Криптографија
- осми део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

19. април 2024.

Диксонов метод случајних квадрата

Пример: Раставити $n = 89893$, користећи границу глаткости $B = 20$

$\sqrt{n} \approx 299.8$

		−1	2	3	5	7	11	13	17	19
$299^2 \equiv -492$	није гладак									
$300^2 \equiv 107$	није гладак									
$298^2 \equiv -1089$	$-1 \cdot 3^2 \cdot 11^2$	1	0	2	0	0	2	0	0	0
$301^2 \equiv 708$	није гладак									
$\sqrt{2n} \approx 424.01$										
$424^2 \equiv -10$	$-1 \cdot 2 \cdot 5$	1	1	0	1	0	0	0	0	0
$425^2 \equiv 839$	није гладак									
$423^2 \equiv -857$	није гладак									
$426^2 \equiv 1690$	$= 2 \cdot 5 \cdot 13^2$	0	1	0	1	0	0	2	0	0

$$298^2 \cdot 424^2 \cdot 426^2 \equiv (-1) \cdot 3^2 \cdot 11^2 \cdot (-1) \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 13^2 \pmod{n}$$
$$(298 \cdot 424 \cdot 426)^2 \equiv ((-1) \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13)^2 \pmod{n}$$

$298 \cdot 424 \cdot 426 \equiv 69938 \pmod{n}$ и $(-1) \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \equiv 85603 \pmod{n}$
Примећујемо да је $\mathrm{nzd}(69938 + 85603, n) = 373$ и $n/373 = 241$.

Верижни разломци

- Сваки рационалан број се може записати у облику верижног разломка

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Верижни разломци

- Сваки рационалан број се може записати у облику верижног разломка

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

- Пример:

$$\frac{107}{19} = 5 + \frac{12}{19} = 5 + \cfrac{1}{\cfrac{19}{12}} = 5 + \cfrac{1}{1 + \cfrac{7}{12}} = 5 + \cfrac{1}{1 + \cfrac{1}{\cfrac{12}{7}}} = 5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{5}{7}}}$$

$$= 5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{7}{5}}}} = 5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{5}}}} = \underline{5} + \cfrac{1}{\underline{1} + \cfrac{1}{\underline{1} + \cfrac{1}{\underline{1} + \cfrac{1}{\underline{2} + \cfrac{1}{\underline{2}}}}}}$$

- Претх. поступак личи на Еуклидов алгоритам ($107 : 19 = 5$ и остатак 12, итд.)
  - извршава се подједнако брзо као и Еуклидов алгоритам

- Претх. поступак личи на Еуклидов алгоритам ($107 : 19 = 5$ и остатак 12, итд.)
  - извршава се подједнако брзо као и Еуклидов алгоритам
- Сваки ирационалан број се може видети лимес верижног разломка

$$a = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

- Претх. поступак личи на Еуклидов алгоритам ($107 : 19 = 5$ и остатак 12, итд.)
  - извршава се подједнако брзо као и Еуклидов алгоритам
- Сваки ирационалан број се може видети лимес верижног разломка

$$a = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

- тј. $a = \lim\limits_{n\to\infty} a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_n}}} = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$ и P_n и Q_n се могу изразити преко $a_0, a_1, \ldots, a_n$

- Претх. поступак личи на Еуклидов алгоритам ($107 : 19 = 5$ и остатак 12, итд.)
  - извршава се подједнако брзо као и Еуклидов алгоритам
- Сваки ирационалан број се може видети лимес верижног разломка
$$a = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$
- тј. $a = \lim\limits_{n\to\infty} a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_n}}} = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$ и P_n и Q_n се могу изразити преко $a_0, a_1, \dots, a_n$
- Пишемо $a = [a_0, a_1, a_2, \dots]$ (коначан низ за $a \in \mathbb{Q}$ и бесконачан за $a \in \mathbb{R} \setminus \mathbb{Q}$)

Пример: Верижни развој $\sqrt{3}$ $\quad ([\sqrt{3}] = 1)$

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$$

$$\frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{2} = 1 + \frac{\sqrt{3}-1}{2} = 1 + \cfrac{1}{\cfrac{2}{\sqrt{3}-1}}$$

$$\frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{2(\sqrt{3}+1)}{3-1} = 2 + \sqrt{3} - 1 = 2 + \cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$$

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}$$

n	0	1	2	3	4	5	6	7
a_n	1	1	2	1	2	1	2	1
P_n	1	2	5	7	19	26	71	97
Q_n	1	1	3	4	11	15	41	56
$\frac{P_n}{Q_n}$	1	2	1.666...	1.75	1.727...	1.733...	1.731...	1.732...

