

# NI-MPI přednáška 15

## Algebra IV

---

Štěpán Starosta

27. 11. 2024

FIT ČVUT

### 35. Množiny se dvěma binárními operacemi

- Okruh
- Těleso

### 36. Okruhy polynomů

- Definice a základní vlastnosti
- Ireducibilní polynom

### 37. Konečná tělesa

### 38. Aplikace konečných těles v kryptografii

- AES
- Eliptické křivky

# Množiny se dvěma binárními operacemi

- Doposud jsme se zabývali množinami vybavenými **jednou** binární operací:
  - grupoidy,
  - pologrupy,
  - monoidy,
  - (abelovské) grupy.

# Množiny se dvěma binárními operacemi

- Doposud jsme se zabývali množinami vybavenými **jednou** binární operací:
  - grupoidy,
  - pologrupy,
  - monoidy,
  - (abelovské) grupy.
- Například čísla, či matice, umíme vzájemně jak „sčítat“ tak „násobit“. Budeme proto dále uvažovat **dvě** binární operace. V následujících přednáškách se seznámíme s
  - **okruhy** a
  - **tělesy**.

## Definice 35.1 (Okruh (*Ring*))

Budte  $M$  neprázdná množina a  $+$  a  $\cdot$  binární operace na této množině. Řekneme, že trojice  $R = (M, +, \cdot)$  je **okruh**, pokud platí:

- $(M, +)$  je **abelovská grupa**,
- $(M, \cdot)$  je **monoid**,
- platí (levý a pravý) **distributivní zákon**:

$$(\forall a, b, c \in M)(a \cdot (b + c) = a \cdot b + a \cdot c \quad \wedge \quad (b + c) \cdot a = b \cdot a + c \cdot a).$$

- Dodržujeme standardní konvenci, že násobení má vyšší prioritu než sčítání. Tím si ušetříme práci se psaním některých závorek,  $a + b \cdot c$  chápeme jako  $a + (b \cdot c)$ . Tečku pro násobení navíc většinou ani nepíšeme, tj.  $a + (b \cdot c) = a + bc$ .
- Někteří autoři nevyžadují existenci neutrálního prvku v  $(M, \cdot)$ .

Bud'  $R = (M, +, \cdot)$  okruh.

- Je-li  $\cdot$  komutativní, je  $R$  **komutativní okruh**,
- $(M, +)$  se nazývá **aditivní grupa** okruhu  $R$ ,
- $(M, \cdot)$  se nazývá **multiplikativní monoid** okruhu  $R$ ,
- neutrální prvek grupy  $(M, +)$  se nazývá **nulový prvek** a značí se  $0$ , inverzní prvek vůči  $+$  k  $a \in M$  pak značíme  $-a$ ,
- v okruhu **můžeme definovat odečítání** předpisem

$$a - b := a + (-b),$$

- neutrálnímu prvku multiplikativního monoidu budeme zpravidla říkat **jednička** a značit jej  $1$ .

# Jednoduché příklady okruhů

- triviální okruh je  $(\{0\}, +, \cdot)$ ,

# Jednoduché příklady okruhů

- triviální okruh je  $(\{0\}, +, \cdot)$ ,
- $(\mathbb{Z}, +, \cdot)$  je okruh, (ale  $(\mathbb{N}, +, \cdot)$  není okruh, neb  $(\mathbb{N}, +)$  není grupa),



# Jednoduché příklady okruhů

- triviální okruh je  $(\{0\}, +, \cdot)$ ,
- $(\mathbb{Z}, +, \cdot)$  je okruh, (ale  $(\mathbb{N}, +, \cdot)$  není okruh, neb  $(\mathbb{N}, +)$  není grupa),
- množina  $(\mathbb{R}^{n,n}, +, \cdot)$  čtvercových reálných matic se sčítáním po prvcích a maticovým násobením je okruh, nulový prvek je nulová matice (podobně pro komplexní matice),

# Jednoduché příklady okruhů

- triviální okruh je  $(\{0\}, +, \cdot)$ ,
- $(\mathbb{Z}, +, \cdot)$  je okruh, (ale  $(\mathbb{N}, +, \cdot)$  není okruh, neb  $(\mathbb{N}, +)$  není grupa),
- množina  $(\mathbb{R}^{n,n}, +, \cdot)$  čtvercových reálných matic se sčítáním po prvcích a maticovým násobením je okruh, nulový prvek je nulová matice (podobně pro komplexní matice),
- množina všech polynomů (s komplexními / reálnými / celočíselnými koeficienty) je okruh, nulový prvek je nulový polynom, tj. polynom splňující  $p(x) = 0$  pro každé  $x$ ,

# Jednoduché příklady okruhů

- triviální okruh je  $(\{0\}, +, \cdot)$ ,
- $(\mathbb{Z}, +, \cdot)$  je okruh, (ale  $(\mathbb{N}, +, \cdot)$  není okruh, neb  $(\mathbb{N}, +)$  není grupa),
- množina  $(\mathbb{R}^{n,n}, +, \cdot)$  čtvercových reálných matic se sčítáním po prvcích a maticovým násobením je okruh, nulový prvek je nulová matice (podobně pro komplexní matice),
- množina všech polynomů (s komplexními / reálnými / celočíselnými koeficienty) je okruh, nulový prvek je nulový polynom, tj. polynom splňující  $p(x) = 0$  pro každé  $x$ ,
- množina všech zbytkových tříd  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  po dělení  $n \in \mathbb{N}$  se sčítáním a násobením modulo  $n$  je okruh.

# Základní vlastnosti okruhu

V libovolném okruhu  $(M, +, \cdot)$  platí:

- **Násobení nulovým prvkem dává opět nulový prvek, tj.**

$$(\forall a \in M)(a \cdot 0 = 0 \wedge 0 \cdot a = 0).$$

Vskutku:  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ .

# Základní vlastnosti okruhu

V libovolném okruhu  $(M, +, \cdot)$  platí:

- **Násobení nulovým prvkem dává opět nulový prvek, tj.**

$$(\forall a \in M)(a \cdot 0 = 0 \wedge 0 \cdot a = 0).$$

Vskutku:  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ .

- Z toho plyne, že  $(\forall a, b \in M)((-a) \cdot b = -a \cdot b)$ .

# Základní vlastnosti okruhu

V libovolném okruhu  $(M, +, \cdot)$  platí:

- **Násobení nulovým prvkem dává opět nulový prvek, tj.**

$$(\forall a \in M)(a \cdot 0 = 0 \wedge 0 \cdot a = 0).$$

Vskutku:  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ .

- Z toho plyne, že  $(\forall a, b \in M)((-a) \cdot b = -a \cdot b)$ .

- **Levý i pravý distributivní zákon pro odečítání, tj.  $\forall a, b, c \in M$**

$$c(b - a) = cb - ca.$$

Vskutku:  $ca + c(b - a) = c(a + b - a) = cb \implies c(b - a) = cb - ca$ .

# Základní vlastnosti okruhu

V libovolném okruhu  $(M, +, \cdot)$  platí:

- **Násobení nulovým prvkem dává opět nulový prvek, tj.**

$$(\forall a \in M)(a \cdot 0 = 0 \wedge 0 \cdot a = 0).$$

Vskutku:  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ .

- Z toho plyne, že  $(\forall a, b \in M)((-a) \cdot b = -a \cdot b)$ .

- **Levý i pravý distributivní zákon pro odečítání, tj.  $\forall a, b, c \in M$**

$$c(b - a) = cb - ca.$$

Vskutku:  $ca + c(b - a) = c(a + b - a) = cb \implies c(b - a) = cb - ca$ .

## Definice 35.2 (Obor integrity (*Integral domain*))

**Nenulové** prvky  $a, b \in M$  z okruhu  $(M, +, \cdot)$  nazýváme **dělitelé nuly**, právě když  $a \cdot b = b \cdot a = 0$ . **Obor integrity** je komutativní okruh, ve kterém neexistují dělitelé nuly.

## Definice 35.3 (těleso (*Field*))

Okruh  $T = (M, +, \cdot)$  se nazývá **těleso**, jestliže  $(M \setminus \{0\}, \cdot)$  je abelovská grupa. Tuto grupu nazýváme **multiplikační grupou** tělesa  $T$ .



## Definice 35.3 (těleso (*Field*))

Okruh  $T = (M, +, \cdot)$  se nazývá **těleso**, jestliže  $(M \setminus \{0\}, \cdot)$  je abelovská grupa. Tuto grupu nazýváme **multiplikativní grupou** tělesa  $T$ .

Jazyková vsuvka:

- V anglosaské literatuře narazíte na tento objekt pod názvem *field*, což by v češtině odpovídalo slovu „pole“. Pole (vektorové) má ale v české matematické terminologii již jiný význam.
- Česká terminologie se v tomto směru drží francouzské (*corps*) a německé (*Körper*). V obou případech je překladem „tělo“, či „těleso“.

## Definice 35.3 (těleso (*Field*))

Okruh  $T = (M, +, \cdot)$  se nazývá **těleso**, jestliže  $(M \setminus \{0\}, \cdot)$  je abelovská grupa. Tuto grupu nazýváme **multiplikativní grupou** tělesa  $T$ .

Jazyková vsuvka:

- V anglosaské literatuře narazíte na tento objekt pod názvem *field*, což by v češtině odpovídalo slovu „pole“. Pole (vektorové) má ale v české matematické terminologii již jiný význam.
- Česká terminologie se v tomto směru drží francouzské (*corps*) a německé (*Körper*). V obou případech je překladem „tělo“, či „těleso“.

Upozornění: pod pojmem těleso se někdy rozumí struktura, kde  $\cdot$  není komutativní.

## Proč musíme vyjmout nulový prvek v $(M \setminus \{0\}, \cdot)$ ?

1 je neutrální prvek  $M \setminus \{0\}$ , tedy v tělese vždy platí  $1 \neq 0$ .

Protože  $a \cdot 0 = 0 \cdot a = 0$ , nemůže k nule existovat inverzní prvek (vzhledem k násobení), tj. nelze dělit nulou.

## Proč musíme vyjmout nulový prvek v $(M \setminus \{0\}, \cdot)$ ?

1 je neutrální prvek  $M \setminus \{0\}$ , tedy v tělese vždy platí  $1 \neq 0$ .

Protože  $a \cdot 0 = 0 \cdot a = 0$ , nemůže k nule existovat inverzní prvek (vzhledem k násobení), tj. nelze dělit nulou.

**Všemi jinými prvky tělesa dělit umíme!**

dělení = násobení inverzním prvkem

$$\frac{a}{b} := a \cdot b^{-1} \quad \text{pro } b \neq 0.$$

Tato notace má dobrý smysl díky komutativitě operace  $\cdot$ .

- Okruh celých čísel  $(\mathbb{Z}, +, \cdot)$  není těleso, neb  $(\mathbb{Z} \setminus \{0\}, \cdot)$  není grupa (chybí inverzní prvky).

# Příklady těles

- Okruh celých čísel  $(\mathbb{Z}, +, \cdot)$  není těleso, neb  $(\mathbb{Z} \setminus \{0\}, \cdot)$  není grupa (chybí inverzní prvky).
- Okruh racionálních čísel  $(\mathbb{Q}, +, \cdot)$  je těleso. Dokonce nejmenší číselné těleso (s obvyklými aritmetickými operacemi).

# Příklady těles

- Okruh celých čísel  $(\mathbb{Z}, +, \cdot)$  není těleso, neb  $(\mathbb{Z} \setminus \{0\}, \cdot)$  není grupa (chybí inverzní prvky).
- Okruh racionálních čísel  $(\mathbb{Q}, +, \cdot)$  je těleso. Dokonce nejmenší číselné těleso (s obvyklými aritmetickými operacemi).
- Nejmenší těleso je tzv. **triviální těleso**  $(\{0, 1\}, +, \cdot)$  s operacemi danými násl. tabulkami:

+			0		1	
0			0		1	
1			1		0	

a

·			0		1	
0			0		0	
1			0		1	

První tabulka odpovídá bitové operaci XOR a druhá AND, nebo také sčítání a násobení modulo 2.

## Některé vlastnosti těles

V každém tělese máme definované aritmetické operace:

sčítání, odčítání, násobení, dělení a všechny z nich odvozené, jako mocnění, odmocňování, logaritmování, ...



## Některé vlastnosti těles

V každém tělese máme definované aritmetické operace:

sčítání, odčítání, násobení, dělení a všechny z nich odvozené, jako mocnění, odmocňování, logaritmování, ...

Triviální těleso nám tyto všechny operace definuje nad jedním bitem. Později si ukážeme, jak je rozšířit nad libovolný počet bitů.

## Některé vlastnosti těles

V každém tělese máme definované aritmetické operace:

sčítání, odčítání, násobení, dělení a všechny z nich odvozené, jako mocnění, odmocňování, logaritmování, ...

