EGYETEMI JEGYZET

Algoritmikus kombinatorika és számelmélet

Bege Antal

bege@math.ubbcluj.ro

Kása Zoltán

kasa@cs.ubbcluj.ro

Kolozsvári Egyetemi Kiadó, 2006.

Készült LaTeX környezetben

Kolozsvári Egyetemi Kiadó, 2006.
ISBN:

Tartalom

1. Generátorfüggvények 7
   - 1.1. Értelmezés és tulajdonságok 7
   - 1.2. Exponenciális generátorfüggvények 14
   - 1.3. Általános tag meghatározása generátorfüggvények segítségével 18
   - 1.4. Azonosságok bizonyítása 26
   - 1.5. Bernoulli-számok és -polinomok 27
   - 1.6. Dirichlet-sorok 29
   - Feladatok 40

2. Kombinációk, permutációk, variációk generálása 45
   - 2.1. Kombinációk generálása 46
   - 2.2. Permutációk generálása 47
   - 2.3. Variációk generálása 50
   - 2.4. Ismétléses kombinációk generálása 51
   - 2.5. Ismétléses variációk generálása 52
   - 2.6. Ismétléses permutációk generálása 53
   - 2.7. Descartes-szorzat elemeinek generálása 55
   - 2.8. Adott halmaz részhalmazainak generálása 56
   - 2.9. Természetes számok partíciója 58
   - Feladatok 66

3. Skatulyaelv 69
   - 3.1. Skatulyaelv 69
   - 3.2. Logikai szita 75
   - Feladatok 85

4. Szókombinatorika 89
   - 4.1. Fibonacci-reprezentáció 89
   - 4.2. Véges szavak 95
   - 4.3. Végtelen szavak 97

4.4. Szógráfok 101
4.5. Szavak bonyolultsága 108
Feladatok 131

5. Euklidészi algoritmusok 135
5.1. Euklidészi algoritmusok 135
5.2. Lánctörtek 141
Feladatok 148

6. Prímszámok 151
6.1. Alapfogalmak 151
6.2. A prímszámok száma és nagysága 152
6.3. Bertrand posztulátuma és alkalmazásai 169
6.4. Prímszámokra vonatkozó képletek 183
6.5. Prímszámok reciprokainak összege 187
6.6. Kutatási feladatok 195
Feladatok 197

Könyvészet 201
Tárgy- és névmutató 207

1.

Generátorfüggvények

1.1. Értelmezés és tulajdonságok

Ebben a fejezetben egy fontos módszert mutatunk be, amelyek segítségével egyenleteket oldhatunk meg, de különböző formulákat is bizonyíthatunk. A generátorfüggvényeket, többek között, felhasználhatjuk rekurzív egyenletek megoldására, bizonyos objektumok (pl. bináris fák) megszámolására, azonosságok bizonyítására, partíciós problémák megoldására. Az objektumok megszámolása rekurzív egyenletek felállításával és megoldásával történik. Ezek a rekurzív egyenletek általában nem lineárisak, megoldásukban segíthetnek a generátorfüggvények.

Egy $(a_n)_{n=0}^{\infty} = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ végtelen számsorozathoz hozzárendelhetünk egy hatványsort a következőképpen:

$$A(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n + \cdots = \sum_{n=0}^{\infty} a_n z^n,$$

amelyet az $(a_n)_{n=0}^{\infty}$ számsorozat *generátorfüggvényének* nevezünk.

Például, ha tekintjük a Fibonacci-számokat

$$f_{n+2} = f_{n+1} + f_n,\ n \geq 0, \quad f_0 = 0,\ f_1 = 1,$$

akkor a sorozat a generátorfüggvénye a következő:

$$F(z) = \sum_{n=0}^{\infty} f_n z^n = z + z^2 + 2z^3 + 3z^4 + 5z^5 + 8z^6 + 13z^7 + \cdots.$$

Ha mindkét oldalt megszorozzuk z-vel, majd z^2-tel, a következőket kapjuk:

$$\begin{aligned} F(z) &= f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots + f_n z^n + \cdots, \\ zF(z) &= f_0 z + f_1 z^2 + f_2 z^3 + \cdots + f_{n-1} z^n + \cdots, \\ z^2 F(z) &= f_0 z^2 + f_1 z^3 + \cdots + f_{n-2} z^n + \cdots. \end{aligned}$$

Ha kivonjuk tagonként az első képletből a másodikat, majd a harmadikat, és figyelembe vesszük a Fibonacci-számokat definiáló képletet, a következőt kapjuk:

$$F(z)(1 - z - z^2) = z,$$

ahonnan

$$F(z) = \frac{z}{1 - z - z^2}\ . \tag{1.1}$$

Megjegyzések.
1. A generátorfüggvényt jellemezhetjük egy vektorral is, az u_n sorozathoz hozzárendelhetjük a következő vektort:

$$(u_0, u_1, \ldots, u_n, \ldots).$$

A generátorfüggvény egyes tulajdonságait vektorral is felírjuk, mert egyes esetekben jobban rámutat a lényegre.
2. A generátorfüggvénynek van egy konvergenciasugara, ennek a kiszámításával mi nem foglalkozunk, formálisan vizsgáljuk a generátorfüggvényt, feltételezve minden esetben egy konvergencia tartomány létezését (sok esetben a generátorfüggvény csak egy eszköz).

