Az euklideszi algoritmus és következményei

Euklidesz egyike volt az emberiség legnagyobb gondolkodóinak. Munkássága még kétezer év távlatából is hat gondolkodásunkra. A róla elnevezett algoritmus a mai napig a számelmélet egyik nagyon hatékony, elméleti szempontból sem nélkülözhet eljárása. Ezért nem meglep, hogy az euklideszi algoritmus a számelméleti munkák középpontjában áll. Segítségével érthetjük meg a legnagyobb közös osztó alapvet tulajdonságait, kiterjesztett változata pedig a lineáris diofantoszi egyenletek és a lineáris kongruenciák megoldásának eszköze. Nem utolsó sorban létezése biztosítja, hogy a természetes számok körében prímnek lenni egyet jelent azzal, hogy az illet számnak nics valódi osztója, vagy másként, az egész számok körében a prím tulajdonság és az irreducibilitás ekvivalens fogalmak.

Legnagyobb közös osztó

Tekintsük az $n = 40$ és az $m = 18$ pozitív egészeket, és soroljuk fel pozitív osztóikat!

40 pozitív osztói	1, 2, 4, 5, 8, 10, 20, 40
18 pozitív osztói	1, 2, 3, 6, 9, 18

Látható, hogy az osztók között vannak olyanok, amelyek mind 40-nek, mind a 18-nak osztói, ezek a közös osztók az 1 és a 2. Két egész szám közös osztóinak halmaza mindíg véges, így ennek a halmaznak van legnagyobb eleme.

9.1.1. Definíció

Az n és m egészek közös osztói közül a legnagyobbat az n és m **legnagyobb közös osztójának** nevezzük, és $lnko(n, m)$-vel jelöljük.

Mivel 1 minden n és m egésznek közös osztója, így $lnko(n, m)$ biztosan pozitív érték, hiszen nem lehet kisebb, mint az 1 közös osztó. Ugyancsak fontos megjegyzni, hogy a legnagyobb közös osztó nem függ a számok sorrendjétl, vagyis $lnko(n, m) = lnko(m, n)$.

Mint láttuk $lnko(40, 18) = 2$. Osszuk el maradékosan 40-et 18-tal

$$40 = 18 \cdot 2 + 4 ,$$

és nézzük meg 4 osztóit. Ezek 1, 2, 4; tehát 18 és 4 közös osztói is 1 és 2. Eszerint 40 és 18 közös osztóinak halmaza megegyezik 18 és 4 közös osztóinak halmazával, így közülük a legnagyobb elemek is szükségképpen megegyeznek

$$lnko(40, 18) = lnko(18, 40 \textbf{ mod } 18) = lnko(18, 4).$$

Ezzel a lépéssel a 40 és 18 legnagyobb közös osztójának meghatározását visszavezettük a 18 és a 4 legnagyobb közös osztójának meghatározására. Azt, hogy ez nem véletlenül sikerült, a következ tétel biztosítja.

9.1.2. Tétel

Tekintsük az n és $m > 0$ egészeket. Ekkor

$$lnko(n, m) = lnko(m, n \bmod m) .$$

Bizonyítás

Azt mutatjuk meg, hogy *n* és *m* közös osztóinak halmaza megegyezik *m* és $r = n \bmod m$ közös osztóinak halmazával. Ebbl tételünk állítása már következik.

Legyen

$$n = m \cdot q + r \ (0 \le r < m).$$

Ha *d* közös osztója *n*-nek és *m*-nek, akkor *d* osztója $m \cdot q$-nak és így $n - m\,q = r$ -nek is. Kaptuk, hogy *d* közös osztója *m*-nek és *r*-nek. Fordítva, ha *d* közös osztója *m*-ek és *r*-nek, akkor *d* osztója $m \cdot q$-nak és $m\,q + r = n$ -nek is. Tehát *d* közös osztója *n*-nek és *m*-nek.

Számpéldánkra visszatérve, a tétel birtokában már bátran felírhatjuk a következket:

$$lnko(40, 18) = lnko(18, 40 \bmod 18) = lnko(18, 4)$$

$$lnko(18, 4) = lnko(4, 18 \bmod 4) = lnko(4, 2) .$$

Tehát azt kaptuk, hogy

$$lnko(40, 18) = lnko(4, 2).$$

Ez utóbbit könny meghatározni, hiszen 2 osztója 4-nek, igy $lnko(4, 2) = 2$. Általánosan is igaz a következ tétel.

9.1.3. Tétel

Az *m* egész szám akkor csak akkor osztója *n*-nek, ha $lnko(n, m) = m$.

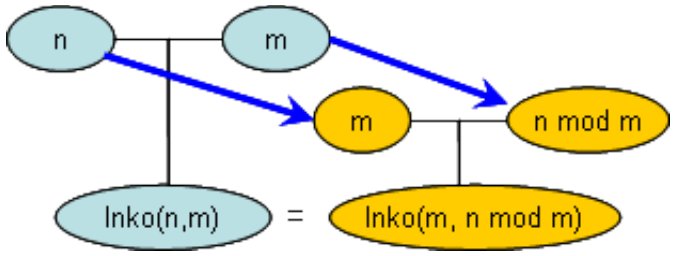
Bizonyítás

Az elégségességhez elegend annyit megjegyezni, hogy $m \mid n$ esetén *n* és *m* közös osztói nem mások, mint *m* osztói. Ez utóbbiak közül pedig maga az *m* a legnagyobb, így $lnko(n, m) = m$. Fordítva, ha $lnko(n, m) = m$, akkor *m* közös osztó, tehát szükségképpen osztója *n*-nek.