Пример: Верижни развој π

$$a_0 = [\pi] = 3$$
$$x_1 = \frac{1}{\pi - a_0} \approx 7.06251\ldots$$
$$a_1 = [x_1] = 7$$
$$x_2 = \frac{1}{x_1 - a_1} \approx 15.9965\ldots$$
$$a_2 = 15$$

$$x_3 = \frac{1}{x_2 - a_2} \approx 1.0034\ldots$$
$$a_3 = 1$$
$$x_4 = \frac{1}{x_3 - a_3} \approx 292.63459\ldots$$
$$a_4 = 292$$
$$x_5 = \frac{1}{x_4 - a_4} \approx 1.57581\ldots$$

$$a_5 = 1$$
$$x_6 = \frac{1}{x_5 - a_5} \approx 1.73665\ldots$$
$$a_6 = 1$$
$$x_7 = \frac{1}{x_6 - a_6} \approx 1.35747\ldots$$
$$a_7 = 1$$

n	0	1	2	3	4	5	6	7
a_n	3	7	15	1	292	1	1	1
P_n	3	22	333	355	103993	104348	208341	312689
Q_n	1	7	106	113	33102	33215	66317	99532
$\frac{P_n}{Q_n}$	3	3.142..	3.14150..	3.1415929..	3.1415926530..	3.1415926539..	3.1415926534..	3.1415926536..

- Верижни разломци могу помоћи код Диксоновог метода

- Верижни разломци могу помоћи код Диксоновог метода
- Уместо погађања x-ева користити верижни развој броја $\sqrt{n} = \lim_{m\to\infty} \frac{P_m}{Q_m}$ (ознаке из Диксоновог метода)

- Верижни разломци могу помоћи код Диксоновог метода
- Уместо погађања x-ева користити верижни развој броја $\sqrt{n} = \lim_{m\to\infty} \frac{P_m}{Q_m}$ (ознаке из Диксоновог метода)
  - тада је $P_m^2 \approx nQ_m^2$, па је $r_n\left(P_m^2\right)$ мало и треба покушати са $x = P_m$

Нека је $n = 17873$. Почетак верижног развоја $\sqrt{n}$ је $[133, 1, 2, 4, 2, 3, 1, 2, 1, 2, 3, 3, \ldots]$. Користићемо базу фактора $\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ при чему нећемо уписивати нуле у таблицу.

			-1	2	3	5	7	11	13	17	19	23	29	
$[133] = 133$	133^2	$\equiv -184 = -1 \cdot 2^3 \cdot 23$	1	1								1		$\pmod 2$
$[133, 1] = 134$	134^2	$\equiv 83 =$ није гладак												
$[133, 1, 2] = \frac{401}{3}$	401^2	$\equiv -56 = -1 \cdot 2^3 \cdot 7$	1	1			1							
$[133, 1, 2, 4] = \frac{1738}{13}$	1738^2	$\equiv 107 =$ није гладак												
$[133, \ldots, 2] = \frac{3877}{29}$	3877^2	$\equiv -64 = -1 \cdot 2^6$	1											
$[133, \ldots, 3] = \frac{13369}{100}$	13369^2	$\equiv 161 = 7 \cdot 23$					1					1		

$(133 \cdot 401 \cdot 13369)^2 \equiv (-1 \cdot 2^3 \cdot 7 \cdot 23)^2 \pmod n$. Сада је $133 \cdot 401 \cdot 13369 \equiv 1288$ и $-1 \cdot 2^3 \cdot 7 \cdot 23 \equiv 16585$, али је $1288 \equiv -16585$. То значи да $\mathrm{nzd}(16585 + 1288, n) = n$ и $\mathrm{nzd}(16585 - 1288, n) = 1$, па нисмо добили ни један фактор. Настављамо даље.

