Kongruence a aritmetické funkce

Pojem kongruence poprvé zavedl Gauss ve své knize *Disquisitiones Arithmeticae*, vydané roku 1801. Jedná se o velmi jednoduchý pojem, který je však v teorii čísel nedocenitelný. Aritmetické funkce jsou pak převážně aplikací věty **??** o jednoznačném rozkladu na součin prvočísel. Společně pak mohou vyjádřit i velmi složité myšlenky.

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

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

Pro vytvoření představy, co to vlastně kongruence je, slouží následující lemma:

Lemma 1. *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. $m \mid a - b$.

Shrnutí vlastností kongruencí uvádí následující věta:

Věta. *(Základní vlastnosti kongruencí)*

1. *Kongruence podle téhož modulu můžeme sčítat. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou. Na libovolnou stranu kongruence můžeme přičíst jakýkoliv násobek modulu.*
2. *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.*
3. *Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem.*

4. *Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.*

5. *Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.*

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

7. *Jestliže kongruence platí podle modulu m, platí podle libovolného modulu d, který je dělitelem čísla m.*

8. *Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana kongruence.*

Aritmetickou funkcí zde rozumíme funkci, jejímž definičním oborem je množina přirozených čísel. V předchozí kapitole jsme se setkali s aritmetickými funkcemi $\tau(n)$ a $\sigma(n)$, nyní uvedeme další, které jsou v teorii čísel důležité.

Definice. Rozložme přirozené číslo n na prvočísla: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hodnotu *Möbiovy funkce* $\mu(n)$ definujeme rovnu 0, pokud pro některé i platí $\alpha_i > 1$ a rovnu $(-1)^k$ v opačném případě. Dále definujeme $\mu(1) = 1$.

Definice. Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

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

Pro jednodušší výpočet Eulerovy funkce se používá následující věta.

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

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Pokud n je mocninou jednoho prvočísla, snadno lze ověřit, že platí

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1) \cdot p^{\alpha-1}.$$

Dalším důležitým pojmem je *multiplikativní funkce*.

Definice. Multiplikativní funkcí přirozených čísel rozumíme takovou aritmetickou funkci, která splňuje, že pro všechny dvojice nesoudělných čísel $a, b \in \mathbb{N}$ platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

Eulerova funkce φ je funkcí multiplikativní. Pro výpočet kongruencí je velmi důležitá, je tedy nutné říci proč.

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

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Věta (Fermatova, Malá Fermatova)**.** *Nechť* $a \in \mathbb{Z}$, p *prvočíslo,* $p \nmid a$. *Pak*

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

Definice. *Úplná soustava zbytků* modulo m je libovolná m-tice čísel po dvou nekongruentních modulo m (nejčastěji $0, 1, \ldots, m-1$).
Redukovaná soustava zbytků modulo m je libovolná $\varphi(m)$-tice čísel nesoudělných s m a po dvou nekongruentních modulo m.

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

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2}$$

Pro výpočet kongruencí je důležitý takzvaný *řád čísla modulo* m. Jak uvidíme, má také úzkou souvislost s Eulerovou funkcí.

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

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

Protože pro vyšší čísla by výpočet řádu podle uvedené definice byl zdlouhavý, používají se k výpočtům následující tvrzení.

Lemma 2. *Nechť* $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. *Jestliže* $a \equiv b \pmod{m}$, *pak obě čísla* a, b *mají stejný řád modulo* m.

Lemma 3. *Nechť* $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Je-li řád čísla* a *modulo* m *roven* $r \cdot s$, *(kde* $r, s \in \mathbb{N}$*), pak řád čísla* a^r *modulo* m *je roven* s.

Řád čísla slouží i k úpravám kongruencí, nebo k výpočtům, které vedou na jejich použití:

Věta. *Nechť* $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Označme* r *řád čísla* a *modulo* m. *Pak pro libovolná* $t, s \in \mathbb{N} \cup \{0\}$ *platí*

$$a^t \equiv a^s \pmod{m} \iff t \equiv s \pmod{r}.$$

Z následující věty je patrná souvislost s Eulerovou funkcí, zmiňovaná dříve.

Věta. *Nechť* $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Označme* r *řád čísla* a *modulo* m.

1. *Pro libovolné* $n \in \mathbb{N} \cup \{0\}$ *platí*

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

2. $r \mid \varphi(m)$

Následující věta je zobecněním předchozí věty a lemmatu **??**.

Věta. *Nechť* $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Je-li řád čísla* a *modulo* m *roven* $r \in \mathbb{N}$, *je řád čísla* a^n *modulo* m *roven* $\frac{r}{(n,r)}$.