Az euklideszi algoritmus (EA)

Két egészszám legnagyobb közös osztójának most ismertetend algoritmusa több, mint 2000 éves. Az Euklidesz Elemek cim mvében található eljárás a mai napig az elemi számelméet egyik legalapvetbb eljárása. Ennek megfelelen ismerete nélkülözhetetlen.

A kulcsot az eljárás megalkotásához elz fejezetbeli két tételünk szolgáltatja. A 8.2 tétel azt mondja, hogy *n* és *m* legnagyobb közös osztójának meghatározása visszavezethet *m* és $n \bmod m$ legnagyobb közös osztójának meghatározására. Mivel a maradékról tudjuk, hogy mindig határozottan kisebb, mint az osztó, így ezzel a lépéssel elértük, hogy két olyan szám legnagyobb közös osztóját elegend meghatározni, melyek közül a második határozottan kisebb az eredeti feladatban szerepl második számnál.



Ahogy ezt ez elz fejelezben is tettük, ismételjük meg ugyanezeket a lépéseket az *m* és az *n* **mod** *m* számokra. Az *n*, vagyis az osztandó szerepét most vegye át *m*, az *m* szerepét pedig az osztás maradéka, *n* **mod** *m*. Kissé precízebben, legyen *n* új értéke *m*, az *m* új értéke pedig *n* **mod** *m*. Tételünk most is biztosítja, hogy *n* és *m* új értékének legnagyobb közös osztója megegyezik az elz lépésben keletkezett legnagyobb közös osztóval. Ha mindezt addig ismételjük, amíg nulla maradékot nem kapunk, akkor az utolsó lépésben fellép osztó megadja a keresett legnagyobb közös osztót. Lássuk hogyan mködik mindez!

	n	*m*	*n* **mod** *m*	Megjegyzés	*n* új értéke legyen *m* és *m* új értéke legyen *n* **mod** *m*
1.	40	24	16	$lnko(40, 24) = lnko(24, 16)$	$n = 24$ és $m = 16$
2.	24	16	8	$lnko(24, 16) = lnko(16, 8)$	$n = 16$ és $m = 8$
3.	16	8	0	$lnko(16, 8) = 8$	

Két fontos megjegyzés.

1. Látható, hogy a maradékok lépésrl lépésre egyre kisebbek. Ez nem véletlen. A második lépésben az osztó az els osztás maradéka. A második osztás maradéka, mivel kisebb, mint az osztó, kisebb az elz osztás maradékánál. Ugyanez igaz a harmadik osztásra is. Ennek osztója a második osztás maradéka. Így a harmadik osztás maradéka, ami kisebb az osztónál, szükségképpen kisebb a második osztás maradékánál is. És így tovább, ez a tulajdonság minden egyes lépésben megmarad, tehát kijelenhetjük, hogy az osztások során keletezett nem negatív maradékok szigorúan csökken sorozatot alkotnak. Így elbb utóbb kötelezen eljutnak nullához. Tehát eljárásunk biztosan véget ér, mégpedig akkor, amikor az elvégzend osztás maradéka nulla.

2. Másrészt az egyes lépésekben meghatározandó legnagyobb közös osztók minden lépésben megegyeznek. Ezeket persze az utolsó lépést kivéve nem ismerjük, ám az utolsó lépésben alkalmazhatjuk tételünket, mely szerint ha *m* osztója *n*-nek akkor $lnko(n, m) = m$.

A 2. észrevételt példánkra alkalmazva azt mondhatjuk, hogy $lnko(16, 8) = 8$, és ez egyben a keresett legnagyobb közös osztó, tehát $lnko(40, 24) = 8$. Mivel ez a 8 az utolsó osztás osztója, egyben nem más, mint az utolsó nem nulla maradék. Ez utóbbi azonban nem mindíg létezik (miért?), így célszerbb az EA outputjának az utolsó osztás osztóját tekinteni.

A kézi számolásnál a javasolt számolótábla inicializálása és az algoritmus végrehajtása az alábbi módon történik, melyet az $n = 55$ és $m = 24$ számokkal mutatunk be.

Inicializálás

osztandó	*osztó*	*maradék*
55	24	

Az táblázat els sorába elhelyezzük *n*-et és *m*-et

Végrehajtás

osztandó	*osztó*	*maradék*
55	24	7
24	7	3
7	3	1
3	**1**	0

Az EA végrehajtásának eredményeképpen azt kaptuk, hogy $lnko(55, 24) = 1$. Emlékeztetünk rá, hogy az ilyen tulajdonságú számokat relatív prímeknek nevezzük.

