

Bevezetés a Számításelméletbe II. 8. előadás

Sali Attila

Budapest Műszaki és Gazdaságtudományi Egyetem

Számítástudományi Tsz.

I. B. 137/b

`sali@cs.bme.hu`

2002 április 2.

Oszthatóság

Oszthatóság

Az $a \in \mathbb{Z}$ szám **osztja** a $b \in \mathbb{Z}$ számot, ha van $c \in \mathbb{Z}$, hogy $b = a \cdot c$, jelölésben $a \mid b$.

Az $a(x) \in \mathbb{R}[x]$ polinom **osztja** a $b(x) \in \mathbb{R}[x]$ polinomot, ha van $c(x) \in \mathbb{R}[x]$, hogy $b(x) = a(x) \cdot c(x)$, jelölésben $a(x) \mid b(x)$.

Oszthatóság

Az $a \in \mathbb{Z}$ szám **osztja** a $b \in \mathbb{Z}$ számot, ha van $c \in \mathbb{Z}$, hogy $b = a \cdot c$, jelölésben $a \mid b$.
Az oszthatóság tranzitív és reflexív.

Az $a(x) \in \mathbb{R}[x]$ polinom **osztja** a $b(x) \in \mathbb{R}[x]$ polinomot, ha van $c(x) \in \mathbb{R}[x]$, hogy $b(x) = a(x) \cdot c(x)$, jelölésben $a(x) \mid b(x)$.
Az oszthatóság tranzitív és reflexív.

Oszthatóság

Az $a \in \mathbb{Z}$ szám **osztja** a $b \in \mathbb{Z}$ számot, ha van $c \in \mathbb{Z}$, hogy $b = a \cdot c$, jelölésben $a \mid b$.

Az oszthatóság tranzitív és reflexív.

Maradékos osztás: $\forall a \in \mathbb{Z}, b \in \mathbb{N} \exists$ egyértelmű $q, r \in \mathbb{Z}: a = bq + r \quad 0 \leq r < b$.

Az $a(x) \in \mathbb{R}[x]$ polinom **osztja** a $b(x) \in \mathbb{R}[x]$ polinomot, ha van $c(x) \in \mathbb{R}[x]$, hogy $b(x) = a(x) \cdot c(x)$, jelölésben $a(x) \mid b(x)$.

Az oszthatóság tranzitív és reflexív.

Maradékos osztás: $\forall a(x), b(x) \in \mathbb{R}[x] \exists$ egyértelmű $q(x), r(x) \in \mathbb{R}[x]: a(x) = b(x)q(x) + r(x) \quad 0 \leq \deg r(x) < \deg b(x)$.

Oszthatóság

Az $a \in \mathbb{Z}$ szám **osztja** a $b \in \mathbb{Z}$ számot, ha van $c \in \mathbb{Z}$, hogy $b = a \cdot c$, jelölésben $a \mid b$.

Az oszthatóság tranzitív és reflexív.

Maradékos osztás: $\forall a \in \mathbb{Z}, b \in \mathbb{N} \exists$ egyértelmű $q, r \in \mathbb{Z}: a = bq + r \quad 0 \leq r < b$.

Például:

$$\begin{array}{lll} 177 & = & 14 \cdot 12 + 9 \quad 0 < 9 < 14 \\ -64 & = & 14 \cdot (-5) + 6 \quad 0 < 6 < 14 \\ 154 & = & 14 \cdot 11 + 0 \quad 0 = 0 < 14 \end{array}$$

Az $a(x) \in \mathbb{R}[x]$ polinom **osztja** a $b(x) \in \mathbb{R}[x]$ polinomot, ha van $c(x) \in \mathbb{R}[x]$, hogy $b(x) = a(x) \cdot c(x)$, jelölésben $a(x) \mid b(x)$.

Az oszthatóság tranzitív és reflexív.

Maradékos osztás: $\forall a(x), b(x) \in \mathbb{R}[x] \exists$ egyértelmű $q(x), r(x) \in \mathbb{R}[x]: a(x) = b(x)q(x) + r(x) \quad 0 \leq \deg r(x) < \deg b(x)$.

Például

$$\begin{array}{lll} x^5 + x^3 + x^2 + 2x + 2 & = & (x^2 + 1)(x^3 + 1) + (2x + 1) \quad 0 < \deg(2x + 1) < \deg(x^2 + 1) \\ 5x^3 + 8x^2 + 3 & = & (x^2 + 1)(5x + 3) + 0 \quad 0 = \deg(0) < \deg(x^2 + 1) \end{array}$$

Legnagyobb közös osztó

Ha d osztja az a_1, a_2, \dots, a_k számokat, akkor *közös osztójuknak* nevezzük. Ezek közül a legnagyobb a *legnagyobb közös osztó*, jelölésben: (a_1, a_2, \dots, a_k) .

Ha $d(x)$ osztja az $a(x)_1, a(x)_2, \dots, a(x)_k$ polinomokat, akkor *közös osztójuknak* nevezzük. Ezek közül a legnagyobb fokú (amely konstans szorzó erejéig egyértelmű) a *legnagyobb közös osztó*, jelölésben: $(a(x)_1, a(x)_2, \dots, a(x)_k)$.

Legnagyobb közös osztó

Ha d osztja az a_1, a_2, \dots, a_k számokat, akkor *közös osztójuknak* nevezzük. Ezek közül a legnagyobb a *legnagyobb közös osztó*, jelölésben: (a_1, a_2, \dots, a_k) .

Ha a többszöröse b -nek, akkor akkor a és b közös osztóinak halmaza megegyezik b osztóinak halmazával. Speciálisan $(a, b) = b$.

Ha $d(x)$ osztja az $a(x)_1, a(x)_2, \dots, a(x)_k$ polinomokat, akkor *közös osztójuknak* nevezzük. Ezek közül a legnagyobb fokú (amely konstans szorzó erejéig egyértelmű) a *legnagyobb közös osztó*, jelölésben: $(a(x)_1, a(x)_2, \dots, a(x)_k)$.

Ha $a(x)$ többszöröse $b(x)$ -nek, akkor akkor $a(x)$ és $b(x)$ közös osztóinak halmaza megegyezik $b(x)$ osztóinak halmazával. Speciálisan $(a(x), b(x)) = b(x)$.

Legnagyobb közös osztó

Ha d osztja az a_1, a_2, \dots, a_k számokat, akkor **közös osztójuknak** nevezzük. Ezek közül a legnagyobb a **legnagyobb közös osztó**, jelölésben: (a_1, a_2, \dots, a_k) .

Ha a többszöröse b -nek, akkor akkor a és b közös osztóinak halmaza megegyezik b osztóinak halmazával. Speciálisan $(a, b) = b$.

Ha $a = bq + c$, akkor a és b közös osztóinak halmaza megegyezik b és c közös osztóinak halmazával. Speciálisan, $(a, b) = (b, c)$.

Ha $d(x)$ osztja az $a(x)_1, a(x)_2, \dots, a(x)_k$ polinomokat, akkor **közös osztójuknak** nevezzük. Ezek közül a legnagyobb fokú (amely konstans szorzó erejéig egyértelmű) a **legnagyobb közös osztó**, jelölésben: $(a(x)_1, a(x)_2, \dots, a(x)_k)$.

Ha $a(x)$ többszöröse $b(x)$ -nek, akkor akkor $a(x)$ és $b(x)$ közös osztóinak halmaza megegyezik $b(x)$ osztóinak halmazával. Speciálisan $(a(x), b(x)) = b(x)$.

Ha $a(x) = b(x)q(x) + c$, akkor $a(x)$ és $b(x)$ közös osztóinak halmaza megegyezik $b(x)$ és $c(x)$ közös osztóinak halmazával. Speciálisan, $(a(x), b(x)) = (b(x), c(x))$.

Euklideszi algoritmus

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$a = h_1 b + m_1 \quad (0 \leq m_1 < b)$$

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{ll} a &= h_1 b + m_1 & (0 \leq m_1 < b) \\ b &= h_2 m_1 + m_2 & (0 \leq m_2 < m_1) \end{array}$$

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{lll} a & = & h_1 b + m_1 \quad (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 \quad (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 \quad (0 \leq m_3 < m_2) \end{array}$$

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{lll} a & = & h_1 b + m_1 & (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 & (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 & (0 \leq m_3 < m_2) \\ & \vdots & & \vdots \end{array}$$

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{lll} a & = & h_1 b + m_1 & (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 & (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 & (0 \leq m_3 < m_2) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2} = h_n m_{n-1}$$

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{lll} a & = & h_1 b + m_1 & (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 & (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 & (0 \leq m_3 < m_2) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2} = h_n m_{n-1}$$

$m_{n-3} = h_{n-1} m_{n-2} + m_{n-1} = (h_{n-1} h_n + 1) m_{n-1}$, ... a és b is m_{n-1} többszöröse lesz,
 $\implies m_{n-1}$ közös osztója a -nak és b -nek.

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{lll} a & = & h_1 b + m_1 \quad (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 \quad (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 \quad (0 \leq m_3 < m_2) \\ & \vdots & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2} = h_n m_{n-1}$$

$m_{n-3} = h_{n-1} m_{n-2} + m_{n-1} = (h_{n-1} h_n + 1) m_{n-1}$, ... a és b is m_{n-1} többszöröse lesz,
 $\implies m_{n-1}$ közös osztója a -nak és b -nek. Megfordítva, a és b tetszőleges közös osztója m_1 -nek is osztója ... m_{n-1} -nek is. Tehát $m_{n-1} = (a, b)$.

Euklideszi algoritmus

Legyen $a, b \in \mathbb{N}$.

$$\begin{array}{rcll} a & = & h_1 b + m_1 & (0 \leq m_1 < b) \\ b & = & h_2 m_1 + m_2 & (0 \leq m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 & (0 \leq m_3 < m_2) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2} = h_n m_{n-1}$$

$m_{n-3} = h_{n-1} m_{n-2} + m_{n-1} = (h_{n-1} h_n + 1) m_{n-1}$, ... a és b is m_{n-1} többszöröse lesz,
 $\implies m_{n-1}$ közös osztója a -nak és b -nek. Megfordítva, a és b tetszőleges közös osztója m_1 -nek is osztója ... m_{n-1} -nek is. Tehát $m_{n-1} = (a, b)$. Másképp: $(a, b) = (b, m_1) = (m_1, m_2) = \dots = (m_{n-2}, m_{n-1}) = m_{n-1} \implies a$ és b közös osztóinak halmaza megegyezik legnagyobb közös osztójuk osztóinak halmazával.