Triviální těleso nám tyto všechny operace definuje nad jedním bitem. Později si ukážeme, jak je rozšířit nad libovolný počet bitů.

### Věta 35.4

*Pokud pro  $a, b$  z tělesa  $T$  platí  $ab = 0$  potom  $a = 0$  nebo  $b = 0$ .*

## Některé vlastnosti těles

V každém tělese máme definované aritmetické operace:

sčítání, odčítání, násobení, dělení a všechny z nich odvozené, jako mocnění, odmocňování, logaritmování, ...

Triviální těleso nám tyto všechny operace definuje nad jedním bitem. Později si ukážeme, jak je rozšířit nad libovolný počet bitů.

### Věta 35.4

*Pokud pro  $a, b$  z tělesa  $T$  platí  $ab = 0$  potom  $a = 0$  nebo  $b = 0$ .*

### Důkaz.

Sporem: kdyby  $a \neq 0$  a  $b \neq 0$  potom  $ab \neq 0$ , protože multiplikativní grupa  $(T \setminus \{0\}, \cdot)$  je uzavřená na násobení. □

Každé těleso je tedy oborem integrity.

# Homomorfismus a izomorfismus okruhů a těles

Podobně jako u grup zavádíme homomorfismus a izomorfismus okruhů a těles.

## Definice 35.5

Zobrazení  $h$  z okruhu  $R$  do okruhu  $S$  je **homomorfismus** těchto okruhů, jestliže je  $h$  homomorfismem z aditivní grupy  $R$  do aditivní grupy  $S$ , homomorfismem<sup>1</sup> z multiplikativního monoidu  $R$  do multiplikativního monoidu  $S$  a platí  $h(1_R) = 1_S$ .

Zobrazení  $h$  z tělesa  $R$  do tělesa  $S$  je **homomorfismus** těchto těles, jestliže je  $h$  homomorfismem z aditivní grupy  $R$  do aditivní grupy  $S$  a homomorfismem z multiplikativní grupy  $R$  do multiplikativní grupy  $S$ .

Je-li navíc  $h$  bijekce (prosté a „na“), jedná se o **izomorfismus** těchto okruhů (resp. těles).

---

<sup>1</sup>použijeme definici pro grupoid

## Definice 35.6

Tělesa  $T$  a  $K$  nazýváme **izomorfní**, právě když existuje izomorfismus z  $T$  na  $K$ . V tomto případě také říkáme, že těleso  $T$  **je izomorfní s** tělesem  $K$ .

## Definice 35.6

Tělesa  $T$  a  $K$  nazýváme **izomorfní**, právě když existuje izomorfismus z  $T$  na  $K$ . V tomto případě také říkáme, že těleso  $T$  **je izomorfní s** tělesem  $K$ .

Relace „být izomorfní“ na třídě všech těles je relace ekvivalence.

### 35. Množiny se dvěma binárními operacemi

- Okruh
- Těleso

### 36. Okruhy polynomů

- Definice a základní vlastnosti
- Ireducibilní polynom

### 37. Konečná tělesa

### 38. Aplikace konečných těles v kryptografii

- AES
- Eliptické křivky

# Polynom nad okruhem

## Definice 36.1 (Polynom nad okruhem)

Mějme okruh  $R$  a  $a_i \in R$ ,  $i = 0, 1, \dots, n$ . Formální výraz tvaru

$$P(x) = \sum_{i=0}^n a_i x^i$$

nazýváme **polynomem nad okruhem  $R$**  (s formální proměnnou  $x$ ).



# Polynom nad okruhem

## Definice 36.1 (Polynom nad okruhem)

Mějme okruh  $R$  a  $a_i \in R$ ,  $i = 0, 1, \dots, n$ . Formální výraz tvaru

$$P(x) = \sum_{i=0}^n a_i x^i$$

nazýváme **polynomem nad okruhem  $R$  (s formální proměnnou  $x$ )**.

Používáme standardní názvosloví:

- $a_i$ ,  $i = 0, 1, \dots, n$ , nazýváme **koeficienty** polynomu  $P(x)$ .
- $x$  nazýváme **formální proměnnou** polynomu  $P(x)$ .
- Dva polynomy se rovnají, pokud se rovnají jejich příslušné koeficienty.
- Členy s nulovým koeficientem se často vynechávají, tedy např.  $1 + 0x = 1$ .
- Pokud pro polynom  $P(x)$  existuje  $k \in \{0, 1, \dots, n\}$  takové, že  $a_k \neq 0$ , pak největší z těchto  $k$  nazýváme **stupněm polynomu  $P(x)$** , značený  $\deg(P(x))$ .
- Polynom  $P(x) = 0$  nazýváme **nulový polynom** a jeho stupeň nedefinujeme.

# Okruh polynomů nad okruhem

Abychom mohli sčítat, odčítat a násobit polynomy, potřebujeme pouze vědět jak sčítat, odčítat a násobit jejich koeficienty. Obecně tedy můžeme vybudovat okruh polynomů podobný tomu, který známe z reálných resp. komplexních čísel, nad libovolným okruhem (a tedy i tělesem).

## Věta 36.2 (Okruh polynomů (*polynomial ring*))

*Bud'  $R$  okruh. Potom množina všech polynomů nad okruhem  $R$  spolu s operacemi sčítání a násobení definovanými předpisy*

$$\sum_{i=0}^n a_i x^i + \sum_{i=0}^n b_i x^i := \sum_{i=0}^n (a_i + b_i) x^i$$
$$\left( \sum_{j=0}^n a_j x^j \right) \cdot \left( \sum_{k=0}^m b_k x^k \right) := \sum_{i=0}^{n+m} \left( \sum_{j+k=i} a_j b_k \right) x^i,$$

*kde  $a_i, b_i \in R$  pro všechny hodnoty  $i$ , tvoří **okruh polynomů nad okruhem  $R$** . Tento okruh značíme  $R[x]$ .*

### **Lemma 36.3 (o násobení polynomů)**

*Bud'  $T$  těleso a  $f(x), g(x) \in T[x]$  nenulové polynomy. Platí*

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

### Lemma 36.4 (o dělení polynomů)

*Bud'  $T$  těleso a  $f(x), g(x) \in T[x]$  nenulové polynomy. Pak existují jednoznačně určené polynomy  $q(x), r(x) \in T[x]$  takové, že*

$$f(x) = q(x)g(x) + r(x),$$

*kde  $r(x)$  je buď nulový nebo má stupeň ostře menší než stupeň  $g(x)$ .*

## Základní vlastnosti (3 ze 4)

Budte  $f(x), g(x) \in T[x]$ . Potom polynom  $h(x) \in T[x]$  nazveme **největší společný dělitel polynomů  $f(x)$  a  $g(x)$** , jestliže

- $h(x)$  dělí  $f(x)$  (tj. existuje  $q(x) \in T[x]$ , tak. že  $f(x) = q(x)h(x)$ ),
- $h(x)$  dělí  $g(x)$ ,
- každý polynom, který dělí  $f(x)$  i  $g(x)$ , dělí také  $h(x)$ .

Tento polynom značíme  $\gcd(f(x), g(x))$  (jedná se o drobné zneužití značení, protože polynom je jednoznačný až na multiplikační konstantu).

## Základní vlastnosti (3 ze 4)

Buďte  $f(x), g(x) \in T[x]$ . Potom polynom  $h(x) \in T[x]$  nazveme **největší společný dělitel polynomů  $f(x)$  a  $g(x)$** , jestliže

- $h(x)$  dělí  $f(x)$  (tj. existuje  $q(x) \in T[x]$ , tak. že  $f(x) = q(x)h(x)$ ),
- $h(x)$  dělí  $g(x)$ ,
- každý polynom, který dělí  $f(x)$  i  $g(x)$ , dělí také  $h(x)$ .

Tento polynom značíme  $\gcd(f(x), g(x))$  (jedná se o drobné zneužití značení, protože polynom je jednoznačný až na multiplikační konstantu).

### Věta 36.5 (Bézoutova rovnost pro polynomy)

*Buďte  $f(x)$  a  $g(x)$  nenulové polynomy nad tělesem  $T$ . Pak existují polynomy  $u(x), v(x) \in T[x]$  tak, že  $\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x)$ .*

### Důkaz.

Důkaz se provádí indukcí na součet stupňů polynomů  $f(x)$  a  $g(x)$  a je uveden v handoutu. □

### Věta 36.6 (*Polynomial factor theorem*)

*Bud'  $T$  těleso a  $p(x) \in T[x]$  polynom stupně  $n$ . Prvek  $\xi \in T$  je kořen polynomu  $p$  právě tehdy, když  $p(x) = (x - \xi)g(x)$ , kde  $g(x) \in T[x]$  je stupně  $n - 1$ .*

Důkaz v handoutu.

## Definice 36.7

Bud'  $P(x) \in K[x]$  stupně alespoň 1. Řekneme, že  $P(x)$  je **ireducibilní nad okruhem  $K$** , jestliže pro každé dva polynomy  $A(x)$  a  $B(x)$  z  $K[x]$  platí

$$A(x) \cdot B(x) = P(x) \implies (\deg(A(x)) = 0 \text{ NEBO } \deg(B(x)) = 0).$$



## Definice 36.7

Bud'  $P(x) \in K[x]$  stupně alespoň 1. Řekneme, že  $P(x)$  je **ireducibilní nad okruhem  $K$** , jestliže pro každé dva polynomy  $A(x)$  a  $B(x)$  z  $K[x]$  platí

$$A(x) \cdot B(x) = P(x) \implies (\deg(A(x)) = 0 \text{ NEBO } \deg(B(x)) = 0).$$

Ireducibilní polynomy jsou definovány analogicky jako jsou prvočísla v množině přirozených celých čísel.

# Ireducibilní polynomy: co o nich víme (1 z 2)

## Věta 36.8

Mějme celé  $n > 1$  a prvočíslo  $p$ . Označme  $N(p, n)$  počet monických polynomů stupně  $n$  ireducibilních nad  $\mathbb{Z}_p$ . Potom

$$N(p, n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} \geq \frac{1}{n} \left( p^n - \sum_{q|n, q \text{ prvoč.}} p^{\frac{n}{q}} \right).$$

## Ireducibilní polynomy: co o nich víme (1 z 2)

### Věta 36.8

Mějme celé  $n > 1$  a prvočíslo  $p$ . Označme  $N(p, n)$  počet monických polynomů stupně  $n$  ireducibilních nad  $\mathbb{Z}_p$ . Potom

$$N(p, n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} \geq \frac{1}{n} \left( p^n - \sum_{q|n, q \text{ prvoč.}} p^{\frac{n}{q}} \right).$$

Kde  $\mu$  je Möbiova funkce definovaná pro celé  $n > 0$  takto:

$$\mu(n) = \begin{cases} 1 & \text{pokud } n \text{ neobsahuje čtverec prvočísla a má sudý počet prvoč. faktorů,} \\ -1 & \text{pokud } n \text{ neobsahuje čtverec prvočísla a má lichý počet prvoč. faktorů,} \\ 0 & \text{pokud } n \text{ obsahuje čtverec prvočísla.} \end{cases}$$

a **monický** polynom je takový polynom, který má za koeficient u nejvyšší mocniny jedničku.

## Ireducibilní polynomy: co o nich víme (2 z 2)

---

**Otázka:** Jak najít ireducibilní polynom?

## Ireducibilní polynomy: co o nich víme (2 z 2)

**Otázka:** Jak najít ireducibilní polynom?

Poznat, jestli je daný polynom ireducibilní je snazší, než poznat jestli dané číslo je prvočíslo:

Dokonce existují polynomiální algoritmy, které nejen rozhodnou o ireducibilitě, ale dokonce najdou rozklad na ireducibilní polynomy (obdoba prvočíselného rozkladu).

## Ireducibilní polynomy: co o nich víme (2 z 2)

**Otázka:** Jak najít ireducibilní polynom?

Poznat, jestli je daný polynom ireducibilní je snazší, než poznat jestli dané číslo je prvočíslo:

Dokonce existují polynomiální algoritmy, které nejen rozhodnou o ireducibilitě, ale dokonce najdou rozklad na ireducibilní polynomy (obdoba prvočíselného rozkladu).

Jedná se o Berlekampův a Cantor–Zassenhausův algoritmus: detaily např. v D. Knuth, *The Art of Computer Programming*, Vol. 2, sekce 4.6.

### 35. Množiny se dvěma binárními operacemi

- Okruh
- Těleso

### 36. Okruhy polynomů

- Definice a základní vlastnosti
- Ireducibilní polynom

### 37. Konečná tělesa

### 38. Aplikace konečných těles v kryptografii

- AES
- Eliptické křivky

# Konečná tělesa

## Definice 37.1 (konečné těleso (*finite field*))

Těleso, které má konečný počet prvků, se nazývá **konečné**.

