ELTE IK Diszkrét modellek alkalmazásai

3. gyakorlat

Koch-Gömöri Richárd

2020. október 1.

Számelmélet

def (oszthatóság): A $b \in \mathbb{Z}$ számot az $a \in \mathbb{Z}$ szám osztójának nevezzük, ha $\exists q \in \mathbb{Z} : a = b \cdot q$

jelölés: $b \mid a$

pl. $2 \mid 6$ mert $6 = 2 \cdot 3$

def (prímszám): Legyen $p \in \mathbb{Z}, p \neq -1, p \neq 0, p \neq 1$. A p számot prímnek nevezzük, ha $\forall b, c \in \mathbb{Z} : p \mid b \cdot c \implies p \mid b \vee p \mid c$

pl. a 4 prím-e? pl. $4 \mid 12 = 3 \cdot 4$, következik-e ebből h $4 \mid 3 \vee 4 \mid 4$?

$4 \mid 3$ hamis de az igaz h $4 \mid 4$

pl. a 4 nem prím, mert pl. $4 \mid 12 = 2 \cdot 6$ de nem igaz h $4 \mid 2 \vee 4 \mid 6$

pl. a 7 prím, mert a $7 \mid 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)$

esetekből következik h $7 \mid 7$ vagy $7 \mid (-7)$, más $b \cdot c$ szorzat csak valamelyik többszöröse lehet

Számelmélet

tétel (maradékos osztás): Tetszőleges $a \in \mathbb{Z}$ és $0 \neq b \in \mathbb{Z}$ számokhoz $\exists | q, r \in \mathbb{Z}$ amelyekre $a = b \cdot q + r \wedge 0 \leq r < |b|$

jelölés: $a \mod b := r$

pl. 14 osztása 3-mal:

hányados: 4, maradék: 2

mert $14 = 3 \cdot 4 + 2$

$14 \mod 3 = 2$

Számelmélet

tétel (a számelmélet alaptétele): Minden nem $-1, 0, 1$ egész szám véges sok prím szorzatára bontható, és ez a felbontás a tényezők sorrendjétől és azok előjelétől eltekintve egyértelmű.

pl. $18 = 2 \cdot 3 \cdot 3$

def (összetett szám): A nem $-1, 0, 1$ és nem prímszámokat összetett számoknak nevezzük.

tétel: A prímszámok száma végtelen.

tétel: Tetszőleges pozitív egész N számhoz megadható egy legalább N hosszú csupa összetett számot tartalmazó intervallum.

($\Longrightarrow$ a prímszámok között tetszőlegesen nagy hézagok lehetnek)

tétel (prímszámtétel): Jelölje $\pi(x)$ az x-ig terjedő prímszámok számát. Ekkor:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

($\Longrightarrow$ a prímszámok sűrűn helyezkednek el)