# MB141 – 11. přednáška
# Kongruence

Martin Čadek
s využitím přednášek pro předmět MB104

Jarní semestr 2020

# Osnova 11. přednášky

- Kongruence a počítání s nimi
- Malá Fermatova věta
- Eulerova funkce a Eulerova věta
- Řešení lineárních rovnic s kongruencemi
- Čínská zbytková věta a řešení soustav lineárních kongruencí

# Pojem kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

## Definice

Jestliže dvě celá čísla $a, b$ mají při dělení přirozeným číslem $m$ týž zbytek $r$, kde $0 \leq r < m$, nazývají se $a, b$ kongruentní modulo m (též kongruentní podle modulu m), což zapisujeme takto:

$$a \equiv b \pmod{m}.$$

V opačném případě řekneme, že $a, b$ nejsou kongruentní modulo $m$, a píšeme

$$a \not\equiv b \pmod{m}.$$

# Kongruence jako ekvivalence

**Lemma**

*Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ jsou následující podmínky ekvivalentní:*

1. $a \equiv b \pmod{m}$,
2. $a = b + mt$ *pro vhodné* $t \in \mathbb{Z}$,
3. $m \mid a - b$.

Přímo z definice plyne, že kongruence podle modulu $m$ je reflexivní (tj. $a \equiv a \pmod{m}$ platí pro každé $a \in \mathbb{Z}$), symetrická (tj. pro každé $a, b \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$) a tranzitivní (tj. pro každé $a, b, c \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$) relace, jde tedy o *ekvivalenci*.

# Základní vlastnosti kongruencí I

Ukážeme nyní další vlastnosti kongruencí, které jsou důležité při počítání:

- Kongruence podle téhož modulu můžeme sčítat. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.

Je-li $a_1 \equiv b_1 \pmod{m}$ a $a_2 \equiv b_2 \pmod{m}$, existují podle lemmatu $t_1, t_2 \in \mathbb{Z}$ tak, že $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. Pak ovšem $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$ a opět podle lemmatu $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$. Sečteme-li kongruenci $a + b \equiv c \pmod{m}$ s kongruencí $-b \equiv b \pmod{m}$, která zřejmě platí, dostaneme $a \equiv c - b \pmod{m}$. Sečteme-li kongruenci $a \equiv b \pmod{m}$ s kongruencí $mk \equiv 0 \pmod{m}$, jejíž platnost je zřejmá, dostaneme $a + mk \equiv b \pmod{m}$.

# Základní vlastnosti kongruencí II

- Kongruence podle téhož modulu můžeme násobit. Obě strany kongruence je možné umocnit na totéž přirozené číslo. Obě strany kongruence je možné vynásobit stejným celým číslem.
- Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem.
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.

Důkazy těchto tvrzení se provádějí stejným způsobem jako důkaz z předchozí strany.

# Základní vlastnosti kongruencí III

- Jestliže kongruence $a \equiv b$ platí podle modulů $m_1, \dots, m_k$, platí i podle modulu, kterým je nejmenší společný násobek $[m_1, \dots, m_k]$ těchto čísel.

Jestliže $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$, podle lemmatu je rozdíl $a - b$ společný násobek čísel $m_1, m_2, \dots, m_k$ a tedy je dělitelný jejich nejmenším společným násobkem $[m_1, m_2, \dots, m_k]$, odkud plyne $a \equiv b \pmod{[m_1, \dots, m_k]}$.

- Jestliže kongruence platí podle modulu $m$, platí podle libovolného modulu $d$, který je dělitelem čísla $m$.
- Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana.

# Poznámka a příklad 1

Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

**Příklad (1)**

Nalezněte zbytek po dělení čísla $5^{20}$ číslem 26.

Protože $5^2 = 25 \equiv -1 \pmod{26}$, platí

$$5^{20} = (5^2)^{10} \equiv (-1)^{10} = 1 \pmod{26},$$

a tedy zbytek po dělení čísla $5^{20}$ číslem 26 je jedna.

# Příklady 2 a 3

## Příklad (2)

Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Platí $37 \equiv 16 \equiv 23 \equiv 2 \pmod 7$, a tedy podle základních vlastností kongruencí platí

$$37^{n+2}+16^{n+1}+23^n \equiv 2^{n+2}+2^{n+1}+2^n = 2^n(4+2+1) \equiv 0 \pmod 7.$$

## Příklad (3)

Dokažte, že číslo $n = (835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

Rozložíme $112 = 7 \cdot 16$. Protože $(7, 16) = 1$, stačí ukázat, že $7 \mid n$ a $16 \mid n$. Platí $835 \equiv 2 \pmod 7$, a tedy

$$n \equiv (2^5 + 6)^{18} - 1 = 38^{18} - 1 \equiv 3^{18} - 1 =$$
$$= 27^6 - 1 \equiv (-1)^6 - 1 = 0 \pmod 7,$$

# Příklad 3

proto $7 \mid n$. Podobně $835 \equiv 3 \pmod{16}$, a tedy

$$n \equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \equiv (3 \cdot 1 + 6)^{18} - 1 = \\ = 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16},$$

proto $16 \mid n$. Celkem tedy $112 \mid n$, což jsme měli dokázat.