Felmerül a kérdés, hogy mire jók a generátorfüggvények? A generátorfüggvények felhasználási területe nagyon változatos: a számelmélet, a kombinatorika, az analízis és természetesen a diszkrét differenciaegyenletek. Itt most felsorolunk pár felhasználási lehetőséget:

1. Bizonyos (legtöbbször rekurzív) sorozatok általános tagjának a meghatározása.

2. Új rekurzív összefüggések bizonyítása vagy felírása.

3. Bizonyos formulák igazolása generátorfüggvények segítségével. Legtöbbször kombinatorikus képletek igazolásánál lehet a legjobban használni.

4. A számelméletben használt generátorfüggvények felhasználhatók bizonyos összegek aszimptotikus képletének a kiszámítására, valamint a multiplikatív számelméleti függvények tulajdonságainak a vizsgálatára.

5. Sorozatokra vonatkozó aszimptotikus képletek meghatározása. Bizonyos bonyolultabb sorozatok esetén az általános tag meghatározása helyett a sorozat nagyságrendjét becsüljük fel. Például az n-dik prímszámra nem tudunk általános képletet felírni, de a nagyságrendjét fel tudjuk becsülni (nagy n értékre megközelíti az $n \log n$-et).

6. Egyenletek megoldása. Ide soroljuk a Lagrange-féle inverziós formulát, mely segítségével bizonyos függvényegyenleteket oldhatunk meg.

Tekintsük az

$$A(z) = \sum_{n=0}^{\infty} a_n z^n \text{ és } B(z) = \sum_{n=0}^{\infty} b_n z^n$$

generátorfüggvényeket.

Az $A(z)$ és $B(z)$ akkor és csakis akkor *egyenlő*, ha $a_n = b_n$ bármely n természetes számra.

A következőkben a generátorfüggvényekkel végezhető műveleteket és a különböző tulajdonságokat mutatjuk be.

• *összeadás*

$$A(z) + B(z) = \sum_{n=0}^{\infty} (a_n + b_n) z^n.$$

• *skalárral való szorzás*

$$cA(z) = \sum_{n=0}^{\infty} (ca_n) z^n$$

• *eltolás*

– eltolás jobbra

$$z^k A(z) = \sum_{n=0}^{\infty} a_n z^{n+k} = \sum_{n=k}^{\infty} a_{n-k} z^n$$

vagy

$$(a_0, a_1, \ldots, a_n, \ldots) \longrightarrow \underbrace{(0, 0, \ldots, 0}_{k}, a_0, a_1, \ldots).$$

– eltolás balra

$$\begin{aligned} \frac{1}{z^k}(A(z) - a_0 - a_1 z - \ldots - a_{k-1} z^{k-1}) &= \sum_{n=k}^{\infty} a_n z^{n-k} = \\ &= \sum_{n=0}^{\infty} a_{n+k} z^n \end{aligned}$$

vagy

$$\underbrace{(0, 0, \ldots, 0}_{k-1}, a_k, a_{k+1}, \ldots) \to (a_k, a_{k+1}, \ldots, \ldots).$$

• *argumentumcsere*

$$A(cz) = \sum_{n=0}^{\infty} c^n a_n z^n.$$

Ebből megkaphatjuk a következőket is:

$$\frac{1}{2}(A(z) + A(-z)) = a_0 + a_2 z^2 + \ldots + a_{2n} z^{2n} + \ldots$$

$$\frac{1}{2}\left(A(z)-A(-z)\right)=a_1z+a_3z^3+\ldots+a_{2n-1}z^{2n-1}+\ldots$$

Ha $A(z)=1+z+z^2+z^3+\cdots=\dfrac{1}{1-z}$, akkor

$$1+z^2+z^4+\cdots=\frac{1}{2}\big(A(z)+A(-z)\big)=\frac{1}{2}\left(\frac{1}{1-z}+\frac{1}{1+z}\right)=\frac{1}{1-z^2}\,,$$

amely megkapható úgyis, hogy z-t z^2-tel helyettesítjük $A(z)$-ben.

Hasonlóképpen, megkaphatjuk a páratlan kitevőjű tagok összegét:

$$z+z^3+z^5+\cdots=\frac{1}{2}\big(A(z)-A(-z)\big)=\frac{1}{2}\left(\frac{1}{1-z}-\frac{1}{1+z}\right)=\frac{z}{1-z^2}\,.$$

• *szorzás*

$$A(z)\cdot B(z)=\sum_{n=0}^{\infty}c_nz^n,$$

ahol

$$c_n=\sum_{k=0}^{n}a_kb_{n-k}.$$

A c_n sorozatot nevezik még az a_n és b_n sorozatok Cauchy-szorzatának vagy konvolúciójának, és használatos az

$$(a*b)_n=\sum_{k=0}^{n}a_kb_{n-k}$$

jelölés is. Sajátos esetben ($b_n=1,\forall n\in\mathbb{N}$) érvényes a következő képlet:

$$\frac{1}{1-z}A(z)=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}a_k\right)z^n.$$

Ha $a_n=1$ minden n-re, akkor

$$\frac{1}{(1-z)^2}=\sum_{n=0}^{\infty}(n+1)z^n$$

• *hatványozás*

$$A^n(z)=\sum_{n_1+n_2+\cdots+n_k=n}a_{n_1}a_{n_2}\cdots a_{n_k}z^n.$$

• *deriválás*

$$A'(z)=\sum_{n=1}^{\infty}na_nz^{n-1}=\sum_{n=0}^{\infty}(n+1)a_{n+1}z^n.$$

• *integrálás*

$$\int_0^z A(t)dt = \sum_{n=1}^{\infty} \frac{1}{n} a_{n-1} z^n = \sum_{n=0}^{\infty} \frac{1}{n+1} a_n z^{n+1}.$$

• *generátorfüggvény reciproka*

Ha $a_0 \neq 0$, akkor az $\dfrac{1}{A(z)}$-nek létezik generátorfüggvénye és

$$\frac{1}{A(z)} = \sum_{n=0}^{\infty} c_n z^n,$$

ahol

$$c_n = \left(-\frac{1}{a(0)}\right) \sum_{k=0}^{n} a_k c_{n-k},$$

amely rekurzív összefüggés a $(c_n)_{n\geq 0}$ sorozatra, de a sorozat tagjai egyértelműen meghatározottak.

