

Posledica 6 (Fermat). Kadar je p praštevilo, imamo $\forall a \in \mathbb{Z} \quad a^p \equiv a \pmod{p}$, oziroma, če a ni večkratnik števila p , $a^{p-1} \equiv 1 \pmod{p}$.

Izrek 6. Linearna kongruenca $ax \equiv b \pmod{m}$, $D(a, m) = 1$, ima natanko eno rešitev (po modulu m), ki jo lahko najdemo, na primer, z Evklidovim algoritmom.

Izrek 7. V primeru, ko je $D(a, m) = d > 1$, ima linearna kongruenca $ax \equiv b \pmod{m}$ natanko d rešitev po modulu m , če $d|b$, sicer pa je nerešljiva.

Racionalna števila (ulomki)

Def. 1: Na kartezičnem produktu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definiramo binarno relacijo \sim s predpisom: $(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = b_1 a_2$.

Posledica 1. Relacija \sim je ekvivalenčna relacija. **Ekvivalenčni razred** s predstavnikom (a, b) bomo označevali z $\frac{a}{b}$. Množici vseh dobljenih ekvivalenčnih razredov pravimo **racionalna števila** (oznaka: \mathbb{Q}).

Def. 2: Računski operaciji seštevanja in množenja na množici \mathbb{Q} podamo s predpisoma: $\frac{a}{b} \oplus \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd}$.

Posledica 2. Obe navedeni operaciji sta korektno definirani. V nadaljevanju ju bomo zapisovali z običajnim znakoma za seštevanje oziroma množenje.

Izrek 1. Operaciji seštevanja in množenja ulomkov sta asociativni in komutativni, povezuje pa ju distributivnostni zakon. Nevtralna elementa za seštevanje in za množenje sta $\frac{0}{1}$ oziroma $\frac{1}{1}$. Vsako racionalno število ima **nasprotno**: $-\frac{a}{b} = \frac{-a}{b}$, vsak neničelni ulomek pa obratnega: $(\frac{a}{b})^{-1} = \frac{b}{a}$. Množica ulomkov z danima operacijama je torej polje.

Izrek 2. Vsako racionalno število lahko na en sam način predstavimo v obliki **okrajšanega** ulomka $\frac{a}{b}$, $D(a, b) = 1$. Množica racionalnih števil je števno neskončna.

Def. 3: Na množici \mathbb{Q} definiramo relacijo urejenosti s predpisom: $\frac{a}{b} < \frac{c}{d} \iff (ad-bc)bd < 0$.

Posledica 3. Relacija "strogo manjši" strogo linearno ureja množico racionalnih števil. Množica \mathbb{Q} je **gosta**, saj med poljubnima dvema ulomkoma obstaja element (neskončno elementov) iz te množice.

Posledica 4. Ulomki z imenovalcem 1 so izomorfni z množico celih števil. Zato je $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Izrek 2. Vsako racionalno število ima **končen** ali **periodičen neskončen mestni** (decimalni) **zapis**.

Izrek 3. Vsako racionalno število se da zapisati v obliki **verižnega** ulomka:

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_k}}}}, \quad q_i \in \mathbb{N}, i = 1, 2, \dots, k.$$

Za števce in imenovalce delnih ulomkov $\frac{P_i}{Q_i}$ pri tem veljata rekurzivni povezavi:

$$P_i = q_{i-1}P_{i-1} + P_{i-2}, \quad Q_i = q_{i-1}Q_{i-1} + Q_{i-2}, \quad i = 2, 3, \dots, k, \quad (P_0 = 1, Q_0 = 0).$$

Izrek 4. Obstajajo iracionalna števila. Množica \mathbb{Q} **ni polna**, ker iz njenih elementov lahko sestavimo Cauchyjeva zapredja, ki v \mathbb{Q} nimajo limite.

Posledica 5. Množica iracionalnih števil je več kot števno neskončna - ima **moč kontinuuma**.

Def. 4: Množico vseh decimalnih zapisov (končnih in neskončnih) imenujemo **realna** števila (oznaka: \mathbb{R}).