**Řádem** tělesa se, podobně jako u grup, označuje počet prvků tělesa. Tedy konečná tělesa jsou tělesa konečného řádu.



# Konečná tělesa

## Definice 37.1 (konečné těleso (*finite field*))

Těleso, které má konečný počet prvků, se nazývá **konečné**.

**Řádem** tělesa se, podobně jako u grup, označuje počet prvků tělesa. Tedy konečná tělesa jsou tělesa konečného řádu.

Základní příklad konečného tělesa je množina (zbytkových tříd modulo  $p$ )  $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$  s operacemi modulo **prvočíslo**  $p$  (viz minulé přednášky).

Např. pro  $p = 5$  dostáváme těleso s násl. operacemi

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

a

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

## O tělese $(\mathbb{Z}_p, +, \cdot)$

Aditivní grupa je  $\mathbb{Z}_p^+$ :

- Má řád  $p$ .

Multiplikativní grupa je  $\mathbb{Z}_p^\times$ :

- Má řád  $p - 1$  a to není jakožto sudé číslo prvočíslo (s výjimkou  $p = 3$ )!

## O tělese $(\mathbb{Z}_p, +, \cdot)$

Aditivní grupa je  $\mathbb{Z}_p^+$ :

- Má **řád**  $p$ .
- Každý nenulový prvek je její **generátor** a má tedy řád  $p$  (to platí pro všechny grupy s prvočíselným řádem).

Multiplikativní grupa je  $\mathbb{Z}_p^\times$ :

- Má **řád**  $p - 1$  a to není jakožto sudé číslo prvočíslo (s výjimkou  $p = 3$ )!
- $\mathbb{Z}_p^\times$  je cyklická (tj. existuje v ní generátor).
- Počet **generátorů** závisí na jejím řádu  $p - 1$ , a je roven počtu čísel nesoudělných s  $p - 1$ , tedy  $\varphi(p - 1)$ .

## O tělese $(\mathbb{Z}_p, +, \cdot)$

Aditivní grupa je  $\mathbb{Z}_p^+$ :

- Má **řád**  $p$ .
- Každý nenulový prvek je její **generátor** a má tedy řád  $p$  (to platí pro všechny grupy s prvočíselným řádem).
- $(\mathbb{Z}_p, +)$  je grupou **i pro**  $p$ , které není prvočíslo.

Multiplikativní grupa je  $\mathbb{Z}_p^\times$ :

- Má **řád**  $p - 1$  a to není jakožto sudé číslo prvočíslo (s výjimkou  $p = 3$ )!
- $\mathbb{Z}_p^\times$  je cyklická (tj. existuje v ní generátor).
- Počet **generátorů** závisí na jejím řádu  $p - 1$ , a je roven počtu čísel nesoudělných s  $p - 1$ , tedy  $\varphi(p - 1)$ .
- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$  je grupou **pouze pro** prvočíselné  $p$ , jinak obsahuje dělitele nuly.)

## O tělese $(\mathbb{Z}_p, +, \cdot)$

Aditivní grupa je  $\mathbb{Z}_p^+$ :

- Má **řád**  $p$ .
- Každý nenulový prvek je její **generátor** a má tedy řád  $p$  (to platí pro všechny grupy s prvočíselným řádem).
- $(\mathbb{Z}_p, +)$  je grupou **i pro**  $p$ , které není prvočíslo.

Multiplikativní grupa je  $\mathbb{Z}_p^\times$ :

- Má **řád**  $p - 1$  a to není jakožto sudé číslo prvočíslo (s výjimkou  $p = 3$ )!
- $\mathbb{Z}_p^\times$  je cyklická (tj. existuje v ní generátor).
- Počet **generátorů** závisí na jejím řádu  $p - 1$ , a je roven počtu čísel nesoudělných s  $p - 1$ , tedy  $\varphi(p - 1)$ .
- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$  je grupou **pouze pro** prvočíselné  $p$ , jinak obsahuje dělitele nuly.)
- Nechť  $k < p$  dělí  $p - 1$ , pak v  $\mathbb{Z}_p^\times$  existuje podgrupa řádu  $k$  a obsahuje právě ty prvky  $a \in \mathbb{Z}_p$ , pro které  $a^k = 1$ .

## Existují další konečná tělesa?

- V předchozí části přednášky jsme pro každé prvočíslo  $p$  našli konečné těleso mající  $p$  prvků,  $(\mathbb{Z}_p, +_p, \times_p)$ .
- Přirozeně se nabízí **otázka**: existují i tělesa s jiným počtem prvků než prvočíselným?

## Existují další konečná tělesa?

- V předchozí části přednášky jsme pro každé prvočíslo  $p$  našli konečné těleso mající  $p$  prvků,  $(\mathbb{Z}_p, +_p, \times_p)$ .
- Přirozeně se nabízí otázka: existují i tělesa s jiným počtem prvků než prvočíselným?
- Například na těleso  $(\mathbb{Z}_2, +_2, \times_2)$  se můžeme dívat jako na model jednoho bitu. Co kdybychom chtěli pracovat se několikabitovým slovem jako s prvkem tělesa (toho se opět využívá v kryptologii, viz další část přednášky).
- Přirozeně by člověka napadlo, například, na  $\mathbb{Z}_2^8$  zavést operace po složkách modulo 2. Tj.

$$(a_1, \dots, a_8) + (b_1, \dots, b_8) := (a_1 +_2 b_1, \dots, a_8 +_2 b_8),$$

$$(a_1, \dots, a_8) \cdot (b_1, \dots, b_8) := (a_1 \times_2 b_1, \dots, a_8 \times_2 b_8).$$

Tato struktura ovšem tvoří **pouze** komutativní okruh. Není to ani obor integrity. (Rozmyslete!)

## Existují další konečná tělesa? Ano!

---

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .



## Existují další konečná tělesa? Ano!

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .

1. Uvažme těleso  $T$  mající  $p$  prvků (ta již umíme konstruovat).

## Existují další konečná tělesa? Ano!

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .

1. Uvažme těleso  $T$  mající  $p$  prvků (ta již umíme konstruovat).
2. Sestrojme okruh  $T[x]$  všech polynomů nad tělesem  $T$  (ten má nekonečně mnoho prvků).

## Existují další konečná tělesa? Ano!

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .

1. Uvažme těleso  $T$  mající  $p$  prvků (ta již umíme konstruovat).
2. Sestrojme okruh  $T[x]$  všech polynomů nad tělesem  $T$  (ten má nekonečně mnoho prvků).
3. Pro zadané kladné celé  $n$  nalezněme polynom  $P(x) \in T[x]$  ireducibilní nad  $T$  mající stupeň  $n$ .