9.2.1. Algoritmus: Euklideszi algoritmus

Szöveges leírás	Maple metakód
1. *Input*: a, b egészek, $b > 0$, a az osztandó, b az osztó 3. Amíg $b > 0$ hajtsuk végre a következ utasításokat Legyen $r := a$ **mod** b Legyen $a := b$ és $b := r$ 4. *Output*: b az inputban megadott számok lnko-ja	*Input*: a, b egészek, $b > 0$, a az osztandó, b az osztó **while** $b > 0$ **do** $r := irem(a, b) : a := b : b := r$ **od** *Output*: b az inputban megadott számok lnko-ja

9.2.2. Maple implementáció

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!" **(1.2.2.1)**

```
> EA(55,24);
```

1 **(1.2.2.2)**

```
> EA(55,24,ini,cal);
Inicializálás(EA):
```

osztandó	*osztó*	*maradék*
55	24	

```
Részletek megjelenítése(EA):
```

$$\begin{bmatrix} osztandó & osztó & maradék \\ 55 & 24 & 7 \\ 24 & 7 & 3 \\ 7 & 3 & 1 \\ 3 & 1 & 0 \end{bmatrix}$$

Eredmény(EA):

$$1 \qquad (1.2.2.3)$$

>

Három következmény

Három olyan tételt bizonyítunk, amelyek bizonyítási módszere közös. Mindhárom esetben az euklideszi algoritmus egyes lépéseiben fellép osztások egy-egy "invariáns" tulajdonságát találjuk meg, vagyis olyan tulajdonságot, ami érvényben marad az eljárás minden egyes lépésében. És mivel azt már tudjuk, hogy az eljárás utolsó osztója a legnagyobb közös osztó, így a vizsgált invariáns tulajdonság egyben legnagyobb közös osztó egy bizonyított tulajdonságává válik.

Elsként rámutatunk a legnagyobb közös osztó lényegi tulajdonságára, miszerint az nem csak egyszeren a legnagyobb a közös osztók között, hanem az összes közös osztónak többszöröse.

9.3.1. Tétel

Az n és m egészek minden közös osztója egyben osztója n és m legnagyobb közös osztójának.

Bizonyítás

Legyen d tetszleges közös osztója n-nek és m-nek. Azt mutatjuk meg, hogy d osztója az euklideszi algoritmus minden egyes lépésében fellép osztónak. Ebbl már állításunk következik, hiszen az euklideszi algoritmus utolsó osztója nem más, mint $lnko(n, m)$.

Az eljárás els lépése az

$$n = m\,q + r\,(0 \le r < m)$$

maradékos osztás elvégzése. Erre lépésre állításunk triviális, hiszen azt feltettük, hogy $d \mid m$.

Ahogy ezt a 8.2 tétel bizonyításában is láttuk, n és m közös osztói egyben osztói r-nek is. Más szóval abból a ténybl, hogy d osztja mind az osztandót, mind pedig az osztót, az következik, hogy d osztja a maradékot is.

Emlékeztetünk rá, hogy az euklideszi algoritmus aktuális lépésében az elz lépésbeli osztót osztjuk az elz lépésbeli maradékkal. Tehát m nem más, mint a második osztás osztandója, r pedig a második osztás osztója. Eszerint d osztója a második osztás osztójának is. És mivel az osztandónak is osztója, így osztója lesz a második osztás maradékának is, ami nem más, mint a harmadik lépésben fellép osztó. Ezt a gondolatmenetet megismételve kapjuk, hogy d osztója az összes további osztás osztójának, így $lnko(n, m)$-nek is. Ezzel a bizonyítást befejeztük.

Figyeljük meg, hogy az elz bizonyításban valójában nem is egy, hanem két invariáns tulajdonsággal dolgoztunk. Az egyik invariáns tulajdonság azt állítja, hogy az osztás eltt a d szám, ami a kiindulási n-nek és m-nek egy közös osztója, osztja az aktuális lépésben fellép osztandót és osztót is. A másik invariáns tulajdonság pedig az aktuális lépésben elvégzett osztás utáni állapotról szól, azt állítja hogy d osztója a keletkez maradéknak is.

Példák

A következ utasításokban kiszámítjuk két természetes szám közös osztóit. Figyeljük meg, hogy ezek közül a legnagyobb valóban többszöröse az összes közös osztónak. A n és m változóknak más-más értékeket adva meggyzdhetünk arról, hogy tételünk hogy is dolgozik a gyakorlatban.

```
> restart;
```

```
> with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!" **(1.3.1)**

```
> n:=60; m:=24;
```

$$n := 60$$
$$m := 24 \qquad \textbf{(1.3.2)}$$

```
> lnko(n,m)=EA(n,m);
```

$$lnko(60, 24) = 12 \qquad \textbf{(1.3.3)}$$

```
> `n osztói`=osztók(n,set);
```

$$n\ osztói = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\} \qquad \textbf{(1.3.4)}$$

```
> `m osztói`=osztók(m,set);
```

$$m\ osztói = \{1, 2, 3, 4, 6, 8, 12, 24\} \qquad \textbf{(1.3.5)}$$

