Algebra

MB104 - jaro 2011

1 Cvičení 1: Teorie čísel

Teorie: V prvním cvičení se budeme zabývat teorií čísel. Vše, co se naučíme, budeme využívat i v dalších cvičeních, proto je důležité porozumět základním pojmům. Ze střední školy byste již měli znát pojmy jako dělitelnost, největší společný dělitel, nejmenší společný násobek. Pro osvěžení si uveďme jejich definice.

Definice 1. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo a dělí celé číslo b, píšeme $a|b$, jestliže existuje $k \in \mathbb{Z}$ tak, že $b = a \cdot k$.

S dělitelností souvisí věta o dělení celých čísel se zbytkem. Tuto větu považujeme za zcela zřejmou. V tomto předmětu si však ukážeme, že ne ve všech okruzích platí.

Věta 1 (O dělení celých čísel se zbytkem)**.** *Nechť $a, b \in \mathbb{Z}$. Potom existují $q, r \in \mathbb{Z}$ taková, že $a = b \cdot q + r$, kde $0 \leq r < |b|$.*

Definice 2. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo d je největším společným dělitelem čísel a, b, píšeme $d = (a, b)$, jestliže platí dvě podmínky

1. $d|a, \ d|b$
2. Pokud existuje celé číslo c takové, že $c|a, \ c|b$, potom $c|d$.

Největší společný dělitel jste na střední škole určovali Euklidovým algoritmem. Toho budeme využívat i v našem předmětu. S největším společným dělitelem úzce souvisí Bezoutova identita.

Věta 2 (Bezoutova)**.** *Nechť $a, b \in \mathbb{Z}$. Potom existují celá čísla m, n taková, že $am + bn = (a, b)$.*

Definice 3. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo n je nejmenším společným násobkem čísel a, b, píšeme $n = [a, b]$, jestliže platí dvě podmínky

1. $a|n, \ b|n$
2. Pokud existuje celé číslo m takové, že $a|m, \ b|m$, potom $n|m$.

Nyní se již dostáváme k pojmu kongruence. Tento pojem zřejmě neslyšíte poprvé. Využívali jste ho jistě už v Úvodu do Informatiky či Automatech a gramatikách.

Definujme tedy, kdy jsou spolu dvě celá čísla kongruentní modulo nějaké přirozené číslo.

Definice 4. Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že $a \equiv b \pmod{m}$, jestliže a i b dávají stejný zbytek po dělení m.

S definicí kongruence se můžete setkat v několika různých podobách, jak nám říká následující věta.

Věta 3. *Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Potom následující podmínky jsou spolu ekvivalentní:*

1. $a \equiv b \pmod{m}$
2. $m|(a-b)$
3. *Existuje celé číslo k takové, že $a = k \cdot m + b$*

To, jak můžeme s kongruencemi pracovat, nám poví následující věta.

Věta 4. *Nechť $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$. Nechť $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. Potom platí*

1. $a + c \equiv b + d \pmod{m}$
2. $a \cdot c \equiv b \cdot d \pmod{m}$

Dále můžeme obě strany kongruence umocnit na stejné přirozené číslo, vynásobit stejným nenulovým celým číslem. Ovšem **pozor**, nemůžeme obě strany kongruence dělit.

Věta 5 (Malá Fermatova věta)**.** *Nechť $a \in \mathbb{Z}$, p je prvočíslo takové, že $(a, p) = 1$. Potom*

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

Relace kongruence modulo přirozené číslo m je relací ekvivalence na množině celých čísel. Uvažme nyní rozklad příslušný této ekvivalenci. Jednotlivým třídám tohoto rozkladu říkámě zbytkové třídy modulo m.

Obsahuje-li zbytková třída modulo m celé číslo a, potom ji značíme $[a]_m$. Zbytkové třídy můžeme sčítat a násobit pomocí reprezentantů. Řekneme, že zbytková třída $[b]_m$ je inverzní ke zbytkové třídě $[a]_m$, jestliže $[a]_m \cdot [b]_m = [1]_m$. K výpočtu inverzních tříd využíváme Euklidova algoritmu.

Nyní si řekneme, co je to eulerova funkce.

Definice 5. Funkci $\varphi : \mathbb{N} \to \mathbb{N}$, která každému přirozenému číslu n přiřadí počet přirozených čísel, které jsou menší nebo rovny n a jsou s n nesoudělné, říkáme Eulerova funkce.

To, jak se hodnota Eulerovy funkce počítá, nám řekne další tvrzení.

Věta 6. *Nechť a, b jsou dvě **nesoudělná** přirozená čísla a nechť $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$ je rozklad přirozeného čísla n na součin prvočísel. Potom*

1. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
2. $\varphi(n) = (p_1 - 1)p_1^{e_1-1} \cdot \dots \cdot (p_k - 1)p_k^{e_k-1}$

Věta 7 (Eulerova věta)**.** *Nechť* $a \in \mathbb{Z}$*,* $m \in \mathbb{N}$ *takové, že* $(a, m) = 1$*. Potom*

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

Definice 6. Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. Řekneme, že řád celého čísla a modulo m je n, jestliže n je nejmenší přirozené číslo takové, že $a^n \equiv 1 \pmod{m}$.