			-1	2	3	5	7	11	13	17	19	23	29
$[133, \ldots, 1] = \frac{17246}{129}$	17246^2	$\equiv -77 = -1 \cdot 7 \cdot 11$	1				1	1					
$[133, \ldots, 2] = \frac{47861}{358}$	47861^2	$\equiv 149 =$ није гладак											
$[133, \ldots, 1] = \frac{65107}{487}$	65107^2	$\equiv -88 = -1 \cdot 2^3 \cdot 11$	1	1				1					

$(401 \cdot 3877 \cdot 17246 \cdot 65107)^2 \equiv ((-1)^2 \cdot 2^6 \cdot 7 \cdot 11)^2 \pmod n$. Сада је $401 \cdot 3877 \cdot 17246 \cdot 65107 \equiv 7272$ и $(-1)^2 \cdot 2^6 \cdot 7 \cdot 11 \equiv 4928$. Добија се $7272 - 4928 = 2344$ и $\mathrm{nzd}(2344, n) = 293$

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$
- Нарочито је популаран код поља $\mathbb{F}_{2^d} \cong \mathbb{Z}_2[x] / (f\mathbb{Z}_2[x])$ (или кад је q степен малог простог броја)

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$
- Нарочито је популаран код поља $\mathbb{F}_{2^d} \cong \mathbb{Z}_2[x]/(f\mathbb{Z}_2[x])$ (или кад је q степен малог простог броја)
- Фаза припреме:
  - Изабере се $B \ll d$ и пронађу се сви нерастављиви полиноми $h_1, h_2, \ldots, h_r$ из $\mathbb{Z}_2[x]$ степена највише B

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$
- Нарочито је популаран код поља $\mathbb{F}_{2^d} \cong \mathbb{Z}_2[x]/(f\mathbb{Z}_2[x])$ (или кад је q степен малог простог броја)
- Фаза припреме:
  - Изабере се $B \ll d$ и пронађу се сви нерастављиви полиноми $h_1, h_2, \ldots, h_r$ из $\mathbb{Z}_2[x]$ степена највише B
  - Израчунају се сви $\log_g h_i$ на следећи начин:
    - за насумично изабрано t проверава се да ли је g^t облика $h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_r^{\alpha_r}$

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$
- Нарочито је популаран код поља $\mathbb{F}_{2^d} \cong \mathbb{Z}_2[x]/(f\mathbb{Z}_2[x])$ (или кад је q степен малог простог броја)
- Фаза припреме:
  - Изабере се $B \ll d$ и пронађу се сви нерастављиви полиноми $h_1, h_2, \dots, h_r$ из $\mathbb{Z}_2[x]$ степена највише B
  - Израчунају се сви $\log_g h_i$ на следећи начин:
    - за насумично изабрано t проверава се да ли је g^t облика $h_1^{\alpha_1} h_2^{\alpha_2} \dots h_r^{\alpha_r}$
    - чувају се само они g^t који су прошли тест (и одговарајући степени $\alpha_1, \dots, \alpha_r$) и помоћу њих се прави систем једначина облика $t \equiv_{q-1} \alpha_1 \log_g h_1 + \alpha_2 \log_g h_2 \dots \alpha_r \log_g h_r$ (по непознатим $\log_g h_1, \log_g h_2, \dots, \log_g h_r$)

Алгоритам за израчунавање индекса

- Индекс је стари назив за дискретни логаритам, алгоритам се користи за рачунање $\log_g a$ у $\mathbb{F}_q^*$
- Нарочито је популаран код поља $\mathbb{F}_{2^d} \cong \mathbb{Z}_2[x]/(f\mathbb{Z}_2[x])$ (или кад је q степен малог простог броја)
- Фаза припреме:
  - Изабере се $B \ll d$ и пронађу се сви нерастављиви полиноми $h_1, h_2, \ldots, h_r$ из $\mathbb{Z}_2[x]$ степена највише B
  - Израчунају се сви $\log_g h_i$ на следећи начин:
    - за насумично изабрано t проверава се да ли је g^t облика $h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_r^{\alpha_r}$
    - чувају се само они g^t који су прошли тест (и одговарајући степени $\alpha_1, \ldots, \alpha_r$) и помоћу њих се прави систем једначина облика $t \equiv_{q-1} \alpha_1 \log_g h_1 + \alpha_2 \log_g h_2 \ldots \alpha_r \log_g h_r$ (по непознатим $\log_g h_1, \log_g h_2, \ldots, \log_g h_r$)
    - поступак се понавља све док не добијемо довољно једначина да систем има јединствено решење