• *összetevés*

$b_0 = 0$ esetén

$$\begin{aligned} A(B(z)) &= \sum_{n=0}^{\infty} a_n B(z)^n = \\ &= a_0 + a_1 b_1 z + \left(a_1 b_2 + a_2 b_1^2\right) z^2 + \dots \end{aligned}$$

Megjegyzések.

1. A $b_0 = 0$ feltétel azért fontos, mert ellenkező esetben az összetevés együtthatói végtelen tagot tartalmaznak, és akkor a konvergencia tárgyalása külön feladat lenne.

2. Abban az esetben, ha az $A(z)$ polinom, akkor a b_0 értéke tetszőleges lehet, mert az összetett függvény együtthatói véges összegek lesznek.

• *generátorfüggvény inverze*

Ha $a_0 = 0$ és $a_1 \neq 0$, akkor az $A(z)$-nek létezik inverze ($A^{-1}(z)$), vagyis

$$A(A^{-1}(z)) = A^{-1}(A(z)) = z.$$

A generátorfüggvények segítségével érdekes képleteket kaphatunk. Legyen például

$$A(z) = \frac{1}{1-z} = 1 + z + z^2 + z^3 + \cdots.$$

Ekkor $zA\big(z(1+z)\big) = F(z)$, vagyis éppen a Fibonacci-számok generátorfüggvénye. A fenti képletből

$$zA\big(z(1+z)\big) = z + z^2(1+z) + z^3(1+z)^2 + z^4(1+z)^3 + \cdots.$$

A z^{n+1} együtthatója a bal oldalon éppen F_{n+1}, vagyis az $(n+1)$-edik Fibonacci-szám, míg a z^{n+1} jobb oldali együtthatója, a binomiális képlet alkalmazása után minden tagban

$$\sum_{k\geq 0}\binom{n-k}{k}.$$

Innen

$$F_{n+1}=\sum_{k\geq 0}\binom{n-k}{k}=\sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n-k}{k}. \tag{1.2}$$

Emlékeztetünk, hogy a binomiális képlet általánosítható tetszőleges valós r-re is, vagyis

$$(1+z)^r=\sum_{n=0}^{\infty}\binom{r}{n}z^n,$$

amely a binomiális együtthatók generátorfüggvénye. Itt az $\binom{r}{n}$ a kombináció általánosítása valós r-re, vagyis

$$\binom{r}{n}=\begin{cases}\dfrac{r(r-1)(r-2)\dots(r-n+1)}{n(n-1)\dots 1}, & \text{ha } n>0,\\ 1, & \text{ha } n=0,\\ 0, & \text{ha } n<0.\end{cases}$$

A binomiális képlet fenti általánosítása segítségével (negatív r-re) egy, sok esetben hasznos képletet kapunk. Legyen

$$\frac{1}{(1-z)^m}=(1-z)^{-m}=\sum_{k\geq 0}\binom{-m}{k}(-z)^k.$$

Mivel egyszerű számítással igazolható, hogy

$$\binom{-m}{k}=(-1)^k\binom{m+k-1}{k},$$

a következő képletet kapjuk:

$$\frac{1}{(1-z)^{m+1}}=\sum_{k\geq 0}\binom{m+k}{k}z^k.$$

Ekkor

$$\frac{z^m}{(1-z)^{m+1}}=\sum_{k\geq 0}\binom{m+k}{k}z^{m+k}=\sum_{k\geq 0}\binom{m+k}{m}z^{m+k}=\sum_{k\geq 0}\binom{k}{m}z^k.$$

Innen pedig

$$\sum_{k\geq 0}\binom{k}{m}z^k=\frac{z^m}{(1-z)^{m+1}}, \tag{1.3}$$

ahol m természetes szám.

Néhány példa a tulajdonságokra:

1. Legyen $A(z)=1+z+z^2+\cdots$. Ekkor a balra tolás képlete alapján

$$\frac{1}{z}\big(A(z)-1\big)=1+z+z^2+\cdots=A(z),$$

ahonnan

$$A(z)=\frac{1}{1-z}.$$

2. Ha deriváljuk az

$$A(z)=1+z+z^2+\cdots=\frac{1}{1-z}$$

összefüggést, akkor

$$A'(z)=1+2z+3z^2+\cdots=\frac{1}{(1-z)^2}.$$

A fenti összefüggést kapjuk, ha kiszámítjuk az $A(z)^2$ mint generátorfüggvény hatványát.

