# Oszthatóság, prímszámok

Számelmélet

Diszkrét modellek alkalmazásai

Számelméletben elsősorban egész számokkal ($\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$) foglalkozunk, ill. speciális esetben természetes számokkal ($\mathbb{N} = \{0, 1, 2, \ldots\}$).

## 1. Osztók

**1.1. Definíció.** $a \in \mathbb{Z}$ *osztója* $b \in \mathbb{Z}$-nek, ha $\exists c \in \mathbb{Z} : b = ac$. Jelölés: $a \mid b$. Tagadás jelölése: $a \nmid b$.
Mondjuk még azt is, hogy $b$ *osztható* $a$-val, ill. $b$ *többszöröse* $a$-nak.
Például a 2 osztója a 6-nak, mert $6 = 2 \cdot 3$.
(Megjegyzés: bár "oszthatóság" a neve, mégsem osztással, hanem szorzással szoktuk definiálni. Egyrészt azért, mert a szorzás egyszerűbb művelet, másrészt pedig így nem kell kilépnünk a $\mathbb{Z}$-ből. Ez majd lehetővé fogja tenni, hogy kiterjesszük az oszthatóságot olyan struktúrákra is, ahol nincs osztás. Vegyük észre azt is, hogy a fenti definíció szerint 0 osztható 0-val, tehát az nem is lenne ekvivalens egy olyan naiv meghatározással, hogy "$a$ osztója $b$-nek, ha $b/a$ egész szám".)
Az oszthatóság tulajdonságai:

1. reflexív: $\forall a \in \mathbb{Z} : a \mid a$ (minden szám osztható önmagával);
2. $\forall a \in \mathbb{Z} : a \mid 0$ (a 0 minden számmal osztható);
3. $\forall a \in \mathbb{Z} : 1 \mid a$ (minden szám osztható 1-gyel);
4. $\forall a \in \mathbb{Z} : 0 \mid a \iff a = 0$ (csak a 0 osztható 0-val);
5. tranzitív: $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ b \mid c \implies a \mid c$;
6. $\mathbb{N}$-ben antiszimmetrikus: $\forall a, b \in \mathbb{N} : a \mid b \ \wedge \ b \mid a \implies a = b$;
7. $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ a \mid c \implies a \mid b + c$ (ha $a$ minden tagnak osztója, akkor az összegnek is);
8. $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ a \mid c \implies a \mid b - c$;
9. $\forall a, b, c, d \in \mathbb{Z} : a \mid b \ \wedge \ c \mid d \implies ac \mid bd$;
10. $\forall a, b \in \mathbb{N}^+ : a \mid b \implies a \leq b$.

Kapcsolódó fogalmak:
**1.2. Definíció.** $a \in \mathbb{N}$ *valódi osztója* $b \in \mathbb{N}$-nek, ha osztója, és $a \neq b$.
**1.3. Definíció.** $b \in \mathbb{Z}$ *triviális osztói* az 1, $-1$, $b$ és $-b$.
Például $\mathbb{N}$-ben a 6 osztói: $1, 2, 3, 6$; valódi osztói: $1, 2, 3$; nemtriviális osztói: $2, 3$.
Mint láttuk, az oszthatóság $\mathbb{N}$-ben antiszimmetrikus, és így részbenrendezés is (részbenrendezés = reflexív + antiszimmetrikus + tranzitív). Igaz-e ez $\mathbb{Z}$-ben is? Először vezessünk be még egy fogalmat:
**1.4. Definíció.** $a$ és $b$ *asszociáltak*, ha $a \mid b$ és $b \mid a$.
$\mathbb{N}$-ben csak az egyenlő számok asszociáltak. $\mathbb{Z}$-ben viszont $a$ és $b$ akkor és csak akkor asszociáltak, ha $a = b$ vagy $a = -b$, tehát nemcsak az egyenlő számok, hanem az ellentettpárok is azok.
Megjegyzés: az asszociáltság ekvivalenciareláció, azaz reflexív, szimmetrikus és tranzitív reláció.

Ha összevetjük az asszociáltság és az antiszimmetria definicióját, akkor látható, hogy az oszthatóság akkor és csak akkor lesz antiszimmetrikus (és így részbenrendezés), ha csak az egyenlő számok asszociáltak, tehát $\mathbb{N}$-ben igen, de $\mathbb{Z}$-ben nem.
(Vegyük észre, hogy $\mathbb{N}$-ben az oszthatóság mint részbenrendezés bár többnyire ugyanúgy "rendez", mint a természetes rendezés ($\leq$) – lásd a fenti utolsó tulajdonságot –, de nem mindig: a kivétel a 0, amely az $\mathbb{N}$ legkisebb eleme, de az oszthatóság szemszögéből a "legnagyobb", hiszen minden szám osztja a 0-t.)
Miért érdekesek az asszociáltak? Ha két szám asszociált, akkor oszthatóság szempontjából pontosan ugyanúgy viselkednek, például $2 \mid 6$-ból következik, hogy $2 \mid -6$, $-2 \mid 6$ és $-2 \mid -6$. Így tehát az asszociáltak közül legtöbbször elég csak az egyiket vizsgálni, például $\mathbb{Z}$-ben elég csak $\mathbb{N}$-nel foglalkozni.
(Megjegyzés: innen még nem látszik, hogy miért van külön neve az asszociáltaknak, és miért nem csak úgy hívjuk őket, hogy "azonos abszolút értékű számok". Később viszont majd általánosítjuk az oszthatóságot más struktúrákra, és ott az asszociáltnak már nem lesz köze az abszolút értékhez és az előjelhez.)
A Sage legfontosabb műveletei az osztással és az oszthatósággal kapcsolatban:

| | | |
|---|---|---|
| `a / b` | osztás (tört eredménnyel) | `36 / 10 == 18/5` |
| `a // b` | maradékos osztás hányadosa | `36 // 10 == 3` |
| `a % b` | maradékos osztás maradéka | `36 % 10 == 6` |
| `a.quo_rem(b)` | hányados és maradék egy párban | `36.quo_rem(10) == (3, 6)` |
| `a.divides(b)` | $a$ osztója $b$-nek? | `5.divides(10) == True` |
| `divisors(a)` | $a$ pozitív osztóinak listája | `divisors(12) == [1,2,3,4,6,12]` |

# 2. Prímszámok

**2.1. Definíció.** Egy $n \in \mathbb{N}$ szám *prímszám*, ha $n > 1$ és csak triviális osztói vannak.
Másképpen megfogalmazva: $n$ prímszám, ha pontosan két pozitív osztója van (1 és $n$).
Az első néhány prímszám: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.
**2.2. Definíció.** Egy $n \in \mathbb{N}$ szám *összetett szám*, ha $n > 1$ és nem prímszám.
Megjegyzés: az 1 nem prímszám és nem is összetett szám. Hogy ezt miért szokás így definiálni, azt majd a számelmélet alaptételénél fogunk megérteni.
A prímszámoknak van egy tulajdonsága, amelyet lehetne definícióként is használni:
**2.3. Tétel.** *Egy $n \in \mathbb{N}$ akkor és csak akkor prímszám, ha $n > 1$ és $\forall a, b \in \mathbb{N} : n \mid ab \implies n \mid a \vee n \mid b$.*
Ez azt jelenti, hogy ha egy prímszám oszt egy szorzatot, akkor annak valamelyik tényezőjét is osztja (pl. $5 \mid 7 \cdot 10$, és valóban, $5 \mid 10$), viszont ez összetett számokra nem minden szorzatra teljesül (pl. $6 \mid 4 \cdot 9$, de $6 \nmid 4$ és $6 \nmid 9$).
(A tételnek azt az irányát, hogy összetett számokra nem teljesül a feltétel, könnyű bizonyítani: akkor ugyanis $n$-nek van nemtriviális osztója, tehát $n = ab$, ahol $1 < a, b < n$. Ekkor persze $n \mid ab$ is igaz, viszont $n \mid a$ és $n \mid b$ egyike sem. A tétel másik irányát picit nehezebb bizonyítani, ezért azt mellőzzük, de megjegyezzük, hogy a számelmélet alaptétele kell hozzá.)
A Sage néhány prímszámokkal kapcsolatos művelete:

| `is_prime(n)` | $n$ prímszám? | `is_prime(7) == True` |
|---|---|---|
| `next_prime(n)` | $n$ utáni következő prímszám | `next_prime(1000) == 1009` |
| `previous_prime(n)` | $n$-et megelőző prímszám | `previous_prime(1000) == 997` |
| `nth_prime(n)` | $n$-edik prímszám ($n$ = 1-től) | `nth_prime(3) == 5` |
| `primes_first_n(n)` | első $n$ prímszám listája | `primes_first_n(4) == [2,3,5,7]` |

Most nézzük meg, hogy hogyan tudjuk eldönteni, hogy egy adott $n \in \mathbb{N}$ szám prímszám-e (a fenti függvények nélkül).

A legegyszerűbben a definíció alapján, azaz megnézzük 2-től $n-1$-ig az összes számra, hogy osztója-e. Ez azonban nagy $n$-ekre nem a leghatékonyabb módszer, és többféleképpen is lehet gyorsítani:

1. Nem kell $n-1$-ig menni, elég $n/2$-ig, hiszen annál nagyobb valódi osztója úgysem lehet az $n$-nek. Ezzel máris megfeleztük a futási időt.
2. De valójában $n/2$-ig sem kell menni, elég $\sqrt{n}$-ig. Ugyanis minden $k$ osztónak van egy $n/k$ párja, amely szintén osztó, és ha $k > \sqrt{n}$, akkor $n/k < \sqrt{n}$, tehát azt már megtaláltuk.
3. Elég kettesével lépkedni: ha ugyanis a 2-t megvizsgáltuk, és az nem osztja az $n$-et, akkor utána már elég csak a páratlan számokat vizsgálni.
4. Ezt a logikát továbbfejleszthetjük, ha először megvizsgáljuk a 2-t és a 3-at, majd hatosával ($6 = 2 \cdot 3$) lépkedünk, és csak a $6k+1$ és $6k+5$ alakú számokat vizsgáljuk, mert a többi úgyis osztható vagy 2-vel, vagy 3-mal.

## 2.1. Prímszámok számossága

Most vizsgáljuk meg azt a kérdést, hogy milyen sok prímszám van. Egyrészt:

**2.4. Tétel.** *Végtelen sok prímszám van.*

(Bizonyítás: tegyük fel, hogy csak véges sok prímszám van, például ezek: $p_1, p_2, p_3, \ldots, p_n$. Ekkor tekintsük a következő számot: $p_1 p_2 p_3 \ldots p_n + 1$. Ez nem lehet prímszám, mert az összes feltételezett prímszámnál nagyobb, de nem lehet összetett szám sem, mert semelyik prímszámunkkal sem osztható – tehát ellentmondásra jutottunk, vagyis valójában végtelen sok prímszámnak kell lennie.)

Ez matematikailag megválaszolja a kérdést, hogy hány prímszám van, de ez még mindig nem a teljes kép. Például végtelen sokan vannak a természetes számok is és a kettőhatványok $(1, 2, 4, 8, 16, \ldots)$ is, de a kettőhatványok mégis jóval ritkábbak. A kérdést matematikailag úgy fogalmazhatjuk meg, hogy 1-től adott $n$-ig hány adott típusú szám (pl. prímszám) van. Például természetes számból $n$ van, páros számból $\lfloor n/2 \rfloor$, kettőhatványból pedig $\lfloor \log_2 n \rfloor + 1$ (ami nagyon kevés, pl. $n = 1000000$ esetén csak 20). Prímszámok esetén ezt a következőképpen jelöljük:

**2.5. Definíció.** Jelölje $\pi(n)$ a prímszámok számát 1-től $n$-ig. Neve: *prímszámláló függvény.*

Például $\pi(7) = 4$, mert 7-ig négy prímszám van: $2, 3, 5, 7$.

A $\pi(n)$ pontos értékét nem tudjuk képlettel felírni, viszont közelítést tudunk adni:

**2.6. Tétel** (Prímszámtétel)**.** $\pi(n) \approx \dfrac{n}{\ln n}$, *pontosabban:* $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n/\ln n} = 1$.

Más szóval annak az esélye, hogy egy 1 és $n$ közötti szám prímszám, kb. $1/\ln n$. Például 100-ig minden negyedik szám prímszám ($\pi(100) = 25$, és $\ln 100 \approx 4{,}6$), 1000000-ig pedig kb. minden tizenharmadik ($\ln 1000000 \approx 13{,}8$).

Sage-ben a $\pi(n)$-t a `prime_pi(n)` függvénnyel kérdezhetjük le. Például a következő kód ábrázolja $\pi(n)$-t és a közelítését 1-től 1000-ig (a felső, lépcsőzetes vonal a $\pi(n)$):

```
sage: var("n"); plot([n/ln(n), prime_pi], (1, 1000))
```

## 2.2. Ikerprímpárok

A másik kérdés, amit megvizsgálunk a prímszámokkal kapcsolatban, hogy a szomszédos prímszámok milyen közel lehetnek egymáshoz. A legközelebbi prímek a 2 és a 3, mert utána már minden prímszám páratlan, tehát a távolságuk páros lesz. Ezen belül a legközelebbieknek nevük is van:

**2.7. Definíció.** Egy $p$ prímszám *ikerprím*, ha $p-2$ vagy $p+2$ is prímszám. A két prímszámot együtt *ikerprímpár*nak nevezzük.

Például ikerprímpár a $(3, 5)$ és a $(17, 19)$. Létezik *hármas ikerprímpár* is: $(3, 5, 7)$, de ez az egyetlen ilyen (hiszen valamelyik mindenképp osztható 3-mal).

Láttuk, hogy prímszámokból végtelen sok van. Igaz-e ez az ikerprímszámokra is? Válasz: nem tudjuk. A matematika még nem tudott választ adni a kérdésre. (De elég sok van ahhoz, hogy azt sejtsük, hogy igen.)

## 2.3. Prímtényezős felbontás

Miért fontosak a prímszámok? Ezt leginkább a következő tétel világítja meg.

**2.8. Tétel** (A számelmélet alaptétele)**.** *Minden pozitív természetes szám a sorrendtől eltekintve* ***egyértelműen*** *felírható prímszámok szorzataként.*

Például $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

**2.9. Definíció.** A fenti tételben szereplő felírást *prímtényezős felbontás*nak vagy *prímfelbontás*nak nevezzük.

A tétel kulcsfontosságú szava az "egyértelműen", azaz olyan nem fordulhat elő, hogy különböző prímfelbontással ugyanazt a számot kapjuk, pl. $2 \cdot 7 \neq 3 \cdot 5$. Az persze lehetséges, hogy ugyanazokat a prímtényezőket különböző sorrendben írjuk fel, pl. $30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3$, de ez a két felírás "lényegében" ugyanaz, erre utal a "sorrendtől eltekintve egyértelműen" kitétel. A teljes egyértelműséget például úgy érhetjük el, ha kikötjük, hogy a prímszámokat növekvő sorrendben kell felsorolni. Rövidítésként az egymás mellé kerülő azonos prímtényezőket hatvány alakban szokás felírni. Ennek az alaknak külön neve van:

**2.10. Definíció.** Egy $n$ pozitív egész szám *kanonikus alakján* az $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$ szorzatot értjük, ahol $p_1 < p_2 < \ldots < p_k$ prímszámok, és az $n_i$-k pozitív egész számok.

Amint láttuk, ez az alak egyértelmű. Például 360 kanonikus alakja: $2^3 \cdot 3^2 \cdot 5$.

A számelmélet alaptételéből megérthetjük, hogy miért fontosak a prímszámok: ezek a pozitív egész számok "építőkockái", azaz minden pozitív egész szám ilyenekre bontható fel. (Megjegyzés: nem kivételek a prímszámok sem, amelyek *egyetlen* prímszám szorzatára, azaz önmagukra bonthatók fel, pl. $13 = 13$, valamint a tételből nem zártuk ki az 1-et sem, amit fel lehet fogni *nulla darab* prímszám szorzatának, összhangban azzal a matematikai konvencióval, hogy az üres szorzat értéke 1, azaz $1 = \prod_{i=1}^{0} p_i^{n_i}$, mint ahogy például $0! = 1$.)

A számelmélet alaptételéből azt is megérhetjük, hogy az 1-et miért nem tekintjük prímszámnak: az ugyanis nem valódi építőkocka, mert 1-gyel szorozva nem változik a szám, így ha azt is prímszámnak tekintenénk, azzal elveszne az egyértelműség, pl. $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$ stb.
Sage-ben a prímfelbontást a `factor()` függvénnyel állíthatjuk elő:

```
sage: factor(360)    # vagy: 360.factor()
2^3 * 3^2 * 5
```

A `factor()` visszatérési értéke egy `Factorization` típusú objektum, amely sorozatként is tud viselkedni, azaz pl. egy `for`-ciklussal felsorolható, ahol az elemek a $(p_i, n_i)$ párok, például:

```
sage: for (p, n) in factor(360):
....:     print(f"prím: {p}, kitevő: {n}")
prím: 2, kitevő: 3
prím: 3, kitevő: 2
prím: 5, kitevő: 1
```

Megjegyzés: a prímfaktorizáció, azaz a prímtényezős felbontás előállítása nagy számok esetén nagyon nehéz feladat. Olyannyira, hogy egyes kriptográfiai rendszerek (pl. az RSA, mint később látni fogjuk) azon alapulnak, hogy senki nem fogja tudni megtalálni a titkos prímtényezőit egy hatalmas számnak.

## 2.4. Eratoszthenész szitája

Hogyan tudjuk előállítani az összes prímszámot adott $n$-ig?
A naiv megoldás az, hogy minden számra megvizsgáljuk a fenti módon, hogy prímszám-e. Ez azonban nem hatékony, mert rengeteg felesleges munkát végzünk (például ha egy számról kiderült, hogy osztható 13-mal, akkor a következő 12 számra ezt felesleges megnézni, mert úgysem lesz az).
Ennél jobb megoldást kínál Eratoszthenész szitája: írjuk fel az egész számokat 2-től $n$-ig, majd szisztematikusan húzzuk ki az összetett számokat a már felfedezett prímszámok segítségével. Az első prímszám a 2, ezért húzzuk ki a többi páros számot, mert azok összetett számok. A következő prímszám a 3, ezért húzzuk ki a többi 3-mal osztható számot. A 4-est már kihúztuk, tehát az nem prímszám. A következő érintetlen szám az 5-ös, tehát az prímszám, ezért húzzuk ki az összes többi 5-tel osztható számot, és így tovább. Végül pontosan a prímszámok maradnak.
Például így néz ki a szita első néhány lépése $n = 25$-ig:

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **2** | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | 9 | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | 15 | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | 21 | ~~22~~ | 23 | ~~24~~ | 25 |
| 2 | **3** | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ | ~~22~~ | 23 | ~~24~~ | 25 |
| 2 | 3 | ~~4~~ | **5** | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ |

Néhány észrevétel, amellyel gyorsítani lehet az algoritmust:

1. Itt is elég csak $\sqrt{n}$-ig menni a prímekkel, hiszen az annál nagyobb prímszámok többszöröseit már kihúztuk valamelyik kisebb prímszámmal. (Például fent valóban elég volt 5-ig menni. A 7 többszöröseit hiába néznénk, azzal már nem tudnánk újabb számot kihúzni: a 14-et már kihúztuk a 2-vel, a 21-et pedig a 3-mal.)
2. Egy adott $p$ prímszámnál nem kell $2p$-től kezdeni az áthúzást, hanem elég $p^2$-től. Miért? Mert a $p$ és $p^2$ közötti $p$-többszörösöknek volt kisebb prím osztója, így azokat már kihúztuk. (Például az 5-tel a 15-öt nem kellett kihúzni, mert azt a 3-mal már megtettük.)

Eratoszthenész szitájának lépései tehát:

1. Készítsünk egy listát 2-től $n$-ig, amelyben kezdetben logikai igaz (`True`) értékek vannak.
2. Menjünk egy ciklussal $i = 2$-től addig, amíg $i^2 \leq n$:
   - Ha a lista $i$. helyén igaz van, akkor:
     - Menjünk egy ciklussal $j = i^2$-től indulva, $i$-esével lépkedve legfeljebb $n$-ig (azaz $j = i^2,\ i^2 + i,\ i^2 + 2i,\ \ldots$):
       - Állítsuk a lista $j$. elemét hamisra (`False`).
3. Ahol a listában igaz értékek maradtak, azok a prímszámok.

Figyeljünk az indexelésre, mert Sage-ben a listákat 0-tól kell indexelni, az algoritmusban pedig 2-től. Ezért vagy mindig vonjunk le 2-t az indexből, vagy menjen a lista 0-tól $n$-ig, és az első két értéket rögtön állítsuk hamisra.

Bebizonyítható, hogy az algoritmus futási ideje nagyságrendileg $n \log\log n$ lépés, amely nagy $n$-ekre sokkal gyorsabb, mint a prímek egyenkénti vizsgálata, amely $n\sqrt{n}$ lépést igényel.