```
> osztók(n,set) intersect osztók(m,set);
```

$$\{1, 2, 3, 4, 6, 12\} \qquad \textbf{(1.3.6)}$$

A következ tétel bizonyításban két euklideszi algoritmust hajtunk végre párhuzamosan. Végrehajtjuk az euklideszi algoritmut az $[n, m]$ számpáron és vele párhuzamosan a $[k \cdot n, k \cdot m]$ számpáron. Itt is két invariáns tulajdonsággal dolgozunk. Az els azt állítja, hogy az aktuális lépésben elvégzend osztás eltt a második algoritmusban az osztandó illetve osztó rendre az els algoritmusban fellép osztandó ill. osztó k-szorosa. A másik invariáns tulajdonság pedig úgy szól, hogy az osztás elvégzése után analóg kapcsolat áll fenn a maradékok között is, vagyis a második eljárásban fellép maradék az els eljárásbeli maradék k-szorosa lesz.

9.3.2. Tétel

Tetszleges n, m egészekre és k természetes számra

$$lnko(k \cdot n, k \cdot m) = k \cdot lnko(n, m).$$

Bizonyítás

A bizonyítás kulcsa a következ egyszer észrevétel. Osszuk el maradékosan n-t m-vel, vagyis legyen

$$n = m \cdot q + r \text{, ahol } 0 \le r < m.$$

Ezt az egyenlséget és a két egyenltlenséget is k-val beszorozva kapjuk, hogy

$$k \cdot n = (k \cdot m) \cdot q + k \cdot r \text{, ahol } 0 \le k \cdot r < k \cdot m \text{,}$$

ez pedig nem mást jelent, mint azt, hogy $k \cdot n$ szám $k \cdot m$-nel képzett osztási maradéka $k \cdot r$.

Most pedig képzeljük el, hogy párhuzamosan végezzük az euklideszi algoritmust az $[n, m]$ számpáron és a $[k \cdot n, k \cdot m]$ számpáron. Írjuk fel az algoritmus els két lépését.

$n = m \cdot q + r$	$k \cdot n = (k \cdot m) \cdot q + k \cdot r$	Az osztó az els oszlopbeli k-szorosa (ezt feltettük). Az osztás elvégzése után a maradék az els oszlopbeli maradék k-szorosa a bizonyítás elején tett észrevételünk szerint.
$m = r \cdot q_1 + r_1$	$k \cdot m = (k \cdot r) \cdot q_1 + k \cdot r_1$	Az osztó az els oszlopbeli k-szorosa, mert egyenl az elz osztás maradékával.. Az osztás elvégzése után a maradék az els oszlopbeli maradék k-szorosa a bizonyítás elején tett észrevételünk szerint.

Azt vettük észre tehát, hogy miközben párhuzamosan végezzük el az euklideszi algoritmus lépéseit, a második oszlopbeli osztók minden lépésben az els oszlopbeli osztók k-szorosai. És mivel az lnko az EA utolsó lépésében fellép osztó, ez az észrevétel már bizonyítja állításunkat.

Az euklideszi algoritmus harmadik következményének elkészítéseként képzeljük el, hogy olyan $[m, d]$ számpáron végzünk euklideszi osztást, amelyeknek legnagyobb közös osztója 1. Ekkor az euklideszi algoritmus els és utolsó eltti osztása

Általánosan	Példa: $m = 35$, $d = 8$
$m = d \cdot q + r$	$35 = 8 \cdot 4 + 3$
...	$8 = 3 \cdot 2 + 2$
$m` = d` \cdot q` + 1$.	$3 = 2 \cdot 1 + 1$

alakú. Megjegyezzük, hogy $d > 1$ esetén mindíg lesz utolsó eltti osztás, mert ilyenkor $lnko(m, d) = 1$ miatt EA legalább két osztásból áll.

Most nem tördünk azzal, hogy az utolsó eltti osztásban szerepl vesszs változók értéke mennyi, csak azt emeljük ki, hogy ennek az osztásnak a maradéka 1, hiszen feltettük, hogy $lnko(m, d) = 1$. És most szorozzuk meg az összes egyenlséget egy olyan n egész számmal, amelyrl feltesszük, hogy $d \mid m \cdot n$. Ekkor az

$$m \cdot n = d \cdot q \cdot n + r \cdot n$$

$$...$$

$$m` \cdot n = d` \cdot q` \cdot n + n$$

egyenlségek közül az elsbl leolvaható, hogy d a maradékot is osztja.

És máris kezd kirajzolódni a korábbi tételekben alkalmazott gondolati séma. Az osztás eltt az osztandóról és az osztóról állíthatunk valamit, amibl azután következtetünk a maradék egy tulajdonságára. Nevezetesen, most azt láttuk, hogy *d* osztja mind az osztót, mind az osztandót, ez az osztás végrehajtása eltti invariáns, majd az osztás során keletkezett maradékra ugyanezt állíthatjuk. Tehát az osztás utáni invariáns szerint *d* osztója az osztás maradékának.

Innen már csak a jól megszokott módon kell tovább menni. Mivel az euklideszi algoritmus következ lépésében a most elvégzett osztás osztója illetve maradéka játsza az osztandó ill. az osztó szerepét, az osztás eltti invariánsunk tehát a második lépésben teljesül. Az osztás utáni pedig ugyanazért fog teljesülni, amiért az els lépésben is tette. Így azután néhány lépés után eljutunk az utolsó osztásig, amelynek maradéka *n*. Erre is teljesül az osztás utáni invariánsunk, miszerint $d \mid n$.

