NEVEZETES SZÁMELMÉLETI FÜGGVÉNYEKRŐL

SZAKDOLGOZAT

Készítette: **Farkas Mariann**

Matematika BSc Tanári szakirány

Témavezető: **Pappné Dr. Kovács Katalin**, egyetemi docens

Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Budapest, 2011

Tartalomjegyzék

Bevezetés

Dolgozatomban négy nevezetes számelméleti függvényről lesz szó $(d(n), \sigma(n), \varphi(n), \mu(n))$. Az ezekről tanult ismereteket foglalom össze, alkalmazással, és feladatokkal kibővítve. Leendő tanárként fontosnak tartom a feladatmegoldást, ezzel sokszor kézzelfoghatóbbá válik az ismeretanyag, könnyebb az elsajátítása, továbbá gondolkodásra sarkall, gyarapodik ötlettárunk a problémamegoldás terén. Az utolsó fejezetben a fent említett függvények hegy- és völgytételeiből mutatok be egy részt a teljesség igénye nélkül.

Célom, hogy dolgozatom jó kiindulópont legyen a téma iránt érdeklődőknek, felhasználható legyen középiskolában az emelt óraszámú matematika csoportok oktatásánál, illetve szakkörökön.

Ezúton szeretném megköszönni témavezetőmnek, Pappné Dr. Kovács Katalinnak a sok segítséget, ötletet és támogatást, amelyet a szakdolgozatom megoldásához nyújtott.

1. Alapfogalmak

1.1. Definíció:[9] Függvényen halmazok közötti egyértelmű hozzárendelést értünk. Az x-hez hozzárendelt elemet $f(x)$-szel jelöljük. Ha X és Y tetszőleges halmazok, akkor

$$f: X \to Y$$

egy olyan függvény, melyre

$$\forall\, x \in D(f) \subset X \text{ esetén } f(x) \in Y.$$

$D(f)$ az f függvény értelmezési tartomány, azaz

$$D(f) = \{x \in X: x\text{-hez } f \text{ hozzárendel valamit}\},$$

ami az X egy részhalmaza. Az $R(f)$ az f függvény értékkészlete, mely Y-nak részhalmaza és

$$R(f) = \{y \in Y: y = f(x) \text{ valamely } x \in D(f)\text{-re}\}.$$

A függvények egy részhalmazát alkotják a számelméleti függvények.
Az alábbi definíciók és tételek a számelmélet jegyzetből és [3] könyvből valók.

1.2. Definíció: Számelméleti függvényeknek nevezzük azokat a függvényeket, amelyek értelmezési tartománya a pozitív egész számok halmaza, értékkészlete pedig a komplex számok egy részhalmaza. Jelöléssel:

$$f: \mathbb{Z}^+ \to \mathbb{C}.$$

1.3. Definíció: Az f számelméleti függvény

i. multiplikatív, ha $\forall\, a, b \in \mathbb{Z}^+, (a, b) = 1$ esetén $f(ab) = f(a) \cdot f(b)$,
ii. teljesen multiplikatív, ha $\forall\, a, b \in \mathbb{Z}^+$ esetén $f(ab) = f(a) \cdot f(b)$.

1.1. Tétel: Ha f multiplikatív, és nem azonosan 0, akkor $f(1) = 1$..

Bizonyítás: Legyen $f(a) \neq 0$, ahol a egy tetszőleges pozitív egész szám. $(a, 1) = 1$ miatt $f(a) = f(a \cdot 1) = f(a) \cdot f(1)$. Ezt $f(a)$-val egyszerűsítve kapjuk, hogy $f(1) = 1$. Ha nem létezik olyan a, melyre $f(a) \neq 0$, akkor kész, és f azonosan 0.

1.4. Definíció: Az f számelméleti függvény

i. additív, ha $\forall\, a, b \in \mathbb{Z}^+, (a, b) = 1$ esetén $f(ab) = f(a) + f(b)$,
ii. teljesen additív, ha $\forall\, a, b \in \mathbb{Z}^+$ esetén $f(ab) = f(a) + f(b)$.

1.2. Tétel: Ha f additív, akkor $f(1) = 0$.

Bizonyítás: Legyen a egy tetszőleges pozitív egész szám. Ekkor $(a, 1) = 1$ miatt $f(a) = f(a \cdot 1) = f(a) + f(1)$. Mindkét oldalból $f(a)$-t elvéve kapjuk, hogy $f(1) = 0$.

1.3. Tétel: Legyen f

i. multiplikatív,

ii. additív számelméleti függvény, és az n szám kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$.

Ekkor

i. $f(n) = f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \dots f\left(p_s^{\alpha_s}\right)$,

ii. $f(n) = f\left(p_1^{\alpha_1}\right) + f\left(p_2^{\alpha_2}\right) + \dots + f(p_s^{\alpha_s})$.

Bizonyítás: A $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_s^{\alpha_s}$ számok páronként relatív prímek, így a multiplikativitás és additivitás definíciójából következik a tétel.

1.4. Tétel: Legyen f

i. teljesen multiplikatív,

ii. teljesen additív számelméleti függvény, és az $n > 1$ szám kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$.

Ekkor

i. $f(n) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \dots f(p_s)^{\alpha_s}$

ii. $f(n) = a_1 f(p_1) + a_2 f(p_2) + \dots + a_s f(p_s)$.

Bizonyítás: Az előző tételből a teljesen additív/multiplikatív definícióját felhasználva következik.

2. A $d(n)$ függvény

2.1. Definíció: $d(n)$-en az $n \geq 1$ természetes szám pozitív osztóinak számát értjük.

2.1. Tétel:[3] Legyen az n szám általánosított kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}.$$

i. Egy d pozitív egész pontosan akkor osztja az n számot, ha kanonikus alakja

$$d = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s},$$

ahol $0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_s \leq \alpha_s$.

ii. Ekkor az n szám pozitív osztóinak száma

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1).$$

Bizonyítás: Ha $d|n$, akkor $n = dq$, tehát d kanonikus alakjában csak a p_i prímek szerepelnek legfeljebb α_i hatványon, $i = 0, 1, \dots, s$.

Ha $d = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s}$, akkor $n = dq$ miatt $q = {p_1}^{\alpha_1 - \beta_1} {p_2}^{\alpha_2 - \beta_2} \dots {p_s}^{\alpha_s - \beta_s}$, és mivel $\alpha_i \geq \beta_i$, így $\alpha_i - \beta_i \geq 0$, tehát q egész szám és $d|n$.

Ahhoz, hogy az n szám összes pozitív osztóját megkapjuk a $d = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s}$ kifejezésben kell jól megválasztani a β_i kitevőket. Minden β_i-re igaz, hogy egymástól függetlenül felveszik a $0, 1, 2, \dots, \alpha_i$ értékeket, tehát minden β_i-t $(\alpha_i + 1)$-képpen választhatok meg. A $d(n)$ ezen számok szorzataként áll elő.

Példa:

Legyen $n = 24$, ekkor az osztói, az $1, 2, 3, 4, 6, 8, 12, 24$ számok, tehát $d(n) = 8$.

Képlettel: $24 = 2^3 3$, $d(24) = (3 + 1)(1 + 1) = 8$.

Tulajdonságok:

- $n = 1$ esetén $d(n) = 1$.
- Ha n prím, vagyis $n = p$, akkor $d(n) = 2$, hiszen egy prímszámnak csak 2 osztója van, 1 és önmaga.
- Ha n prímhatvány, vagyis $n = p^\alpha$, akkor $d(n) = \alpha + 1$, mivel az osztói az $1, p, p^2, \dots, p^\alpha$.

2.2. Tétel: A $d(n)$ függvény multiplikatív.

Bizonyítás: Azt kell belátnunk, hogy ha $(a, b) = 1$, akkor $d(ab) = d(a) \cdot d(b)$.

Legyen az a és b prímtényezős felbontása a következő:

$$a = p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} \dots p_{i_s}^{\alpha_s},$$

$$b = p_{j_1}{}^{\beta_1} p_{j_2}{}^{\beta_2} \dots p_t{}^{\beta_t},$$

ahol $p_{i_1}, p_{i_2}, \dots, p_{i_s}, p_{j_1}, p_{j_2}, \dots, p_{j_t}$ különböző prímek.

Ekkor az ab prímtényezős felbontása:

$$ab = p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} \dots p_{i_s}^{\alpha_s} p_{j_1}{}^{\beta_1} p_{j_2}{}^{\beta_2} \dots p_t{}^{\beta_t}.$$

A $d(n)$ függvény képletét alkalmazva:

$$d(a) \cdot d(b) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)(\beta_1 + 1)(\beta_2 + 1) \dots (\beta_t + 1) = d(ab).$$

Példa: $n = 15$-re

$$d(3) = 1 + 1 = 2$$

$$d(5) = 1 + 1 = 2$$

$$d(15) = (1 + 1)(1 + 1) = 4$$

$$d(3) \cdot d(5) = d(15)$$

Megjegyzés: A $d(n)$ függvény nem teljesen multiplikatív. Ennek igazolásához elég egy példát mutatni.

Példa: $n = 18$-ra

$$d(3) = 1 + 1 = 2$$

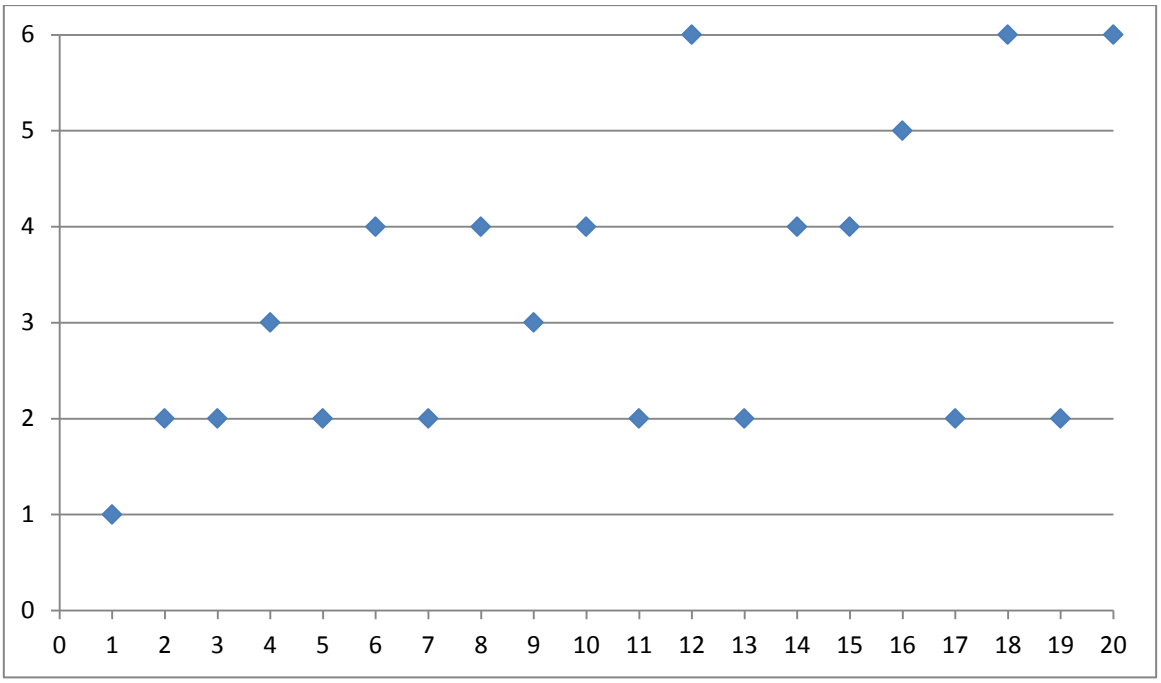
$$d(6) = (1 + 1)(1 + 1) = 4$$

$$d(18) = (1 + 1)(2 + 1) = 6$$

$$d(3) \cdot d(6) = 8 \neq 6 = d(18)$$

A $d(n)$ függvény néhány értéke:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6	2	6



Értékkészlete: A $d(n)$ függvény minden pozitív egész számot felvesz végtelen sokszor, kivéve az 1-et, melyet csak egyszer az $n = 1$ helyen. Ez következik abból a tulajdonságából, hogy $d(p^{\alpha}) = \alpha + 1$, ahol α és p prím tetszőlegesek.

