19. OPERÁCIE MODULO M

V kapitole o kongruenciách sme videli, že niekedy nás ani nezaujímajú konkrétne čísla, ale iba ich zvyšky po delení nejakým číslom. V danej kapitole sme vytvorili na ich skúmanie určitý aparát. Teraz si ukážeme, ako môžeme tento aparát zjednodušiť pomocou formálnych úprav. Pripomeňme si, že pre $n \in \mathbb{N}$ máme definované množiny $\mathbb{Z}_m$ a $\mathbb{R}_m$, pričom $\mathbb{R}_m \subset \mathbb{Z}_m$.

Nech $m \in \mathbb{N}$, $m > 1$. Na množine $\mathbb{Z}_m$ si zadefinujeme operácie sčítania modulo m a násobenia modulo m nasledovne: Ak $a, b \in \mathbb{Z}_m$, potom

$$a \oplus_m b = a + b \mod m, \; a \odot_m b = a \cdot b \mod m.$$

Teda namiesto súčtu dvoch čísel budeme počítať jeho zvyšok po delení m a namiesto súčinu dvoch čísel budeme počítať jeho zvyšok po delení m.

Úloha 409. Nech $a, b, c \in \mathbb{Z}_m$. Dokážte, že platí:
$a \oplus_m b = b \oplus_m a$, $a \odot_m b = b \odot_m a$,
$(a \oplus_m b) \oplus_m c = a \oplus_m (b \oplus_m c)$,
$(a \odot_m b) \odot_m c = a \odot_m (b \odot_m c)$,
$(a \oplus_m b) \odot_m c = (a \odot_m c) \oplus_m (b \odot_m c)$,
$a \oplus_m 0 = a$, $a \oplus_m (m - a) = 0$,
$a \odot_m 1 = a$.

Tvrdenie v úlohe 409 nám hovorí, že $\mathbb{Z}_m$ tvorí vzhľadom na operácie $\oplus_m, \odot_m$ komutatívny okruh s jednotkou. O tom budeme hovoriť neskôr.

Pretože zápis pomocou symbolov $\oplus_m, \odot_m$ je pomerne komplikovaný a neprehľadný, budeme v prípadoch, keď nehrozí nedorozumenie, používať pre tieto operácie obyčajné symboly pre sčítanie a násobenie. Budeme teda predpokladať, že je dané číslo $m \in \mathbb{N}, m > 1$ a budeme používať označenia

$$a \oplus_m b = a + b \; , \; a \odot_m b = a \cdot b.$$

Úloha 410. Dokážte, že $a \in \mathbb{R}_m$ práve vtedy, keď existuje také číslo $a' \in \mathbb{Z}_m$, že $a \cdot a' = 1$. Dokážte, že v tomto prípade existuje jediné takéto číslo a'.

(Návod: Použite úlohu 128.)

Prvok a' z úlohy 410 budeme nazývať inverzným prvkom k a modulo m a budeme ho označovať a^{-1}.

Úloha 411. Dokážte, že ak $a, b \in \mathbb{R}_m$, potom aj $a \cdot b \in \mathbb{R}_m$.

Úloha 412. Nech $a \in \mathbb{R}_m$ a $b, c \in \mathbb{Z}_m$. Ak

$$a \cdot b = a \cdot c$$

potom

$$b = c.$$

Dokážte.

(Návod: Použite úlohu 410.)

Podobne ako pomocou násobenia celých čísel môžeme definovať mocninu, aj tu môžeme definovať mocninu pomocou operácie $\odot_m$. Ak $n \in \mathbb{N}$, potom

$$(a^n)_m = a \odot_m ... \odot_m a, \text{(} n \text{ činiteľov)}.$$

Úloha 413.
a) Dokážte, že pre $a \in \mathbb{Z}_m$, $n \in \mathbb{N}$ platí

$$(a^n)_m \equiv a^n \pmod{m}.$$

b) Dokážte, že pre n_1, n_2 platí

$$(a^{n_1})_m \cdot (a^{n_2})_m = (a^{n_1+n_2})_m$$

a

$$(((a^{n_1})_m)^{n_2})_m = (a^{n_1 n_2})_m.$$

Pre jednoduchosť budeme namiesto $(a^n)_m$ písať iba a^n.

Teraz sa budeme zaoberať dôkazom Eulerovej vety (vety 7) iným spôsobom, ako sme ju dokazovali v kapitole o kongruenciách.

Úloha 414. Dokážte, že Eulerova veta je ekvivalentná s rovnosťou

$$a^{\varphi(m)} = 1$$

pre každé $a \in \mathbb{R}_m$.

Úloha 415. Dokážte, že pre každé $a \in \mathbb{R}_m$ existuje také číslo k, že $0 < k \leq \varphi(m)$ a

$$a^k = 1.$$

(Návod: Postupnosť $1, a, a^2, ..., a^{\varphi(m)}$ obsahuje aspoň dva rovnaké prvky.)

Označme pre $a \in \mathbb{R}_m$

$$rad_m a = \min\{k > 0, a^k = 1\}.$$

Úloha 416. Dokážte, že pre $a \in \mathbb{R}_m$ platí

$$a^{k+rad_m a} = a^k.$$

Označme pre $a \in \mathbb{R}_m$

$$[a] = \{1, a, ..., a^{rad_m a - 1}\}.$$

Úloha 417. Dokážte, že pre $a \in \mathbb{R}_m$ platí

$$|[a]| = rad_m a.$$

Nech $H \subset \mathbb{R}_m, b \in \mathbb{R}_m$. Označme

$$bH = \{b \cdot h; h \in H\}.$$

Úloha 418. Nech $a \in \mathbb{R}_m$ a $b \in \mathbb{R}_m$. Dokážte, že

$$|b[a]| = rad_m a.$$

(Návod: Použite úlohy 417 a 410.)

Úloha 419. Nech $b_1, b_2, a \in \mathbb{R}_m$. Ak $b_1[a] \cap b_2[a] \neq \emptyset$, potom existujú také čísla $0 \leq r_1, r_2 \leq rad_m a$, že

$$b_1 = b_2 \cdot a^{r_2},\ b_2 = b_1 \cdot a^{r_1}.$$

Dokážte.

Úloha 420. Nech $b_1, b_2, a \in \mathbb{R}_m$. Potom buď $b_1[a] \cap b_2[a] = \emptyset$ alebo $b_1[a] = b_2[a]$. Dokážte.

(Návod: Použite úlohu 419.)

Úloha 421. Nech $a \in \mathbb{R}_m$. Nech k označuje počet rôznych prvkov množiny $\{b[a]; b \in \mathbb{R}_m\}$. Dokážte, že

$$k \cdot rad_m a = \varphi(m).$$

(Návod: Použite úlohy 420, 421 a to, že $b \in b[a]$.)

Úloha 422. Dokážte, že pre $a \in \mathbb{R}_m$ platí

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

(Návod: Použite úlohu 421.)

Úloha 423. Dokážte Eulerovu vetu (vetu 7).