## Existují další konečná tělesa? Ano!

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .

1. Uvažme těleso  $T$  mající  $p$  prvků (ta již umíme konstruovat).
2. Sestrojme okruh  $T[x]$  všech polynomů nad tělesem  $T$  (ten má nekonečně mnoho prvků).
3. Pro zadané kladné celé  $n$  nalezněme polynom  $P(x) \in T[x]$  ireducibilní nad  $T$  mající stupeň  $n$ .
4. Uvažme množinu  $F$  všech polynomů z  $T[x]$  stupně menšího nebo rovno  $n - 1$ , včetně nulového polynomu, (těch je  $p^n$ ) a zaveďme na této množině operace:

sčítání: stejně jako v  $T[x]$ ;

násobení:  $R(x) \cdot S(x) := (R(x) \cdot_{T[x]} S(x)) \bmod P(x)$ .

## Existují další konečná tělesa? Ano!

Následující konstrukce nám již dá těleso neprvočíselného řádu. Mějme zadáno prvočíslo  $p$  a celé  $n \geq 2$ .

1. Uvažme těleso  $T$  mající  $p$  prvků (ta již umíme konstruovat).
2. Sestrojme okruh  $T[x]$  všech polynomů nad tělesem  $T$  (ten má nekonečně mnoho prvků).
3. Pro zadané kladné celé  $n$  nalezněme polynom  $P(x) \in T[x]$  ireducibilní nad  $T$  mající stupeň  $n$ .
4. Uvažme množinu  $F$  všech polynomů z  $T[x]$  stupně menšího nebo rovno  $n - 1$ , včetně nulového polynomu, (těch je  $p^n$ ) a zaveďme na této množině operace:

sčítání: stejně jako v  $T[x]$ ;

násobení:  $R(x) \cdot S(x) := (R(x) \cdot_{T[x]} S(x)) \bmod P(x)$ .

$F$  s takto zavedenými operacemi tvoří těleso mající  $p^n$  prvků.

## Příklad (1 z 2)

### Příklad 37.2

Výše uvedenou konstrukci demonstrujeme na  $p = 2$ ,  $T = (\mathbb{Z}_2, +_2, \times_2)$ ,  $n = 4$  a

$$P(x) = x^4 + x + 1.$$

Pro zjednodušení zápisu ztotožňeme polynomy s řetězci, tj.

$$\sum_{i=0}^3 a_i x^i \longleftrightarrow a_3 a_2 a_1 a_0$$

pro  $a_i \in T = \mathbb{Z}_2$ ,  $i = 0, 1, 2, 3$ .

**Sečtěte** 1011 a 0111:

$$1011 + 0111 = 1100.$$

Skutečně pouze sečteme koeficienty polynomů u stejných mocnin modulo 2, protože tyto koeficienty žijí v  $T$ .

## Příklad (2 z 2)

---

Vynásobte 1101 a 0110:

## Příklad (2 z 2)

**Vynásobte** 1101 a 0110:

Součinem polynomů  $R(x) = x^3 + x^2 + 1$  a  $S(x) = x^2 + x$  v  $T[x]$  je polynom

$$Q(x) := R(x) \cdot S(x) = x^5 + x^3 + x^2 + x.$$



## Příklad (2 z 2)

**Vynásobte** 1101 a 0110:

Součinem polynomů  $R(x) = x^3 + x^2 + 1$  a  $S(x) = x^2 + x$  v  $T[x]$  je polynom

$$Q(x) := R(x) \cdot S(x) = x^5 + x^3 + x^2 + x.$$

Pomocí známého algoritmu dělení polynomu  $Q(x)$  polynomem  $P(x)$  získáme vztah

$$Q(x) = x \cdot P(x) + x^3.$$

Tudíž zbytkem po dělení polynomu  $Q(x)$  polynomem  $P(x)$  je polynom  $x^3$ . To je výsledek operace násobení, uzavíráme

$$1101 \cdot 0110 = 1000.$$

## Příklad (2 z 2)

**Vynásobte** 1101 a 0110:

Součinem polynomů  $R(x) = x^3 + x^2 + 1$  a  $S(x) = x^2 + x$  v  $T[x]$  je polynom

$$Q(x) := R(x) \cdot S(x) = x^5 + x^3 + x^2 + x.$$

Pomocí známého algoritmu dělení polynomu  $Q(x)$  polynomem  $P(x)$  získáme vztah

$$Q(x) = x \cdot P(x) + x^3.$$

Tudíž zbytkem po dělení polynomu  $Q(x)$  polynomem  $P(x)$  je polynom  $x^3$ . To je výsledek operace násobení, uzavíráme

$$1101 \cdot 0110 = 1000.$$

**Znovu zdůrazňujeme:** nejde o násobení modulo 2 (AND) po složkách, to by nám dalo  $1101 \cdot 0110 = 0100$ . S touto operací ale **nedostaneme** těleso, viz předchozí poznámky.

## Tělesa kterých řádů existují?

---

Zatím jsme si ukázali konstrukci konečných těles řádu  $p = p^1$  a  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo. Existují tělesa libovolného řádu?

## Tělesa kterých řádů existují?

Zatím jsme si ukázali konstrukci konečných těles řádu  $p = p^1$  a  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo. Existují tělesa libovolného řádu?

### Věta 37.3

*Řádem konečného tělesa musí být mocnina prvočísla, tedy číslo zapsatelné jako  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo.*

*Navíc platí, že všechna tělesa řádu  $p^n$  jsou **navzájem izomorfní**.*

## Tělesa kterých řádů existují?

Zatím jsme si ukázali konstrukci konečných těles řádu  $p = p^1$  a  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo. Existují tělesa libovolného řádu?

### Věta 37.3

*Řádem konečného tělesa musí být mocnina prvočísla, tedy číslo zapsatelné jako  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo.*

*Navíc platí, že všechna tělesa řádu  $p^n$  jsou **navzájem izomorfní**.*

**Důsledek:** neexistuje těleso s 6, 10, 12, 14, ... prvky.

## Tělesa kterých řádů existují?

Zatím jsme si ukázali konstrukci konečných těles řádu  $p = p^1$  a  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo. Existují tělesa libovolného řádu?

