Eliptické křivky a jejich aritmetika -1

Evropský sociální fond
Investujeme do vaší budoucnosti

Alena Šolcová, FIT ČVUT

2014

OPPA
PRAHA PRAGUE PRAGA PRAG
EVROPSKÁ UNIE

Definice eliptické křivky

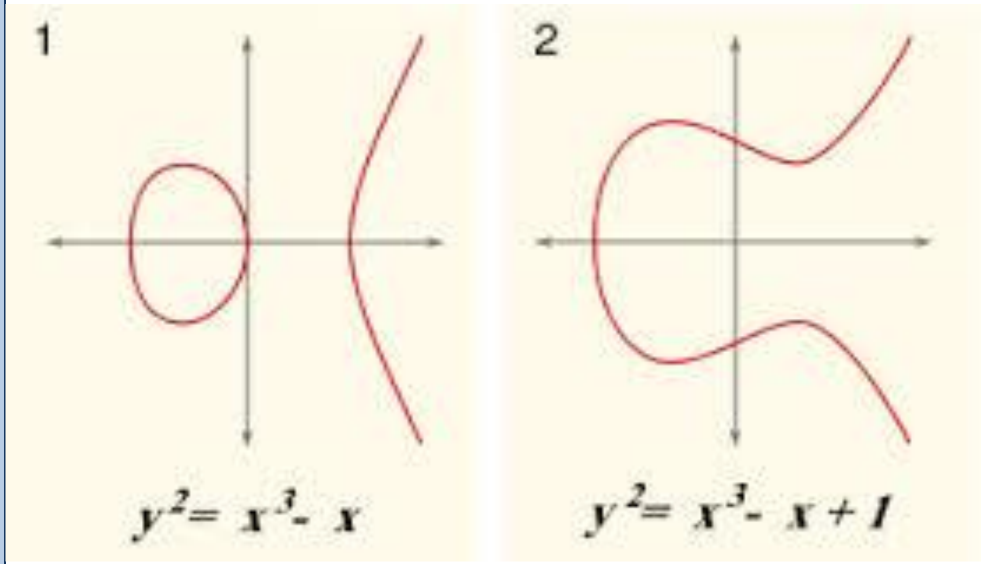
Rovnice:

$$y^2 = x^3 + Ax + B$$

vyjadřuje pro různé parametry A, B eliptickou křivku.

Příklad 1: A = -1, B = 0

Příklad: A = -1, B = 1



Algebraické křivky byly studovány již před 150 lety.

Eliptická křivka

- Křivka, která splňuje vlastnosti grupy.
- Zákony pro tyto grupy jsou geometrické.
- Eliptické křivky nemaji nic společného s elipsou nebo jinými kuželosečkami.
- Eliptické křivky mají aplikace v různých oblastech matematiky a informatiky:

  od teorii čísel ke komplexní analýze, od kryptografie k matematické fyzice.

Taniyamova domněnka

Každá eliptická křivka nad Q je modulární.

- Poprvé zformulována v roce 1955.
- Dokázal ji Andrew Wiles v roce 1993.

Poincarého věta (kolem roku 1900)

- Nechť K je těleso.

- Předpokládejme,

  že eliptická křivka E je dána rovnicí $y^2 = x^3 + Ax + B$, kde A, B $\in$ K.
- Označme E(K) množinu bodů křivky E se souřadnicemi bodů z K takto

  $$E(K) = \{ (x,y) \in E: x, y \in K\} \cup \{O\}.$$
- Pak E(K) je podgrupou grupy všech bodů E.

Jak vypadají E(Q)?

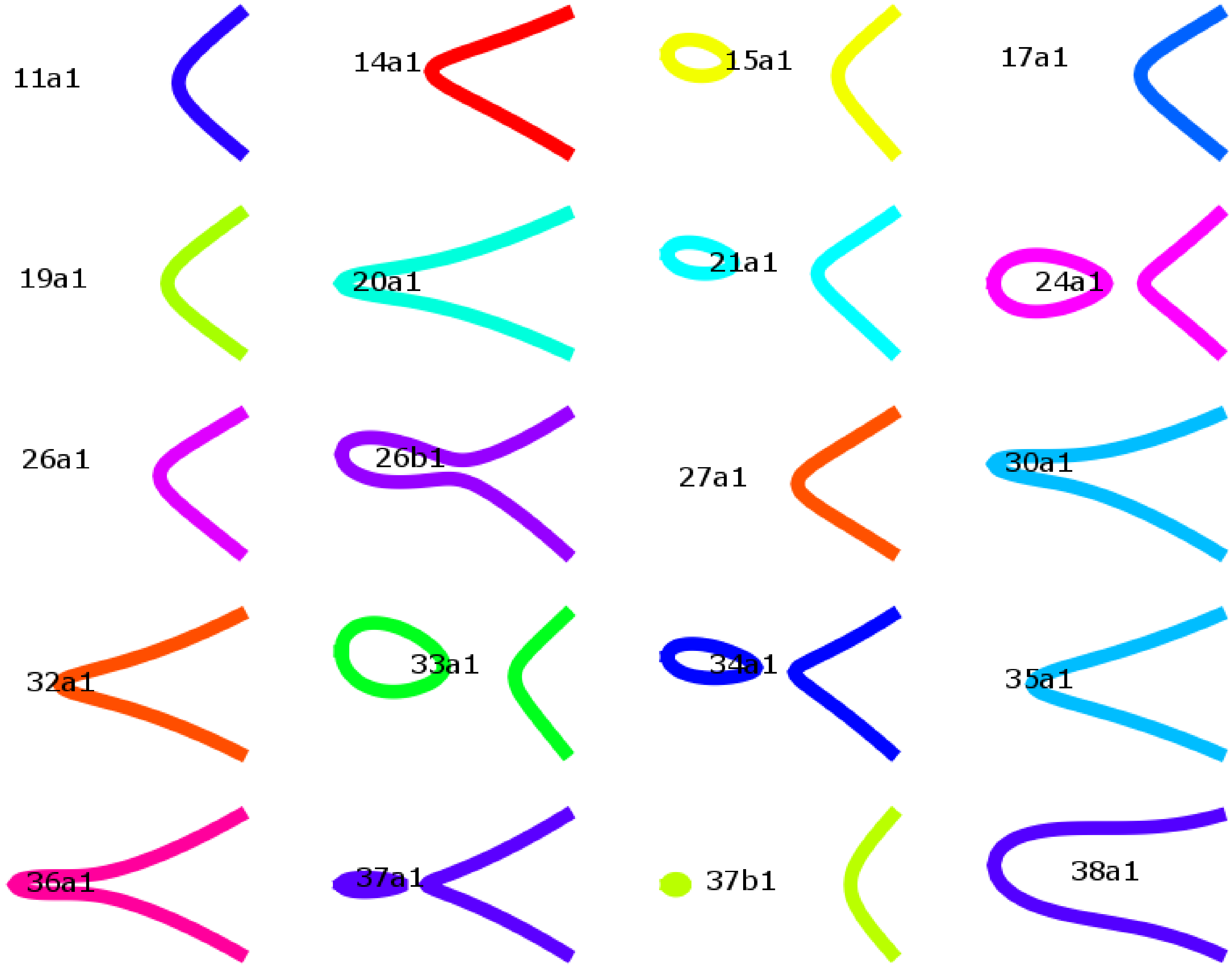
- Grupa racionálních bodů E(Q) je podgrupou reálných bodů E(R).
- Studium grupy E(Q) hraje důležitou roli v různých částech teorie čísel.
- Např. moderní teorie řešení diofantických rovnic s celočíselnými nebo racionálními koeficienty využívá výsledek L. J. Mordella z roku 1922, v němž znamenitě popsal E(Q).

Mordellova věta

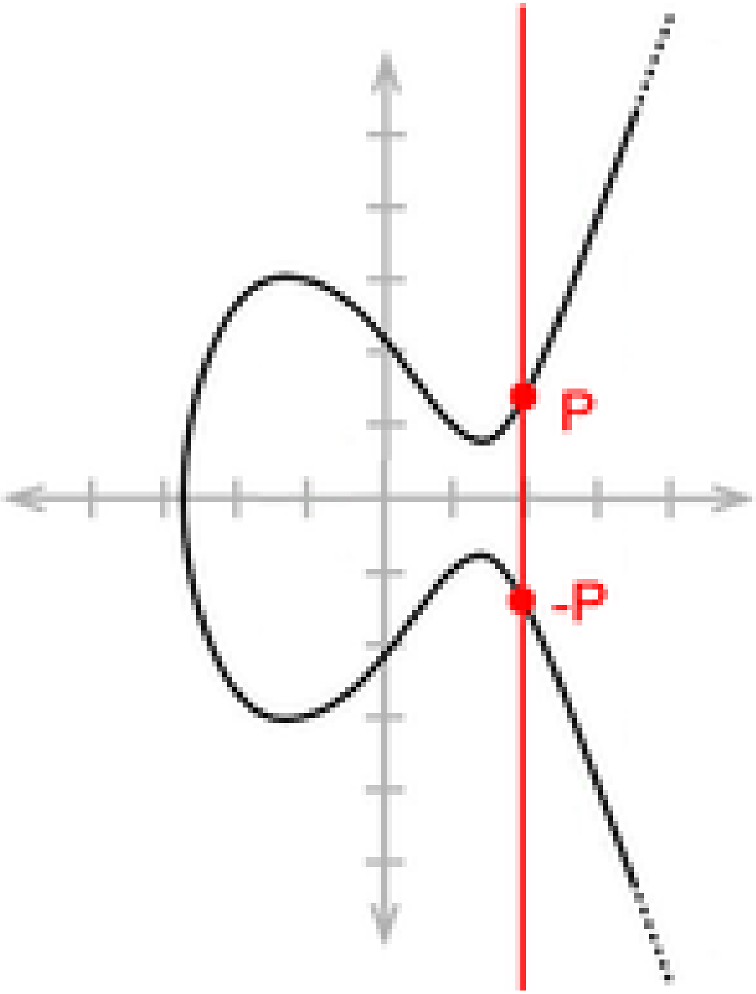
- Nechť E je eliptická křivka daná rovnicí

  $E: y^2 = x^3 + Ax + B$, kde A, B $\in$ Q.