3. Ha integráljuk az

$$A(z)=1+z+z^2+\cdots=\frac{1}{1-z}$$

összefüggést, akkor

$$\int_0^z A(x)dx=z+\frac{1}{2}z^2+\frac{1}{3}z^3+\cdots=\int_0^z\frac{1}{1-x}dx=\ln\frac{1}{1-z}.$$

4. Ha a

$$H_n=1+\frac{1}{2}+\frac{1}{3}+\cdots\frac{1}{n}$$

harmonikus számok generátorfüggvényét szeretnénk kiszámítani, akkor összeszorozzuk az

$$1+z+z^2+\cdots=\frac{1}{1-z}$$

valamint a

$$z+\frac{1}{2}z^2+\frac{1}{3}z^3+\cdots=\ln\frac{1}{1-z},$$

generátorfüggvényeket, és a szorzás alapján

$$\sum_{n=1}^{\infty} H_n \cdot z^n = \frac{1}{1-z}\ln\frac{1}{1-z}.$$

Néhány gyakran használt generátorfüggvény:

$$\sum_{n=1}^{\infty} z^n = 1+z+z^2+z^3+\ldots = \frac{1}{1-z}$$

$$\sum_{n=0}^{\infty} (-1)^n z^n = 1-z+z^2-z^3+\ldots = \frac{1}{1+z}$$

$$\sum_{n=0}^{\infty} \binom{n+p}{p} z^n = \binom{p}{p} + \binom{p+1}{p} z + \binom{p+2}{p} z^2 + \ldots = \frac{1}{(1-z)^{p+1}}, \quad p \in \mathbf{N}$$

$$\sum_{n=1}^{\infty} \frac{1}{n} z^n = z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \ldots = \ln\frac{1}{1-z}$$

$$\sum_{n=0}^{\infty} z^{2n} = 1+z^2+z^4+z^6\ldots = \frac{1}{1-z^2}$$

$$\sum_{n=0}^{\infty} \binom{r}{n} z^n = 1 + \binom{r}{1} z + \binom{r}{2} z^2 + \binom{r}{3} z^3 \ldots = (1+z)^r, \quad r \in \mathbf{R}$$

$$\sum_{n=0}^{\infty} \binom{n}{p} z^n = \binom{p}{p} z^p + \binom{p+1}{p} z^{p+1} + \binom{p+2}{p} z^{p+2} + \ldots = \frac{x^p}{(1+x)^{p+1}}, \quad p \in \mathbf{N}$$

$$\sum_{n=0}^{\infty} \binom{2n}{n} z^n = 1 + \binom{2}{1} z + \binom{4}{2} z^2 + \binom{6}{3} z^3 + \ldots = \frac{1}{\sqrt{1-4z}}$$

$$\sum_{n=0}^{\infty} \frac{-1}{2n-1} \binom{2n}{n} z^n = 1 - \binom{2}{1} z - \frac{1}{3}\binom{4}{2} z^2 - \frac{1}{5}\binom{6}{3} z^3 - \ldots = \sqrt{1-4z}$$

$$\sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} z^n = 1 + \frac{1}{2}\binom{2}{1} z + \frac{1}{3}\binom{4}{2} z^2 + \frac{1}{4}\binom{6}{3} z^3 + \ldots = \frac{1-\sqrt{1-4z}}{2z}$$

$$\sum_{n=0}^{\infty} 2^n z^n = 1 + 2z + 2^2 z^2 + 2^3 z^3 + \ldots = \frac{1}{1-2z}$$

1.2. Exponenciális generátorfüggvények

A következőkben külön értelmezzük az exponenciális generátorfüggvényt, és megnézzük a klasszikus és exponenciális generátorfüggvény kapcsolatát.

1.1. értelmezés. *Az adott u_n sorozat **exponenciális generátorfüggvénye** a következő hatványsor:*

$$\hat{G}(z) = \sum_{n=0}^{\infty} \frac{u_n}{n!} z^n.$$

z előbbiekhez hasonlóan nézzük meg az exponenciális generátorfüggvény néhány olyan tulajdonságát, amelyek alátámasztják a fenti értelmezés külön bevezetését.

Legyenek az $(a_n)_{n\geq 0}$ illetve $(b_n)_{n\geq 0}$ sorozatok exponenciális generátorfüggvényei

$$\hat{A}(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n,$$

$$\hat{B}(z) = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n.$$

• *deriválás*

$$\hat{A}'(z) = \sum_{n=0}^{\infty} \frac{a_{n+1}}{n!} z^n,$$

valamint

$$\hat{A}^k(z) = \sum_{n=0}^{\infty} \frac{a_{n+k}}{n!} z^n. \tag{1.4}$$

• *szorzás*

$$\hat{A}(z) \cdot \hat{B}(z) = \sum_{n=0}^{\infty} \frac{c_n}{n!} z^n,$$

ahol

$$c(n) = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}.$$

• *hatványozás*

$$\hat{A}^k = \sum_{r_1+r_2+\cdots+r_k=n} \frac{n!}{r_1! r_2! \cdots r_k!} a_{r_1} a_{r_2} \cdots a_{r_k}.$$

Példák.

1. A Fibonacci-sorozat exponenciális generátorfüggvénye

Legyen

$$E(z) = \sum_{n=0}^{\infty} \frac{f_n}{n!} z^n,$$

a Fibonacci-sorozat exponenciális generátorfüggvénye. Ekkor az

$$f_{n+2} = f_{n+1} + f_n$$

rekurzív képlet alapján, felhasználva (1.4)-et, az

$$E'' = E' + E$$

lineáris differenciálegyenletet kapjuk. Felírva és megoldva a fenti differenciálegyenlet karakterisztikus egyenletét, azt kapjuk, hogy

$$E(z) = c_1 e^{r_1 x} + c_2 e^{r_2 x},$$

ahol

$$r_1 = \frac{\sqrt{5}+1}{2},\ r_2 = \frac{\sqrt{5}-1}{2}.$$

Az

$$E(0) = f_0 = 0,\ E'(0) = f_1 = 1$$

kezdeti feltételekből meghatározhatjuk a c_1 illetve c_2 állandókat, és az exponenciális generátorfüggvényre azt kapjuk, hogy