### Věta 37.3

*Řádem konečného tělesa musí být mocnina prvočísla, tedy číslo zapsatelné jako  $p^n$ , kde  $p$  je prvočíslo a  $n$  je kladné celé číslo.*

*Navíc platí, že všechna tělesa řádu  $p^n$  jsou **navzájem izomorfní**.*

**Důsledek:** neexistuje těleso s 6, 10, 12, 14, ... prvky.

### Definice 37.4

Těleso s  $p^n$  prvky nazýváme *konečné těleso* nebo též *Galoisovo těleso* (*Galois field*) a značíme ho  $GF(p^n)$ . Prvočíslo  $p$  se nazývá **charakteristikou** tělesa  $GF(p^n)$ .

## $GF(p^n)$ : aditivní grupa

Co víme o aditivní grupě tělesa  $GF(p^n)$ :

## $GF(p^n)$ : aditivní grupa

Co víme o aditivní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n$ .



## $GF(p^n)$ : aditivní grupa

Co víme o aditivní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n$ .
- Neutrální prvek je  $0 = 00 \cdots 0 = 0^n$ .

## $GF(p^n)$ : aditivní grupa

Co víme o aditivní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n$ .
- Neutrální prvek je  $0 = 00 \cdots 0 = 0^n$ .
- Inverze k prvku  $b_1 b_2 \cdots b_n$  je  $(p - b_1)(p - b_2) \cdots (p - b_n)$ .

## $GF(p^n)$ : aditivní grupa

Co víme o aditivní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n$ .
- Neutrální prvek je  $0 = 00 \cdots 0 = 0^n$ .
- Inverze k prvku  $b_1 b_2 \cdots b_n$  je  $(p - b_1)(p - b_2) \cdots (p - b_n)$ .
- Pro  $n > 1$  není cyklická, dokonce pro každý prvek  $v$  platí, že  $(p + 1) \times v = v$ , resp.  $p \times v = 0$ .

## $GF(p^n)$ : multiplikativní grupa

---

Co víme o multiplikativní grupě tělesa  $GF(p^n)$ :

## $GF(p^n)$ : multiplikativní grupa

---

Co víme o multiplikativní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n - 1$ .

## $GF(p^n)$ : multiplikativní grupa

---

Co víme o multiplikativní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n - 1$ .
- Neutrální prvek je  $00 \cdots 1 = 0^{n-1}1$ .

## $GF(p^n)$ : multiplikatívni grupa

Co víme o multiplikatívni grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n - 1$ .
- Neutrální prvek je  $00 \cdots 1 = 0^{n-1}1$ .
- Inverzi ke každému prvku umíme nalézt pomocí EEA v polynomiálním čase.

## $GF(p^n)$ : multiplikativní grupa

Co víme o multiplikativní grupě tělesa  $GF(p^n)$ :

- Má řád  $p^n - 1$ .
- Neutrální prvek je  $00 \cdots 1 = 0^{n-1}1$ .
- Inverzi ke každému prvku umíme nalézt pomocí EEA v polynomiálním čase.
- Je vždy cyklická (důkaz není moc složitý, ale zabral by nám moc času).



### 35. Množiny se dvěma binárními operacemi

- Okruh
- Těleso

### 36. Okruhy polynomů

- Definice a základní vlastnosti
- Ireducibilní polynom

### 37. Konečná tělesa

### 38. Aplikace konečných těles v kryptografii

- AES
- Eliptické křivky

- Při šifrované výměně delšího textu, jsou asymetrické šifry (RSA, Diffie-Hellman a spol.) neefektivní.

- Při šifrované výměně delšího textu, jsou asymetrické šifry (RSA, Diffie-Hellman a spol.) neefektivní.
- Proto se používá **symetrické šifrování**, kde se předpokládá, že Alice a Bob znají nějaký společný soukromý klíč, který nikdo jiný nezná a který šifrování výrazně usnadní. Asymetrické šifry se použijí pouze k výměně (resp. vytvoření) tohoto společného soukromého klíče.

- Při šifrované výměně delšího textu, jsou asymetrické šifry (RSA, Diffie-Hellman a spol.) neefektivní.
- Proto se používá **symetrické šifrování**, kde se předpokládá, že Alice a Bob znají nějaký společný soukromý klíč, který nikdo jiný nezná a který šifrování výrazně usnadní. Asymetrické šifry se použijí pouze k výměně (resp. vytvoření) tohoto společného soukromého klíče.
- Velmi používaná metoda je bloková šifra (*block cipher*) zvaná *Advanced Encryption Standard* (AES). Zde se seznámíme s matematickým podhoubím této metody.

- Kódovaný text si rozdělíme na bloky o (např.) 8 bitech. Ty zašifrujeme pomocí klíče tak, že dešifrování lze snadno provést pouze se znalostí toho samého klíče.

- Kódovaný text si rozdělíme na bloky o (např.) 8 bitech. Ty zašifrujeme pomocí klíče tak, že dešifrování lze snadno provést pouze se znalostí toho samého klíče.
- Toto šifrování v AES je založeno na tom, že operace s  $n = 8$  bity lze chápat jako aritmetické operace v konečném tělese s  $2^n$  prvky pro  $n = 8$ . Tělesa s  $2^n$  prvky zveme binární tělesa a značíme  $GF(2^n)$ .

- Kódovaný text si rozdělíme na bloky o (např.) 8 bitech. Ty zašifrujeme pomocí klíče tak, že dešifrování lze snadno provést pouze se znalostí toho samého klíče.
- Toto šifrování v AES je založeno na tom, že operace s  $n = 8$  bity lze chápat jako aritmetické operace v konečném tělese s  $2^n$  prvky pro  $n = 8$ . Tělesa s  $2^n$  prvky zveeme binární tělesa a značíme  $GF(2^n)$ .
- Dle specifikace AES se násobení počítá modulo

$$x^8 + x^4 + x^3 + x + 1.$$

K reprezentaci prvků se tedy používá 8 (= stupeň polynomu výše) bitů.

- Kódovaný text si rozdělíme na bloky o (např.) 8 bitech. Ty zašifrujeme pomocí klíče tak, že dešifrování lze snadno provést pouze se znalostí toho samého klíče.
- Toto šifrování v AES je založeno na tom, že operace s  $n = 8$  bity lze chápat jako aritmetické operace v konečném tělese s  $2^n$  prvky pro  $n = 8$ . Tělesa s  $2^n$  prvky zveeme binární tělesa a značíme  $GF(2^n)$ .
- Dle specifikace AES se násobení počítá modulo

$$x^8 + x^4 + x^3 + x + 1.$$

K reprezentaci prvků se tedy používá 8 (= stupeň polynomu výše) bitů.

- (Aritmetické operace v  $GF(2^n)$  nejsou jedinými operacemi s bloky v AES.)



