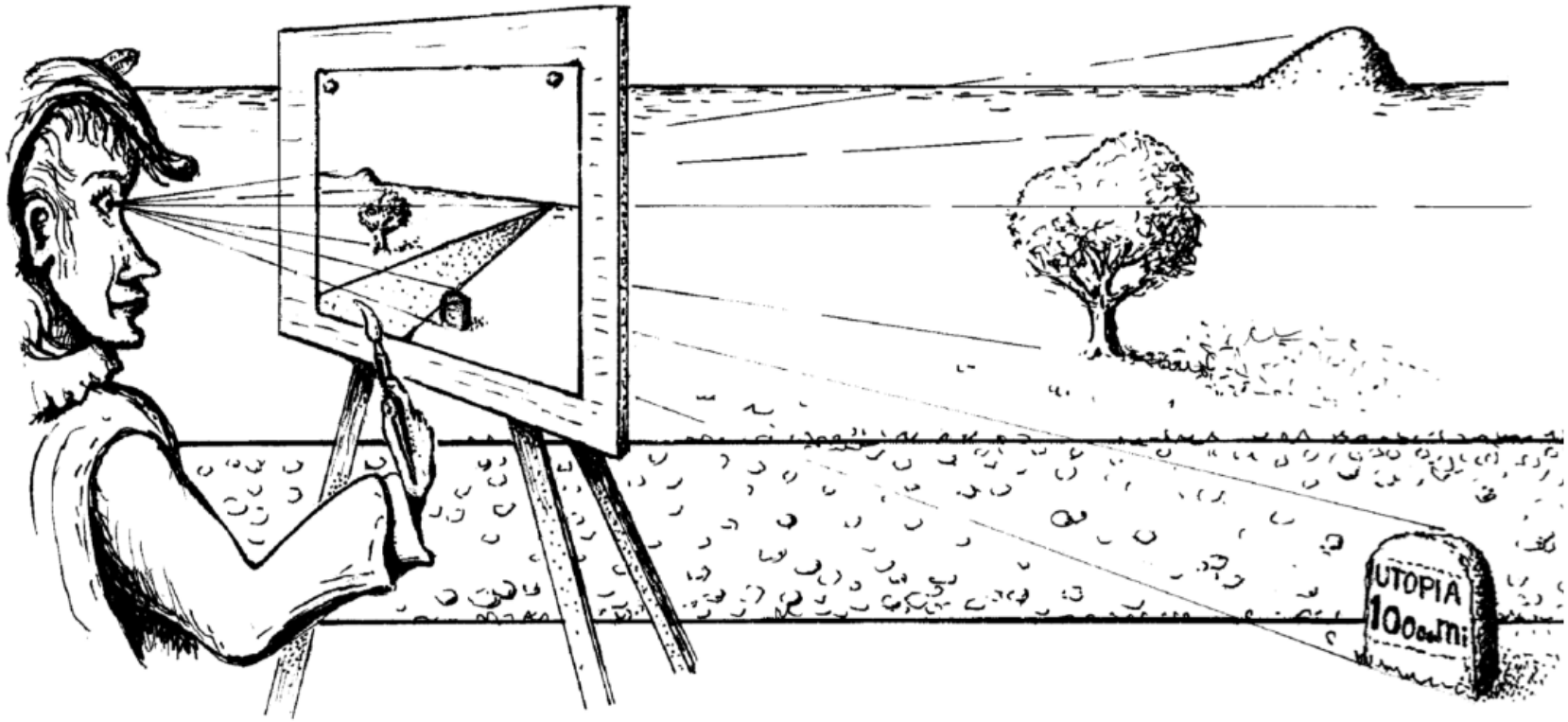
- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \big(\mathbb{R}^3 \setminus \{(0,0,0)\}\big)\big/ \sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$
- Ако је $Z \neq 0$ имамо $(X,Y,Z) \sim \left(\frac{X}{Z},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