$$E(z) = \frac{1}{\sqrt{5}}(e^{r_1 x} - e^{r_2 x}). \tag{1.5}$$

2. A Bell-számok exponenciális generátorfüggvénye.
A Bell-számok általános alakja

$$b_n = \frac{1}{e}\sum_{k=o}^{\infty}\frac{k^n}{k!},$$

és a rekurzív összefüggés, amit kielégítenek,

$$b_{n+1} = \sum_{k=0}^{n}\binom{n}{k} b_k,\ n \geq 0, \tag{1.6}$$

ahol $b(0) = 1$.
Ha ebből az összefüggésből szeretnénk kiszámítani az exponenciális generátorfüggvényt

$$B(z) = \sum_{n=0}^{\infty}\frac{b_n}{n!}z^n,$$

akkor a (1.4) alapján a baloldal exponenciális generátorfüggvénye $B'(z)$, valamint a szorzási művelet alapján ($a_n = 1$), a baloldal exponenciális generátor függvénye

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}b_k\right)z^n = \sum_{n=0}^{\infty}\frac{z^n}{n!}\sum_{n=0}^{\infty}\frac{b_n}{n!}z^n = e^z B(z).$$

Így a következő differenciálegyenletet írhatjuk fel:

$$B'(z) = e^z B(z),$$

a $B(0) = b(0) = 1$ kezdeti feltétellel. Ez szétválasztható változójú egyenlet, így a megoldása

$$B(z) = ce^{e^z},$$

és a kezdeti feltételből következik, hogy $c = \frac{1}{e}$, vagy

$$B(z) = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n = e^{e^z - 1}.$$

A következő tétel egy sorozat generátorfüggvénye és exponenciális generátorfüggvénye közötti kapcsolatot mutatja meg.

1.2. tétel. *Legyen az a_n sorozat generátorfüggvénye*

$$A(z) = \sum_{n=0}^{\infty} a_n z^n,$$

valamint exponenciális generátorfüggvénye

$$\hat{A}(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n.$$

Ekkor

$$A(z) = \int_0^{\infty} e^{-s} \hat{A}(zs) ds.$$

Bizonyítás. Az Euler-féle Γ függvényre

$$\Gamma_n = n! = \int_0^{\infty} e^{-s} s^n ds$$

(erről meggyőződhetünk parciális integrálással). Így

$$\begin{aligned} A(z) &= \sum_{n=0}^{\infty} a_n z^n = \\ &= \sum_{n=0}^{\infty} a_n \frac{1}{n!} z^n \int_0^{\infty} e^{-s} s^n ds = \\ &= \int_0^{\infty} e^{-s} \sum_{n=0}^{\infty} a_n \frac{(st)^n}{n!} ds = \\ &= \int_0^{\infty} e^{-s} \hat{A}(zs) ds. \end{aligned}$$

□

Például az

$$A(z) = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$$

esetén

$$\hat{A}(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} = e^z,$$

a tételbeli összefüggés pedig azt jelenti, hogy

$$\frac{1}{1-z} = \int_0^{\infty} e^{-s} e^{zs} ds.$$

1.3. Általános tag meghatározása generátorfüggvények segítségével

Ebben a részben a generátorfüggvények legfontosabb tulajdonságára összpontosítunk, nevezetesen a diszkrét kezdetiérték-feladatok megoldására. Adunk egy általános módszert, amelyet majd a konkrét egyenleteknél alkalmazunk az u_n sorozat n-nel kifejezett zárt alakjára. Lineáris, állandó együtthatójú rekurzív egyenletek esetén a módszer mindig eredményhez vezet.
A módszert lépésekben adjuk meg, és ezek a lépések számítógépen is programozhatók.

1. Szorozzuk meg az egyenlet mindkét oldalát z^n-nel és összegezzük n-re.

2. Az egyenlet mindkét oldalát alakítsuk úgy, hogy a $G(z) = \sum_{n=0}^{\infty} u_n z^n$-t tartalmazó kifejezések legyenek. Ha szükséges, akkor feltételezzük, hogy a sorozat negatív argumentumú tagjai egyenlők 0-val ($u_{-1} = u_{-2} = \ldots = 0$).

3. Oldjuk meg az így kapott egyenletet, így zárt alakban kapjuk meg a $G(z)$-t.

4. Fejtsük hatványsorba $G(z)$-t, és olvassuk le z^n együtthatóját. Ez lesz az u_n sorozat n-ben kifejezett zárt alakja.

A fenti módszer állandó együtthatójú homogén egyenlet esetén a következőképpen néz ki. Adott a következő k-ad rendű homogén egyenlet:

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = 0,$$

ahol $a_1, a_2, \ldots, a_k$ valós együtthatók, és $a_k \neq 0$. A fenti módszer lépései a következők:

1.

$$\sum_{n=0}^{\infty} u_{n+k} z^n + a_1 \sum_{n=0}^{\infty} u_{n+k-1} z^n + \cdots + a_k \sum_{n=0}^{\infty} u_n z^n = 0 \tag{1.7}$$

2. Legyen az u_n sorozat generátorfüggvénye

$$G(z) = \sum_{n=0}^{\infty} u_n z^n.$$

Az összegeket rendre a következő alakokban írjuk:

$$\sum_{n=0}^{\infty} u_{n+k}z^n = \sum_{n=k}^{\infty} u_n z^{n-k} = \frac{1}{z^k}(G(z) - u(0) - u_1 z - \ldots - u_{k-1}z^{k-1}),$$

$$\sum_{n=0}^{\infty} u_{n+k-1}z^n = \sum_{n=k-1}^{\infty} u_n z^{n-k+1} = \frac{1}{z^{k-1}}(G(z) - u_0 - u_1 z - \ldots - u_{k-2}z^{k-2})\ldots$$

$$\sum_{n=0}^{\infty} u_n z^n = G(z).$$

Ezeket visszahelyettesítjük a (1.7) egyenletbe.