## Příklad

Najděte “inverzi” k číslu 39 modulo 47, tj. najděte $x$ takové, že $39 \cdot x \equiv 1 \pmod{47}$.

Počítáme $\pmod{47}$: $39 \equiv -8$, proto $-8x \equiv 1$. Vynásobíme 6 a odečteme $47x \equiv 0$, dostaneme $x \equiv -6 \equiv 41$.

## Příklad (4)

Najděte “inverzi” k číslu 39 modulo 235, tj. najděte $x$ takové, že $39 \cdot x \equiv 1 \pmod{235}$.

Protože $235 = 5 \cdot 47$ a čísla 5 a 47 jsou nesoudělná, je kongruence $39x \equiv 1 \pmod{235}$ ekvivalentní se dvěma kongruencemi
$39x \equiv 1 \pmod{47}$ a $39x \equiv 1 \pmod{5}$
Podle předchozí úlohy má prvá řešení $x \equiv 41 \pmod{47}$.
Řešení druhé je $x \equiv 4 \pmod{5}$. Tedy podle prvé kongruence je $x = 47y + 41$, dosazením do druhé dostaneme $47y + 41 \equiv 4 \pmod{5}$, ekvivalentně $2y + 1 \equiv 4 \pmod{5}$, $2y \equiv 3 \pmod{5}$, $2y \equiv= 2 \pmod{5}$, tedy $y \equiv -1 \equiv 4 \pmod{5}$. Tedy $y = 5z + 4$. Zpětným dosazením do $x$ dostaneme $x = 47(5z + 4) + 41 = 235z + 229 \equiv 229$.

# Malá Fermatova věta

Tato tvrzení patří mezi nejdůležitější výsledky elementární teorie čísel.

**Věta (Malá Fermatova věta)**

*Nechť $p$ je prvočíslo a nechť $a \in \mathbb{Z}$ je takové, že $p \nmid a$. Pak*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Prvně dokážeme indukcí, že $a^p \equiv a \pmod{p}$ pro všechna $a$ přirozená. Pro $a = 1$ to platí. Předpokládejme, že $a^p \equiv a$ pro nějaké $a \geq 1$. Potom pomocí binomické věty $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1$, neboť pro všechna $k = 1, 2, \dots, p-1$ platí, že $p \mid \binom{p}{k} = \frac{p!}{k!(p-k)!}$ díky tomu, že $p$ je prvočíslo. Dále použijeme indukční předpoklad $(a+1)^p \equiv a^p + 1 \equiv a + 1$. Platí-li, že $a^p \equiv a \pmod{p}$, pak číslem $a$, které není násobkem $p$, můžeme dělit a dostaneme $a^{p-1} \equiv 1 \pmod{p}$.

# Příklad 5

Všimněte si, že jsme při důkazu dokázali $a^p \equiv a \pmod{p}$ pro všechna $a$.

**Příklad (5)**

Zjistěte zbytek po dělení čísla $21^{480}$ číslem 47.

47 je prvočíslo. $47 - 1 = 46$ a $480 = 10 \cdot 46 + 20$. Proto podle Fermatovy věty dostáváme
$21^{480} = (21^{46})^{10} \cdot 21^{20} \equiv 1^{10} \cdot 21^{20} \equiv (21^2)^{10} \equiv 441^{10} \equiv 18^{10} \equiv (18^2)^5 \equiv (-5)^5 \equiv 625 \cdot (-5) \equiv 14 \cdot (-5) \equiv 24 \pmod{47}$.

# Eulerova funkce

Malou Fermatovu větu lze zobecnit. K tomu budeme potřebovat Eulerovu funkci. Je-li $p$ prvočíslo, pak počet celých čísel v intervalu $[1, p]$, která jsou nesoudělná s $p$ je $p - 1$. To je exponent vyskytující se ve Fermatově větě.

## Definice

Nechť $n \in \mathbb{N}$. Eulerovu funkci $\varphi$ definujeme jako počet celých čísel v intervalu $[1, n]$ nesoudělných s $p$,

$$\varphi(n) = |\{a \in \mathbb{N} \,|\, 0 < a \leq n,\ (a, n) = 1\}|$$

## Příklad

$\varphi(1) = 1, \varphi(5) = 4, \varphi(12) = 4$, je-li p prvočíslo, je zřejmě $\varphi(p) = p - 1$.