# 3. Osztók száma és összege

Vizsgáljunk meg még néhány érdekes fogalmat az osztókkal kapcsolatban. Például:

**3.1. Definíció.** Jelölje $\tau(n)$ az $n \in \mathbb{N}^+$ pozitív osztóinak számát.

Például $n = 6$-nak 4 pozitív osztója van: 1, 2, 3 és 6, ezért $\tau(6) = 4$.

A függvény első néhány értéke:

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

Az osztószám-függvény jól elkülöníti a prímszámokat, az összetett számokat és az 1-et:

- $\tau(1) = 1$,
- $\tau(n) = 2$, ha $n$ prímszám, és
- $\tau(n) \geq 3$, ha $n$ összetett szám.

Hogyan tudjuk kiszámítani az osztószám-függvényt? A legegyszerűbben (és a legkevésbé hatékonyan) úgy, hogy megszámoljuk az osztóit. Ha viszont ismerjük a szám prímtényezős felbontását, akkor hatékonyabb megoldást is tudunk adni:

**3.2. Tétel.** *Ha $n$ kanonikus alakja $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, akkor $\tau(n) = (n_1 + 1)(n_2 + 1)\cdots(n_k + 1)$.*

Például $360 = 2^3 \cdot 3^2 \cdot 5$, ezért $\tau(360) = (3 + 1)(2 + 1)(1 + 1) = 24$.

(Bizonyítás: az $n$ bármely $m$ osztójában csak ugyanazok a prímtényezők lehetnek, mint $n$-ben, és legfeljebb ugyanakkora hatványon. Ezért $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, ahol a $p_i$-k ugyanazok, mint $n$-ben, és minden $m_i$ kitevő 0 és $n_i$ között lehet, ami $(n_i + 1)$-féle lehetőség. Hány ilyen $m$ osztó van? Ahányféleképpen kiválaszthatjuk az $m_i$-ket, azaz $(n_1 + 1)(n_2 + 1)\cdots(n_k + 1)$. De honnan tudjuk, hogy ezek mind különböző osztók lesznek? A számelmélet alaptételéből, amely szerint a prímtényezős felbontás egyértelmű.)

Megjegyzés: vegyük észre, hogy az osztók száma legtöbbször páros. Miért van ez így? Mert az osztók általában párban vannak: ha $k \mid n$, akkor $\frac{n}{k} \mid n$. Kivétel akkor lehet, ha $k$ párja önmaga, azaz $k = \frac{n}{k}$, átrendezve $k^2 = n$. Azaz:

**3.3. Tétel.** *$\tau(n)$ akkor és csak akkor páratlan, ha $n$ négyzetszám.*

Most nézzünk egy másik nevezetes számelméleti függvényt:

**3.4. Definíció.** Jelölje $\sigma(n)$ az $n \in \mathbb{N}^+$ pozitív osztóinak összegét.

Például $n = 6$-ra $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

A függvény első 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 |

Ezt is ki lehet számítani a prímfelbontásból:

**3.5. Tétel.** *Ha $n$ kanonikus alakja $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, akkor* $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{n_i+1} - 1}{p_i - 1}$.

Sage-ben $\sigma(n)$ neve `sigma(n)`, $\tau(n)$-é pedig `number_of_divisors(n)`.

Néha használjuk a $\sigma(n)$ egy változatát, ahol az $n$-et magát kihagyjuk az osztók közül:

**3.6. Definíció.** Jelölje $s(n)$ az $n \in \mathbb{N}^+$ valódi osztóinak összegét. (Angol elnevezés: *aliquot sum.*)

Más szóval: $s(n) := \sigma(n) - n$.

Ezen függvény segítségével definiálhatunk néhány érdekes számtulajdonságot:

**3.7. Definíció.** $n \in \mathbb{N}^+$ *tökéletes szám*, ha $s(n) = n$.

Például a 6 tökéletes szám, mert $s(6) = 1 + 2 + 3 = 6$.

(Megjegyzés: a tökéletes számokról sem tudjuk, hogy végtelen sokan vannak-e.)

**3.8. Definíció.** $a \in \mathbb{N}^+$ és $b \in \mathbb{N}^+$ *barátságos számpár*, ha $s(a) = b$ és $s(b) = a$. (Angolul: *amicable numbers.*)

Például a 220 és a 284 barátságos számpár, mert $s(220) = 1+2+4+5+10+11+20+22+44+55+110 = 284$ és $s(284) = 1 + 2 + 4 + 71 + 142 = 220$.

# 4. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva Nagy Ádám jegyzetét:
https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.