Alkalmazása: *Diofantikus problémák*

A $d(n)$ függvény lesz a segítségünkre abban, hogy meghatározzuk, az alábbi diofantikus egyenletnek hány megoldása van.

Tekintsük a következő egyenletet:

$$x^2 - y^2 = n,$$

ahol n egy rögzített pozitív egész szám. Az $x, y \in \mathbb{Z}$ megoldásokat keressük.

Az $x^2 - y^2$ nevezetes azonosság felírható $(x - y)(x + y)$ alakban. Az $x - y$ és $x + y$ kifejezések paritása megegyezik, mivel $x - y \equiv x + y \ (mod\ 2)$.

A kérdés, hogy milyen n esetén lehet az egyenletnek megoldása?

a) n páratlan

Hányféleképpen írható fel az n szám $d_1 \cdot d_2$ alakban, ahol d_1 és d_2 is páratlan számok? Két eset lehetséges, az elsőben d_1 és d_2 pozitív egész számok, a másodikban azonban negatív egész számok, vagyis minden osztópár jó lesz. Bármelyik felírásnál $d(n)$ megoldása van az egyenletnek, így összesen $2d(n)$ megoldás adódik.

Példa: $x^2 - y^2 = 15$.

$x-y$	$x+y$	x	y
1	15	8	7
15	1	8	-7
3	5	4	1
5	3	4	-1
-1	-15	-8	-7
-15	-1	-8	7
-3	-5	-4	-1
-5	-3	-4	1

b) $4|n$

$$n = (x-y)(x+y) = d_1 \cdot d_2$$

$$\frac{n}{4} = \frac{x-y}{2} \cdot \frac{x+y}{2} = \frac{d_1}{2} \cdot \frac{d_2}{2}$$

Mivel $\frac{n}{4}$ pozitív egész szám, ezért d_1 és d_2 is páros szám kell, hogy legyen. Ekkor a megoldások száma $\frac{n}{4}$ osztóinak a száma, a pozitív és negatív eseteket is számolva, vagyis összesen $2d\left(\frac{n}{4}\right)$.

Példa:

$x-y$	$x+y$	x	y
2	4	3	1
4	2	3	-1
-4	-2	-3	1
-2	-4	-3	-1

Feladatok:

2.1. Feladat:[7] Igazoljuk, hogy $d(n) \leq 2\sqrt{n}$!

Megoldás: Az n szám összes osztójából párokat alkotunk. Ezek legyenek a $\langle d_1, \frac{n}{d_1} \rangle, \langle d_2, \frac{n}{d_2} \rangle, \dots, \langle d_k, \frac{n}{d_k} \rangle$. Feltehetjük, hogy minden esetben $d_i \leq \frac{n}{d_i}\ \forall\, i = 1, \dots, k$. A $d \leq \frac{n}{d}$-t alakítva kapjuk, hogy $d^2 \leq n$, ahonnan $d \leq \sqrt{n}$. Vagyis a párok száma legfeljebb $\sqrt{n}$. Innen kapjuk, hogy $d(n)$ legfeljebb a párok számának kétszeres, azaz $2\sqrt{n}$.

Megjegyzés: Ha n négyzetmentes, akkor pontosan $2k$ darab osztója van, különben $2k - 1$.

2.2. Feladat: Mely n természetes számokra teljesül, hogy

a) $d(3n) = 2d(n)$,

b) $d(3n) = d(2n)$?

Megoldás:

a) Először írjuk fel az n, és a $3n$ kanonikus alakját:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots p_s^{\alpha_s},$$

$$3n = {p_1}^{\alpha_1} {p_2}^{\alpha_2 + 1} \dots p_s^{\alpha_s}, \text{ ahol } p_1 = 2, p_2 = 3.$$

Ezután a képlet segítségével megkapjuk $d(n)$-t és $d(3n)$-t:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1),$$

$$d(3n) = (\alpha_1 + 1)(\alpha_2 + 2) \dots (\alpha_s + 1).$$

Ezeket helyettesítsük be az eredeti egyenletbe:

$$(\alpha_1 + 1)(\alpha_2 + 2) \dots (\alpha_s + 1) = 2(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1).$$

Az egyszerűsítés után azt kapjuk, hogy:

$$\alpha_2 + 2 = 2(\alpha_2 + 1),$$

$$\alpha_2 + 2 = 2\alpha_2 + 2$$

$$\alpha_2 = 0.$$

Vagyis a képletet azok a számok elégítik ki, amelyek prímtényezős felbontásában nem szerepel a 3.

b) Hasonló módon járunk el itt is. A kanonikus alakok:

$$2n = 2^{\alpha_1 + 1} 3^{\alpha_2} \dots p_s^{\alpha_s},$$

$$3n = 2^{\alpha_1} 3^{\alpha_2 + 1} \dots p_s^{\alpha_s}.$$

Írjuk fel $d(2n)$-t és $d(3n)$-t, majd tegyük őket egyenlővé, és oldjuk meg az egyenletet:

$$d(2n) = (\alpha_1 + 2)(\alpha_2 + 1) \dots (\alpha_s + 1)$$
$$d(3n) = (\alpha_1 + 1)(\alpha_2 + 2) \dots (\alpha_s + 1)$$
$$(\alpha_1 + 2)(\alpha_2 + 1) \dots (\alpha_s + 1) = (\alpha_1 + 1)(\alpha_2 + 2) \dots (\alpha_s + 1)$$
$$(\alpha_1 + 2)(\alpha_2 + 1) = (\alpha_1 + 1)(\alpha_2 + 2)$$
$$\alpha_1\alpha_2 + \alpha_1 + 2\alpha_2 + 2 = \alpha_1\alpha_2 + 2\alpha_1 + \alpha_2 + 2$$
$$\alpha_1 = \alpha_2$$

Tehát az egyenlet gyökei azok a számok, amelyek prímtényezős felbontásában a 2 és a 3 azonos hatványkitevőn szerepelnek.

2.3. Feladat:[7] Mely n természetes számokra teljesül, hogy $2d(n^2) = 3d(n)$?

Megoldás: Az előbbi feladat mintájára írjuk fel az n és az n^2 kanonikus alakjait:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$
$$n^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_s^{2\alpha_s}.$$

Innen kapjuk, hogy:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1),$$
$$d(n^2) = (2\alpha_1 + 1)(2\alpha_2 + 1) \dots (2\alpha_s + 1).$$

Az egyenletünk:

$$2(2\alpha_1 + 1)(2\alpha_2 + 1) \dots (2\alpha_s + 1) = 3(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1).$$

Átrendezve:

$$\frac{2\alpha_1 + 1}{\alpha_1 + 1} \cdot \frac{2\alpha_2 + 1}{\alpha_2 + 1} \cdot \dots \cdot \frac{2\alpha_s + 1}{\alpha_s + 1} = \frac{3}{2}.$$

Ha minden $\alpha_i = 0$, akkor a bal oldal 1 lenne, tehát létezik olyan α_i, mely nagyobb, mint 0. Ekkor az egyenlet bal oldalán minden tört értéke nagyobb vagy egyenlő, mint 1.

$$1 < \frac{2\alpha_i + 1}{\alpha_i + 1} \leq \frac{3}{2},$$
$$1 < 1 + \frac{\alpha_i}{\alpha_i + 1} \leq \frac{3}{2},$$
$$0 < \frac{\alpha_i}{\alpha_i + 1} = 1 - \frac{1}{\alpha_i + 1} \leq \frac{1}{2}.$$

Tehát $\alpha_i \leq 1$ lehet csak. Több α_i nem lehet 0-tól különböző, mert akkor az egyenlet bal oldalán legalább $2 \cdot \frac{3}{2}$ szerepelne, a többi tényező pedig legalább 1, ami ellentmond a $\frac{2\alpha_1+1}{\alpha_1+1} \cdot \frac{2\alpha_2+1}{\alpha_2+1} \cdot \dots \cdot \frac{2\alpha_s+1}{\alpha_s+1} = \frac{3}{2}$-nek. Tehát valamelyik $\alpha_i = 1$ és a többi 0, azaz n prímszám.

2.4. Feladat: Milyen n természetes számokra igaz, hogy $d(n) = n - 2$?

Megoldás: Tudjuk, hogy $d(n) \leq 2\sqrt{n}$, tehát $n - 2 \leq 2\sqrt{n}$. Négyzetre emelés és nullára rendezés után kapjuk, hogy $n^2 - 8n + 4 \leq 0$. A másodfokú egyenletet megoldva kapjuk, hogy $1 \leq n \leq 7$. Ezekre az n-ekre ellenőrizve kapjuk, hogy $n = 6$.

2.5. Feladat:[7] Keressük meg a legkisebb n természetes számot, melyre

a) $d(n) = 23$,

b) $d(n) = 25$,

c) $d(n) = 24$.

Megoldás: Minden esetben az n szám kibővített kanonikus alakja $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots p_s^{\alpha_s}$, és

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1).$$

a) A képletbe helyettesítve: $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1) = 23$. Mivel 23 prímszám, ezért valamelyik $\alpha_i + 1$ tényező egyenlő 23-mal és $\alpha_i = 22$, a többi 0. Azonos kitevőjű hatványok közül az a legkisebb, ahol a hatványalap is legkisebb. Így a legkisebb természetes szám, ami megoldást ad az $n = 2^{22}$.

b) Az előző mintájára: $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1) = 25$. Itt két esetet kell vizsgálnunk a szorzattá alakítás szerint:

- $25 = 25 \cdot 1$

  Ekkor az a) esethez hasonlóan járunk el, így $n = 2^{24}$-et kapunk.

- $25 = 5 \cdot 5$

  Itt a legjobb eset, mikor $(\alpha_1 + 1)(\alpha_2 + 1) = 5 \cdot 5$, ahonnan $\alpha_1 = \alpha_2 = 4$ és $n = 2^4 \cdot 3^4$.

A két eset közül az utóbbi adja a helyes megoldást.

c) Az $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1) = 24$ esetben szintén esetszétválasztást alkalmazunk. Az eredményeket táblázatba foglalom:

Szorzatalak	Kanonikus alak és konkrét érték
$24 \cdot 1$	$2^{23} = 8388608$
$12 \cdot 2$	$2^{11} \cdot 3 = 6144$
$2 \cdot 12$	$2 \cdot 3^{11} = 354294$
$8 \cdot 3$	$2^7 \cdot 3^2 = 1152$

$3 \cdot 8$	$2^2 \cdot 3^7 = 8748$
$6 \cdot 4$	$2^5 \cdot 3^3 = 864$
$4 \cdot 6$	$2^3 \cdot 3^5 = 1944$
$6 \cdot 2 \cdot 2$	$2^5 \cdot 3 \cdot 5 = 480$
$2 \cdot 6 \cdot 2$	$2 \cdot 3^5 \cdot 5 = 2430$
$2 \cdot 2 \cdot 6$	$2 \cdot 3 \cdot 5^5 = 18750$
$4 \cdot 3 \cdot 2$	$2^3 \cdot 3^2 \cdot 5 = 360$
$4 \cdot 2 \cdot 3$	$2^3 \cdot 3 \cdot 5^2 = 600$
$3 \cdot 4 \cdot 2$	$2^3 \cdot 3^3 \cdot 5 = 1080$
$3 \cdot 2 \cdot 4$	$2^3 \cdot 3 \cdot 5^3 = 3000$
$2 \cdot 4 \cdot 3$	$2 \cdot 3^3 \cdot 5^2 = 1350$
$2 \cdot 3 \cdot 4$	$2 \cdot 3^2 \cdot 5^3 = 2250$
$3 \cdot 2 \cdot 2 \cdot 2$	$2^2 \cdot 3 \cdot 5 \cdot 7 = 420$
$2 \cdot 3 \cdot 2 \cdot 2$	$2 \cdot 3^2 \cdot 5 \cdot 7 = 630$
$2 \cdot 2 \cdot 3 \cdot 2$	$2 \cdot 3 \cdot 5^2 \cdot 7 = 1050$
$2 \cdot 2 \cdot 2 \cdot 3$	$2 \cdot 3 \cdot 5 \cdot 7^2 = 1470$

A megoldás: $n = 2^3 \cdot 3^2 \cdot 5 = 360$.

3. A $\sigma(n)$ függvény

3.1. Definíció: $\sigma(n)$-en az $n \geq 1$ szám pozitív osztóinak összegét értjük.

3.1. Tétel:[3] Legyen az n szám általánosított kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Ekkor az n szám pozitív osztóinak összege

$$\sigma(n) = \left(p_1^0 + p_1^1 + \dots + p_1^{\alpha_1}\right)\left(p_2^0 + p_2^1 + \dots + p_2^{\alpha_2}\right) \dots \left(p_s^0 + p_s^1 + \dots + p_s^{\alpha_s}\right) = \prod_{i=1}^{s} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Bizonyítás: Már az előzőekben láttuk, hogy n összes osztója előáll

$$d = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s}$$

alakban, ahol egymástól függetlenül minden $i = 0, 1, \dots, s$-re β_i felveszi a $0, 1, \dots \alpha_i$ számokat. Másrészt n minden osztója előáll ilyen alakban, és mindegyik csak egyféleképpen, tehát ezen d-k összege, az n szám összes osztóinak összege, azaz $\sigma(n)$.

Ha a

$$\prod_{i=1}^{s} (1 + p_i + {p_i}^2 + \dots + {p_i}^{\alpha_i})$$

szorzást elvégezzük, akkor is az előbbi összeget kapjuk. Például a ${p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s}$ szorzat úgy keletkezik, ha $\prod_{i=1}^{s}(1 + p_i + {p_i}^2 + \dots + {p_i}^{\alpha_i})$-ből minden i. tagból összeszorzom a ${p_i}^{\beta_i}$-ket, ahol $i = 0, 1, \dots, s$.

A

$$\prod_{i=1}^{s} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

úgy adódik, hogy az első képletre alkalmazzuk a mértani sorozat összegképletét.

Példa: Legyen $n = 24$, ekkor az osztói, az $1, 2, 3, 4, 6, 8, 12, 24$ számok. Ezek összege: $1 + 2 + 3 + 4 + 6 + 8 + 12 + 24 = 60$.

Képlettel:

$$\sigma(24) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 60.$$

Tulajdonságok:

- $n = 1$ esetén $\sigma(n) = 1$.
- Ha n prím, vagyis $n = p$, akkor

$$\sigma(n) = \frac{p^2 - 1}{p - 1} = p + 1,$$

ez következik a prímszám definíciójából.

- Ha n prímhatvány, vagyis $n = p^\alpha$, akkor

$$\sigma(n) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

3.2. Tétel: A $\sigma(n)$ függvény multiplikatív.

Bizonyítás: Azt kell belátnunk, hogy ha $(a, b) = 1$, akkor $\sigma(ab) = \sigma(a) \cdot \sigma(b)$.

Legyen az a és b prímtényezős a felbontása a következő:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

$$b = {p_{s+1}}^{\beta_{s+1}} {p_{s+2}}^{\beta_{s+2}} \dots {p_{s+t}}^{\beta_s + t},$$

ahol $p_1, p_2, \dots, p_{s+t}$ különböző prímek.

Ekkor az ab prímtényezős felbontása:

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{s+t}^{\alpha_{s+t}}.$$

A $\sigma(n)$ függvény képletét alkalmazva kapjuk, hogy:

$$\sigma(a) \cdot \sigma(b) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_{s+t}^{\alpha_{s+t}+1} - 1}{p_{s+t} - 1} = \sigma(ab).$$

Példa: $n = 15$-re

$$\sigma(3) = \frac{3^2 - 1}{3 - 1} = 4$$

$$\sigma(5) = \frac{5^2 - 1}{5 - 1} = 6$$

$$\sigma(15) = \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 24$$

$$\sigma(3) \cdot \sigma(5) = \sigma(15)$$

Megjegyzés: A $\sigma(n)$ függvény nem teljesen multiplikatív.

Példa: $n = 18$-ra

$$\sigma(3) = \frac{3^2 - 1}{3 - 1} = 4$$

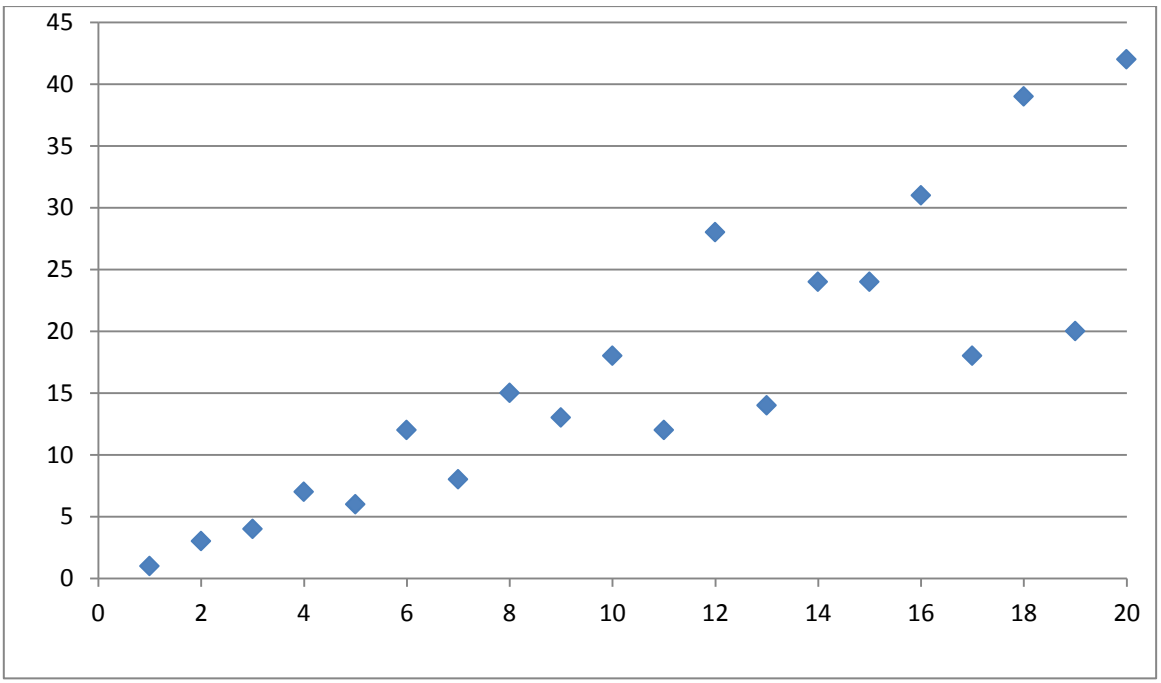
$$\sigma(6) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 12$$

$$\sigma(18) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 39$$

$$\sigma(3) \cdot \sigma(6) = 48 \neq 39 = \sigma(18)$$

A $\sigma(n)$ függvény néhány értéke:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20	42



Alkalmazása: *A tökéletes számok*

3.2. Definíció: Az n pozitív egész számot tökéletes számnak nevezzük, ha n egyenlő a nála kisebb pozitív osztóinak összegével, vagyis $\sigma(n) = 2n$.

Például:

$n = 6$ esetén:

$$\sigma(6) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 2 \cdot 6 = 12$$

$n = 28$ esetén:

$$\sigma(28) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 2 \cdot 28 = 56$$

3.3. Tétel: Az n szám pontosan akkor tökéletes, ha felírható $2^{p-1}(2^p - 1)$ alakban, ahol $2^p - 1$ prímszám és p is prímszám.

3.4. Tétel: A $2^n - 1$ nem prímszám, ha n összetett szám.

Bizonyítás: Mivel $n = ab$, ahol a és b is nagyobbak 1-nél. Ekkor $2^n - 1 = (2^b)^a - 1^a$ miatt osztható $(2^b - 1)$-gyel és $1 < 2^b - 1 < 2^n - 1$.

Következmény: Ha $2^n - 1$ prím, akkor n is prím.

3.3. Definíció: Ha $2^p - 1$ prím, akkor azt Mersenne-prímnek hívjuk. Jelölése: M_p

A névadó Marin Mersenne (1588-1648) megállapítása, hogy $2^p - 1$ prím, ha $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257,$ de minden más $0 < p < 257$ számra összetett. Állítását nem igazolta. Az 1588-ig az első 7 eset már ismert volt. A $p = 31$-et 1772-ben Euler igazolta. Az első hibát a listában 1876-ban Lucas fedezte fel, miszerint a $2^{67} - 1$ összetett szám. Később további hibákat is felfedeztek. 1883-ban Pervushin kiegészítette a felsorolást a $2^{61} - 1$ számmal, majd Powers is még kettővel, a $2^{89} - 1$-gyel (1911) és a $2^{107} - 1$-gyel (1914). 1947-re derült ki, hogy $p = 257$ is összetett szám, így a helyes lista $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89,\ 107, 127.$

Jelenleg 47 Mersenne-prímet ismerünk. A legújabb felfedezések:

- A 45.-et 2008. augusztus 23-án találták meg. Ez a $2^{43\,112\,609} - 1$ alakú szám, mely 12 978 189 számjegyből áll. Ez a ma ismert legnagyobb prímszám is.
- A 46.-at nem sokkal az előző után, 2008. szeptember 6-án fedezték fel. Ez, az előzőnél kisebb, 11 185 272 számjegyet számláló $2^{37\,156\,667} - 1$ szám.
- A 47. megtalálására 2009. április 12-én került sor. A $2^{42\,643\,801} - 1$ szám 12 837 064 darab számjegyével a második legnagyobb jelenleg ismert prímszám.[10],[13]

A páros tökéletes számok egy kettő hatvány és egy Mersenne-prím szorzataként állnak elő.

A matematika egyik legrégebbi nyitott kérdése, hogy léteznek-e páratlan tökéletes számok. A témában számos eredmény született, de mindmáig nem sikerült ilyen számot találniuk és cáfolni a létezésüket.

Bármelyik n páratlan tökéletes számnak ki kell elégítenie a következő feltételeket:

- $n > 10^{300}$. Egy kutatásban próbaképpen megmutatták, hogy $n > 10^{1500}$, de bebizonyítani még nem tudták.
- $n = {p_1}^{2\alpha_1} {p_2}^{2\alpha_2} \dots {p_s}^{2\alpha_s} q^{\alpha}$, ahol $p_1, p_2, \dots, p_s, q$ különböző prímek,és $q \equiv \alpha \equiv 1\ (mod\ 4)$.
- Az n szám legnagyobb prímtényezője nagyobb, mint 10^8.
- A második legnagyobb prímtényezője nagyobb, mint 10^4.
- A harmadik legnagyobb prímtényezője nagyobb, mint 100.
- n-nek legalább 75 prímtényezőből áll, amiben van legalább 9 különböző.
- Ha a 3 nem szerepel n prímtényezős felbontásában, akkor n-nek van legalább 12 különböző prímtényezője.[11]

Feladatok:

3.1. Feladat: Bizonyítsuk be, hogy bármely páros tökéletes szám utolsó számjegye 6 vagy 8.

Megoldás: A páros tökéletes számok $2^{p-1}(2^p - 1)$ alakúak, ahol p prímszám. Készítsünk táblázatot p különböző értékeihez. Mivel a 10-es számrendszerben vizsgálódunk, ezért $mod\ 10$ nézzük az értékeket, hiszen ez adja meg a szám utolsó számjegyét.

p	$2^{p-1}\ (mod\ 10)$	$2^p - 1\ (mod\ 10)$	$n\ (mod\ 10)$
1	1	1	1
2	2	3	6
3	4	7	8
4	8	5	0
5	6	1	6
6	2	3	6
7	4	7	8
8	8	5	0
9	6	1	6
10	2	3	6
11	4	7	8

$2^a \equiv 2^b\ (mod\ 2)$, és $2^a \equiv 2^b\ (mod\ 5)$, ha $a \equiv b\ (mod\ 4)$, ugyanis $2^a \equiv 2^{4+a}\ (mod\ 5)$, átalakítva $2^a \equiv 16 \cdot 2^a\ (mod\ 5)$, azaz $2^a \equiv 2^a\ (mod\ 5)$. Mivel 2 és 5 relatív prímek, így $2^a \equiv 2^b\ (mod\ 10)$, ha $a \equiv b\ (mod\ 4)$, tehát a 2^{p-1} értékei már $p = 6$-tól négyesével ismétlődnek, A kettő hatványokhoz hasonlóképp ismétlődnek a $2^p - 1$ értékei is, mivel ezek eggyel kisebb számok azoknál. Emiatt n utolsó számjegyei is periodikusak. Minden páratlan p esetén n 6-ra vagy 8-ra végződik, így minden páratlan prímszám esetén is. $p = 2$-re $2^{p-1}(2^p - 1) = 6$, tehát bebizonyítottuk, hogy minden páros tökéletes szám utolsó számjegye 6 vagy 8.

3.2. Feladat: Mennyi egy tökéletes szám pozitív osztóinak reciprokösszege?

Megoldás: Az n pozitív osztói: $d_1, d_2, d_3, \dots, d_{d(n)}$, ahol d_i és $d_{d(n)-i+1}$ osztópárok.

A kérdés, hogy mennyi a következő összeg értéke:

$$\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_{d(n)}}.$$

A kifejezést alakítsuk át úgy, hogy közös nevezőre hozzuk a törtet, mivel minden tört nevezője n-nek egy osztója, és az összes pozitív osztót felsoroltuk, így a legkisebb közös többszörösük, az n szám lesz a közös nevező.

$$\frac{d_{d(n)} + d_{d(n)-1} + \cdots + d_2 + d_1}{n}$$

A számlálóba ekkor minden szám osztópárja kerül. Amennyiben n -nek páratlan sok osztója van, tehát létezik d_k, melynek nincs osztópárja, vagyis $d_k = \sqrt{n}$, akkor $\frac{1}{d_k} = \frac{d_k}{\sqrt{n}}$. Így a számlálóba n összes osztója kerül, amiről tudjuk, hogy az összege $2n$. Tehát a reciprokösszeg:

$$\frac{d_{d(n)} + d_{d(n)-1} + \cdots + d_2 + d_1}{n} = \frac{\sigma(n)}{n} = \frac{2n}{n} = 2.$$

3.3. Feladat:[7] Mutassuk meg, hogy végtelen sok x természetes számra a $\sigma(n) = x$ egyenletnek

a) legalább 2,
b) legalább 3

megoldása van!

Megoldás: A $\sigma(n)$ függvény multiplikatív tulajdonságát használjuk ki, azaz ha $(a, b) = 1$, akkor $\sigma(ab) = \sigma(a) \cdot \sigma(b)$.

a) Ha $\sigma(a) = \sigma(b)$ és $(ab, c) = 1$, akkor $\sigma(ac) = \sigma(bc)$. És mivel végtelen sok prímszám van, így létezik végtelen sok c is, amely kielégíti az egyenletet.
   Például, a táblázatból látható, hogy $\sigma(6) = \sigma(11) = 12$. Legyen $c = 5$, ekkor a $\sigma(30) = \sigma(55) = 72$ is egy jó megoldás.
b) Az a) részhez hasonlóan járunk el. Ha $\sigma(a) = \sigma(b) = \sigma(c)$ és $(abc, d) = 1$, akkor $\sigma(ad) = \sigma(bd) = \sigma(cd)$.
   Például, tudjuk, hogy $\sigma(14) = \sigma(15) = \sigma(23) = 24$. Legyen $d = 11$, ekkor a $\sigma(154) = \sigma(165) = \sigma(253) = 288$ is jó megoldást ad.

3.4. Feladat: Mely n természetes számokra páratlan $\sigma(n)$ értéke?

Megoldás: A következő képletet használjuk fel:

$$\prod_{i=1}^{s} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Ez akkor páratlan, ha minden tényezője is az.

Esetszétválasztással vizsgáljuk a szorzat tényezőit.

1) Ha $p_i = 2$, akkor a $\frac{2^{\alpha_1+1}-1}{2-1}$ hányados páratlan.
2) Ha $p_i \neq 2$.
   A képletet alakítsuk át a következő módon:

$$\frac{p^{\alpha+1}-1}{p-1} = (p^{\alpha} + p^{\alpha-1} + \cdots + p + 1).$$

A $(p^{\alpha} + p^{\alpha-1} + \cdots + p + 1)$ kifejezésben minden tag páratlan. Az összeg paritása csak α-tól függ. Ha α páros, akkor az összeg páratlan tagú, így értéke is páratlan, ha, α páratlan, akkor az összeg páros sok tagból áll, ezért az értéke is páros.

Ez alapján azok a számok elégítik ki a feladatot, amelyek négyzetszámok, vagy egy négyzetszám kétszeresei.

3.5. Feladat: Mely n természetes számokra teljesül, hogy $\sigma(2n) = 3\sigma(n)$?

Megoldás: A $\sigma(n)$ függvény képletét használjuk fel a megoldás során.

Felírjuk n és $2n$ kibővített kanonikus alakját, majd behelyettesítjük őket a képletbe:

$$n = 2^{\alpha_1}3^{\alpha_2} \dots p_s^{\alpha_s},$$

$$2n = 2^{\alpha_1+1}3^{\alpha_2} \dots p_s^{\alpha_s},$$

$$\sigma(n) = \frac{2^{\alpha_1+1}-1}{2-1} \cdot \frac{3^{\alpha_2+1}-1}{3-1} \cdot \dots \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1},$$

$$\sigma(2n) = \frac{2^{\alpha_1+2}-1}{2-1} \cdot \frac{3^{\alpha_2+1}-1}{3-1} \cdot \dots \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1}.$$

Ezek segítségével felírhatjuk az egyenletünket:

$$\frac{2^{\alpha_1+2}-1}{2-1} \cdot \frac{3^{\alpha_2+1}-1}{3-1} \cdot \dots \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1} = 3 \cdot \frac{2^{\alpha_1+1}-1}{2-1} \cdot \frac{3^{\alpha_2+1}-1}{3-1} \cdot \dots \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1}.$$

Egyszerűsítés után:

$$2^{\alpha_1+2} - 1 = 3 \cdot 2^{\alpha_1+1} - 3,$$

$$4 \cdot 2^{\alpha_1} - 1 = 6 \cdot 2^{\alpha_1} - 3,$$

$$2 = 2 \cdot 2^{\alpha_1},$$

$$1 = 2^{\alpha_1},$$

ahonnan az eredmény $\alpha_1 = 0$. Tehát azon n-ekre teljesül az egyenlet, ahol n páratlan szám.

3.6. Feladat: Keressük meg azt az n természetes számot, melyre

a) $\sigma(n) = 3$,

b) $\sigma(n) = 10$.

Megoldás:

a) A $\sigma(n) \geq n + 1$, tehát $n \leq 2$ lehet, ahonnan $n = 2$ jó.

b) $\sigma(n) \geq n + 1$ miatt n legfeljebb 9 lehet. 1-től 9-ig ellenőrizve $\sigma(n)$-t arra jutunk, hogy a feladatnak nincs megoldása.

3.7. Feladat: Mely n természetes számokra teljesül, hogy

a) $\sigma(n) = n + 2$,

b) $\sigma(n) = n + 3$?

Megoldás:

a) Mivel 1 és n osztja n-et,

$$\sigma(n) = n + 1 + \sum_{\substack{d|n \\ 1<d<n}} d,$$

tehát $\sum_{\substack{d|n \\ 1<d<n}} d = 1$, ez viszont ellentmondás, tehát nincs megoldás.

b) Az a) feladathoz hasonlóan $\sum_{\substack{d|n \\ 1<d<n}} d = 2$, tehát n osztói: 1, 2, n, ahonnan $d = 2$ lehet csak. Így $n = 4$.

3.8. Feladat:[7] Bizonyítsuk be, hogy ha n 1-nél nagyobb természetes szám, mely nem prímszám, vagy prímszám négyzete, akkor $\sigma(n) \geq (\sqrt{n} + 1)^2$.

Megoldás: Legyen n legkisebb prímosztója p. Ekkor $\sigma(n) \geq 1 + p + \frac{n}{p} + n$. Azt kell belátni, hogy $1 + p + \frac{n}{p} + n \geq (\sqrt{n} + 1)^2$. Vizsgáljuk ezt az egyenlőtlenséget:

$$1 + p + \frac{n}{p} + n \geq n + 2\sqrt{n} + 1,$$

$$p + \frac{n}{p} \geq 2\sqrt{n},$$

$$\frac{p + \frac{n}{p}}{2} \geq \sqrt{p \cdot \frac{n}{p}}.$$

Ez mindig igaz a számtani és mértani közép közti egyenlőtlenség miatt. Ezzel beláttuk a feladatot.

4. A $\varphi(n)$ függvény

4.1. Definíció: $\varphi(n)$-en az $[1, n]$-ban az n-hez relatív prímek számát értjük.

4.1. Tétel:[3] Legyen n kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Ekkor az n-hez relatív prímek száma

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \dots \left(p_s^{\alpha_s} - p_s^{\alpha_s - 1}\right).$$

A képlet egyéb formái:

$$\varphi(n) = \prod_{i=1}^{s}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) = n\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \mid n \\ p\ prím}} \left(1 - \frac{1}{p}\right)$$

Bizonyítás: A logikai szitaformulát használjuk fel hozzá.

A cél, hogy kiszámítsuk, hány olyan szám van az $1, 2, \dots, n$ egészek között, amelyek relatív prímek az n-hez. Ez azt jelenti, hogy nem oszthatók a $p_1, p_2, \dots, p_s$ prímek egyikével sem.

Azoknak a számoknak a száma, amelyek egy rögzítetett p_j-vel oszthatók:

$$\frac{n}{p_j}.$$

Vegyük most azokat, amelyek több prímmel is oszthatóak. Egy egész pontosan akkor osztható adott prímek mindegyikével, ha a szorzatukkal is osztható. Például ha egy szám osztható p_j-vel és p_k-val is, akkor osztható a szorzatukkal, vagyis $p_j p_k$-val is.

Ezek alapján felírhatjuk a logikai szitaformulát:

$$\varphi(n) = n - \frac{n}{p_1} - \dots - \frac{n}{p_s} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \dots + \frac{n}{p_{s-1} p_s} - \frac{n}{p_1 p_2 p_3} \dots$$

A képlet jobb oldala egyenlő

$$\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)$$

szorzattal, mely számolással ellenőrizhető, és ez a tételben szereplő képlet egy formája.

Példa: Legyen $n = 24$, ekkor a hozzá relatív prímek, az $1, 5, 7, 11, 13, 17, 19, 23$ számok.

Képlettel: $\varphi(24) = (2^3 - 2^2)(3^1 - 3^0) = 8.$

Tulajdonságok:

- $n = 1$ esetén $\varphi(n) = 1$.
- Ha n prím, vagyis $n = p$, akkor $\varphi(n) = p - 1$.
- Ha n prímhatvány, vagyis $n = p^{\alpha}$, akkor $\varphi(n) = p^{\alpha} - p^{\alpha-1}$.

4.2. Tétel: A $\varphi(n)$ függvény multiplikatív.

Bizonyítás: [5] A következő képletet kell belátni:

$$\varphi(ab) = \varphi(a) \cdot \varphi(b), \text{ ha } (a, b) = 1.$$

Táblázatba írjuk az 1 és ab közti számokat a következőképpen:

1	2	$\cdots$	a
$a+1$	$a+2$	$\cdots$	$2a$
$2a+1$	$2a+2$	$\cdots$	$3a$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$ra+1$	$ra+2$	$\cdots$	$(r+1)a$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(b-1)a+1$	$(b-1)a+2$	$\cdots$	ba

Azoknak a számoknak a száma, amelyek ab-hez relatív prímek: $\varphi(ab)$.

Egy szám akkor és csak akkor relatív prím az ab-hez, ha külön az a-hoz és külön a b-hez is relatív prím. Így azokat az elemeket kell kikeresni a táblázatból, amelyek a-hoz is és b-hez is relatív prímek. A táblázat minden egyes oszlopa ugyanabba a maradékosztályba tartozik $mod\ a$, és minden egyes sora teljes maradékrendszert alkot $mod\ a$, tehát azoknak az oszlopoknak a száma, amelyek elemei relatív prímek a-hoz: $\varphi(a)$.

Például egy ilyen oszlop:

$$q, a+q, 2a+q, \dots, (b-1)a+q.$$

Azt kell még belátni, hogy ez teljes maradékrendszert alkot $mod\ b$ szerint is.

A $0, 1, 2, \dots, b-1$ számok teljes maradékrendszert alkotnak $mod\ b$-re nézve. Feltettük, hogy $(a, b) = 1$, így az előbbi számokat a-val szorozva, majd mindegyikhez q-t hozzáadva, újfent teljes maradékrendszert kapunk $mod\ b$ ([3] 2.2.4 Tétele alapján). Tehát minden oszlopban a b-hez relatív prímek száma: $\varphi(b)$. Ezek alapján az a-hoz is és b-hez is relatív prímek száma: $\varphi(a) \cdot \varphi(b)$, ez az érték a fentiek alapján egyenlő $\varphi(ab)$-vel, tehát a függvény multiplikatív.

Példa: $n = 15$-re

$$\varphi(3) = 3 - 1 = 2$$
$$\varphi(5) = 5 - 1 = 4$$
$$\varphi(15) = (3 - 1)(5 - 1) = 8$$
$$\varphi(3) \cdot \varphi(5) = \varphi(15)$$

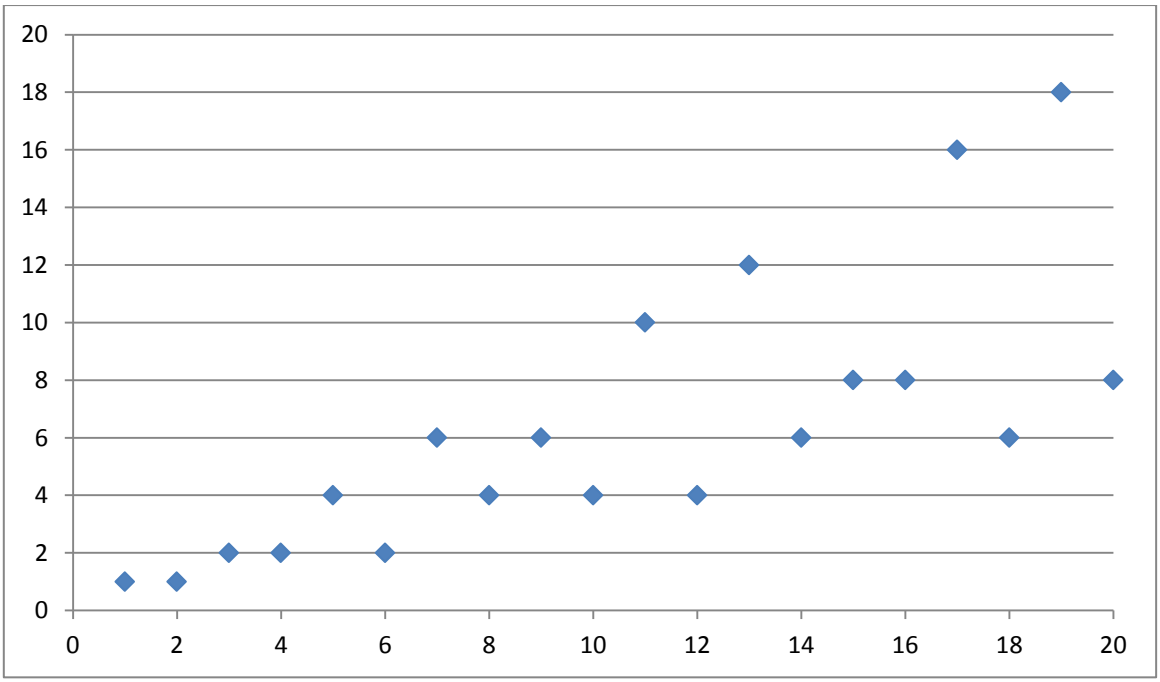
Megjegyzés: A $\varphi(n)$ függvény nem teljesen multiplikatív.

Példa: $n = 18$-ra

$$\varphi(3) = 3 - 1 = 2$$
$$\varphi(6) = (2 - 1)(3 - 1) = 2$$
$$\varphi(18) = (2 - 1)(3^2 - 3) = 6$$
$$\varphi(3) \cdot \varphi(6) = 4 \neq 6 = \varphi(18)$$

A $\varphi(n)$ függvény néhány értéke:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8



Alkalmazása: *Maradékosztályok, maradékrendszerek, az Euler – Fermat-tétel*

4.2. Definíció: Adott n modulusra azonos maradékot adó számok halmaza egy maradékosztály.
Jelölése az a-val kongruens elemek halmazára n modulus mellett: $(a)_n$.

Példa: $(7)_3 = \{\dots, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, \dots\} = (40)_3$

4.3. Definíció: Adott n modulusra a teljes maradékrendszer olyan számhalmaz, amely minden maradékosztályból pontosan egy elemet tartalmaz.

Példa: $\{-11, 17, 3\}$ teljes maradékrendszer $mod\ 3$.

4.4. Definíció: Adott n modulusra a redukált maradékosztály olyan maradékosztály, amelynek elemei n-hez relatív prímek.

4.5. Definíció: Adott n modulusra a redukált maradékrendszer olyan számhalmaz, amely minden redukált maradékosztályból pontosan egy elemet tartalmaz.

Példa: $\{-15, 11, -3, 7\}$ redukált maradékosztály $mod\ 8$.

4.3. Tétel: Az $a_1, a_2, \dots, a_k$ számok pontosan akkor alkotnak redukált maradékrendszert $mod\ n$, ha

(1) $k = \varphi(n)$,
(2) $mod\ n$ páronként inkongruensek,
(3) Minden i-re, ahol $i = 1, 2, \dots, k$ $(a_i, n) = 1$.

4.5. Tétel (Euler – Fermat-tétel): Ha $m > 1$, $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor

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

Feladatok:

4.1. Feladat:[7] Milyen n pozitív egészekre igaz a $\varphi(2n) = \varphi(3n)$ egyenlet?

Megoldás: Az n kibővített kanonikus alakja $n = 2^{\alpha_1}3^{\alpha_2} \dots p_s^{\alpha_s}$, másképp $n = 2^{\alpha_1}3^{\alpha_2}x$, ahol $x = {p_3}^{\alpha_3}{p_4}^{\alpha_4} \dots {p_s}^{\alpha_s}$ és $(x, 2 \cdot 3) = 1$. A megoldás menete során különböző eseteket vizsgálunk, mivel φ kiszámításánál a kanonikus alak használható csak.

- Tegyük fel, hogy $\alpha_1, \alpha_2 \geq 1$.

  $$\varphi(2^{\alpha_1+1}3^{\alpha_2}x) = \varphi(2^{\alpha_1}3^{\alpha_2+1}x)$$

  A φ multiplikatív tulajdonsága miatt ez átalakítható a következőképp:

  $$\varphi(2^{\alpha_1+1}3^{\alpha_2}) \cdot \varphi(x) = \varphi(2^{\alpha_1}3^{\alpha_2+1}) \cdot \varphi(x)$$

  Ezt $\varphi(x)$-szel egyszerűsítve, és a képletbe behelyettesítve kapjuk, hogy:

  $$(2^{\alpha_1+1} - 2^{\alpha_1})(3^{\alpha_2} - 3^{\alpha_2-1}) = (2^{\alpha_1} - 2^{\alpha_1-1})(3^{\alpha_2+1} - 3^{\alpha_2})$$

  $$2(2^{\alpha_1} - 2^{\alpha_1-1})(3^{\alpha_2} - 3^{\alpha_2-1}) = (2^{\alpha_1} - 2^{\alpha_1-1})3(3^{\alpha_2} - 3^{\alpha_2-1})$$

  Ebből $2 = 3$-at kapunk eredményül, ami ellentmondás, tehát az $\alpha_1, \alpha_2 \geq 1$ esetben nincs megoldása az egyenletnek.

- Legyen $\alpha_1 = 0, \alpha_2 = 0$.

  Ekkor $\varphi(2x) = \varphi(3x)$, ahol $(x, 6) = 1$, azaz $\varphi(2) = \varphi(3)$, ami ellentmondás.

- Legyen $\alpha_1 = 0, \alpha_2 \geq 1$.

  Ekkor $\varphi(2 \cdot 3^{\alpha_2} \cdot x) = \varphi(3^{\alpha_2+1} \cdot x)$, ahol $(x, 6) = 1$, vagyis

  $$\varphi(2) \cdot \varphi(3^{\alpha_2}) \cdot \varphi(x) = \varphi(3^{\alpha_2+1}) \cdot \varphi(x),$$

  tehát $\varphi(3^{\alpha_2}) = \varphi(3^{\alpha_2+1})$, ami ellentmondás.

- Legyen $\alpha_1 \geq 1, \alpha_2 = 0$.

  Ekkor $\varphi(2^{\alpha_1+1} \cdot x) = \varphi(2^{\alpha_1} \cdot 3 \cdot x)$, ahol $(x, 6) = 1$, azaz

  $$\varphi(2^{\alpha_1+1}) = \varphi(2^{\alpha_1}) \cdot \varphi(3),$$

  ami igaz. Tehát ebben az esetben van az egyenletnek megoldása, és azon számok elégítik ki, ahol $n = 2^k x$, ahol $(x, 6) = 1$ és $k \in \mathbb{Z}^+$.

4.2. Feladat:[7] Oldjuk meg a $2\varphi(n) = n$ egyenletet!

Megoldás: A feladat megoldásához a $\varphi(n)$ következő képletét használjuk fel:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

ahol p prím. Ezt behelyettesítjük az eredeti egyenletbe.

$$2n\prod_{p|n}\left(1-\frac{1}{p}\right)=n$$

$$2\prod_{p|n}\left(1-\frac{1}{p}\right)=1$$

$$\prod_{p|n}\left(1-\frac{1}{p}\right)=\frac{1}{2}$$

Ez pontosan akkor teljesül, ha a prímtényezős felbontásban csak a 2 szerepel. Vagyis az $n=2^k$ alakú számok lesznek jók, ahol $k\in\mathbb{Z}^+$.

4.3. Feladat:[3] Bizonyítsuk be, hogy $n>2$ esetén $\varphi(n)$ értéke páros szám!

Megoldás: A feladat menete során $\varphi(n)$ egyik képletét használjuk:

$$\varphi(n)=\prod_{i=1}^{s}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)$$

- Ha az n prímtényezős felbontásában van páratlan p_i, akkor annak hatványai is páratlanok. Két páratlan szám különbsége páros, tehát $\varphi(n)$ is páros.
- Ha nincs páratlan p_i, akkor $n=2^k$ alakú, ahol $k>1$. Ekkor

  $$\varphi(n)=2^k-2^{k-1}=2^{k-1},$$

  ami páros, mert $k-1>0$.

4.4. Feladat:[7] Melyek azok a természetes számok, amelyekre $\varphi(n)$ értéke páratlan?

Megoldás: Az előző feladatban láthattuk, hogy $n>2$ esetén $\varphi(n)$ páros lesz. Így elég ellenőrizni az $n=1$ és $n=2$ esetet.

- A függvény tulajdonsága, hogy $n=1$ esetén $\varphi(n)=1$, tehát páratlan.
- $n=2$-t helyettesítve:

  $$\varphi(n)=2-1=1,$$

  ez szintén páratlan.

Így mindkét eset jó megoldást ad.

4.5. Feladat:[7] Oldjuk meg a $\varphi(n)=n-2$ egyenletet!

Megoldás: Mivel $\varphi(n)\neq n-1$, vagyis n nem prímszám, és $n\neq 1$, ezért n csak összetett szám lehet. Legyen az n legkisebb prímosztója p. Ekkor biztosan $p\leq\sqrt{n}$.

Indirekt tegyük fel, hogy $3 \leq \sqrt{n}$, vagyis $9 \leq n$. Ebben az esetben $1 < p < 2p < 3p \leq n$, mivel $p \leq \sqrt{n}$ és $3 \leq \sqrt{n}$, továbbá $(ip, n) > 1$, ahol $i = 1, 2, 3$. Így n-hez van három nem relatív prím n-ig, tehát $\varphi(n) \leq n - 3$, ami ellentmondás.
A fentiek miatt $n < 9$ és összetett szám, azaz csak a 4, 6 vagy 8 lehet. Ezeket behelyettesítve $\varphi(n)$ képletébe kapjuk, hogy az egyetlen jó megoldás az $n = 4$.

4.6. Feladat: Mely n természetes számokra lesz

a) $\varphi(n) = 9$,

b) $\varphi(n) = 18$?

Megoldás:

a) $\varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)$ alapján p_i csak 2 lehet, hogy a szorzat páratlan legyen. Ha $n = 2^{\alpha}$, akkor $\varphi(n) = 2^{\alpha - 1}$, mely sosem egyenlő 9-cel, tehát nincs ilyen n szám.

b) $\varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)$-ből következik, hogy $p_i - 1 | 18$ és $p_i^{\alpha_i - 1} | 18$.
A $p_i - 1 | 18$-ból $p_i - 1 = 1, 2, 3, 6, 9, 18$, így $p_i = 2, 3, 7, 19$ lehet. Legyenek ezek kitevői rendre $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. A $p_i^{\alpha_i - 1} | 18$ alapján $\alpha_1 \leq 2, \alpha_2 \leq 3, \alpha_3 \leq 1, \alpha_4 \leq 1$. Mivel 4 nem osztja 18-at ezért n-nek nem lehet két különböző páratlan prímosztója. Tegyük fel, hogy $\alpha_1 = 2$. Mivel $n = 2^2$ nem jó, ezért $\alpha_2, \alpha_3, \alpha_4$ nem mind 0. Ekkor $\prod_{i=1}^{4} p_i^{\alpha_i - 1}(p_i - 1)$ szorzatban van legalább két páros tényező, ami azt jelentené, hogy $4 | \varphi(n)$, ami ellentmondás, tehát $\alpha_1 \leq 1$. Tegyük fel, hogy $\alpha_3 = 1$. Ekkor azonban sem az $n = 7$, sem az $n = 14$ nem jó, tehát $\alpha_3 = 0$. $\alpha_1 = 0$ esetén $n = 3^{\alpha_2}$ vagy $n = 19^{\alpha_4}$. Ezek közül a 27 és a 19 ad jó megoldást. $\alpha_1 = 1$ esetén $n = 2 \cdot 3^{\alpha_2}$ vagy $n = 2 \cdot 19^{\alpha_4}$, amelyekből 54 és 38 lesz jó.

5. A $\mu(n)$ függvény

5.1. Definíció:[3] A $\mu(n)$ függvényen az alábbi számelméleti függvényt értjük:

- $\mu(n) = 1$, ha $n = 1$,
- $\mu(n) = (-1)^s$, ha az $n = p_1 p_2 \dots p_s$, vagyis az n szám négyzetmentes,
- $\mu(n) = 0$, ha $\exists\, p$, melyre $p^2 \mid n$, vagyis az n szám nem négyzetmentes.

5.1. Tétel: A $\mu(n)$ függvény multiplikatív.

Bizonyítás: A következő képletet kell belátni:

$$\mu(ab) = \mu(a) \cdot \mu(b), \text{ ha } (a, b) = 1.$$

Esetszétválasztással dolgozunk.

1. $a = b = 1$:
   Triviális.
2. $a = 1$, $b = p_1 p_2 \dots p_s$:
   Ekkor a $\mu(ab) = \mu(b)$, $\mu(a) = 1$, tehát $\mu(ab) = \mu(a) \cdot \mu(b)$ igaz.
   Szimmetria okok miatt ugyanígy igaz, ha $b = 1$ és $a = p_1 p_2 \dots p_s$.
3. $a = 1$, $\mu(b) = 0$:
   Tehát $\mu(a) = 1$, $\mu(ab) = \mu(b)$, így $\mu(ab) = \mu(a) \cdot \mu(b)$.
   Ugyanez igaz, a $b = 1$, $\mu(a) = 0$ esetre is.
4. $a = p_{\alpha_1} p_{\alpha_2} \dots p_{\alpha_s}$, $b = p_{\beta_1} p_{\beta_2} \dots p_{\beta_t}$:
   Definíció szerint $\mu(a) = (-1)^s$, $\mu(a) = (-1)^t$, ezért $\mu(a) \cdot \mu(b) = (-1)^{s+t}$,
   Az $ab = p_{\alpha_1} p_{\alpha_2} \dots p_{\alpha_s} p_{\beta_1} p_{\beta_2} \dots p_{\beta_t}$ miatt $\mu(ab) = (-1)^{s+t}$.
5. $a = p_1 p_2 \dots p_s$, $\mu(b) = 0$:
   Vagyis $\mu(a) = (-1)^s$, $\mu(a) \cdot \mu(b) = 0$
   Mivel b nem négyzetmentes, így ab sem lesz az, tehát $\mu(ab) = 0$.
   Ugyanez igaz a $b = p_1 p_2 \dots p_s$, $\mu(a) = 0$ esetre is.
6. $\mu(a) = 0$, $\mu(b) = 0$:
   Tehát $\mu(a) \cdot \mu(b) = 0$. És mivel sem az a sem a b nem négyzetmentes, így a szorzatuk sem lesz az, vagyis $\mu(ab) = 0$.