# Výpočet Eulerovy funkce

## Věta

*Nechť $n \in \mathbb{N}$, jehož rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak*

$$\begin{aligned}\varphi(n) &= p^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Předchozí výsledek lze obdržet z následujících dvou tvrzení.

- Nechť $a, b \in \mathbb{N}$, $(a, b) = 1$. Pak $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
- $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p - 1) \cdot p^{\alpha-1}$.

## Příklad (6)

Vypočtěte $\varphi(72)$.

$72 = 2^3 \cdot 3^2 \implies \varphi(72) = 72 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 24$,
alternativně $\varphi(72) = \varphi(8) \cdot \varphi(9) = 4 \cdot 6 = 24$.

# Eulerova věta

**Věta (Eulerova)**

*Nechť* $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. *Pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m*:

**Definice**

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $(a, m) = 1$. Řádem čísla $a$ modulo $m$ rozumíme nejmenší přirozené číslo $n$ splňující

$$a^n \equiv 1 \pmod{m}.$$

# Primitivní kořeny

To, že je řád definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Velmi důležitá jsou právě ta čísla, jejichž řád je roven právě $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo $m$.

**Příklad**

Pro libovolné $m \in \mathbb{N}$ má číslo 1 modulo $m$ řád 1. Číslo $-1$ má řád

- 1 pro $m = 1$ nebo $m = 2$
- 2 pro $m > 2$

# Příklad 7

## Příklad (7)

Určete řád čísla 2 modulo 7.

Řešení:

$$\begin{aligned} 2^1 &= 2 \not\equiv 1 \pmod 7 \\ 2^2 &= 4 \not\equiv 1 \pmod 7 \\ 2^3 &= 8 \equiv 1 \pmod 7 \end{aligned}$$

Řád čísla 2 modulo 7 je tedy roven 3.

# Lineární kongruence o jedné neznámé

## Věta

*Nechť* $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. *Označme* $d = (a, m)$. *Pak kongruence*

$$ax \equiv b \pmod{m}$$

*(o jedné neznámé x) má řešení právě tehdy, když* $d \mid b$.
*Pokud platí* $d \mid b$, *má tato kongruence právě d řešení (modulo m).*

Řešením modulo $m$ myslíme zbytkovou třídu. Např. zbytková třída $3 \pmod{7}$ je množina $\{7k + 3 \in \mathbb{Z};\ k \in \mathbb{Z}\}$.

## Příklad

1. Kongruence $2x \equiv 1 \pmod{3}$ má jedno řešení (modulo 3).
2. Kongruence $10x \equiv 5 \pmod{15}$ má pět řešení (modulo 15).

# Důkaz

Kongruence $2x \equiv 1 \pmod 3$ má řešení $x \equiv 2 \pmod 3$.
Kongruence $10x \equiv 5 \pmod{15}$ má řešení $2$, $3+2=5$, $6+2=8$, $9+2=11$, $12+2=14 \pmod{15}$.

Důkaz předchozí věty provedeme pomocí Eulerovy věty:

Dokážeme nejprve, že uvedená podmínka je nutná. Je-li celé číslo $c$ řešením této kongruence, pak nutně $m \mid a \cdot c - b$. Pokud $d = (a, m)$, pak $d$ dělí také $a \cdot c - b$. A protože dělí $a$, musí dělit také $b$.

Obráceně dokážeme: pokud $d \mid b$, pak má daná kongruence právě $d$ řešení modulo $m$. Označme $a_1, b_1 \in \mathbb{Z}$ a $m_1 \in \mathbb{N}$ tak, že $a = d \cdot a_1$, $b = d \cdot b_1$ a $m = d \cdot m_1$. Řešená kongruence je tedy ekvivalentní s kongruencí

$$a_1 \cdot x \equiv b_1 \pmod{m_1},$$

kde $(a_1, m_1) = 1$.

# Dokončení důkazu

Tuto kongruenci můžeme vynásobit číslem $a_1^{\varphi(m_1)-1}$ a díky Eulerově větě obdržíme

$$x \equiv a_1^{\varphi(m_1)} \cdot x \equiv a_1^{\varphi(m_1)-1} \cdot b_1 \pmod{m_1}.$$

Tato kongruence má jediné řešení modulo $m_1$ a tedy $d = m/m_1$ řešení modulo m. Ta jsou $a_1^{\varphi(m_1)-1} \cdot b_1 + km_1$, kde $k = 0, 1, 2, \dots, d-1$.