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$a(x) = h_1(x)b(x) + m_1(x) \quad (0 \leq \deg m_1(x) < \deg b(x))$$

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{ll} a(x) &= h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) &= h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \end{array}$$

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \end{array}$$

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \\ & \vdots & & \vdots \end{array}$$

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2}(x) = h_n(x)m_{n-1}(x)$$

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2}(x) = h_n(x)m_{n-1}(x)$$

$m_{n-3}(x) = h_{n-1}(x)m_{n-2}(x) + m_{n-1}(x) = (h_{n-1}(x)h_n(x) + 1)m_{n-1}(x)$, ... $a(x)$ és $b(x)$ is $m_{n-1}(x)$ többszöröse lesz, $\implies m_{n-1}(x)$ közös osztója $a(x)$ -nak és $b(x)$ -nek.

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2}(x) = h_n(x)m_{n-1}(x)$$

$m_{n-3}(x) = h_{n-1}(x)m_{n-2}(x) + m_{n-1}(x) = (h_{n-1}(x)h_n(x) + 1)m_{n-1}(x)$, ... $a(x)$ és $b(x)$ is $m_{n-1}(x)$ többszöröse lesz, $\implies m_{n-1}(x)$ közös osztója $a(x)$ -nak és $b(x)$ -nek. Megfordítva, $a(x)$ és $b(x)$ tetszőleges közös osztója $m_1(x)$ -nek is osztója ... $m_{n-1}(x)$ -nek is. Tehát $m_{n-1}(x) = (a(x), b(x))$.

Euklideszi algoritmus, polinomokkal

Legyen $a(x), b(x) \in \mathbb{R}[x]$.

$$\begin{array}{lll} a(x) & = & h_1(x)b(x) + m_1(x) & (0 \leq \deg m_1(x) < \deg b(x)) \\ b(x) & = & h_2(x)m_1(x) + m_2(x) & (0 \leq \deg m_2(x) < \deg m_1(x)) \\ m_1(x) & = & h_3(x)m_2(x) + m_3(x) & (0 \leq \deg m_3(x) < \deg m_2(x)) \\ & \vdots & & \vdots \end{array}$$

Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2}(x) = h_n(x)m_{n-1}(x)$$

$m_{n-3}(x) = h_{n-1}(x)m_{n-2}(x) + m_{n-1}(x) = (h_{n-1}(x)h_n(x) + 1)m_{n-1}(x)$, ... $a(x)$ és $b(x)$ is $m_{n-1}(x)$ többszöröse lesz, $\implies m_{n-1}(x)$ közös osztója $a(x)$ -nak és $b(x)$ -nek. Megfordítva, $a(x)$ és $b(x)$ tetszőleges közös osztója $m_1(x)$ -nek is osztója ... $m_{n-1}(x)$ -nek is. Tehát $m_{n-1}(x) = (a(x), b(x))$. Másképp: $(a(x), b(x)) = (b(x), m_1(x)) = (m_1(x), m_2(x)) = \dots = (m_{n-2}(x), m_{n-1}(x)) = m_{n-1}(x) \implies a(x)$ és $b(x)$ közös osztóinak halmaza megegyezik legnagyobb közös osztójuk osztóinak halmazával.

LNKO tulajdonságai

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc$

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$. Fordítva, $(c, b) \mid ac$ és $(c, b) \mid b$, azaz $(c, b) \mid (ac, b)$.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$. Fordítva, $(c, b) \mid ac$ és $(c, b) \mid b$, azaz $(c, b) \mid (ac, b)$. Tehát (ac, b) és (c, b) kölcsönösen osztják egymást, azaz egyenlőek.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$. Fordítva, $(c, b) \mid ac$ és $(c, b) \mid b$, azaz $(c, b) \mid (ac, b)$. Tehát (ac, b) és (c, b) kölcsönösen osztják egymást, azaz egyenlőek.

A második esetben $(ac, b) = (c, b)$ és $b \mid ac \implies (ac, b) = b$, azaz $(c, b) = b \implies b \mid c$.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$. Fordítva, $(c, b) \mid ac$ és $(c, b) \mid b$, azaz $(c, b) \mid (ac, b)$. Tehát (ac, b) és (c, b) kölcsönösen osztják egymást, azaz egyenlőek.

A második esetben $(ac, b) = (c, b)$ és $b \mid ac \implies (ac, b) = b$, azaz $(c, b) = b \implies b \mid c$.

Ha $(a, b) = 1$, akkor a és b **relatív prímeknek** neveztetnek.

LNKO tulajdonságai

1. Állítás. 1. $\forall a, b, m \in \mathbb{N} \quad (am, bm) = (a, b)m$

2. Ha d közös osztója a -nak és b -nek, akkor $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$, speciálisan $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

BIZONYÍTÁS Az Euklideszi algoritmusban minden egyenletet m -el megszorozunk.

2. Állítás. Ha $(a, b) = 1$, akkor $(ac, b) = (c, b)$. Ha $(a, b) = 1$, és $b \mid ac$, akkor $b \mid c$.

BIZONYÍTÁS $(ac, b) \mid ac$ és $(ac, b) \mid bc \implies (ac, b) \mid (ac, bc) = (a, b)c = c$. $(ac, b) \mid b \implies (ac, b) \mid (c, b)$. Fordítva, $(c, b) \mid ac$ és $(c, b) \mid b$, azaz $(c, b) \mid (ac, b)$. Tehát (ac, b) és (c, b) kölcsönösen osztják egymást, azaz egyenlőek.

A második esetben $(ac, b) = (c, b)$ és $b \mid ac \implies (ac, b) = b$, azaz $(c, b) = b \implies b \mid c$.

Ha $(a, b) = 1$, akkor a és b **relatív prímeknek** nevezetnek.

3. Következmény. Ha az a_1, a_2, \dots, a_m számok mindegyike relatív prím a b_1, b_2, \dots, b_n számok mindegyikével, akkor az $a_1 a_2 \dots a_m$ szorzat is relatív prím a $b_1 b_2 \dots b_n$ szorzathoz.

Legkisebb közös többszörös

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.
Legyen $(a, b) = d$, M az a és b egy közös többszöröse.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak, \frac{ak}{b}$ egész.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak, \frac{ak}{b}$ egész. $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak$, $\frac{ak}{b}$ egész. $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$. $\frac{ak}{b} = \frac{a_1k}{b_1} \implies k$ osztható b_1 -el: $k = b_1t = \frac{b}{d}t$, ahol t egész.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak, \frac{ak}{b}$ egész. $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$. $\frac{ak}{b} = \frac{a_1k}{b_1} \implies k$ osztható b_1 -el: $k = b_1t = \frac{b}{d}t$, ahol t egész. \implies

$$M = \frac{ab}{d}t$$

a és b összes közös többszöröse ilyen alakú.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak, \frac{ak}{b}$ egész. $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$. $\frac{ak}{b} = \frac{a_1k}{b_1} \implies k$ osztható b_1 -el: $k = b_1t = \frac{b}{d}t$, ahol t egész. \implies

$$M = \frac{ab}{d}t$$

a és b összes közös többszöröse ilyen alakú.

4. Állítás. Két szám közös többszörösei egybe esnek legkisebb közös többszörösük többszöröseivel. Két szám legkisebb közös többszöröse egyenlő szorzatuk és legnagyobb közös osztójuk hányadosával: $\text{l.k.k.t.}(a, b) = \frac{ab}{(a, b)}$ Speciálisan, páronként relatív prím számok legkisebb közös többszöröse egyenlő a szorzatukkal.

Legkisebb közös többszörös

A legkisebb pozitív közös többszörös a *legkisebb közös többszörös*.

Legyen $(a, b) = d$, M az a és b egy közös többszöröse. $\implies M = ak, \frac{ak}{b}$ egész. $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$. $\frac{ak}{b} = \frac{a_1k}{b_1} \implies k$ osztható b_1 -el: $k = b_1t = \frac{b}{d}t$, ahol t egész. \implies

$$M = \frac{ab}{d}t$$

a és b összes közös többszöröse ilyen alakú.

4. Állítás. Két szám közös többszörösei egybe esnek legkisebb közös többszörösük többszöröseivel. Két szám legkisebb közös többszöröse egyenlő szorzatuk és legnagyobb közös osztójuk hányadosával: $\text{l.k.k.t.}(a, b) = \frac{ab}{(a, b)}$ Speciálisan, páronként relatív prím számok legkisebb közös többszöröse egyenlő a szorzatukkal.

Legnagyobb közös osztóra és legkisebb közös többszörösre vonatkozó állítások számok helyett polinomokkal is érvényesek.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója. Ha q nem törzsszám, akkor van $1 < q_1 < q$ osztója.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója. Ha q nem törzsszám, akkor van $1 < q_1 < q$ osztója. Ekkor $q_1 \mid a$, ellentmondás.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója. Ha q nem törzsszám, akkor van $1 < q_1 < q$ osztója. Ekkor $q_1 \mid a$, ellentmondás.

7. Állítás. $\text{Prím} \implies \text{törzsszám}$.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója. Ha q nem törzsszám, akkor van $1 < q_1 < q$ osztója. Ekkor $q_1 \mid a$, ellentmondás.

7. Állítás. $\text{Prím} \implies \text{törzsszám}$.

BIZONYÍTÁS Ha p prím és $1 < d < p$ egy osztója, akkor $p = db$, $1 < b < p$.

Törzsszámok, prímek

5. Definíció. Egy egynél nagyobb q egész szám **törzsszám**, (irreducibilis, felbonthatatlan), ha csak két pozitív osztója van, 1 és önmaga. Egy egynél nagyobb p egész szám **prím**, ha $p \mid ab$ -ből következik, hogy p a tényezők valamelyikét, a -t vagy b -t osztja.

6. Állítás. Minden egynél nagyobb egész számnak van törzsszám osztója.

BIZONYÍTÁS Legyen q az $a > 1$ szám legkisebb 1-nél nagyobb osztója. Ha q nem törzsszám, akkor van $1 < q_1 < q$ osztója. Ekkor $q_1 \mid a$, ellentmondás.

7. Állítás. $\text{Prím} \implies \text{törzsszám}$.

BIZONYÍTÁS Ha p prím és $1 < d < p$ egy osztója, akkor $p = db$, $1 < b < p$. A prím tulajdonság miatt p vagy d -t, vagy b -t kell, hogy ossza, ellentmondás.

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámhoz, vagy osztható p -vel.

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámhoz, vagy osztható p -vel.

BIZONYÍTÁS (a, p) osztja p -t, így vagy 1, vagy p .

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámmal, vagy osztható p -vel.

BIZONYÍTÁS (a, p) osztja p -t, így vagy 1, vagy p .

9. Állítás. Törzsszám \implies prím.

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámmal, vagy osztható p -vel.

BIZONYÍTÁS (a, p) osztja p -t, így vagy 1, vagy p .

9. Állítás. Törzsszám \implies prím.

BIZONYÍTÁS Legyen $p \mid ab$.

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámmal, vagy osztható p -vel.

BIZONYÍTÁS (a, p) osztja p -t, így vagy 1, vagy p .

9. Állítás. Törzsszám \implies prím.

BIZONYÍTÁS Legyen $p \mid ab$. p vagy relatív prím a -hoz, illetve b -hez, vagy osztja a -t, illetve b -t. Ha mindkettőhöz relatív prím, akkor a szorzatukhoz is, ellentmondás.

8. Állítás. Minden a egész szám vagy relatív prím a megadott p törzsszámhoz, vagy osztható p -vel.

BIZONYÍTÁS (a, p) osztja p -t, így vagy 1, vagy p .

9. Állítás. Törzsszám \implies prím.

BIZONYÍTÁS Legyen $p \mid ab$. p vagy relatív prím a -hoz, illetve b -hez, vagy osztja a -t, illetve b -t. Ha mindkettőhöz relatív prím, akkor a szorzatukhoz is, ellentmondás.

Később az absztrakt algebrában majd látunk példát olyan struktúrákra (gyűrűkre), ahol a prím tulajdonság nem ekvivalens a felbonthatatlansággal, Amíg maradékos

osztás van, addig ez a probléma nem jelentkezik.

osztás van, addig ez a probléma nem jelentkezik. A maradék „kisebb”, mint az osztó.

osztás van, addig ez a probléma nem jelentkezik. A maradék „kisebb”, mint az osztó. Számok esetén a nagysága, polinomok esetén a foka.

Polinomok

Polinomok

Irreducibilitás, prímtulajdonság értelmes polinomokra is.

Polinomok

Irreducibilitás, prímtulajdonság értelmes polinomokra is.

- $\mathbb{C}[x]$ esetén az irreducibilisek legfeljebb elsőfokúak („Algebra alaptétele”)

Polinomok

Irreducibilitás, prímtulajdonság értelmes polinomokra is.

- $\mathbb{C}[x]$ esetén az irreducibilisek legfeljebb elsőfokúak („Algebra alaptétele”)
- $\mathbb{R}[x]$ esetén legfeljebb másodfokúak (ha $z \in \mathbb{C}$ gyöke egy valós együtthatós egyenletnek, akkor \bar{z} is)

Polinomok

Irreducibilitás, prímtulajdonság értelmes polinomokra is.

- $\mathbb{C}[x]$ esetén az irreducibilisek legfeljebb elsőfokúak („Algebra alaptétele”)
- $\mathbb{R}[x]$ esetén legfeljebb másodfokúak (ha $z \in \mathbb{C}$ gyöke egy valós együtthatós egyenletnek, akkor \bar{z} is)
- $\mathbb{Q}[x]$ esetén akármilyen nagy fokúak lehetnek.

Számelmélet alaptétele

10. Tétel. *Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.*

BIZONYÍTÁS 1. Létezik felbontás.

Számelmélet alaptétele

10. Tétel. *Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.*

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás.

Számelmélet alaptétele

10. Tétel. *Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.*

BIZONYÍTÁS 1. **Létezik felbontás.** n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. **Létezik felbontás.** n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. **Létezik felbontás.** n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. **Létezik felbontás.** n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. **Létezik felbontás.** n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű. n szerinti teljes indukció.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re egyértelmű a felbontás.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re egyértelmű a felbontás. Legyen $n = p_1 p_2 \dots p_r$ és $n = q_1 q_2 \dots q_s$. q_1 osztja a $p_1 p_2 \dots p_r$ szorzatot, így valamelyik tényezőjét is, mondjuk p_1 -et.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re egyértelmű a felbontás. Legyen $n = p_1 p_2 \dots p_r$ és $n = q_1 q_2 \dots q_s$. q_1 osztja a $p_1 p_2 \dots p_r$ szorzatot, így valamelyik tényezőjét is, mondjuk p_1 -et. $\implies p_1 = q_1$. Mivel $1 < n' = \frac{n}{q_1} < n$, ezért indukció szerint a felbontása egyértelmű, azaz $p_2 \dots p_r$ és $q_2 \dots q_s$ csak a tényezők sorrendjében különbözhet.

Számelmélet alaptétele

10. Tétel. Minden egynél nagyobb n szám felbontható törzs(prím)tényezők szorzatára a tényezők sorrendjétől eltekintve egyértelműen.

BIZONYÍTÁS 1. Létezik felbontás. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re létezik felbontás. Ha n törzsszám, akkor $n = n$ jó. Ha n -nek van valódi osztója $1 < d < n$, akkor $n = dd'$, és $1 < d' < n$. Az indukciós feltétel szerint d -nek és d' -nek létezik felbontása: $d = p_1 p_2 \dots p_r$, $d' = q_1 q_2 \dots q_s$. $n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ egy felbontása n -nek.

2. A felbontás egyértelmű. n szerinti teljes indukció. $n = 2$ nyilvánvaló, tegyük fel, hogy minden $n' < n$ -re egyértelmű a felbontás. Legyen $n = p_1 p_2 \dots p_r$ és $n = q_1 q_2 \dots q_s$. q_1 osztja a $p_1 p_2 \dots p_r$ szorzatot, így valamelyik tényezőjét is, mondjuk p_1 -et. $\implies p_1 = q_1$. Mivel $1 < n' = \frac{n}{q_1} < n$, ezért indukció szerint a felbontása egyértelmű, azaz $p_2 \dots p_r$ és $q_2 \dots q_s$ csak a tényezők sorrendjében különbözhet. Ez n tetszőleges két felbontására igaz.

Osztók

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása.

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n$

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$
mint az alaptételnél: $\forall i \exists j: q_i \mid p_j$

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$
mint az alaptételnél: $\forall i \exists j: q_i \mid p_j \implies q_i = p_j$.

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$ mint az alaptételnél: $\forall i \exists j: q_i \mid p_j \implies q_i = p_j$.

Tegyük fel, hogy $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ és valamely i -re $\beta_i > \alpha_i$.

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$ mint az alaptételnél: $\forall i \exists j: q_i \mid p_j \implies q_i = p_j$.

Tegyük fel, hogy $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ és valamely i -re $\beta_i > \alpha_i$.

$$\left(\frac{n}{p_i^{\alpha_i}}, \frac{d}{p_i^{\alpha_i}} \right) = \frac{(n, d)}{p_i^{\alpha_i}}$$

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$ mint az alaptételnél: $\forall i \exists j: q_i \mid p_j \implies q_i = p_j$.

Tegyük fel, hogy $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ és valamely i -re $\beta_i > \alpha_i$.

$$\left(\frac{n}{p_i^{\alpha_i}}, \frac{d}{p_i^{\alpha_i}} \right) = \frac{(n, d)}{p_i^{\alpha_i}} = \frac{d}{p_i^{\alpha_i}}.$$

Osztók

Egyértelmű prímtenyezős felbontás: minden $n \in \mathbb{N}$ egyértelműen írható $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ alakban, ahol $2 \leq p_1 < p_2 < \dots < p_s$ (különböző) prímek és $\alpha_i \in \mathbb{N}$.

11. Állítás. Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. $d \mid n \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, ahol $0 \leq \beta_i \leq \alpha_i$.

BIZONYÍTÁS Legyen $d = q_1^{\beta_1} q_2^{\beta_2} \dots q_r^{\beta_r}$ a d prímtenyezős felbontása. $\implies \forall i: q_i \mid n \implies$ mint az alaptételnél: $\forall i \exists j: q_i \mid p_j \implies q_i = p_j$.

Tegyük fel, hogy $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ és valamely i -re $\beta_i > \alpha_i$.

$$\left(\frac{n}{p_i^{\alpha_i}}, \frac{d}{p_i^{\alpha_i}} \right) = \frac{(n, d)}{p_i^{\alpha_i}} = \frac{d}{p_i^{\alpha_i}}.$$

Ez utóbbit osztja p_i , de $\frac{n}{p_i^{\alpha_i}}$ -t nem, ellentmondás.

Osztók száma

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói *kölcsönösen egyértelműen* megfelelnek az (s -hosszú) $(\beta_1, \beta_2, \dots, \beta_s)$ sorozatoknak, ahol $0 \leq \beta_i \leq \alpha_i$.

Osztók száma

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói *kölcsönösen egyértelműen* megfelelnek az $(s\text{-hosszú})$ $(\beta_1, \beta_2, \dots, \beta_s)$ sorozatoknak, ahol $0 \leq \beta_i \leq \alpha_i$.

Az ilyen sorozatok (tehát az n osztóinak) száma:

Osztók száma

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói *kölcsönösen egyértelműen* megfelelnek az $(s\text{-hosszú})$ $(\beta_1, \beta_2, \dots, \beta_s)$ sorozatoknak, ahol $0 \leq \beta_i \leq \alpha_i$.

Az ilyen sorozatok (tehát az n osztóinak) száma: $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$.

Osztók száma

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói *kölcsönösen egyértelműen* megfelelnek az $(s\text{-hosszú})$ $(\beta_1, \beta_2, \dots, \beta_s)$ sorozatoknak, ahol $0 \leq \beta_i \leq \alpha_i$.

Az ilyen sorozatok (tehát az n osztóinak) száma: $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$. $\alpha_1 + 1$ választásunk van az első helyre...

Osztók száma

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói *kölcsönösen egyértelműen* megfelelnek az $(s\text{-hosszú})$ $(\beta_1, \beta_2, \dots, \beta_s)$ sorozatoknak, ahol $0 \leq \beta_i \leq \alpha_i$.

Az ilyen sorozatok (tehát az n osztóinak) száma: $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$. $\alpha_1 + 1$ választásunk van az első helyre...

MEGJEGYZÉS (CSAK ÉRDEKLŐDŐKNEK): Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ osztói által alkotott *részben rendezett* halmaz $(a \preceq b \iff a \mid b)$ *izomorf* az $\{(x_1, x_2, \dots, x_s) : 0 \leq x_i \leq \alpha_i\}$ sorozatok által alkotott részben rendezett halmazzal, ahol $(x_1, x_2, \dots, x_s) \preceq (y_1, y_2, \dots, y_s) \iff \forall i: x_i \leq y_i$.