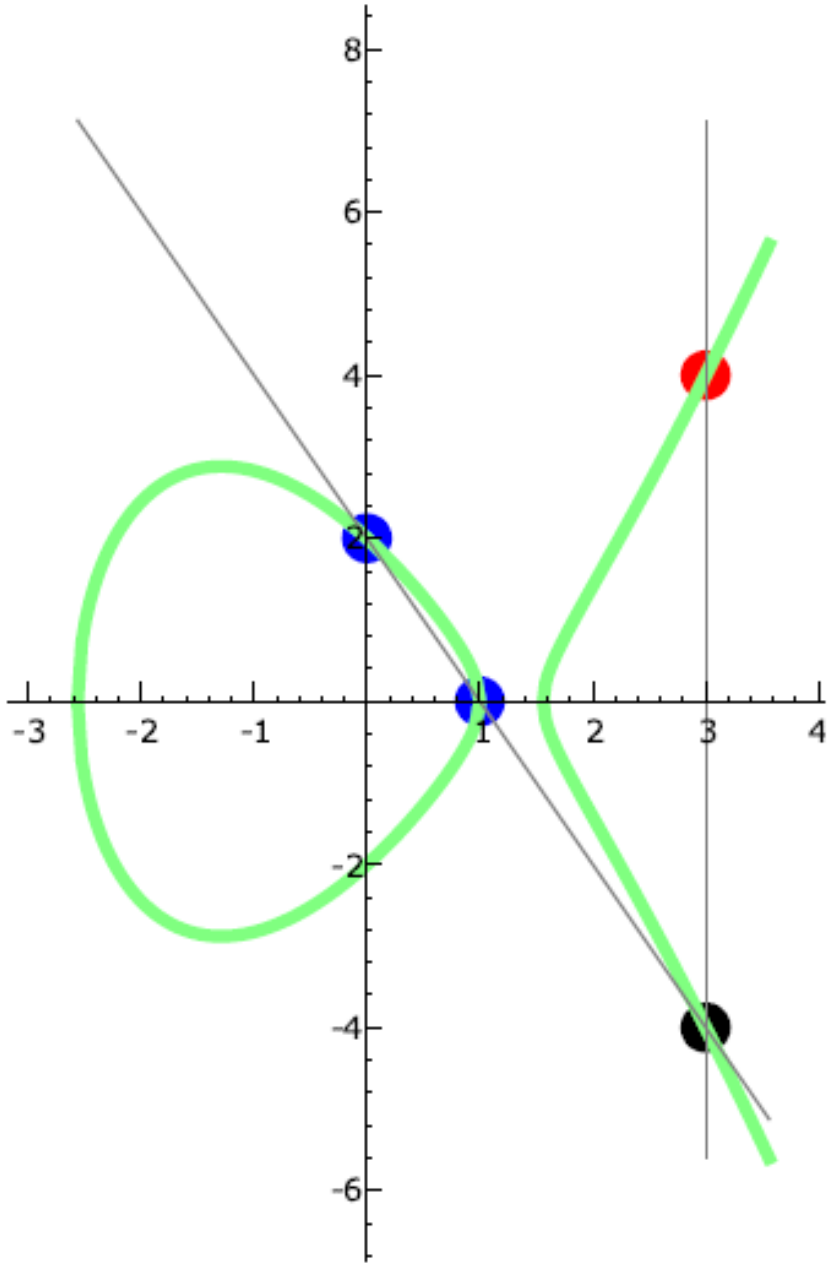
- ЕК $E(\mathbb{R})$ је допуњена тачком $\mathcal{O} = (0, 1, 0)$
- права l је исто допуњена бесконачно далеком тачком $(x, y, 0)$ која не мора бити $\mathcal{O}$

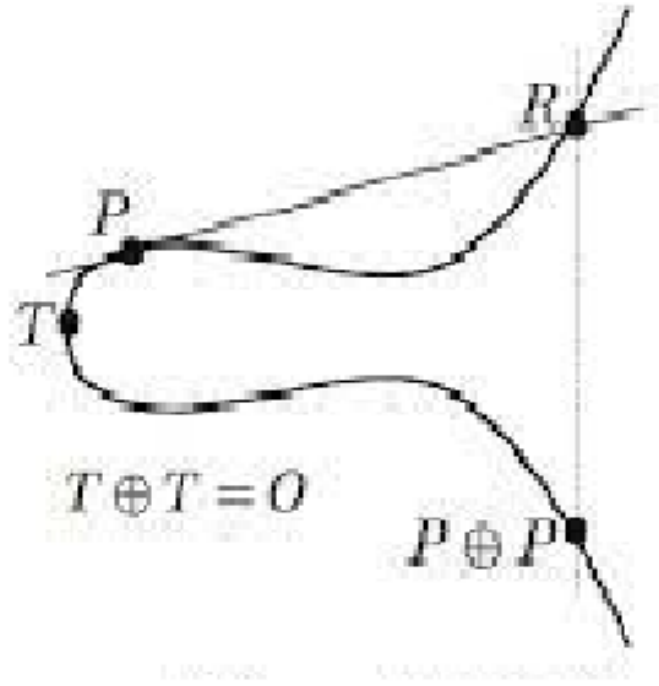
Теорема (Групни закон на ЕК)