Následující příklad ukáže, že postup uvedený v důkazu věty obvykle není tím nejefektivnějším – s výhodou lze použít jak Bezoutovu větu, tak ekvivalentní úpravy řešené kongruence.

# Příklad 8

## Příklad (8)

Řešte $39x \equiv 41 \pmod{47}$

(1) Nejprve využijeme Eulerovu větu, stejně jako v důkazu.
(2) Další možností je využít Bezoutovu větu. Najdeme $a, b \in \mathbb{Z}$ tak, že $39a + 47b = 1$. Pak vynásobíme číslem 41. Řešení je $x \equiv 41a$.
(3) Obvykle nejrychlejším, ale nejhůře algoritmizovatelným způsobem řešení je metoda takových úprav kongruence, které zachovávají množinu řešení.

$$\begin{aligned} 39x \equiv 41 \pmod{47} &\iff -8x \equiv -6 \pmod{47} \iff \\ 4x \equiv 3 \pmod{47} &\iff 4x \equiv -44 \pmod{47} \iff \\ x \equiv -11 \pmod{47} &\iff x \equiv 36 \pmod{47} \end{aligned}$$

Více ve cvičení.

# Soustavy lineárních kongruencí

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich. V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$
\begin{aligned}
x &\equiv c_1 \pmod{m_1} \\
&\vdots \\
x &\equiv c_k \pmod{m_k}
\end{aligned}
$$

Zřejmě stačí vyřešit případ $k = 2$, řešení soustavy více kongruencí snadno obdržíme opakovaným řešením soustav dvou kongruencí.

**Věta**

*Nechť $c_1, c_2$ jsou celá čísla, $m_1, m_2$ přirozená. Označme $d = (m_1, m_2)$. Soustava dvou kongruencí*

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$

*v případě $c_1 \not\equiv c_2 \pmod{d}$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod{d}$, pak existuje celé číslo $c$ tak, že $x \in \mathbb{Z}$ vyhovuje soustavě, právě když vyhovuje kongruenci*

$$x \equiv c \pmod{[m_1, m_2]}.$$

Má-li soustava nějaké řešení $x \in \mathbb{Z}$, platí nutně $x \equiv c_1 \pmod{d}$, $x \equiv c_2 \pmod{d}$, a tedy i $c_1 \equiv c_2 \pmod{d}$.

# Náznak důkazu

Předpokládejme dále $c_1 \equiv c_2 \pmod{d}$. První kongruenci řešené soustavy vyhovují všechna celá čísla $x$ tvaru $x = c_1 + tm_1$, kde $t \in \mathbb{Z}$ je libovolné. Toto $x$ bude vyhovovat i druhé kongruenci soustavy, právě když bude platit $c_1 + tm_1 \equiv c_2 \pmod{m_2}$, tj. $tm_1 \equiv c_2 - c_1 \pmod{m_2}$. Podle věty o řešitelnosti lineárních kongruencí má tato kongruence (vzhledem k $t$) řešení, neboť $d = (m_1, m_2)$ dělí $c_2 - c_1$.

# Čínská zbytková věta

Ve čtvrtém století se čínský matematik Sun Ze (Sun Tsu) ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

**Věta (Čínská zbytková věta)**

*Nechť $m_1, \ldots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná, $a_1, \ldots, a_k \in \mathbb{Z}$. Pak platí: soustava*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

*má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.*

Řešení hledáme stejně jako v předchozím důkazu, jak uvidíte v následujícím příkladu.

## Příklad (9)

Řešte systém kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

Řešení: Z první kongruence plyne, že $x = 10y + 1$. Dosazením do druhé kongruence dostaneme $10y \equiv 4 \pmod{18}$, ekvivalentně $5y \equiv 2 \pmod{9}$. Řešení je $y = 9z + 4$, proto $x = 90z + 41$. Dosazením do poslední kongruence dostaneme $90z \equiv -45 \pmod{25}$, ekvivalentně $18z \equiv -9 \pmod{5}$, vydělíme 9 a dostaneme $2z \equiv -1 \pmod{5}$. Tedy $z = 5a + 2$. Dosazením $x = 90(5a + 2) + 41 = 450 + 180 + 41 \equiv 221 \pmod{450}$. Výsledkem je $x \equiv 221 \pmod{450}$.

# Příklad 10

Čínskou zbytkovou větu můžeme použít také „v opačném směru“.

**Příklad (10)**

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a má tedy kongruence řešení. Protože $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak.

# Dokončení příkladu 10

Víme, že $x \in \mathbb{Z}$ řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11}. \end{aligned}$$

Vyřešíme-li postupně každou z kongruencí soustavy, dostaneme ekvivalentní soustavu

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11}, \end{aligned}$$

odkud snadno postupem pro řešení soustav kongruencí dostaneme $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence.