

**MUNI**  
**PED**

# **Aritmetika 2 – jaro 2021**

## **8. prezentace**

Mgr. Helena Durnová, Ph.D.

RNDr. Petra Bušková

# Jaké relace na množině celých (přirozených) čísel již známe?

– rovnost, značíme =

- „menší nebo rovno“, značíme  $\leq$

- dělitelnost, značíme svislou čarou:  $a \mid b$  – čteme „a dělí b“

zavedeme novou relaci: „dávát stejný zbytek po dělení m“

- kongruence, značíme  $\equiv$

Příklady:

Číslo 7 dává stejný zbytek po dělení číslem 5 jako číslo 12 – zapíšeme:

$$7 \equiv 12 \pmod{5}$$

Číslo 13 dává po dělení číslem 3 stejný zbytek jako číslo 22 – zapíšeme:

$$13 \equiv 22 \pmod{3}$$

# Připomenutí: věta o dělení se zbytkem

—

## Věta:

Nechť  $a$ ,  $b$  jsou celá čísla,  $b$  je různé od nuly. Potom existují čísla  $q$ ,  $r$  splňující vztah  $a = bq + r$ , kde  $0 \leq r < |b|$ , přičemž toto vyjádření je jednoznačné

- Číslo  $q$  se nazývá **podíl** (někdy také **kvocient**)
- Číslo  $r$  se nazývá **zbytek**. Zbytek  $r$  musí být vždy v rozmezí od  $0$  do  $(b-1)$ , a to včetně krajních hodnot, pouze přirozená čísla, tj. pro dělení číslem  $4$  dostáváme zbytky  $0, 1, 2, 3$ ; pro dělení číslem  $5$  zbytky  $0, 1, 2, 3, 4$ , atd.
- Jednoznačnosti vyjádření jsme využívali při řešení diofantických rovnic

# Kongruence a zbytkové třídy: jak souvisí?

- Někdy nás zajímá pouze zbytek po dělení, nikoliv podíl.  
V takovém případě můžeme použít kongruence.
  - Příklad 1: dny v týdnu se opakují po sedmi dnech. Víme-li, že např. 8. daného měsíce je středa, potom 15. bude také středa; dále 18. bude sobota
  - Příklad 2: potřebujeme rozdělit ovoce mezi tři děti, ale máme 17 kusů ovoce. Číslo 17 dává po dělení třemi zbytek 2, tedy když přidáme 1 nebo 4 nebo 7, ... kusů ovoce, budeme mít počet kusů dělitelný třemi
- Všechna přirozená čísla můžeme rozdělit na třídy podle toho, jaký zbytek dávají po dělení číslem  $m$  – těmto třídám říkáme zbytkové třídy modulo  $m$

# Sčítání a násobení ve zbytkových třídách: $m=3$

Modulo 3

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| (krát) | 0 | 1 | 2 |
|--------|---|---|---|
| 0      | 0 | 0 | 0 |
| 1      | 0 | 1 | 2 |
| 2      | 0 | 2 | 1 |

Můžeme zkoumat vlastnosti operací:

Sčítání:

Komutativní

Neutrální prvek: 0 (agresivní prvek pro násobení)

Inverzní prvky: existují

Násobení:

Komutativní, Neutrální prvek: 1

Inverzní prvky: hledáme pouze pro nenulové prvky – 1 i 2 jsou inverzní samy k sobě

# Sčítání a násobení ve zbytkových třídách: $m=4$

Modulo 4

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| (krát) | 0 | 1 | 2 | 3 |
|--------|---|---|---|---|
| 0      | 0 | 0 | 0 | 0 |
| 1      | 0 | 1 | 2 | 3 |
| 2      | 0 | 2 | 0 | 2 |
| 3      | 0 | 3 | 2 | 1 |

Můžeme zkoumat vlastnosti operací:

Sčítání:

Komutativní

Neutrální prvek: 0

Inverzní prvky: existují

Násobení:

Komutativní

Neutrální prvek: 0

Inverzní prvky: hledáme pouze pro nenulové prvky, ale ani 2 nemá inverzní prvek

# Sčítání a násobení ve zbytkových třídách: $m=5$

Modulo 5

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 |   |   |   |   |   |
| 1 |   |   |   |   |   |
| 2 |   |   |   |   |   |
| 3 |   |   |   |   |   |
| 4 |   |   |   |   |   |

| (krát) | 0 | 1 | 2 | 3 | 4 |
|--------|---|---|---|---|---|
| 0      |   |   |   |   |   |
| 1      |   |   |   |   |   |
| 2      |   |   |   |   |   |
| 3      |   |   |   |   |   |
| 4      |   |   |   |   |   |

Můžeme zkoumat vlastnosti operací:

Sčítání:

Komutativní Neutrální prvek: 0

Inverzní prvky: existují

Násobení:

Komutativní, Neutrální prvek: 1

Inverzní prvky: hledáme pouze pro nenulové prvky, inverzní prvky existují pro čísla 1-4

# Sčítání a násobení ve zbytkových třídách: $m=6$

## Modulo 6

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 |   |   |   |   |   |   |
| 1 |   |   |   |   |   |   |
| 2 |   |   |   |   |   |   |
| 3 |   |   |   |   |   |   |
| 4 |   |   |   |   |   |   |
| 5 |   |   |   |   |   |   |

| (krát) | 0 | 1 | 2 | 3 | 4 | 5 |
|--------|---|---|---|---|---|---|
| 0      |   |   |   |   |   |   |
| 1      |   |   |   |   |   |   |
| 2      |   |   |   |   |   |   |
| 3      |   |   |   |   |   |   |
| 4      |   |   |   |   |   |   |
| 5      |   |   |   |   |   |   |

Opět dopadá skoro všechno analogicky, nacházíme dva dělitele nuly: čísla 2 a 3.

Nápad: pokud je modulo prvočíslo, dělitelé nuly nebudou, jinak ano – děliteli nuly budou vždy všichni dělitelé daného čísla



# Příklady

## —Příklad 1.

Víme, že číslo  $n$  dává při dělení sedmi zbytek 1. Jaký zbytek dává po dělení 7 výraz

*a)*  $n^2 + 6$

*b)*  $(n + 1)(n + 6)$

## Příklad 2.

Číslo  $n$  dává při dělení čtyřmi zbytek 3. Jaký zbytek po dělení čtyřmi dává výraz

*a)*  $n^2 + 3$

*b)*  $n^2 + 1$

# Úlohy k opakování základů algebry 1

## Příklad 1:

Uvedte, jaké vlastnosti má relace rovnosti

- a) Na množině přirozených čísel
- b) Na množině celých čísel
- c) Na množině racionálních čísel

Určete, zda se jedná o relaci typu

**ekvivalence nebo uspořádání**

## Příklad 2:

Uvedte, jaké vlastnosti má relace menší nebo rovno.

- a) Na množině přirozených čísel
- b) Na množině celých čísel
- c) Na množině racionálních čísel

Určete, zda se jedná o relaci typu

**ekvivalence nebo uspořádání**

# Úlohy k opakování základů algebry 2

## Příklad 3:

Určete, jaké vlastnosti má relace dělitelnosti na množině přirozených čísel.

*Připomínáme: číslo  $a$  je v relaci s číslem  $b$  tehdy, pokud platí:  $a$  dělí  $b$*

*(tj. např. 3 dělí 3 --- dvojice 3, 3 je v relaci; 2 dělí 4, tj. dvojice 2, 4 je v relaci,*

*ale 4 nedělí 2, tj. dvojice 4, 2 v relaci není*

## Příklad 4:

Určete, jaké vlastnosti má relace kongruence na množině celých čísel.