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

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

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

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

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

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

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

- Сад је теже видети геометријски, али $\oplus$ и $\ominus$ се могу рачунати алгебарски (помоћу формула са претх. слајда)

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

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

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

- Сад је теже видети геометријски, али $\oplus$ и $\ominus$ се могу рачунати алгебарски (помоћу формула са претх. слајда)
- $(E(\mathbb{F}_q), \oplus, \ominus, \mathcal{O})$ је Абелова група

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

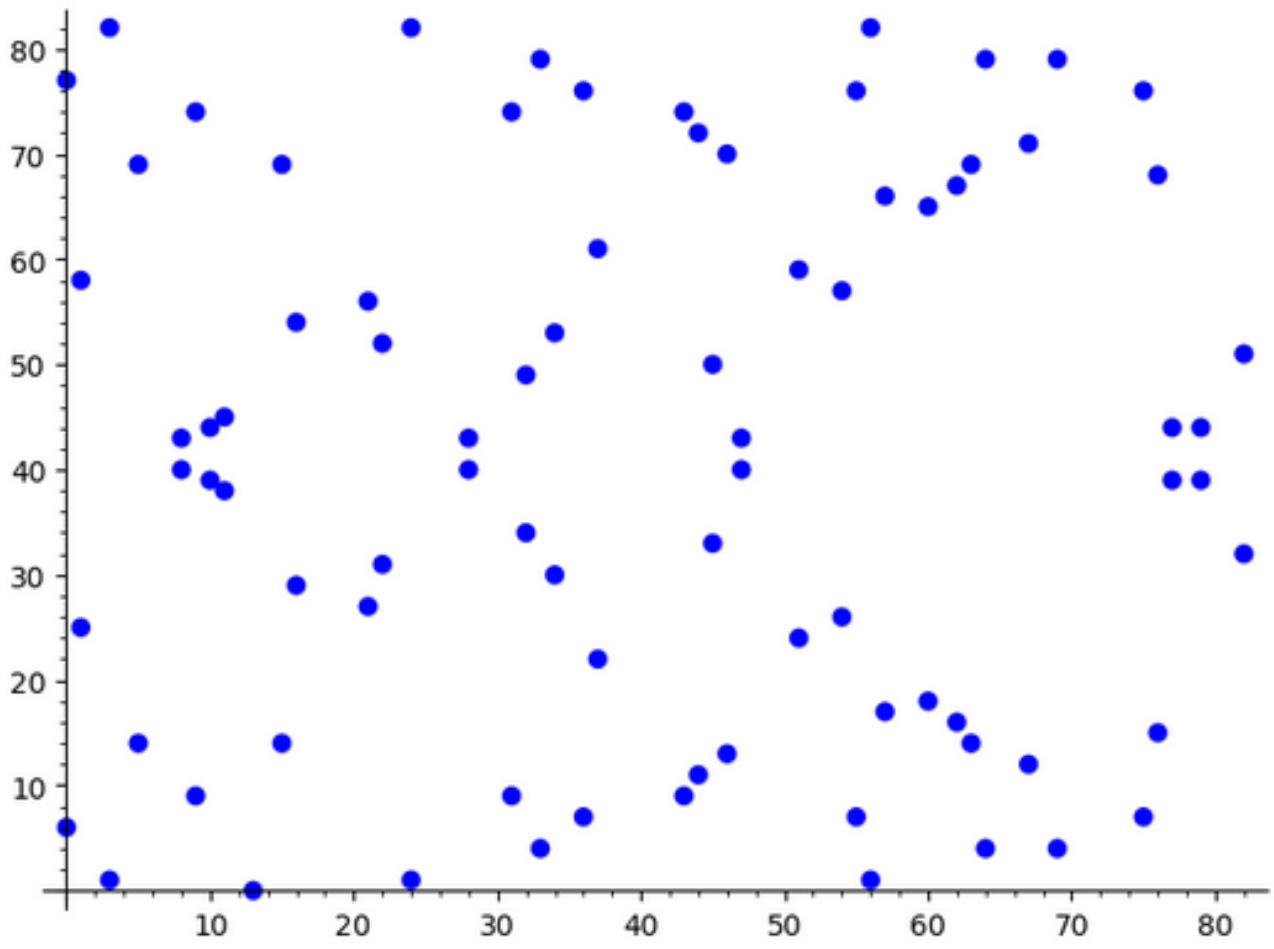
$$E\left(\mathbb{F}_q\right) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \;\middle|\; y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\},$$

