Democvičení

MB104 - 18. 2. 2013

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 říkáme 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 největší společný dělitel čísel a, b a určete příslušné koeficienty v Bezoutově rovnosti

1. $a = 113,\ b = 50$
2. $a = 3^{77} - 1,\ b = 3^{21} - 1$

Příklad 2. Určete $[17]_{78}^{-1}$.

Příklad 3. Určete $[2^k + 1]_{2^{2k}+1}^{-1}$.

Příklad 4. Určete všechna celá čísla x tak, aby

$$3x \equiv 5 \pmod{17}.$$

Příklad 5. Určete všechna celá čísla x tak, aby

$$37x \equiv 82 \pmod{105}.$$

Příklad 6. Skupině třinácti pirátů se podařilo uloupit bednu zlatých mincí. Zkusili je rozdělit rovným dílem na třináct hromádek, ale deset mincí jim zbylo. O zbylé mince se strhla rvačka, při níž jednoho piráta propíchli. Přestali tedy bojovat a zkusili mezi sebe znovu rozdělit mince rovným dílem. Tentokrát zbyly tři mince, o které opět začali bojovat. V boji zahynul další pirát a tak si ostatní opět zkusili mince spravedlivě rozdělit, tentokrát úspěšně. Na základě těchto informací určete nejmenší možný počet mincí, které mohla bedna obsahovat.

Příklad 7. Určete $\varphi(735)$.

Příklad 8. Určete poslední cifru čísla $13^{11^{9^7}}$.

Příklad 9. Určete zbytek po dělení čísla$2^{181} + 3^{181} + 5^{181}$ číslem 37.

Příklad 10. Dokažte, že pro všechna prvočísla p větší než 7 platí, že

$$p^{36} \equiv 1 \pmod{945}.$$

Příklad 11. Určete všechna $n \in \mathbb{N}$ tak, aby $\varphi(n) = \frac{n}{4}$.

Příklad 12. Určete všechna $n \in \mathbb{N}$ tak, aby $\varphi(n) = 6$.

Příklad 13. Určete všechna celá čísla x, y tak, aby

$$2^x = 11 + 7y.$$