*Připomínáme: číslo  $a$  je kongruentní modulo  $m$  s číslem  $b$  tehdy, pokud  $a$  i  $b$  dávají stejný*

*zbytek po dělení číslem  $m$ .*

# Kalendář

Když 1. ledna je pondělí, co je

1. února? - čtvrtek

1. března? - čtvrtek (nepřestupný rok)

1. dubna? - sobota

1. května? - pondělí

1. června? - čtvrtek

1. července? - sobota

1. srpna? - úterý

1. září? - pátek

1. října? - pondělí

1. listopadu? - čtvrtek

1. prosince? - sobota

1. prosince? - sobota

Namátkou – loni bylo 1. září i 1. prosince **úterý**

Letos – 1. ledna byl pátek, 1. března pondělí, také  
1. listopadu bude pondělí

|   |   |   |
|---|---|---|
| 0 | 3 | 3 |
| 6 | 1 | 4 |
| 6 | 2 | 5 |
| 0 | 3 | 5 |

# Přestupné roky a počáteční hodnota

- Každý čtvrtý rok, tj. rok dělitelný 4, avšak nikoliv 100
- Rok 1900 přestupný nebyl
- Přestupné roky ve 20. století:  
1904, 1908, ....., 1992, 1996
- A co rok 2000? – vzhledem k potřebě další (zpětné) korekce jsou roky dělitelné 400 přestupné, tedy i rok 2000 byl přestupný
- Krása výpočtu dne podle data ve 20. století spočívá v tom, že 1. 1. 1900 bylo pondělí (výhoda viz výpočet v tabulce).

# Postup výpočtu ve 20. století

Datum 1. ledna 1900: 17. 11. 1989

výpočty modulo 7 – počet dnů v týdnu

| Den – pořadové číslo | Měsíc (z tabulky) | Rok – pořadové číslo | Rok – podle počtu přestupných |
|----------------------|-------------------|----------------------|-------------------------------|
| 1 / 17 ... 3         | 0 / 3             | 1 / 89 ... 5         | 0 / 88:4 = 22 ...1            |

Součet:  $1 + 0 + 0 + 0 = 1$  .... Bylo to pondělí

součet:  $3 + 3 + 5 + 1 = 12$  kongr. 5 ... pátek

Kódy dnů:

| pondělí | úterý | středa | čtvrtek | pátek | sobota | neděle |
|---------|-------|--------|---------|-------|--------|--------|
| 1       | 2     | 3      | 4       | 5     | 6      | 0      |

-

|                |   |   |   |
|----------------|---|---|---|
| I. čtvrtletí   | 0 | 3 | 3 |
| II. čtvrtletí  | 6 | 1 | 4 |
| III. čtvrtletí | 6 | 2 | 5 |
| IV. čtvrtletí  | 0 | 3 | 5 |

# Postup výpočtu pro 21. století

Datum 1. ledna 1900 / 11. 9. 2001 – jako pokračování 20. století

| Den – pořadové číslo | Měsíc (z tabulky) | Rok – pořadové číslo | Rok – podle počtu přestupných |
|----------------------|-------------------|----------------------|-------------------------------|
| 1 / 11 ... 4         | 0 / 5             | 1 / 101 ... 3        | 0 / 101:4 = 25 ... 4          |

Součet:  $1 + 0 + 0 + 0 = 1$  .... Bylo to pondělí      součet:  $4 + 5 + 3 + 4 = 16$  kongr. 2 ... úterý

Kódy dnů:

| pondělí | úterý | středa | čtvrtek | pátek | sobota | neděle |
|---------|-------|--------|---------|-------|--------|--------|
| 1       | 2     | 3      | 4       | 5     | 6      | 0      |

-

|                |   |   |   |
|----------------|---|---|---|
| I. čtvrtletí   | 0 | 3 | 3 |
| II. čtvrtletí  | 6 | 1 | 4 |
| III. čtvrtletí | 6 | 2 | 5 |
| IV. čtvrtletí  | 0 | 3 | 5 |