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

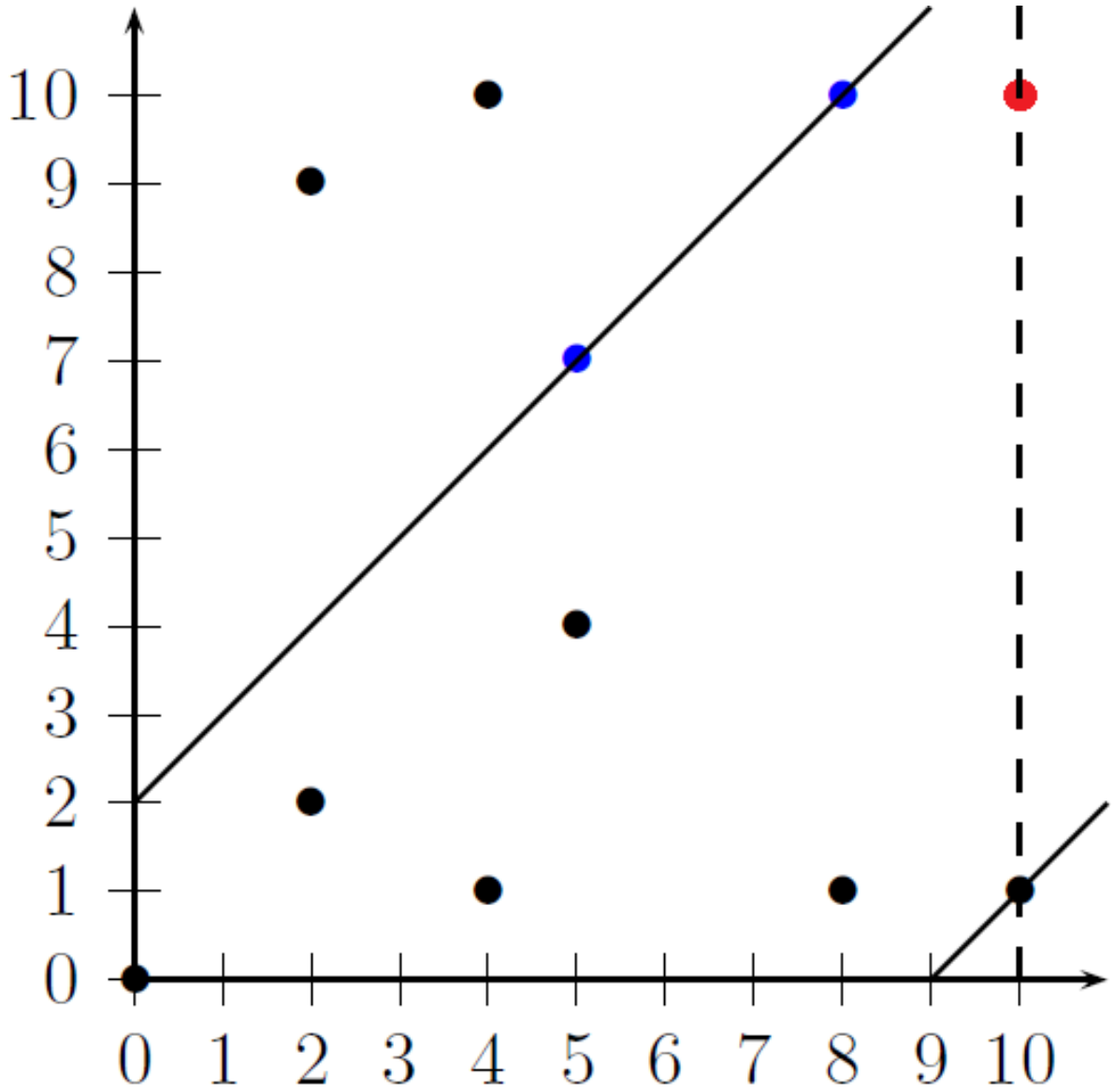
- Сад је теже видети геометријски, али $\oplus$ и $\ominus$ се могу рачунати алгебарски (помоћу формула са претх. слајда)
- $\left(E\left(\mathbb{F}_q\right), \oplus, \ominus, \mathcal{O}\right)$ је Абелова група
- Уобичајено је да се пише $E\left(\mathbb{F}_q\right)$, али је можда исправније $E\left(\mathbb{F}_q; a, b\right)$ јер зависи од 3 параметра q, a и b