Ezzel az a tételt beláttuk.

Példa: $n = 15$-re

$$\mu(3) = -1$$
$$\mu(5) = -1$$
$$\mu(15) = (-1)^2 = 1$$
$$\mu(3) \cdot \mu(5) = \mu(15)$$

Megjegyzés: A $\mu(n)$ függvény nem teljesen multiplikatív.

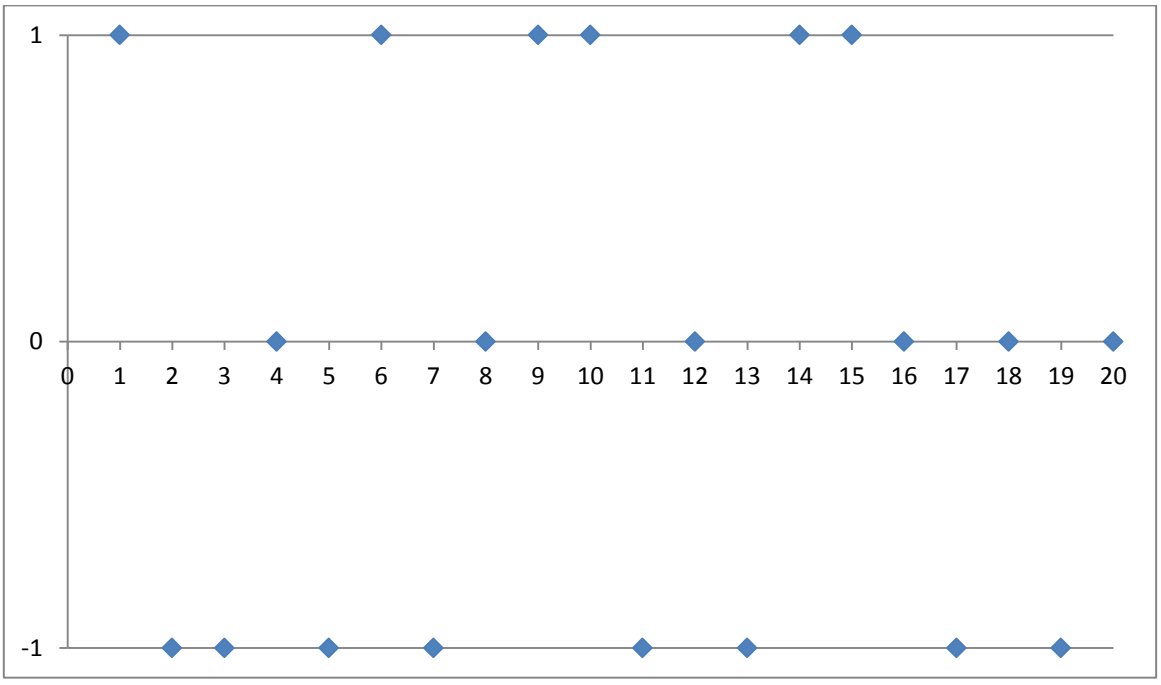
Példa: $n = 18$-ra

$$\mu(3) = -1$$
$$\mu(6) = 1$$
$$\mu(18) = 0$$
$$\mu(3) \cdot \mu(6) = -1 \neq 0 = \mu(18)$$

A $\mu(n)$ függvény néhány értéke:

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

n	11	12	13	14	15	16	17	18	19	20
$\mu(n)$	-1	0	-1	1	1	0	-1	0	-1	0



Alkalmazása: *A primitív n-edik egységgyökök összege*

5.2. Tétel: A primitív n-edik egységgyökök összege $\mu(n)$.

Bizonyítása:[8] A tétel igazolásához a gyökök és együtthatók közti összefüggést használjuk fel. Jelöljük $S(n)$-nel a primitív n-edik egységgyökök összegét, melyek a $\Phi_n(x)$, az n-edik körosztási polinom gyökei. A gyökök és együtthatók összefüggése miatt $S(n)$ egyenlő az $x^{\varphi(n)-1}$ együtthatójának ellentettjével. Továbbá [4] 3.9.5. lemma szerint, ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$. Az x^{n-1}-es tag együtthatóját vizsgáljuk mindkét oldalon. A jobb oldalon ez az érték 0, kivéve, ha $n = 1$, mert abban az esetben -1. A bal oldalon úgy kapjuk meg az x^{n-1}-es tagot, ha egy polinomból a második legmagasabb fokút, a többiből pedig a legmagasabb fokút vesszük. $\Phi_d(x)$-ben a második legmagasabb fokú tag együtthatója $-S(d)$, így x^{n-1} együtthatója az összes $-S(d)$ összege lesz. Ezek alapján felírható, hogy

$$\sum_{d|n} S(d) = \begin{cases} 1, ha\ n = 1, \\ 0, ha\ n \neq 1. \end{cases}$$

A [3] 6.2.4 Tétele alapján:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, ha\ n = 1, \\ 0, ha\ n \neq 1. \end{cases}$$

A [3] 6.5.2 Tétele szerint a számelméleti függvényekre a függvény – összegzési függvény kölcsönösen egyértelmű megfeleltetés, így $S = \mu$.

Feladatok:

5.1. Feladat:[3] Hány egymást követő szám adható meg, hogy $\mu(n)$ azok egyikén sem nulla?

Megoldás: A $\mu(n)$ függvény abban az esetben 0, ha n nem négyzetmentes. Mivel bármelyik négy szomszédos szám között található egy, amelyik osztható 4-gyel, ezért legfeljebb három szám adható meg.

5.2. Feladat:[3] Hány egymást követő szám adható meg, hogy $\mu(n)$ azok mindegyikén nulla legyen?

Megoldás: Azt kell belátni, hogy tetszőleges nagy k természetes számhoz található olyan n természetes szám, hogy $\mu(n+1) = \mu(n+2) = \cdots = \mu(n+k) = 0$.

Tekintsük a következő szimultán kongruenciarendszert, ahol jelölje p_i az i. prímszámot:

$$n + 1 \equiv 0 \ (mod \ {p_1}^2)$$
$$n + 2 \equiv 0 \ (mod \ {p_2}^2)$$
$$\vdots$$
$$n + k \equiv 0 \ (mod \ {p_k}^2).$$

A kínai maradéktétel ([3] 2.6.2 Tétel) miatt ez megoldható, tehát meg tudunk adni akármilyen hosszú nulla sorozatot.

6. Vegyes feladatok

6.1. Feladat: Oldjuk meg az alábbi egyenleteket:

a) $\sigma(n) \cdot \varphi(n) = 10$,

b) $\sigma(n) \cdot \varphi(n) = n^2$.

Megoldás:

a) Tudjuk, hogy $\sigma(n) \geq n \geq \varphi(n)$. Ezért elég két esetet vizsgálni:

- $\sigma(n) = 10$ és $\varphi(n) = 1$

  Ha $\varphi(n) = 1$, akkor $n = 1$ vagy 2, ezek viszont nem megoldások.

- $\sigma(n) = 5$ és $\varphi(n) = 2$

  Ekkor $n < 5$, ezekre a számokra ellenőrizve a feladatot sem kapunk helyes megoldást.

b) $n = 1$-re $\sigma(1) \cdot \varphi(1) = 1 \cdot 1 = 1$, tehát ez jó megoldás.

Ha $n \neq 1$, akkor felírható $n = \prod_{i=1}^{s} {p_i}^{\alpha_i}$ alakban, ahol $\alpha_i > 0$.

Mivel $\sigma(n) = \prod_{i=1}^{s} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$ és $\varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i-1}(p_i - 1)$, ezért

$$\sigma(n) \cdot \varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i-1}\left(p_i^{\alpha_i+1} - 1\right) = \prod_{i=1}^{s}\left({p_i}^{2\alpha_i} - p_i^{\alpha_i-1}\right).$$

Másrészt $n^2 = \prod_{i=1}^{s} {p_i}^{2\alpha_i} > \prod_{i=1}^{s}\left({p_i}^{2\alpha_i} - p_i^{\alpha_i-1}\right)$, így $n^2 > \sigma(n) \cdot \varphi(n)$.

Tehát $n = 1$ ez egyetlen megoldás.

6.2. Feladat:[7] Bizonyítsuk be, hogy tetszőleges n természetes számra $d(n) + \varphi(n) \leq n + 1$.

Megoldás: 2-től n-ig minden szám legfeljebb az egyik tulajdonsággal rendelkezik: vagy osztója n-nek, vagy relatív prím hozzá, és lehetnek még egyéb számok is. Egyedül az 1 rendelkezik mindkét tulajdonsággal, így őt kétszer számoljuk.

6.3. Feladat: Mely n természetes számokra igaz, hogy $d(n) + \varphi(n) = \sigma(n)$?

Megoldás: Az előző feladatot felhasználva elég azt vizsgálnunk, hogy mely n-ekre lesz $n \leq \sigma(n) \leq n + 1$. Ha $\sigma(n) = n$, akkor $n = 1$, ekkor viszont $d(n) + \varphi(n) = 2$, ami ellentmondás. Ha $\sigma(n) = n + 1$, akkor ez azt jelenti, hogy n prím, ekkor $d(n) + \varphi(n) = 2 + n - 1 = n + 1$, tehát az egyenlet megoldásai a prímszámok.

6.4. Feladat:[7] Oldjuk meg az $n + d(n) = \sigma(n)$ (n természetes szám) egyenletet!

Megoldás: Két korábban belátott állításra fogunk támaszkodni: $d(n) \leq 2\sqrt{n}$, illetve ha n 1-nél nagyobb természetes szám, mely nem prím és nem egy prím négyzete, akkor $\sigma(n) \geq \left(\sqrt{n}+1\right)^2$. Eszerint $n + 2\sqrt{n} \geq n + d(n) = \sigma(n) \geq \left(\sqrt{n}+1\right)^2 = n + 2\sqrt{n} + 1$, vagyis $0 \geq 1$, ami viszont ellentmondás. Így megoldás csak abban az esetben lehetséges, ha $n = 1$, prím vagy prímnégyzet. $n = 1$-re $2 = 1$-et kapunk, mely szintén ellentmondás. Ha n helyére prímet helyettesítünk, akkor $p + 2 = p + 1$ újfent ellentmondás. Ha n prímnégyzet, akkor a következő egyenletet kapjuk: $p^2 + 3 = 1 + p + p^2$, ahonnan $p = 2$, tehát $n = 4$ az egyetlen jó megoldás.