3. Az így kapott egyenletből kifejezzük $G(z)$-t. A fenti képletek alapján a generátorfüggvény két polinom hányadosa lesz:

$$G(z) = \frac{P(z)}{Q(z)}$$

4. A $\frac{P(z)}{Q(z)}$-t elemi törtekre bontjuk, és felhasználva a $\frac{1}{1-az}$, $\frac{1}{(1-az)^k}$, $\frac{1}{1+z^2}$, valamint $\frac{1}{(1+z^2)^k}$ hatványsorait, $G(z)$-t hatványsorba fejthetjük, és ebből a hatványsorból leolvassuk z^n együtthatóját. Ez lesz az u_n sorozat zárt alakja.

Megjegyzés. Inhomogén rekurzív egyenletre is alkalmazhatjuk a fenti módszert, a szabad tag alakjától függ, hogy a generátorfüggvény két polinom hányadosa lesz vagy nem. Polinomiális szabad tag esetén biztosan polinomok hányadosát kapjuk generátorfüggvényként.

Oldjunk meg néhány lineáris és nemlineáris egyenletet a generátorfüggvény módszerével.

1. példa. Adott az

$$u_{n+1} - 3u_n = n \tag{1.8}$$

elsőrendű nemlineáris egyenlet az $u_0 = 1$ kezdeti feltétellel. Legyen

$$G(z) = \sum_{n=0}^{\infty} u_n z^n.$$

Az egyenletet beszorozva z^n-nel, rendre a következő egyenleteket írhatjuk fel:

$$\sum_{n=0}^{\infty} u_{n+1}z^n - 3\sum_{n=0}^{\infty} u_n z^n = \sum_{n=0}^{\infty} n z^n,$$

$$\frac{G(z)-1}{z} - 3G(z) = \frac{z}{(1-z)^2}.$$

Innen

$$G(z) = \frac{1}{(1-3z)(1-z^2)}.$$

Elemi törtekre bontva, majd sorba fejtve

$$G(z) = \frac{9}{8}\frac{1}{1-3z} - \frac{1}{4}\frac{1}{1-z} + \frac{1}{8}\frac{1}{1+z},$$

$$G(z) = \sum_{n=0}^{\infty}\left(\frac{9}{8}3^n - \frac{1}{4} + \frac{1}{8}(-1)^n\right)z^n.$$

Innen

$$u(n) = \frac{9}{8}3^n - \frac{1}{4} + \frac{1}{8}(-1)^n.$$

2. példa. Adott az

$$u_n = u_{n-1} + 2u_{n-2} + (-1)^n,\ n \geq 2, \tag{1.9}$$

másodrendű, állandó együtthatójú lineáris egyenlet, az

$$u_0 = u_1 = 1$$

kezdeti feltételekkel.
Feltételezhetjük, hogy $u_{-2} = u_{-1} = 0$, ahonnan

$$u_0 = u_{-1} + 2u_{-2} + (-1)^0,$$

$$u_1 = u_0 + 2(-1) + (-1)^1 + 1$$

Ha $G(z)$-vel jelöljük a sorozat generátorfüggvényét, akkor a fentiek alapján

$$\sum_{n=0}^{\infty} u_n z^n = \sum_{n=0}^{\infty} u_{n-1}z^n + 2\sum_{n=0}^{\infty} u_{n-2}z^n + \sum_{n=0}^{\infty}(-1)^n z^n + z,$$

és a jobbra tolás képlete alapján

$$G(z) = zG(z) + 2z^2G(z) + \frac{1}{1+z} + z.$$

Innen

$$\begin{aligned} G(z) &= \frac{1+z+z^2}{(1-2z)(1+z)^2} = \\ &= \frac{7}{9}\cdot\frac{1}{1-2z} + \frac{2}{9}\cdot\frac{1}{1+z} + \frac{1}{3}\cdot\frac{1}{(1+z)^2}. \end{aligned}$$

Sorba fejtve a megfelelő tagokat

$$G(z) = \sum_{n=0}^{\infty} \left(\frac{7}{9}2^n + \frac{2}{9}(-1)^n + \frac{1}{3}n(-1)^n \right) z^n,$$

ahonnan

$$u(n) = \frac{7}{9}2^n + \frac{2}{9}(-1)^n + \frac{1}{3}n(-1)^n.$$

3. példa. *Bináris fák száma*

Jelöljük b_n-nel az n csúcsú bináris fák számát. Ekkor $b_1 = 1$, $b_2 = 2$, $b_3 = 5$ (lásd a **??**. ábrát). Legyen $b_0 = 1$. (Később látni fogjuk, hogy ez jó választás.)