Osztók összege

1. feladat

2. feladat

3. feladat

4. feladat

5. feladat

6. feladat

7. feladat

8. feladat

9. feladat

10. feladat

11. feladat

12. feladat

13. feladat

14. feladat

15. feladat

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

$$t = \frac{d}{d_a d_b} \text{ és } t \mid ab \implies t = (ab, t) = 1.$$

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

$t = \frac{d}{d_a d_b}$ és $t \mid ab \implies t = (ab, t) = 1$. Azaz ab egy osztója a és b egy osztójának szorzata.

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

$t = \frac{d}{d_a d_b}$ és $t \mid ab \implies t = (ab, t) = 1$. Azaz ab egy osztója a és b egy osztójának szorzata. Legyenek a osztói c_1, c_2, \dots, c_m , b osztói d_1, d_2, \dots, d_k .

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

$t = \frac{d}{d_a d_b}$ és $t \mid ab \implies t = (ab, t) = 1$. Azaz ab egy osztója a és b egy osztójának szorzata. Legyenek a osztói c_1, c_2, \dots, c_m , b osztói d_1, d_2, \dots, d_k . Ekkor

$$\sigma(ab) = \sum_{i=1}^m \sum_{j=1}^k c_i d_j = (c_1 + c_2 + \dots + c_m)(d_1 + d_2 + \dots + d_k) = \sigma(a)\sigma(b).$$

Osztók összege

Az n osztóinak összegét $\sigma(n)$ jelöli.

1. Legyen $n = p^\alpha$. Ekkor n osztói: $1, p, p^2, \dots, p^\alpha$. $\sigma(n) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
2. Legyen $(a, b) = 1$. Ekkor $\sigma(ab) = \sigma(a)\sigma(b)$. Tegyük fel, hogy $d \mid ab$. Legyen $(a, d) = d_a$ és $(b, d) = d_b$. Ekkor $(d_a, d_b) = 1$ és d közös többszörösük. $\implies d = d_a d_b t$ valamely $t \in \mathbb{N}$. Viszont

$$\left(a, \frac{d}{d_a d_b}\right) = 1 \text{ és } \left(b, \frac{d}{d_a d_b}\right) = 1 \implies \left(ab, \frac{d}{d_a d_b}\right) = 1$$

$t = \frac{d}{d_a d_b}$ és $t \mid ab \implies t = (ab, t) = 1$. Azaz ab egy osztója a és b egy osztójának szorzata. Legyenek a osztói c_1, c_2, \dots, c_m , b osztói d_1, d_2, \dots, d_k . Ekkor

$$\sigma(ab) = \sum_{i=1}^m \sum_{j=1}^k c_i d_j = (c_1 + c_2 + \dots + c_m)(d_1 + d_2 + \dots + d_k) = \sigma(a)\sigma(b).$$

3. Innen egyszerű indukció adja, hogy ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, akkor

$$\sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_s + p_s^2 + \dots + p_s^{\alpha_s}).$$

Egymás utáni prímszámok

12. Állítás. *A prímszámok száma végtelen.*

Egymás utáni prímszámok

12. Állítás. *A prímszámok száma végtelen.*

BIZONYÍTÁS Tegyük fel indirekt, hogy nem, és p_1, p_2, \dots, p_n az összes létező prímszám listája.

Egymás utáni prímszámok

12. Állítás. *A prímszámok száma végtelen.*

BIZONYÍTÁS Tegyük fel indirekt, hogy nem, és p_1, p_2, \dots, p_n az összes létező prímszám listája. Tekintsük az $N = p_1 p_2 \dots p_n + 1$ számot. Ennek van prímszám osztója, ami nem lehet a p_1, p_2, \dots, p_n számok egyike sem, ellentmondás.

Egymás utáni prímszámok

12. Állítás. *A prímszámok száma végtelen.*

BIZONYÍTÁS Tegyük fel indirekt, hogy nem, és p_1, p_2, \dots, p_n az összes létező prímszám listája. Tekintsük az $N = p_1 p_2 \dots p_n + 1$ számot. Ennek van prímszám osztója, ami nem lehet a p_1, p_2, \dots, p_n számok egyike sem, ellentmondás.

13. Állítás. *Bármely $m \in \mathbb{N}$ számhoz van m egymás után következő egész, melyek egyike sem prím.*

Egymás utáni prímszámok

12. Állítás. *A prímszámok száma végtelen.*

BIZONYÍTÁS Tegyük fel indirekt, hogy nem, és p_1, p_2, \dots, p_n az összes létező prímszám listája. Tekintsük az $N = p_1 p_2 \dots p_n + 1$ számot. Ennek van prímszám osztója, ami nem lehet a p_1, p_2, \dots, p_n számok egyike sem, ellentmondás.

13. Állítás. *Bármely $m \in \mathbb{N}$ számhoz van m egymás után következő egész, melyek egyike sem prím.*

BIZONYÍTÁS Tekintsük az $(m+1)! + 2, (m+1)! + 3, \dots, (m+1)! + m + 1$ számokat. Ez m egymást követő egész, egyikük sem lehet prím: az i -ik osztható $i + 1$ -el.

Néhány megoldatlan probléma

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt?

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p+2$ is prím: $(p, p+2)$ *ikerprímek*.

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p+2$ is prím: $(p, p+2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p+2$ is prím: $(p, p+2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

MEGOLDATLAN PROBLÉMA (GOLDBACH SEJTÉS): Igaz-e, hogy minden 4-nél nagyobb páros szám felírható két prímszám összegeként?