7. Hegy- és völgytételek

7.1. Tétel:[3] *(A $d(n)$ függvény hegytétele):* Tetszőleges K pozitív egészhez végtelen sok olyan n található, amelyre egyszerre teljesül, hogy

$$d(n) - d(n-1) > K \text{ és } d(n) - d(n+1) > K.$$

Bizonyítás: Legyen n az első r prímszám szorzata, azaz $n = p_1 p_2 \dots p_r$. Ekkor $d(n) = 2^r$. A $d(n+1)$-re vonatkozó egyenlőtlenséget bizonyítjuk, a $d(n-1)$-es eset igazolása is ugyanígy történik. Az $n+1$ prímek szorzataként a következő alakba írható: $n+1 = q_1 q_2 \dots q_s$, ahol előfordulhat, hogy nem mindegyik prímtényező különböző. Mivel $(n, n+1) = 1$, és n-et az első r prímszám szorzatának választottuk, ezért $q_i > p_r$ bármely i-re. Az $n+1$ osztóit úgy képezzük, hogy a q_i számokból választunk néhányat, és ezeket összeszorozzuk. Mivel a q_i-k között egyformák is lehetnek, ezért előfordulhat olyan eset, mikor egy osztót többféleképpen megkapunk, emiatt $d(n+1) \leq 2^s$. Tegyük fel, hogy $s \geq r$, ekkor

$$n+1 = q_1 q_2 \dots q_s \geq {p_r}^s + 1 \geq {p_r}^r + 1 \geq p_1 p_2 \dots p_r + 2 = n + 2,$$

ami ellentmondás, tehát $s \leq r-1$. Így $d(n+1) \leq 2^{r-1}$. Ebből következik, hogy

$$d(n) - d(n+1) \geq 2^{r-1}, \text{ azaz } 2^{r-1} > K$$

esetén teljesül a tétel.

7.2. Tétel:[3],[7] *(A $\varphi(n)$ függvény hegytétele):* Tetszőlegesen nagy K pozitív egészhez végtelen sok olyan n található, amelyre egyszerre teljesül, hogy

$$\varphi(n) - \varphi(n-1) > K \text{ és } \varphi(n) - \varphi(n+1) > K.$$

Bizonyítás: Legyen n elég nagy prímszám. Ekkor $n-1$ és $n+1$ páros számok lesznek, és $\varphi(n) = n-1$. A $\varphi(n+1)$-re vonatkozó egyenlőtlenséget bizonyítjuk, a $\varphi(n-1)$-es eset igazolása is ugyanígy történik. Mivel $n+1 = 2^{\alpha_1} x$ alakú, ezért a $\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prím}}} \left(1 - \frac{1}{p}\right)$ képlet alapján $\varphi(n+1) \leq \frac{n+1}{2}$. Tehát $\varphi(n+1) \leq \frac{n+1}{2} < \varphi(n) - K$, azaz $\frac{n+1}{2} < n - 1 - K$, amiből $\frac{n-3}{2} > K$ adódik, és végtelen sok olyan n prím van, amire ez igaz.

7.3. Tétel:[3] *(A $d(n)$ függvény völgytétele):* Tetszőleges K pozitív egészhez végtelen sok olyan n található, amelyre egyszerre teljesül, hogy

$$d(n-1)-d(n)>K \text{ és } d(n+1)-d(n)>K.$$

Bizonyítás: Legyen n prímszám, ekkor $d(n)=2$. Ez azt jelenti, hogy $d(n-1)>K+2$, $d(n+1)>K+2$, tehát $n-1$-nek és $n+1$-nek is van legalább $K+3$ osztója. Ez teljesül abban az esetben, ha $2^{K+2}|n-1$ és $3^{K+2}|n+1$, vagyis, ha n megoldása a következő szimultán kongruenciarendszernek:

$$x\equiv 1\ (mod\ 2^{K+2})$$
$$x\equiv -1\ (mod\ 3^{K+2}).$$

Ez a kínai maradéktétel miatt biztosan megoldható, így az összes megoldás:

$$x=x_0+k\cdot 6^{K+2}, k\geq 0.$$

Kell még, hogy az $x_0+k\cdot 6^{K+2}$ számtani sorozatban végtelen sok prím legyen. Mivel $(x_0,2)=1$, $(x_0,3)=1$ ezért $(x_0,6^{K+2})=1$ is igaz, így a Dirichlet-tétel ([3] 5.3.1 Tétel) miatt teljesül.

7.4. Tétel:[3],[7] *(A $\sigma(n)$ függvény völgytétele)*: Tetszőlegesen nagy K pozitív egészhez végtelen sok olyan n található, amelyre egyszerre teljesül, hogy

$$\sigma(n-1)-\sigma(n)>K \text{ és } \sigma(n+1)-\sigma(n)>K.$$

Bizonyítás: Legyen n elég nagy prímszám, így $n-1$, $n+1$ összetett számok lesznek és $\sigma(n)=n+1$. A $\sigma(n+1)$-re vonatkozó egyenlőtlenséget bizonyítjuk, a $\sigma(n-1)$-es eset igazolása is ugyanígy történik. $\sigma(n+1)-(n+1)\geq\sqrt{n+1}+1$, mivel $n+1$ összetett szám, így van $n+1$-nél kisebb, de $\sqrt{n+1}$-nél nem kisebb osztója, tehát

$$\sigma(n+1)\geq n+1+\sqrt{n+1}+1.$$

Másrészt $\sigma(n+1)>K+n+1$ miatt $n+1+\sqrt{n+1}+1>K+n+1$, ahonnan $\sqrt{n+1}+1>K$ adódik, és végtelen sok olyan n prím van, amire ez igaz.

7.5. Tétel:[3],[7] *(A $\varphi(n)$ függvény völgytétele):* Tetszőlegesen nagy K pozitív egészhez végtelen sok olyan n található, amelyre egyszerre teljesül, hogy

$$\varphi(n-1)-\varphi(n)>K \text{ és } \varphi(n+1)-\varphi(n)>K.$$

Bizonyítás: Legyen n az első r prímszám szorzata, azaz $n=p_1p_2\dots p_r$. Ekkor

$$\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)\leq n\cdot\left(1-\frac{1}{p_r}\right)^r.$$

A $\varphi(n+1)$-re vonatkozó egyenlőtlenséget bizonyítjuk, a $\varphi(n-1)$-es eset igazolása is ugyanígy történik. Az $n+1$ prímtényezős felbontása ${q_1}^{\alpha_1}{q_2}^{\alpha_2} \dots {q_s}^{\alpha_s}$. Mivel $(n, n+1) = 1$, és n az első r prímszám szorzata, ezért $q_i > p_r$ bármely i-re. Ekkor

$$\varphi(n+1) = (n+1)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\dots\left(1-\frac{1}{q_s}\right) \geq (n+1)\left(1-\frac{1}{p_r}\right)^s.$$

Tegyük fel, hogy $s \geq r$, ekkor

$$n+1 \geq q_1 q_2 \dots q_s \geq {p_r}^s + 1 \geq {p_r}^r + 1 \geq p_1 p_2 \dots p_r + 2 = n+2,$$

ami ellentmondás, tehát $s \leq r-1$.Tehát $\varphi(n+1) \geq (n+1)\left(1-\frac{1}{p_r}\right)^{r-1}$. Ezekből következik, hogy:

$$\varphi(n+1) - \varphi(n) \geq (n+1)\left(1-\frac{1}{p_r}\right)^{r-1} - n\left(1-\frac{1}{p_r}\right)^r = \left(1-\frac{1}{p_r}\right)^{r-1}\left(1+\frac{n}{p_r}\right) \geq$$
$$\geq \left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_{r-1}}\right)p_1 \dots p_{r-1} = (p_1-1)\dots(p_{r-1}-1),$$

ami elég nagy r esetén nagyobb, mint K.

7.6. Tétel:

[3],[7] (*A $\mu(n)$ függvény völgytétele):* A $\mu(n)$ függvényben végtelen sok 1 mélységű völgy található, azaz létezik végtelen sok olyan m, melyre $\mu(m-1) = \mu(m+1) = 0$ és $\mu(m) = -1$.

Bizonyítás: Legyenek m, p_1, p_2 prímek, ekkor definíció szerint $\mu(m) = -1$, és írjuk fel a következő szimultán kongruenciarendszert:

$$m - 1 \equiv 0 \ (mod\ {p_1}^2),$$
$$m + 1 \equiv 0 \ (mod\ {p_2}^2).$$

Ez a kínai maradéktétel miatt megoldható, és az összes megoldás $m = m_0 + t{p_1}^2{p_2}^2$ alakra hozható. Mivel m_0 kielégíti a szimultán kongruenciarendszert, ezért $({m_0}, {p_1}^2) = 1$, $({m_0}, {p_2}^2) = 1$ miatt $({m_0}, {p_1}^2{p_2}^2) = 1$ is teljesül, így a Dirichlet-tétel alapján az $m = m_0 + t{p_1}^2{p_2}^2$ számtani sorozatban végtelen sok prímszám van.

Irodalomjegyzék

[1] BEGE ANTAL: *Bevezetés a számelméletbe* Scientia Kiadó, Kolozsvár, 2002.

[2] BEGE ANTAL, DEMETER ALBERT, LUKÁCS ANDOR: *Számelméleti feladatgyűjtemány* Scientia Kiadó, Kolozsvár, 2002.

[3] FREUD RÓBERT, GYARMATI EDIT: *Számelmélet* Nemzeti Tankönyvkiadó, Budapest

[4] KISS EMIL: *Bevezetés az algebrába* TYPOTEX, Budapest, 2007

[5] LÁNG CSABÁNÉ: *Számelmélet – Példák és feladatok* ELTE Eötvös Kiadó, Budapest

[6] RUZSA Z. IMRE: *Különlenyomat Matematika Lapok 27. évfolyam 1-2. számából* Bolyai János Matematikai Társulat, Budapest, 1976-1979.

[7] SÁRKÖZY – SURÁNYI: *Számelmélet feladatgyűjtemény* Tankönyvkiadó, Budapest, 1979.

Internetes oldalak:

[8] http://www.cs.elte.hu/~ewkiss/bboard/algebrabook/Kiss_Algebra_megoldasok.pdf

[9] http://www.cs.elte.hu/~seszter

[10] http://www.mersenne.org

[11] http://www.oddperfect.org

[12] http://www.ttk.pte.hu/matek/ltoth

[13] http://hu.wikipedia.org/wiki