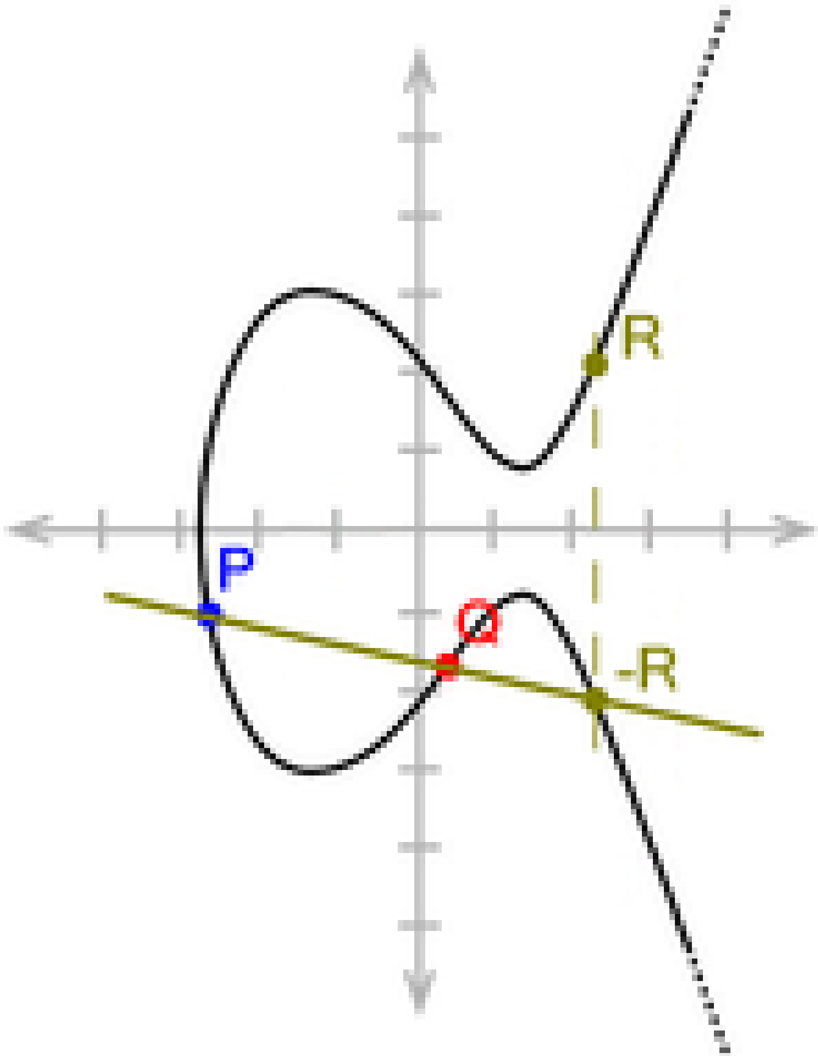
- Pak grupa racionálních bodů E(Q) je konečně generovaná Abelova grupa.
- Jinak řečeno:
- Jestli je $P_1, P_2, \ldots P_t \in E(Q)$, pak každý bod P z může být vyjádřen pomocí bodů konečné množiny bodů P_i takto:
- $P = n_1P_1 + n_2P_2 + \ldots + n_tP_t$, kde $n_1, n_2, \ldots, n_t \in Z$


11a1
14a1
15a1
17a1
19a1
20a1
21a1
24a1
26a1
26b1
27a1
30a1
32a1
33a1
34a1
35a1
36a1
37a1
37b1
38a1

Sčítání bodů na eliptických křivkách



Sčítání bodů na eliptických křivkách



Aritmetika eliptických křivek nad tělesem F_p

- Sčítání bodů na eliptické křivce nad tělesem F_p již nelze provádět graficky efektivně,

  používá se pouze algebraický postup.

- Algebraický postup se od sčítání na eliptické křivce nad reálnými čísly příliš neliší.
- Veškeré rovnice pouze budeme uvažovat nad tělesem F_p, tedy modulo p.

Literatura

Joseph H. Silvermann:

An Introduction to the Theory of Elliptic Curves,

Brown University, Wyoming 2006