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(83), [7,36])
E.plot(pointsize=45)
```



Елиптичка крива $y^2 = x^3 + 7x + 36$ над пољем $\mathbb{Z}_{83}$, тачка $\mathcal{O}$ се не види



$(5, 7) \oplus (8, 10) = (10, 1)$ на ЕК $y^2 = x^3 - 2x$ над пољем $\mathbb{Z}_{11}$

Пример: Одредити све тачке Елиптичке криве $y^2 = x^3 + 3x + 8$ на пољем $\mathbb{Z}_{13}$

y	0	±1	±2	±3	±4	±5	±6
y^2	0	1	4	9	3	12	10

Sada možemo da za svako $x \in \{0, 1, 2, \ldots 12\}$ odredimo vrednost za y^2 jednostavnom zamenom vrednosti u jednačinu krive.

$x = 0 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=0.

$x = 1 \to y^2 = 12 \to$ Iz tabele dobijamo da je $y = \pm5$ pa dobijamo dve tačke krive: (1, 5) i (1, 8).

$x = 2 \to y^2 = 9 \to$ Iz tabele dobijamo da je $y = \pm3$ pa dobijamo dve tačke krive: (2, 3) i (2, 10).

$x = 3 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=3.

$x = 4 \to y^2 = 6 \to 6$ se ne nalazi u tabeli, stoga nema tačke za x=4.

$x = 5 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=5.

$x = 6 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=6.

$x = 7 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=7.

$x = 8 \to y^2 = 11 \to 11$ se ne nalazi u tabeli, stoga nema tačke za x=8.

$x = 9 \to y^2 = 10 \to$ Iz tabele dobijamo da je $y = \pm6$ pa dobijamo dve tačke krive: (9, 6) i (9, 7).

$x = 10 \to y^2 = 11 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=10.

$x = 11 \to y^2 = 7 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=11.

$x = 12 \to y^2 = 4 \to$ Iz tabele dobijamo da je $y = \pm2$ pa dobijamo dve tačke krive: (12, 2) i (12, 11).

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$$

Израчунати $\underbrace{(1,8)}_{P} \oplus \underbrace{(9,7)}_{Q}$ на ел. кривој $E: y^2 = x^3 + 3x + 8$ над $\mathbb{Z}_{13}$

Сав рачун mod 13:

Права l која садржи P и Q: $y - 8 = \underbrace{\frac{8-7}{1-9}}_{= \frac{1}{-8} = \frac{1}{5} = 8}(x-1)$ тј. $y - 8 = 8(x-1)$

$y = 8x$

$E \cap l$: $(8x)^2 = x^3 + 3x + 8$

$x^3 \underbrace{-64}_{+1} x^2 + 3x + 8 = 0$

$P \oplus Q = \ominus R$

Вијетова правила $x_P + x_Q + x_R = -1$, $x_P = 1$, $x_Q = 9$

$x_R = -11 = 2$

$y_R = 8 \cdot 2 = 3$

$P \oplus Q = (2, -3) = (2, 10)$

Израчунајмо $2(9,7)$ на ел. кривој $E: y^2 = x^3 + 3x + 8$ над $\mathbb{Z}_{13}$

Лаб рачунат mod 13:

Тангента на E у тачки P: $y - 7 = f'(9)(x-9)$

$y = f(x) = \sqrt{x^3+3x+8}$ (део E који $\ni P$)

$f'(x) = \frac{3x^2+3}{2\sqrt{x^3+3x+8}} = \frac{3x^2+3}{2y}$

$f'(9) = \frac{3\cdot 81+3}{2\cdot 7} = \frac{3\cdot 3+3}{1} = 12$ $\quad \uparrow_P$

$\Rightarrow$: $y - 7 = 12(x-9)$

$= 12x + 9$

$y = 12x + 16$

$= -x + 3$

$E \cap \ell$: $(-x+3)^2 = x^3 + 3x + 8$

$x^3 - x^2 + \ldots = 0$

Виетова правила $\Rightarrow$ $2P = \ominus R$

$2x_P + x_R = +1$

$2\cdot 9 = 5$

$x_R = 1 - 5 = 9$

$y_R = -9 + 3 = -6$

$2P = (9, 6)$

Таблица сабирања на кривој $y^2 = x^3 + x + 2$ на пољем $\mathbb{Z}_{13}$