Pro řád daného čísla a modulo m platí, že dělí každé takové číslo k, pro které je $a^k \equiv 1 \pmod{m}$.

Příklad 1. Určete podíl q a zbytek r po dělení čísla a číslem b

1. $a = -47,\ b = 11$
2. $a = -47,\ b = -11$
3. $a = 47,\ b = -11$
4. $a = n^3 - 1,\ b = n + 1,\ n \in \mathbb{N}$

Výsledek.

1. $a = -5, b = 8$
2. $a = 5, b = 8$
3. $a = -4, b = 3$
4. $a = n^2 - n, b = n - 1$

Příklad 2. Určete největší společný dělitel čísel a, b a určete příslušné koeficienty v Bezoutově rovnosti

1. $a = 21,\ b = 98$
2. $a = 10175,\ b = 2277$

Výsledek.

1. $7 = 5 \cdot 21 + (-1) \cdot 98$
2. $11 = (-32) \cdot 10175 + 143 \cdot 2277$

Příklad 3. Nechť $a \in \mathbb{Z}$. Dokažte, že

1. a^2 dává po dělení čtyřmi zbytek 0 nebo 1.
2. a^4 dává po dělení osmi zbytek 0 nebo 1.

Řešení.

1. Uvažujme $a = 2k + 1$ a $a = 2k$. Po umocnění dostáváme požadované tvrzení.
2. Použijeme výsledek předchozího příkladu, tedy uvažujme $a^2 = 4k + 1$ a $a^2 = 4k$. Opět po umocnění dostaneme požadované tvrzení.

Příklad 4. Určete všechna celá čísla x tak, aby

1. $4x \equiv 1 \pmod 7$
2. $7x \equiv 3 \pmod{11}$

Výsledek.

1. $x \equiv 2 \pmod 7$
2. $x \equiv 2 \pmod{11}$

Příklad 5. Určete inverzní zbytkové třídy k zadaným zbytkovým třídám

1. $[67]_{517}$
2. $[172]_{235}$
3. $[116]_{153}$
4. $[49]_{226}$

Výsledek.

1. $[463]_{517}$
2. $[138]_{235}$
3. $[62]_{153}$
4. $[143]_{226}$

Příklad 6. Určete

1. $\varphi(2010)$
2. $\varphi(1212)$

Výsledek.

1. 528
2. 400

Příklad 7. Určete všechna přirozená čísla n taková, že

1. $\varphi(n) = 6$
2. $\varphi(n) = 20$
3. $\varphi(n) = 11$

Výsledek.

1. $7, 9, 14, 18$
2. $25, 33, 44, 50, 66$
3. žádné neexistuje

Příklad 8. Určete všechna dvojciferná přirozená čísla n taková, že $9|\varphi(n)$

Výsledek. $19, 27, 37, 38, 54, 57, 63, 73, 74, 76, 81, 91, 95$

Příklad 9. Určete všechna přirozená čísla n taková, že

1. $\varphi(n) = \frac{n}{2}$
2. $\varphi(n) = \frac{n}{3}$

Nápověda: Napište n jako součin mocniny dvou (resp. tří) a čísla s dvojkou (resp. trojkou) nesoudělného.

Výsledek.

1. $n = 2^k$
2. $n = 2^k \cdot 3^l$

Příklad 10. Dokažte, že

1. je číslo $2^{60} + 7^{30}$ dělitelné 13.
2. pro libovolné $n \in \mathbb{N}$ je číslo $72^{2n+2} - 47^{2n} + 28^{2n-1}$ dělitelné číslem 25.

Příklad 11. Řešte soustavu kongruencí:

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 8 \pmod{11} \end{aligned}$$

Výsledek. $x \equiv -3 \pmod{55}$

Příklad 12. Řešte soustavu kongruencí:

$$\begin{aligned} 4x &\equiv 3 \pmod{7} \\ 5x &\equiv 4 \pmod{6} \end{aligned}$$

Výsledek. Nemá řešení.

Příklad 13. Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.

Výsledek. 12

Příklad 14. Určete poslední cifru čísla

1. $3^{5^{7^9}}$
2. $37^{37^{37}}$

Výsledek.

1. 3
2. 7

Příklad 15. Určete poslední dvě cifry čísla

1. 7^{9^9}
2. $14^{14^{14}}$

Výsledek.

1. 07
2. 36

Příklad 16. Určete zbytek po dělení čísla $5^{33} + 7^{33}$ číslem 17.

Výsledek. 12

Příklad 17. Určete zbytek po dělení čísla $2^{181} + 3^{181} + 5^{181}$ číslem 37.

Výsledek. 10

Příklad 18. Dokažte, že je pro každé přirozené číslo n číslo $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Příklad 19. Určete řád čísla 5 modulo 13.

Výsledek. 4

Příklad 20. Určete všechna přirozená čísla n, pro která je číslo $3^n + 4^n - 5^n$ dělitelné jedenácti.

Výsledek. $n \equiv 2 \pmod 5$