- Фаза рачунања $\log_g a$:
  - Покуша се да се a напише у облику $h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_r^{\alpha_r}$

- Фаза рачунања $\log_g a$:
  - Покуша се да се a напише у облику $h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_r^{\alpha_r}$
    - Ако не може, покуша се исто са ag^t, за разне t-ове све док се не нађе одговарајући

- Фаза рачунања $\log_g a$:
  - Покуша се да се a напише у облику $h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_r^{\alpha_r}$
    - Ако не може, покуша се исто са ag^t, за разне t-ове све док се не нађе одговарајући
  - Тада се $\log_g a$ рачуна као $-t + \alpha_1 \log_g h_1 + \alpha_2 \log_g h_2 \ldots \alpha_r \log_g h_r \mod q - 1$

- Фаза рачунања $\log_g a$:
  - Покуша се да се a напише у облику $h_1^{\alpha_1} h_2^{\alpha_2} \dots h_r^{\alpha_r}$
    - Ако не може, покуша се исто са ag^t, за разне t-ове све док се не нађе одговарајући
  - Тада се $\log_g a$ рачуна као $-t + \alpha_1 \log_g h_1 + \alpha_2 \log_g h_2 \dots \alpha_r \log_g h_r \mod q - 1$
- У фази припреме се практично имитира база чинилаца из претх. алгоритама
  - али сада радимо са полиномима из $\mathbb{Z}_2[x]$
    - Растављање полинома је још теже од растављања бројева, али овде је довољан и неки елементаран (спор) алгоритам када је B мало
  - „величина“ $f \in \mathbb{Z}_2[x]$ се мери помоћу $\deg f$

- Фаза рачунања $\log_g a$:
  - Покуша се да се a напише у облику $h_1^{\alpha_1} h_2^{\alpha_2} \dots h_r^{\alpha_r}$
    - Ако не може, покуша се исто са ag^t, за разне t-ове све док се не нађе одговарајући
  - Тада се $\log_g a$ рачуна као $-t + \alpha_1 \log_g h_1 + \alpha_2 \log_g h_2 \dots \alpha_r \log_g h_r \mod q - 1$
- У фази припреме се практично имитира база чинилаца из претх. алгоритама
  - али сада радимо са полиномима из $\mathbb{Z}_2[x]$
    - Растављање полинома је још теже од растављања бројева, али овде је довољан и неки елементаран (спор) алгоритам када је B мало
  - „величина“ $f \in \mathbb{Z}_2[x]$ се мери помоћу $\deg f$
- Посебно применљиво за рачунање више дискретних логаритама са истом основом - тада се фаза припреме ради само једном

Пример: $\log_x y = ?$ у $\mathbb{F}^*_{2^{11}}$, где је
$y(x) = x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + 1$
($g(x) = x$ је генератор $\mathbb{F}_{2^{11}} \cong \mathbb{Z}_2[x]/(f\mathbb{Z}_2[x])$, где је
$f(x) = x^{11} + x^4 + x^2 + x + 1$)

- Припрема: има 8 нерастављивих полинома степена највише 4, нека су њихови логаритми (у основи $g(x)$):

$1 = \log(x)$ $\quad a = \log(x+1)$ $\quad c = \log(x^2+x+1)$ $\quad d = \log(x^3+x+1)$
$e = \log(x^3+x^2+1)$ $\quad h = \log(x^4+x+1)$ $\quad j = \log(x^4+x^3+1)$ $\quad k = \log(x^4+x^3+x^2+x+1)$.

Израчунавајући разне степенове g^t добијамо

$g^{11} = (x+1)(x^3+x^2+1)$ $\quad 11 = a + e \pmod{2047 = q-1}$
$g^{41} = (x^3+x^2+1)(x^3+x+1)^2$ $\quad 41 = e + 2d$
$g^{56} = (x^2+x+1)(x^3+x+1)(x^3+x^2+1)$ $\quad 56 = c + d + e$
$g^{59} = (x+1)(x^4+x^3+x^2+x+1)^2$ $\quad 59 = a + 2k$
$\cancel{g^{71} = (x^3+x^2+1)(x^2+x+1)^2 \quad 71 = e + 2c}$ линеарно зависна са претходним
$g^{83} = (x^3+x+1)(x+1)^2,$ $\quad 83 = d + 2a.$
$g^{106} = (x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ $\quad 106 = a+j+k$
$g^{126} = (x^4+x+1)(x^4+x^3+x^2+x+1)(x+1)2$ $\quad 126 = h+k+2a$

Дакле $a = 846$, $c = 453$, $d = 438$, $e = 1212$, $h = 1898$, $j = 677$, $k = 630$.

Сада прелазимо на други корак. Израчунавамо yg^t за разне вредности t. Проналазимо да је $yg^{19} = (x^4+x^3+x^2+x+1)^2$. Дакле $\log(y) + 19\log(g) = 2k$. Пошто је $\log(g) = \log(x) = 1$, добија се $\log(y) = 2k - 19 \equiv 1241 \pmod{2047}$,

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
```

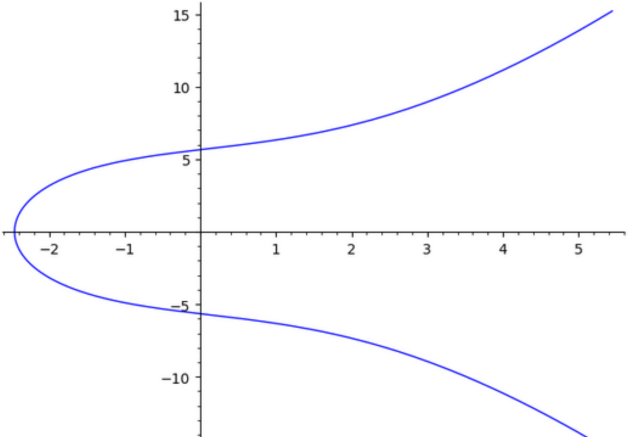
Sage има имплементиране функције за рад са ЕК

Save Copy Run Sage-10.1

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

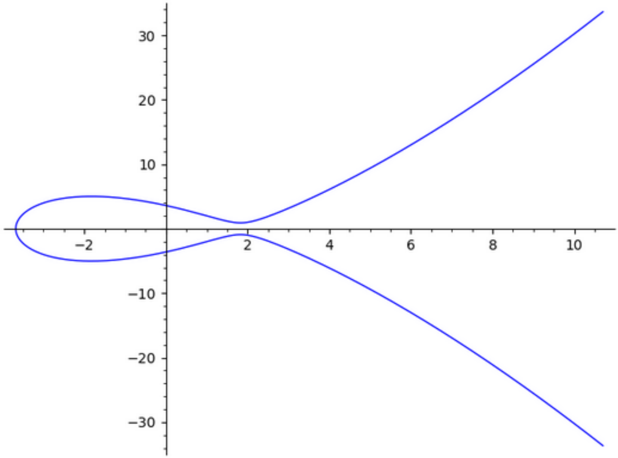
```
Elliptic Curve defined by y^2 = x^3 - 5*x + 4 over Rational Field
```

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

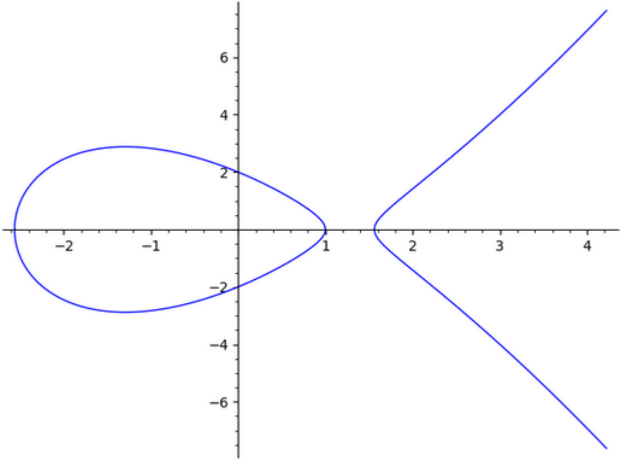


Save Copy Run SageMath 10.1

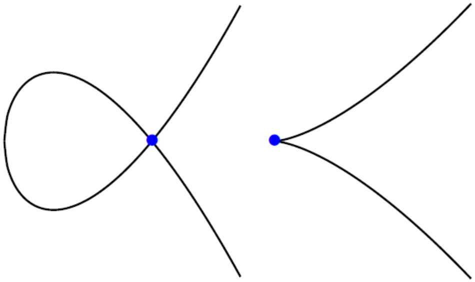
```
E = EllipticCurve([-10, 13])
E.plot()
```



```
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 $\mathbb{RP}^2 = \left(\mathbb{R}^3 \setminus \{(0,0,0)\}\right)/\sim$, 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 $Z = 0$

- $E(\mathbb{R})$ 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 $(X,Y,Z) \sim \big(\frac{X}{Z}, \frac{Y}{Z}, 1\big)$ 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 $(x,y) = \big(\frac{X}{Z}, \frac{Y}{Z}\big) \leftrightarrow \big(\frac{X}{Z}, \frac{Y}{Z}, 1\big)$ и $(0,1,0) \leftrightarrow \mathcal{O}$

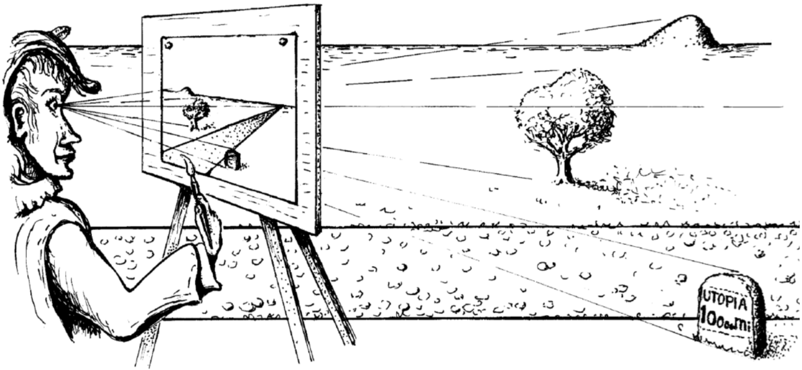
- $E(\mathbb{R})$ се може видети као крива у пројективној равни $\mathbb{RP}^2 = \left(\mathbb{R}^3 \setminus \{(0,0,0)\}\right)/\sim$, где је $(X,Y,Z) \sim (X',Y',Z')$ ако $\lambda(X,Y,Z) = (X',Y',Z')$, за неко $\lambda \in \mathbb{R} \setminus \{0\}$
- Ако је $Z \neq 0$ имамо $(X,Y,Z) \sim \left(\frac{X}{Z},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

Save Copy Run SageMath 10.1

```
E = EllipticCurve([-5,4])
P = E([3,4])
P
```

```
(3 : 4 : 1)
```

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 je $P = \mathcal{O}$: $\mathcal{O} \oplus Q = Q$
  2. ако je $Q = \mathcal{O}$: $P \oplus \mathcal{O} = P$
  3. ако je $Q = \ominus P \neq \mathcal{O}$: $P \oplus Q = \mathcal{O}$
  4. ако je $P, Q \neq \mathcal{O}$, $Q \neq P, \ominus P$: 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 je l тангентна на ЕК у једној од тачака P и Q, означимо je са R

     тада je $P \oplus Q = \ominus R$
  5. ако je $P = Q \neq \mathcal{O}, \ominus P$: повучемо тангенту l на ЕК у тачки P, она ће пресећи ЕК у још тачно једној тачки R (различитој од P). Тада je $2P = P \oplus P = \ominus R$
- Случај 4.1 je 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 $\mathbb{RP}^2$:

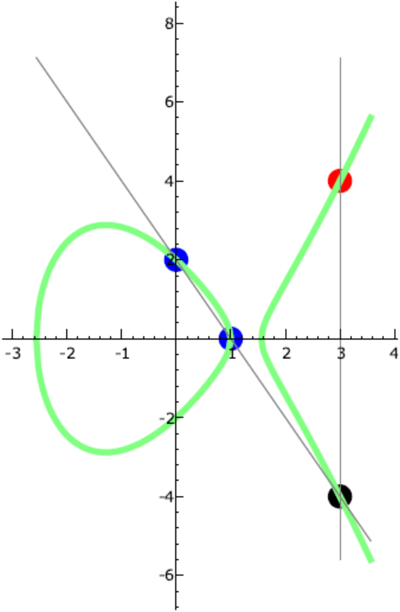
- ЕК $E(\mathbb{R})$ је допуњена тачком $\mathcal{O} = (0, 1, 0)$
- права l је исто допуњена бесконачно далеком тачком $(x, y, 0)$ која не мора бити $\mathcal{O}$

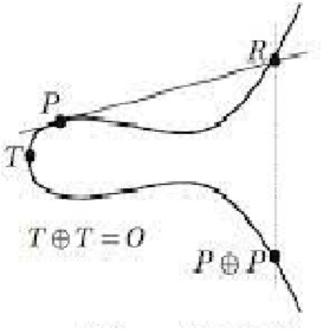
Теорема (Групни закон на ЕК)

$(E(\mathbb{R}), \oplus, \ominus, \mathcal{O})$ 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 $$\left[\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2; \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{aligned}\right.$$

За P = Q $$\left[\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1; \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{aligned}\right.$$

($x_1 \neq x_2$ 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

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

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)

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

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

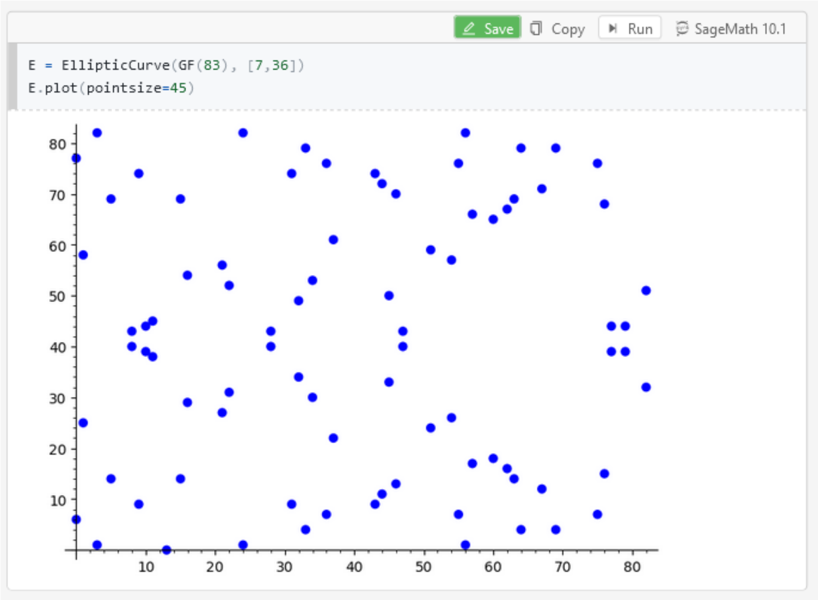
Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

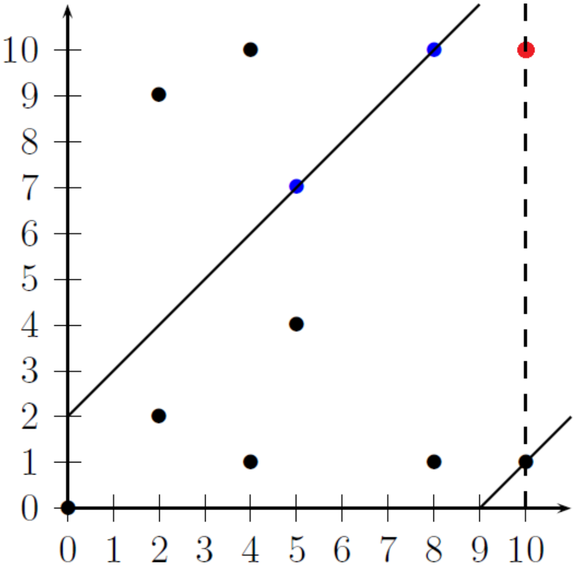
$$E(\mathbb{F}_q) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\},$$

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
- Уобичајено је да се пише $E(\mathbb{F}_q)$, али је можда исправније $E(\mathbb{F}_q; a, b)$ јер зависи од 3 параметра q, a и b



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 $\mathbb{Z}_{11}$