+	∞	(1.2)	(1.11)	(2.5)	(2.8)	(6.4)	(6.9)	(7.1)	(7.12)	(9.5)	(9.8)	(12.0)
∞	∞	(1.2)	(1.11)	(2.5)	(2.8)	(6.4)	(6.9)	(7.1)	(7.12)	(9.5)	(9.8)	(12.0)
(1.2)	(1.2)	(12.0)	∞	(6.9)	(7.1)	(2.8)	(9.5)	(9.8)	(2.5)	(7.12)	(6.4)	(1.11)
(1.11)	(1.11)	∞	(12.0)	(7.12)	(6.4)	(9.8)	(2.5)	(2.8)	(9.5)	(6.9)	(7.1)	(1.2)
(2.5)	(2.5)	(6.9)	(7.12)	(9.8)	∞	(1.11)	(6.4)	(1.2)	(7.1)	(2.8)	(12.0)	(9.5)
(2.8)	(2.8)	(7.1)	(6.4)	∞	(9.5)	(6.9)	(1.2)	(7.12)	(1.11)	(12.0)	(2.5)	(9.8)
(6.4)	(6.4)	(2.8)	(9.8)	(1.11)	(6.9)	(2.5)	∞	(9.5)	(12.0)	(1.2)	(7.12)	(7.1)
(6.9)	(6.9)	(9.5)	(2.5)	(6.4)	(1.2)	∞	(2.8)	(12.0)	(9.8)	(7.1)	(1.11)	(7.12)
(7.1)	(7.1)	(9.8)	(2.8)	(1.2)	(7.12)	(9.5)	(12.0)	(2.5)	∞	(1.11)	(6.9)	(6.4)
(7.12)	(7.12)	(2.5)	(9.5)	(7.1)	(1.11)	(12.0)	(9.8)	∞	(2.8)	(6.4)	(1.2)	(6.9)
(9.5)	(9.5)	(7.12)	(6.9)	(2.8)	(12.0)	(1.2)	(7.1)	(1.11)	(6.4)	(9.8)	∞	(2.5)
(9.8)	(9.8)	(6.4)	(7.1)	(12.0)	(2.5)	(7.12)	(1.11)	(6.9)	(1.2)	∞	(9.5)	(2.8)
(12.0)	(12.0)	(1.11)	(1.2)	(9.5)	(9.8)	(7.1)	(7.12)	(6.4)	(6.9)	(2.5)	(2.8)	∞

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост
- Интуитивно:

$$\underbrace{1}_{\mathcal{O}} + \text{број реш. по } x,\ y$$

$$= 1 + \sum_{x \in \mathbb{F}_p} \text{број реш. по } y \text{ за фикс. } x$$

$$= 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right)$$

$$= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост
- Интуитивно:

$$\underbrace{1}_{\mathcal{O}} + \text{број реш. по } x,\ y$$

$$= 1 + \sum_{x \in \mathbb{F}_p} \text{број реш. по } y \text{ за фикс. } x$$

$$= 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right)$$

$$= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$

- Како $\left(\frac{\cdot}{p}\right)$ насумично узима вредности ± 1 очекујемо да је сума мала

Хасеова теорема

Кардиналност групе $E(\mathbb{F}_q)$ је $q+1+s$, где је $s \leqslant 2\sqrt{q}$.
Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E(\mathbb{F}_q)$ тд. је $|E(\mathbb{F}_q)| = q+1+s$

Хасеова теорема

Кардиналност групе $E(\mathbb{F}_q)$ је $q+1+s$, где је $s \leqslant 2\sqrt{q}$.
Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E(\mathbb{F}_q)$ тд. је $|E(\mathbb{F}_q)| = q+1+s$

Кључна идеја:

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E(\mathbb{F}_q), \oplus\right)$

Хасеова теорема

Кардиналност групе $E(\mathbb{F}_q)$ је $q+1+s$, где је $s \leqslant 2\sqrt{q}$. Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E(\mathbb{F}_q)$ тд. је $|E(\mathbb{F}_q)| = q+1+s$

Кључна идеја:

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E(\mathbb{F}_q), \oplus\right)$
- Уместо фиксне кардиналности $q-1$ имамо слободу $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$

Помоћу Sage-а можемо наћи тачке са елиптичких кривих над $\mathbb{Z}_7$ (видимо да њихов број није увек исти!)

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[1,3])
E.points()
```

```
[(0 : 1 : 0), (4 : 1 : 1), (4 : 6 : 1), (5 : 0 : 1), (6 : 1 : 1), (6 : 6 : 1)]
```

