Cela števila

Def. 1: Na kartezičnem produktu $\mathbb{N} \times \mathbb{N}$ definirajmo binarno relacijo $\sim$ s predpisom: $(m_1, n_1) \sim (m_2, n_2) \iff m_1 + n_2 = n_1 + m_2$.

Posledica 1. Relacija $\sim$ je ekvivalenčna relacija. **Ekvivalenčni razred** s predstavnikom (m, n) bomo označevali z $[m, n]$. Množici vseh dobljenih ekvivalenčnih razredov pravimo **cela števila** (oznaka: $\mathbb{Z}$).

Def. 2: Računski operaciji seštevanja in množenja na množici $\mathbb{Z}$ podamo s predpisoma: $[m_1, n_1] \oplus [m_2, n_2] = [m_1 + m_2, n_1 + n_2]$, $[m_1, n_1] \odot [m_2, n_2] = [m_1 m_2 + n_1 n_2, m_1 n_2 + n_1 m_2]$.

Posledica 2. Obe navedeni definiciji sta **korektni** (**neodvisni** od izbire predstavnikov). V nadaljevanju bomo obe operaciji zapisovali z običajnima znakoma za seštevanje oziroma množenje.

Izrek 1. Operaciji seštevanja in množenja sta asociativni in komutativni, povezuje pa ju distributivnostni zakon. Obstajata tudi nevtralna elementa za seštevanje ($0 = [n, n]$) in za množenje ($1 = [n + 1, n]$). Poleg tega ima vsako celo število **nasprotno**: $-[m, n] = [n, m]$, vsa neničelna cela števila pa so regularna glede na operacijo množenja ($ax = ay \Rightarrow x = y$).

Def. 3: Na množici $\mathbb{Z}$ definiramo relacijo urejenosti s predpisom: $[m_1, n_1] < [m_2, n_2] \iff m_1 + n_2 < n_1 + m_2$, relacijo deljivosti pa enako kot na množici $\mathbb{N}$.

Posledica 3. Relacija "strogo manjši" strogo linearno ureja množico celih števil, ki jih po primerjavi s številom 0 razdelimo na **pozitivna** in **negativna**. Neenakosti dopuščajo **krajšanje** z enakim seštevancem ali pozitivnim množencem, pri krajšanju z negativnim faktorjem pa se neenakost obrne.

Posledica 4. Pozitivna cela števila so izomorfna z $\mathbb{N}$. Zato je $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$.

Def. 4: Vpeljimo na množico $\mathbb{Z}$ še družino **kongruenčnih** relacij. Naj bo za določeno naravno število $m > 1$ (pravimo mu **modul**) $a \equiv b \bmod m$ natanko tedaj, ko data celi števili a in b pri deljenju z m enaka ostanka.

Posledica 5. $a \equiv b \bmod m \iff m | a - b$. Vse kongruence so ekvivalenčne relacije.

Izrek 2. Če cela števila a, b, c, d zadoščajo kongruencama $a \equiv b \bmod m$ in $c \equiv d \bmod m$, veljata tudi kongruenci $a + c \equiv b + d \bmod m$ in $ac \equiv bd \bmod m$.

Izrek 3. $a \equiv b \bmod m$ natanko tedaj, ko je $ca \equiv cb \bmod cm$ za poljubno naravno število c. Iz $a \equiv b \bmod m$ sledi $a \equiv b \bmod n$ za vsak $n > 1$, ki deli število m. V primeru, ko je $\mathrm{D}(c, m) = 1$, iz kongruence $ca \equiv cb \bmod m$ sledi $a \equiv b \bmod m$.

Def. 5: Na **polni množici ostankov** $\mathbb{Z}_m = \{[0], [1], \ldots, [m - 1]\}$ pri deljenju s številom $m > 1$ imamo inducirani operaciji seštevanja in množenja: $[a] \oplus [b] = [a + b]$ in $[a] \odot [b] = [ab]$. (Korektnost obeh definicij nam jamči osnovna lastnost kongruenc - izrek 2.)

Izrek 4. Polna množica ostankov pri deljenju s poljubnim modulom m tvori z induciranima operacijama seštevanja in množenja komutativen kolobar, v primeru praštevila m pa (končno) polje.

Def. 6: Predstavniki **reducirane** množice ostankov po modulu m so naravna števila k, manjša od m, za katera velja $\mathrm{D}(k, m) = 1$. Taka množica ostankov ima torej moč $\varphi(m)$.

Izrek 5 (Euler). Za poljubno celo število a, tuje z modulom m, velja: $a^{\varphi(m)} \equiv 1 \bmod m$.