Ha rögzítjük egy n csúcsú bináris fa gyökerét, akkor még $n-1$ csúcs marad a bal és jobb részfában összesen. Ha k csúcs van a bal oldali, $n-1-k$ pedig a jobb oldali részfában, akkor összesen $b_k b_{n-1-k}$ ilyen bináris fa létezik. Összegezve $k = 0, 1, \ldots, n-1$ értékekre, pontosan b_n-t kapjuk. Tehát tetszőleges $n \geq 1$ természetes számra a b_n-ben megoldandó rekurzív egyenlet a következő:

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0. \tag{1.10}$$

Ez még így is írható:

$$b_n = \sum_{k=0}^{n-1} b_k b_{n-1-k}.$$

A fenti rekurzív egyenlet mindkét oldalát z^n-nel szorozva, majd n szerint összegezve, a következőt kapjuk:

$$\sum_{n=1}^{\infty} b_n z^n = \sum_{n=1}^{\infty} \left(\sum_{k=0}^{n-1} b_k b_{n-1-k} \right) z^n. \tag{1.11}$$

Legyen $B(z) = \sum_{n=0}^{\infty} b_n z^n$ a b_n számok generátorfüggvénye. A (1.10) összefüggés bal oldala éppen $B(z) - 1$ (mivel $b_0 = 1$). A jobb oldal nagyon hasonlít két generátorfüggvény szorzatához. Hogy észrevegyük, melyik két függvényről van szó, használjuk a következő jelölést:

$$A(z) = zB(z) = \sum_{n=0}^{\infty} b_n z^{n+1} = \sum_{n=1}^{\infty} b_{n-1} z^n.$$

Ekkor a (1.11) jobb oldala éppen $A(z)B(z)$, ami egyenlő $zB^2(z)$-vel. Innen

$$B(z) - 1 = zB^2(z), \quad B(0) = 1.$$

Oldjuk meg ezt az egyenletet $B(z)$-ben! Ekkor

$$B(z) = \frac{1 \pm \sqrt{1-4z}}{2z}\,.$$

Mivel $B(0) = 1$ csak a negatív jel megfelelő. Tehát

$$\begin{aligned}
B(z) &= \frac{1}{2z}\left(1-\sqrt{1-4z}\right) = \frac{1}{2z}\left(1-(1-4z)^{1/2}\right) \\
&= \frac{1}{2z}\left(1-\sum_{n=0}^{\infty}\binom{1/2}{n}(-4z)^n\right) = \frac{1}{2z}\left(1-\sum_{n=0}^{\infty}\binom{1/2}{n}(-1)^n 2^{2n} z^n\right) \\
&= \frac{1}{2z} - \binom{1/2}{0}\frac{2^0 z^0}{2z} + \binom{1/2}{1}\frac{2^2 z}{2z} - \cdots - \binom{1/2}{n}(-1)^n \frac{2^{2n} z^n}{2z} + \cdots \\
&= \binom{1/2}{1}2 - \binom{1/2}{2}2^3 z + \cdots - \binom{1/2}{n}(-1)^n 2^{2n-1} z^{n-1} + \cdots \\
&= \sum_{n\geq 0}\binom{1/2}{n+1}(-1)^n 2^{2n+1} z^n = \sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n} z^n.
\end{aligned}$$

Innen $b_n = \dfrac{1}{n+1}\binom{2n}{n}$, amely azonos a C_n-nel jelölt ún. Catalan-számmal.

Megjegyzés. Az utolsó átalakításnál felhasználtuk a következő, könnyen bizonyítható összefüggést:

$$\binom{1/2}{n+1} = \frac{(-1)^n}{2^{2n+1}(n+1)}\binom{2n}{n}.$$

4. példa *Levelek száma n csúcsú bináris fák halmazában*

Számítsuk ki az n csúcsú bináris fák halmazában a levelek (azaz első fokú csúcsok) számát. Jelöljük ezt a számot f_n-nel. Megjegyezzük, hogy a gyökeret akkor sem tekintjük levélnek, ha a fokszáma 1. Könnyű belátni, hogy $f_2 = 2$, $f_3 = 6$. Legyen $f_0 = 0$ és $f_1 = 1$ konvenció alapján.

Ahogy a bináris fák megszámolásánál, tekintsük most is az olyan n csúcsú bináris fákat, amelyeknek bal oldala k csúcsot, a jobb oldala pedig $n-k-1$ csúcsot tartalmaz. Bal oldalon b_k ilyen részfa van, jobb oldalon pedig b_{n-1-k}. Ha rögzítünk egy ilyen bal oldali részfát, akkor az összes jobb oldali részfát figyelembe véve, ott f_{n-1-k} levél van. Könnyen belátható tehát, hogy adott k-ra $b_{n-1-k}f_k + b_k f_{n-1-k}$ levél van. Ekkor, összegzés után

$$f_n = \sum_{k=0}^{n-1}(f_k b_{n-1-k} + b_k f_{n-1-k}).$$

Egyszerű számítással azt kapjuk, hogy

$$f_n = 2(f_0 b_{n-1} + f_1 b_{n-2} + \cdots + f_{n-1} b_0), \quad n \geq 2. \tag{1.12}$$

Ez a megoldandó rekurzív egyenlet, amelynek megoldása f_n. Legyen

$$F(z) = \sum_{n=0}^{\infty} f_n z^n \quad \text{és} \quad B(z) = \sum_{n=0}^{\infty} b_n z^n.$$

A (1.12) összefüggés mindkét oldalát z^n-nel szorozva, majd n szerint összeadva

$$\sum_{n\geq 2} f_n z^n = 2 \sum_{n\geq 2} \left(\sum_{k=0}^{n-1} f_k b_{n-1-k} \right) z^n.$$

De, mivel $f_0 = 0$ és $f_1 = 1$,

$$F(z) - z = 2zF(z)B(z).$$

Innen

$$F(z) = \frac{z}{1 - 2zB(z)},$$

de mivel

$$B(z) = \frac{1}{2z}\left(1 - \sqrt{1-4z}\right),$$

következik, hogy

$$F(z) = \frac{z}{\sqrt{1-4z}} = z(1-4z)^{-1/2} = z \sum_{n=0}^{\infty} \binom{-1/2}{n} (-4z)^n.$$

A számítások elvégzése után

$$F(z) = \sum_{n\geq 0} \binom{2n}{n} z^{n+1} = \sum_{n=1}^{\infty} \binom{2n-2}{n-1} z^n,$$

innen pedig

$$f_n = \binom{2n-2}{n-1} \quad \text{vagy} \quad f_{n+1} = \binom{2n}{n} = (n+1)b_n.$$

A kombináció általánosítása alapján f_0 és f_1 a konvenció alapján megadott értékekkel lesznek egyenlők.