- Pod **eliptickou křivkou** nad tělesem  $T$  rozumíme množinu všech bodů  $(x, y) \in T^2$  splňující zjednodušenou Weierstrassovu rovnici

$$y^2 = x^3 + ax + b,$$

případně Weierstrassovu rovnici

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

kde  $a, b \in T$  a  $a_i \in T$  jsou zadány.

- Za jistých předpokladů na koeficienty lze na množině všech bodů na eliptické křivce obohatené o jeden nový prvek zavést binární operaci vytvářející strukturu abelovské grupy.

# Počítání na eliptických křivkách

S body  $(x, y) \in T^2$  na eliptické křivce dané zjednodušenou Weierstrassovou rovnicí se počítá následovně (operace se tradičně, ovšem bez zvláštního důvodu, značí +):

## Definice 38.1

Pro dva body  $P = (x_1, y_1)$  a  $Q = (x_2, y_2)$ ,  $x_1 \neq x_2$ , definujeme  $P + Q = (x_3, y_3)$  takto:

$$x_3 = s^2 - x_1 - x_2$$

$$y_3 = s(x_1 - x_3) - y_1$$

kde

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{pokud } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{pokud } P = Q. \end{cases}$$

Parametr  $a$  je převzat z rovnice dané eliptické křivky. Neutrální prvek  $\mathcal{O}$  je „uměle“ přidán tak, aby měl vlastnosti neutrálního prvku.

Dále pro dva body  $P = (x_1, y_1)$  a  $Q = (x_1, y_2)$  klademe  $P + Q = \mathcal{O}$ .

# Eliptické křivky nad tělesem reálných čísel (1 ze 3)

Názorněji se dá vysvětlit počítání nad eliptickými křivkami, pokud bereme body  $(x, y)$  ze *souvislé* roviny  $\mathbb{R}^2$ .

## Definice 38.2

Eliptickou křivkou rozumíme množinu bodů splňující rovnici

$$y^2 = x^3 + ax + b,$$

kde pro reálné koeficienty  $a, b$  platí, že  $-16(4a^3 + 27b^2) \neq 0$ .

Grupovou operaci sčítání definovanou dříve pak lze interpretovat geometricky (pro názornou grafickou ukázkou viz [Wolfram Demonstrations Project](#)).

## Eliptické křivky nad tělesem reálných čísel (2 ze 3)

Mějme dva různé body  $P$  a  $Q$  na eliptické křivce  $E$  nad  $\mathbb{R}$ , potom pro jejich součet platí:

- Sestroj přímku  $p$  procházející body  $P$  a  $Q$ .
- Pokud přímka  $p$  má s  $E$  ještě jeden průsečík  $R = (x, y)$  různý od  $P$  a  $Q$ , pak  $P + Q = (x, -y)$ .
- Pokud průnik přímky  $p$  a eliptické křivky  $E$  je právě množina  $\{P, Q\}$ , pak  $P + Q = \mathcal{O}$ .

## Eliptické křivky nad tělesem reálných čísel (2 ze 3)

Mějme dva různé body  $P$  a  $Q$  na eliptické křivce  $E$  nad  $\mathbb{R}$ , potom pro jejich součet platí:

- Sestroj přímku  $p$  procházející body  $P$  a  $Q$ .
- Pokud přímka  $p$  má s  $E$  ještě jeden průsečík  $R = (x, y)$  různý od  $P$  a  $Q$ , pak  $P + Q = (x, -y)$ .
- Pokud průnik přímky  $p$  a eliptické křivky  $E$  je právě množina  $\{P, Q\}$ , pak  $P + Q = \mathcal{O}$ .

Mějme jeden bod  $P$  na eliptické křivce  $E$ , potom pro součet  $P + P$  platí

- Sestroj tečnu  $p$  křivky  $E$  v bodě  $P$ .
- Pokud tato tečna prochází ještě jedním bodem  $R = (x, y)$  křivky  $E$ , pak  $P + P = (x, -y)$
- Pokud tato tečna protíná  $E$  právě v  $P$ , pak  $P + P = \mathcal{O}$ .

- **Poznámka:** Při sčítání bodů tedy hledáme průsečíky nějaké přímky  $y = sx + d$ , kde  $s$  je směrnice a  $d \in \mathbb{R}$ , a eliptické křivky  $y^2 = x^3 + ax + b$ . To vede na řešení rovnice

$$(sx + d)^2 = x^3 + ax + b,$$

což je polynomiální rovnice 3. stupně a ta, jak víme, může mít 1 až 3 různé reálné kořeny (jedno řešení máme vždy ze zadání).

## Eliptické křivky nad tělesem reálných čísel (3 ze 3)

- **Poznámka:** Při sčítání bodů tedy hledáme průsečíky nějaké přímky  $y = sx + d$ , kde  $s$  je směrnice a  $d \in \mathbb{R}$ , a eliptické křivky  $y^2 = x^3 + ax + b$ . To vede na řešení rovnice

$$(sx + d)^2 = x^3 + ax + b,$$

což je polynomiální rovnice 3. stupně a ta, jak víme, může mít 1 až 3 různé reálné kořeny (jedno řešení máme vždy ze zadání).

- Např. situace, kdy pro různé  $P$  a  $Q$  dostaneme pouze dva kořeny, odpovídá tomu, že  $Q = -P$  a výsledkem součtu je neutrální prvek  $\mathcal{O}$ .

## Eliptické křivky nad tělesem reálných čísel (3 ze 3)

- **Poznámka:** Při sčítání bodů tedy hledáme průsečíky nějaké přímky  $y = sx + d$ , kde  $s$  je směrnice a  $d \in \mathbb{R}$ , a eliptické křivky  $y^2 = x^3 + ax + b$ . To vede na řešení rovnice

$$(sx + d)^2 = x^3 + ax + b,$$

což je polynomiální rovnice 3. stupně a ta, jak víme, může mít 1 až 3 různé reálné kořeny (jedno řešení máme vždy ze zadání).

- Např. situace, kdy pro různé  $P$  a  $Q$  dostaneme pouze dva kořeny, odpovídá tomu, že  $Q = -P$  a výsledkem součtu je neutrální prvek  $\mathcal{O}$ .
- Místo nad  $\mathbb{R}$  můžeme pracovat nad tělesem  $GF(p^n)$ . I v tomto případě dále mluvíme o „eliptické křivce“, ačkoliv příslušnou diskrétní množinu bodů bychom na obrázku za křivku jistě neoznačili.