9.3.3. Tétel (Osztási lemma)

Ha *d* osztója az $n \cdot m$ szorzatnak úgy, hogy $lnko(m, d) = 1$, akkor *d* osztja *n*-et, vagyis $d \mid n$.

Bizonyítás

Bár az osztási lemmát már a felvezetjében bebizonyítottuk, most egy második bizonyításként rámutatunk arra, hogy az osztási lemma a 8.6 tétel következménye. Ugyanis a $d \mid n \cdot m$ feltétel miatt alkalmas *q* egészre

$$n \cdot m = d \cdot q \ .$$

Ekkor egyrészt az elz tétel szerint

$$lnko(m \cdot n, d \cdot n) = n \cdot lnko(m, d) = 1 \cdot n = n \ .$$

Másrészt felhasználva az $n \cdot m = d \cdot q$ egyenlséget és még egyszer az elz tételt

$$lnko(m \cdot n, d \cdot n) = lnko(d \cdot q, d \cdot n) = d \cdot lnko(q, n).$$

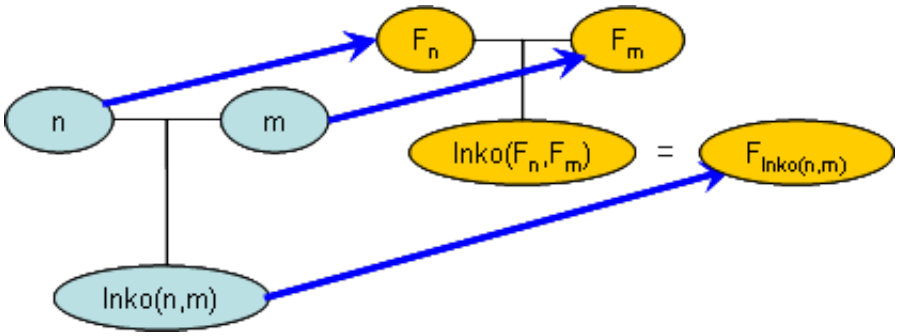
A bal oldalak egyenlsége maga után vonja a jobb oldalak egyenlségét így

$$n = d \cdot lnko(q, n).$$

Ezzel nyertük, hogy $d \mid n$. A bizonyítás kész.

Lucas tétele

Lucas tétele a Fibonacci számok egy újabb gyönyör tulajdonságát tárja elénk. Már az is meglep, hogy mint látni fogjuk, két Fibonacci szám legnagyobb közös osztója maga is Fibonacci szám. Ám Lucas tétele ennél többet állít, amit az alábbi ábrával szemléltethetünk.



A n és m egészek legnagyobb közös osztóját vettük. A nyilak azt reprezentálják, hogy m-hez és n-hez hozzárendeltük az m-edik illetve n-edik Fibonacci számot. Értelemszeren az $lnko(m, n)$-hez rendelt Fibonacci szám $F_{lnko(n,\, m)}$, ami megegyezik F_n és F_m legnagyobb közös osztójával.

Ez a tulajdonság úgy is kifejezhet, hogy a Fibonacci számok képzése felcserélhet a legnagyobb közös osztó képzésével. És valóban errl van szó. Ugyanis Lucas tétele pontosan azt mondja, hogy ugyanarra az eredményre jutunk, ha elször vesszük m és n legnagyobb közös osztóját, majd az ehhez tartozó Fibonacci számot, vagy ha fordítva járunk el, és elbb vesszük az m-hez és n-hez tartozó Fibonacci számokat és képezzük azok legnagyobb közös osztóját.

Az euklideszi algoritmus tárgyalása során megállapítottuk, hogy ha az n és m természetes számokon maradékos osztást végzünk, vagyis ha

$$n = m \cdot q + r \quad (0 \le r < m),$$

akkor az $[n, m]$ pár közös osztóinak halmaza megegyezik az $[m, r]$ pár közös osztóinak halmazával. Ebbl pedig azonnal következett az

$$lnko(n, m) = lnko(m, n \bmod m)$$

egyenlség, ami az euklideszi algoritmus alapjául szolgált.

A Fibonacci számok sok-sok szép tulajdonsága közül is kiemelkedik a fenti egyenlség analogonja

$$lnko\left(F_n, F_m\right) = lnko\left(F_m, F_{n \bmod m}\right).$$

Ez az egyenlség nem kevesebbet állít, mint azt, hogy az n-edik és az m-edik Fibonacci szám legnagyobb közös osztója megegyezik az m-edik és az $n \bmod m$-edik Fibonacci szám legnagyobb közös osztójával. Numerikus példaként legyen $n = 20$ és $m = 12$.

A huszadik Fibonacci szám $F_{20} = 6765$, a tizenkettedik pedig $F_{12} = 144$. Végrehajtjuk az euklideszi algoritmust a $[6765, 144]$ számpáron.

osztandó	*osztó*	*maradék*
6765	144	141
144	141	3

Mivel $20 \bmod 12 = 8$, és a nyolcadik Fibonacci szám $F_8 = 21$, most a $[144,21]$ számpáron hajtjuk végre az euklideszi algoritmust.

osztandó	*osztó*	*maradék*
144	21	18
21	18	3
18	3	0

141	3	0

Azt kaptuk, hogy

$$lnko(F_{20}, F_{12}) = lnko(6765, 144) = 3.$$

Mint látható,

$$lnko(F_{12}, F_{20 \bmod 12}) = lnko(F_{12}, F_8)$$
$$= lnko(144, 21) = 3.$$

Példák

Az alábbi Maple utasítások arra szolgálnak, hogy kísérletezzünk különböz Fibonacci számok legnagyobb közös osztóival. Az alias parancsot hagyjuk változatlanul, azt a célt szolgálja, hogy a Fibonacci sorozat elemeire az általunk megszokott F betvel, a legnagyobb közös osztóra pedig *lnko*-val hivatkozhassunk.

Az *n* és az *m* értékének azonban tetszleges értékeket adhatunk, majd az Enter billenty többszöri leütésével végrehajtathatjuk sorra a kiadott utasításokat. Mindig értelmezzük a kapott eredményt, és gyzzük meg magunkat arról, hogy észrevételeink helytállóak.