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[2,6])
E.points()
```

```
[(0 : 1 : 0), (1 : 3 : 1), (1 : 4 : 1), (2 : 2 : 1), (2 : 5 : 1), (3 : 2 : 1), (3 : 5 : 1), (4 : 1
: 1), (4 : 6 : 1), (5 : 1 : 1), (5 : 6 : 1)]
```

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[6,6])
E.points()
```

```
[(0 : 1 : 0), (3 : 3 : 1), (3 : 4 : 1), (5 : 0 : 1)]
```

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

Проблем дискретног логаритма

Ако је познато P и nP одредити n.

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

Проблем дискретног логаритма

Ако је познато P и nP одредити n.

У пракси, ово се решава још спорије од дискретног логаритма у $\mathbb{F}_q^*$

За елиптичку криву $y^2 = x^3 + 2x + 6$ над $\mathbb{Z}_7$ добијамо цикличну групу реда 11 чији је генератор $P = (1, 4)$

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[2,6])
E.points()
```

```
[(0 : 1 : 0), (1 : 3 : 1), (1 : 4 : 1), (2 : 2 : 1), (2 : 5 : 1), (3 : 2 : 1), (3 : 5 : 1), (4 : 1
: 1), (4 : 6 : 1), (5 : 1 : 1), (5 : 6 : 1)]
```

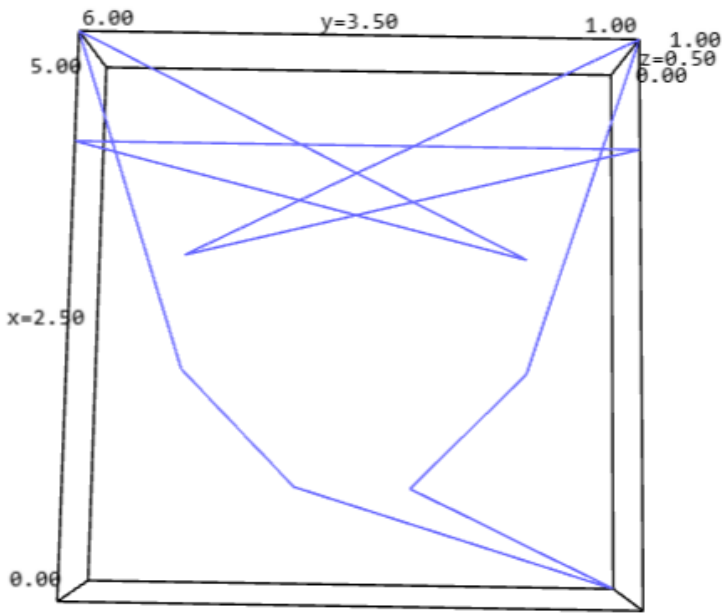
Save Copy Run SageMath 10.1

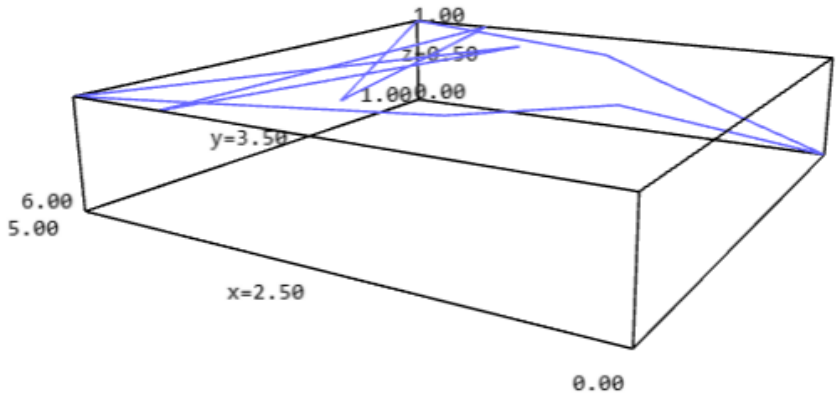
```
E = EllipticCurve(GF(7),[2,6])
P=E([1,4])
s=[n*P for n in range(1,12)]
s
```