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p+2$ is prím: $(p, p+2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

MEGOLDATLAN PROBLÉMA (GOLDBACH SEJTÉS): Igaz-e, hogy minden 4-nél nagyobb páros szám felírható két prímszám összegeként?

MEGOLDATLAN PROBLÉMA: Van-e végtelen sok olyan p prím, melyre $p-1$ négyzetszám? ($17-1=4^2$)

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p + 2$ is prím: $(p, p + 2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

MEGOLDATLAN PROBLÉMA (GOLDBACH SEJTÉS): Igaz-e, hogy minden 4-nél nagyobb páros szám felírható két prímszám összegeként?

MEGOLDATLAN PROBLÉMA: Van-e végtelen sok olyan p prím, melyre $p - 1$ négyzetszám? ($17 - 1 = 4^2$)

MEGOLDATLAN PROBLÉMA: Igaz-e, hogy két négyzetszám közt mindig van prímszám?

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p + 2$ is prím: $(p, p + 2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

MEGOLDATLAN PROBLÉMA (GOLDBACH SEJTÉS): Igaz-e, hogy minden 4-nél nagyobb páros szám felírható két prímszám összegeként?

MEGOLDATLAN PROBLÉMA: Van-e végtelen sok olyan p prím, melyre $p - 1$ négyzetszám? ($17 - 1 = 4^2$)

MEGOLDATLAN PROBLÉMA: Igaz-e, hogy két négyzetszám közt mindig van prímszám?

Tudjuk: prímszámok „sűrűbben” vannak, mint a négyzetszámok.

Néhány megoldatlan probléma

Mekkora lehet a legkisebb különbség két szomszédos prím közt? $3-2=1$: csak egyszer lehet. $2 = 5 - 3 = 7 - 5 = 13 - 11 = 19 - 17 = 31 - 29 = \dots$ sokszor. Ha p és $p + 2$ is prím: $(p, p + 2)$ *ikerprímek*.

MEGOLDATLAN PROBLÉMA: Létezik-e végtelen sok ikerprím pár?

MEGOLDATLAN PROBLÉMA (GOLDBACH SEJTÉS): Igaz-e, hogy minden 4-nél nagyobb páros szám felírható két prímszám összegeként?

MEGOLDATLAN PROBLÉMA: Van-e végtelen sok olyan p prím, melyre $p - 1$ négyzetszám? ($17 - 1 = 4^2$)

MEGOLDATLAN PROBLÉMA: Igaz-e, hogy két négyzetszám közt mindig van prímszám?

Tudjuk: prímszámok „sűrűbben” vannak, mint a négyzetszámok. Ha n elég nagy, akkor n^3 és $(n + 1)^3$ között van prímszám (Ingham, 1937)

Prímszámok eloszlásáról

14. Definíció. *Tetszőleges $x \geq 2$ valós számra $\pi(x)$ jelöli az x -nél nem nagyobb prímek számát.*

Prímszámok eloszlásáról

14. Definíció. Tetszőleges $x \geq 2$ valós számra $\pi(x)$ jelöli az x -nél nem nagyobb prímek számát.

15. Tétel (Csebisev). Tetszőleges $n \in \mathbb{N}$ -re $\pi(2n) > \pi(n)$, azaz van p prím, melyre $n < p \leq 2n$.

16. Tétel (Prímszámtétel).

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

17. Tétel. *Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.*

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

$n = 2k + 1 > 4$:

$$\prod_{p < 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right)$$

.

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

$n = 2k + 1 > 4$:

$$\prod_{p < 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right)$$

.Az első szorzat indukció alapján kisebb, mint 4^{k+1} .

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

$n = 2k + 1 > 4$:

$$\prod_{p < 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right)$$

.Az első szorzat indukció alapján kisebb, mint 4^{k+1} . A második pedig osztja a

$$(k+2)(k+3) \dots (2k+1) = \frac{(2k+1)!}{(k+1)!} = k! \binom{2k+1}{k}$$

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

$n = 2k + 1 > 4$:

$$\prod_{p < 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right)$$

.Az első szorzat indukció alapján kisebb, mint 4^{k+1} . A második pedig osztja a

$$(k+2)(k+3) \dots (2k+1) = \frac{(2k+1)!}{(k+1)!} = k! \binom{2k+1}{k}$$

viszont $k!$ -hoz relatív prím, így osztja $\binom{2k+1}{k}$ -t.

17. Tétel. Tetszőleges $n \geq 2$ -re $\prod_{p < n} p < 4^n$.

BIZONYÍTÁS Indukció n -re. $n = 2$ eset triviális.

$n = 2k$: $\prod_{p < 2k} p = \prod_{p < 2k-1} p < 4^{2k-1} < 4^{2k}$.

$n = 2k+1 > 4$:

$$\prod_{p < 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right)$$

.Az első szorzat indukció alapján kisebb, mint 4^{k+1} . A második pedig osztja a

$$(k+2)(k+3)\dots(2k+1) = \frac{(2k+1)!}{(k+1)!} = k! \binom{2k+1}{k}$$

viszont $k!$ -hoz relatív prím, így osztja $\binom{2k+1}{k}$ -t. Látható, hogy $\binom{2k+1}{k} < 4^k \implies \prod_{p < 2k+1} p < 4^{k+1} 4^k = 4^{2k+1}$.