```
> alias(F=combinat
  [fibonacci],lnko=igcd):

> n:=20:m:=12:

> F(n),F(m);
          6765, 144                (1.4.1)

> lnko(F(n),F(m));
               3                   (1.4.2)

>
```

```
> n mod m;
               8                   (1.4.3)

> F(m),F(n mod m);
            144, 21                (1.4.4)

> lnko(F(m),F(n mod m));
               3                   (1.4.5)

>
```

Ennyi elkészítés után mondjuk ki tétel formájában is állításunkat.

9.4.1. Tétel

Minden *m* és *n* egészre

$$lnko(F_n, F_m) = lnko(F_m, F_{n \bmod m}) .$$

Bizonyítás

Végezzünk maradékos osztást a *n* és *m* egészeken, tehát legyen

$$n = m \cdot q + r .$$

Ugyanúgy, ahogy azt az euklideszi algoritmus vizsgálata során tettük, azt mutatjuk meg, hogy F_n és F_m közös osztóinak halmaza megegyezik F_m és F_r közös osztóinak halmazával. Ebbl már tételünk állítása következik.

Korában láttuk, hogy $F_{m+k} = F_k \cdot F_{m+1} + F_{k-1} \cdot F_m$. Ezt az egyenlséget az $m \cdot q + r$ összegre alkalmazva kapjuk, hogy

$$F_n = F_{m \cdot q + r} = F_r \cdot F_{m \cdot q + 1} + F_{r-1} \cdot F_{m \cdot q}.$$

Tekintsük most az F_m és F_r és közös osztóját, mondjuk d-t. Mivel $d \mid F_r$ így $d \mid F_r \cdot F_{m \cdot q}$. Másrészt $d \mid F_m$, ami viszont osztója $F_{m \cdot q}$-nak, így d is osztója $F_{m \cdot q}$-nak, és ebbl következen $F_{r-1} \cdot F_{m \cdot q}$-nak is. Kaptuk, hogy d osztója a jobb oldali összeg mindkét tagjának, ekkor viszont osztója magának sz összegnek, vagyis F_n-nek is. Ezzel beláttuk, hogy F_m és F_r és közös osztói egyben közös osztói F_n-nek és F_r-nek.

A fordított állítás belátásához már a osztási lemmára is szükségünk lesz. Tegyük fel ugyanis, hogy d közös osztója F_n-nek és F_m-nek. Ekkor d osztója $F_{m \cdot q}$-nak, és ebbl kifolyólag

$$d \mid F_n - F_{r-1} \cdot F_{m \cdot q} = F_r \cdot F_{m \cdot q + 1}$$

Vegyük észre, hogy d és $F_{m \cdot q + 1}$ bármely közös osztója egyben $F_{m \cdot q}$ és $F_{m \cdot q + 1}$ közös osztója is. Ez utóbbiak viszont relatív prímek. Így szükségképpen

$$lnko\left(d, F_{m \cdot q + 1}\right) = 1,$$

és az osztási lemma alkalmazható. Eredményeképpen azt kapjuk, hogy $d \mid F_r$, és pont ez az amit látni akartunk.

Ez a tétel lehetvé teszi, hogy az n és m számokon végrehajtott euklideszi algoritmus egyes lépéseiben ne csak n és m legnagyobb közös osztójára, hanem F_n és F_m legnagyobb közös osztójára is következtetéseket vonhassunk le. Nézük meg példaként $n = 20$ és $m = 12$ számokra elvégzett euklideszi algoritmust.

osztandó	*osztó*	*maradék*	*Állítás*
20	12	8	$lnko\left(F_{20}, F_{12}\right) = lnko\left(F_{12}, F_8\right)$
12	8	4	$lnko\left(F_{12}, F_8\right) = lnko\left(F_8, F_4\right)$
8	4	0	$lnko\left(F_8, F_4\right) = F_4$

Az állítás oszlop egyenlségeit összeolvasva kapjuk, hogy $lnko\left(F_{20}, F_{12}\right) = F_4$, ám $4 = lnko(20, 12)$, amibl

$$lnko\left(F_{20}, F_{12}\right) = F_{lnko(20, 12)}.$$

És ez már a Lucas tételének állítása, melynek bizonyítása a numerikus példa analógiájára töténik.

9.4.2. Tétel (Lucas tétele)

Minden m és n egészre

$$F_{lnko(m, n)} = lnko\left(F_m, F_n\right).$$

Bizonyítás

Végezzük el az euklideszi algoritmust az n és m számokon! Az elz tétel szerint az eljárás minden lépésében érvényes, hogy az $F_{osztandó}$ és az $F_{osztó}$ legnagyobb közös osztója egyenl az $F_{osztó}$ és az $F_{maradék}$ legnagyobb közös osztójával, tehát

$$lnko\left(F_n, F_m\right) = lnko\left(F_{osztandó}, F_{osztó}\right).$$

Ez az els lépésre nyilvánvaló, hiszen itt az osztandó maga az n, az osztó pedig az m.

Az elz tétel szerint azonban

$$lnko\left(F_{osztandó}, F_{osztó}\right) = lnko\left(F_{osztó}, F_{maradék}\right),$$

ami azzal a következménnyel jár, hogy az $lnko(n, m) = lnko\left(F_{osztandó}, F_{osztó}\right)$ egyenség az euklideszi algoritmus második osztására is teljesül, hiszen a második lépésben az osztandó és az osztó rendre egyenl az elz osztás osztójával, illetve maradékával. Gondolatmenetünket a második osztásra alkalmazva kapjuk, hogy a bizonyítandó egyenlség a harmadik osztásra is teljesül, és így tovább. Az utolsó osztás maradéka azonban zérus, és így

$$lnko\left(F_{osztandó}, F_{osztó}\right) = F_{osztó},$$

ahol $osztó = lnko(n, m)$. Ezzel beláttuk, hogy

$$lnko\left(F_n, F_m\right) = F_{lnko(n, m)}.$$

A 3. eladásban megismertük a Fibonacci számok egy oszthatósági tulajdonságát. Nevezetesen arra tulajdonságra gondolunk, hogy F_k osztója $F_{k \cdot q}$ -nak, amit másként úgy is fogalmazhatunk, hogy

$$\text{ha } m \mid n \text{ , akkor } F_m \mid F_n .$$

Lucas tétele segítségével megmutatható az állítás megfordítása is. Ám a manver némi óvatosságot követel. Ugyanis $m = 2$ esetben $F_2 = 1$ és ez minden egésznek, így speciálisan minden Fibonacci számnak is osztója. Tehát például F_2 osztója F_3 miközben 2 nem osztója 3-nak. Ha azonban a renitens $m = 2$ esetet kizárjuk, akkor a dolgok mködni kezdenek.

9.4.3. Tétel

Legyen $m \neq 2$ és n tetszleges természetes szám. Ekkor $m \mid n$ akkor és csak akkor teljesül, ha $F_m \mid F_n$.

Bizonyítás

Csak azt kell bizonyítani, hogy $m \neq 2$ esetén $F_m \mid F_n$ -bl $m \mid n$ következik. Az $m = 1$ eset triviális hiszen ekkor $m \mid n$ nyilvánvalóan teljesül. Feltehetjük tehát, hogy $m > 2$. Az $F_m \mid F_n$ feltételbl

$$lnko\left(F_m, F_n\right) = F_m$$

következik, másrést Lucas tétele miatt

$$lnko\left(F_m, F_n\right) = F_{lnko(m, n)}.$$

A bal oldalak egyenlsége maga után vonja a jobb oldalak egyenlségét

$$F_{lnko(m,\,n)} = F_m .$$

Kettnél nagyobb index esetén a különböz index Fibonacci számok különbözk, így a kapott egyenlség csak úgy teljesülhet, ha

$$lnko(m, n) = m ,$$

amibl az $m \mid n$ állítás már következik.

Prímszámok és felbonthatatlan számok

9.5.1. Definíció

A p egész számot **irreducibilisnek** (felbonthatatlannak) nevezzük, ha p-*nek* $\pm p$-n és ± 1-en kívül nincs más osztója.

Tetszleges p egész számnak a $\pm p$ és a ± 1 osztója. Ezeket az osztókat szokás **triviális osztóknak** is nevezni, míg a nem triviális osztókat **valódi osztóknak** hívjuk. Az irrecducibilis egészeknek tehát a triviális osztóin kívül nincs más osztójuk. Ilyen például az 5, 13 vagy a 29.

9.5.2. Definíció

A p nem nulla és nem egység egész számot **prímszámnak** vagy csak egyszeren **prímnek** nevezzük, ha valahányszor p osztója két szám szorzatának, mindannyiszor p valamelyik számnak is osztója. Rövien

$$\text{ha } p|m\cdot n \text{ , akkor } p|m \text{ vagy } p|n.\square$$

Külön felhívjuk a figyelmet a definíció első fél mondatára, mely szerint sem a 0, sem pedig a ± 1 nem prímszám, annak ellenére, hogy például az 1 teljesíti a definíció második részében megfogalmazott feltételt. A prím tulajdonság ersebb az irreducibitási tulajdonságnál, ugyanis érvényes következ tétel.

9.5.3. Tétel

Ha a p egésszám prím, akkor irreducibilis.

Bizonyítás

Tekintsük a p prímet és tegyük fel, hogy $c \mid p$. Ekkor $p = c\cdot q$, vagyis $p \mid c\cdot q$. A prím tulajdonság miatt $p \mid c$ vagy $p \mid q$. Az els esetben $c = \pm p$. Ha pedig $p \mid q$ teljesül, akkor $q = p\cdot t$, amit a $p = c\cdot q$ egyenlségbe helyettesítve a $p = c\cdot p\cdot t$ egyenlséghez jutunk. Ebbl a egyszersítés után $1 = c\cdot t$ adódik, amibl $c = \pm 1$következik, tehát c egység. Ezzel megmutattuk, hogy tetszleges p prímszámnak csak triviális osztói vannak, tehát felbonthatatlan.

A most bizonyított tétel szerint a prím tulajdonsággal rendelkez egész számok részhalmazát képezik a felbonthatatlan egészek halmazának. Ez az állítás minden olyan számkörre igaz, ami rendelkezik az egész számok alapvet tulajdonságaival. Lássunk ilyen számkörrre egy példát.

Tekintsük a páros számok halmazát. Ez a halmaz zárt az összeadás és szorzás mveleteire, ugyanis két páros szám összege és szorzata is páros. Mivel az egész számok egy részhalmazáról van szó, az is világos, hogy az összeadás és szorzás mveleti tulajdonságai (asszociativitás,

kommutativitás, diszributivitás, stb.) megmaradnak a páros számok körében is.

Így azután itt is bevezethet az oszthatóság fogalma. Az m páros szám osztója az n páros számnak, ha létezik olyan q páros szám, hogy $n = m \cdot q$ teljesül. Eszerint 6 osztója 12-nek mert $12 = 6 \cdot 2$. Ugyanakkor 6 nem osztója 18-nak, mert nincs olyan páros szám, amivel 6-ot megszorozva 18-at kapnánk. Ez elég furcsa elsre. További furcsaság, hogy a páros számok halmazában egy szám nem osztója önmagának. Ez annak köszönhet, hogy az 1 nem páros szám, tehát nincs benne a páros számkörben. Olyan páros szám (a 0 kivételével) nincs, amit egy másik páros számmal összeszorozva önmagát kapjuk. Mivel nincsenek egységek, ezért nincsenek triviális osztók sem a páros számkörben.

Viszont ha már van oszthatóság fogalmunk, akkor könnyen bevezethetjük a irreducibilitás fogalmát. Az n páros számot irreducubilisnek (felbonthatatlannak) nevezzük, ha nincs egyetlen osztója sem a páros számok körében. Így például 6 irreducibilis, ugyanis nem áll el két páros szám szorzataként. Ugyancsak irreducibilis a 10, 14 és a 18. Ezzel szemben például a 12 és a 56 összetett számok, mert $12 = 6 \cdot 2$, illetve $56 = 14 \cdot 4$.

A prím tulajdonság analóg módon vezethet be. Az n páros szám prím, ha valahányszor osztója két páros szám szorzatának, mindannyiszor osztója legalább az egyik tényeznek is. Ha egy páros szám nem irreducibilis, akkor nem is prím (miért?). Ez azt jelenti, hogy a 8.13 tétel a páros számokra is teljesül. Ugyanakkor a 6 nem prím, ugyanis osztója a $18 \cdot 2$-nek, ám sem 18-nak, sem pedig 2-nek nem osztója. Tehát a 6 páros számra nem teljesül a prímtulajdonság, miközben, mint láttuk irreducibilis.

Ideje azonban visszatérni az egész számok körébe. Itt az euklideszi algoritmus létezésének alapvet következményeként az irreducibilis egész számok rendelkeznek a prím tulajdonsággal..

9.5.4. Tétel

Ha a p egész szám irreducibilis, akkor prím.

Bizonyítás

Tekintsük a p irreducibilis egész számot, és tegyük fel, hogy $p \mid m \cdot n$. Ha $p \mid m$ teljesül, akkor készen vagyunk. Ellenkez esetben $lnko(m, p) = 1$, ugyanis maga p nem osztója az m-nek, egyéb osztója a ±1-gyen kívül pedig nincs, hiszen felbonthatatlan. Az 8.6 tétel szerint

$$lnko(m \cdot n, p \cdot n) = n \, .$$

Ekkor viszont $m \cdot n$ és $p \cdot n$ minden közös osztója osztója n-nek is, így speciálisan p is osztója n-nek, hiszen feltettük, hogy $p \mid m \cdot n$, az pedig nyilvánvaló, hogy $p \mid p \cdot n$. Megmutattuk tehát, hogy $p \mid m \cdot n$ esetén $p \mid m$ vagy $p \mid n$ teljesül, tehát p prím.

Összefoglalólag kimondhatjuk, hogy az euklideszi algoritmus létezésének következtében az egész számok körében a prímtulajdonság és a felbonthatatlanság ekvivalens fogalmak.

Ellenrz kérdések

1 Definiáljuk két egész szám legnagyobb közös osztóját!

2 Határozzuk meg euklideszi algoritmussal $lnko(38, 22)$-t!

3 Határozzuk meg euklideszi algoritmussal $lnko(138, 422)$-t!

4 Irjuk le az euklideszi algoritmust!

5 Mi a kapcsolat két szám közös osztói és legnagyobb közös osztója között?

6 Mivel egyenl $lnko(k \cdot n, k \cdot m)$?

7 Mondjuk ki az osztási lemmát!

8 Hogy szól Lucas tétele a Fibonacci számokról?

9 Mit mondhatunk m-rl és n-rl, ha $F_m \mid F_n$-et és $m \neq 2$?

10 Mikor mondjuk, hogy a p egész szám felbonthatatlan?

11 Mikor mondjuk, hogy a p szám prím?

12 Van-e olyan prímszám, ami nem felbonthatatlan?

13 Van-e olyan felbonthatatlan szám, ami nem prím.?