```
[(1 : 4 : 1),
 (2 : 5 : 1),
 (5 : 6 : 1),
 (3 : 2 : 1),
 (4 : 6 : 1),
 (4 : 1 : 1),
 (3 : 5 : 1),
 (5 : 1 : 1),
 (2 : 2 : 1),
 (1 : 3 : 1),
 (0 : 1 : 0)]
```

Save Copy Run Sage-10.1

```
E=EllipticCurve(GF(7),[2,6])
P=E([1,4])
s=[n*P for n in range(1,13)]
plot(line(s))
```





Изломљена линија спаја P, $2P$, $\ldots$, $10P$, $11P = \mathcal{O}$ и $12P = P$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$
- Прво се m преведе у нумерички еквивалент M (као раније)

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$
- Прво се m преведе у нумерички еквивалент M (као раније)
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$
- Прво се m преведе у нумерички еквивалент M (као раније)
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$
- Прво се m преведе у нумерички еквивалент M (као раније)
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- Уколико претх. нема решења покушавамо даље са $Mk + 1$, $Mk + 2, \ldots, Mk + k - 1$ све док не пронађемо (x_0, y_0)

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m дужине N тд. $Nk < q$
- Прво се m преведе у нумерички еквивалент M (као раније)
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- Уколико претх. нема решења покушавамо даље са $Mk + 1$, $Mk + 2, \ldots, Mk + k - 1$ све док не пронађемо (x_0, y_0)
- Квадратна конгруенција има решење у $\frac{1}{2}$ случајева, па је вероватноћа да ћемо у k покушаја бар једном бити успешни $1 - \frac{1}{2^k}$

Општи случај: $q = p^\alpha$ и
$\mathbb{F}_q \cong \left\{ a_0 + a_1 t + \cdots + a_{\alpha-1} t^{\alpha-1} \,\middle|\, 0 \leqslant a_0, a_1, \ldots, a_{\alpha-1} \leqslant p-1 \right\}$

- Све исто као на прошлом слајду сем:
  - Када се кодира M број $Mk + j$ (редом за $j = 0, 1, \ldots, k-1$) се запише у основи p као

$$Mk + j = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

($r \leqslant \alpha - 1$ јер је $M < q$) и покуша се да се за полином $x_0 = x_0(t) = a_0 + a_1 t + \cdots + a_{r-1} t^{r-1}$ нађе полином $y_0 = y_0(t)$ тд. (x_0, y_0) припада ЕК

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$
  - Објашњење: $\left[\frac{x_0}{k}\right] = \left[M + \frac{j}{k}\right] = M$ (не знамо шта је j, само знамо да је из $[0, k-1]$)

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$
  - Објашњење: $\left[\frac{x_0}{k}\right] = \left[M + \frac{j}{k}\right] = M$ (не знамо шта је j, само знамо да је из $[0, k-1]$)
- За $q = p^\alpha$: имамо додатно корак да полином $x_0(t) = a_0 + a_1 t + \cdots + a_{r-1} t^{r-1}$ преведемо у број $a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}$, даље аналогно претх. случају