5. példa *n csúcsú k levelű bináris fák száma*

Egy kicsit nehezebb feladat: hány n csúcsú k levelű bináris fa létezik? Jelöljük ezek számát $b_n^{(k)}$-val. Könnyű belátni, hogy $b_n^{(k)} = 0$, ha $k > \lfloor (n+1)/2 \rfloor$. Egyszerű

okoskodással ki lehet számítani a $k=1$ esetet, vagyis $b_n^{(1)} = 2^{n-1}$ tetszőleges $n \geq 1$ természetes számra. Legyen $b_0^{(0)} = 1$ konvenció alapján. Akárcsak az előző feladatoknál, itt is a bal és jobb oldali részfákat vizsgáljuk meg. Ha a bal oldali részfában i csúcs és j levél van, akkor a jobb oldaliban $n-i-1$ csúcs és $k-j$ levél van. A $b_i^{(j)} b_{n-i-1}^{(k-j)}$ szorzat éppen ezeknek a fáknak a száma. Összegezve k és j szerint, a következő rekurzív képletet kapjuk:

$$b_n^{(k)} = 2b_{n-1}^{(k)} + \sum_{i=1}^{n-2} \sum_{j=1}^{k-1} b_i^{(j)} b_{n-i-1}^{(k-j)}. \tag{1.13}$$

Ennek a rekurzív egyenletnek a megoldására használjuk a következő generátorfüggvényt:

$$B^{(k)}(z) = \sum_{n=0}^{\infty} b_n^{(k)} z^n, \quad \text{ahol } k \geq 1.$$

A (1.13) egyenlet mindkét oldalát z^n-nel megszorozva, majd összeadva $n = 0, 1, 2, \ldots$ értékekre, a következőt kapjuk:

$$\sum_{n=1}^{\infty} b_n^{(k)} z^n = 2 \sum_{n=1}^{\infty} b_{n-1}^{(k)} z^n + \sum_{n=1}^{\infty} \left(\sum_{i=1}^{n-2} \sum_{j=1}^{k-1} b_i^{(j)} b_{n-i-1}^{(k-j)} \right) z^n.$$

Az összegezés sorrendjét felcserélve

$$\sum_{n=1}^{\infty} b_n^{(k)} z^n = 2 \sum_{n=1}^{\infty} b_{n-1}^{(k)} z^n + \sum_{j=1}^{k-1} \sum_{n=1}^{\infty} \left(\sum_{i=1}^{n-2} b_i^{(j)} b_{n-i-1}^{(k-j)} \right) z^n.$$

Innen

$$B^{(k)}(z) = 2zB^{(k)}(z) + z \left(\sum_{j=1}^{k-1} B^{(j)}(z) B^{(k-j)}(z) \right)$$

vagy

$$B^{(k)}(z) = \frac{z}{1-2z} \left(\sum_{j=1}^{k-1} B^{(j)}(z) B^{(k-j)}(z) \right). \tag{1.14}$$

Lépésről lépésre haladva, felírhatjuk a következőket.

$$B^{(2)}(z) = \frac{z}{1-2z} \left(B^{(1)}(z) \right)^2,$$

$$B^{(3)}(z) = \frac{2z^2}{(1-2z)^2} \left(B^{(1)}(z) \right)^3,$$

$$B^{(4)}(z) = \frac{5z^3}{(1-2z)^3} \left(B^{(1)}(z) \right)^4.$$

Az általános megoldást megpróbáljuk a következő alakban keresni:

$$B^{(k)}(z) = \frac{c_k z^{k-1}}{(1-2z)^{k-1}} \left(B^{(1)}(z)\right)^k,$$

ahol, amint láttuk, $c_2 = 1$, $c_3 = 2$, $c_4 = 5$. A (1.14) képletbe behelyettesítve, a c_k számokra egy rekurzív összefüggést kapunk:

$$c_k = \sum_{i=1}^{k-1} c_i c_{k-i}.$$

Ezt szintén a generátorfüggvények segítségével oldjuk meg. Ha $k = 2$, akkor $c_2 = c_1 c_1$, és innen $c_1 = 1$. Legyen $c_0 = 1$. Ha $C(z) = \sum_{n=0}^{\infty} c_n z^n$ a c_n számok generátorfüggvénye, akkor – figyelembe véve a generátorfüggvények szorzási képletét –

$$C(z) - 1 - z = (C(z)-1)^2 \quad \text{vagy} \quad C^2(z) - 3C(z) + z + 2 = 0,$$

amelyet $C(z)$-re nézve megoldunk, és a

$$C(z) = \frac{3 - \sqrt{1-4z}}{2}$$

képletet kapjuk. $C(0) = 1$ miatt csak a negatív előjel jó. Sorba fejtés után

$$\begin{aligned} C(z) &= \frac{3}{2} - \frac{1}{2}(1-4z)^{1/2} = \frac{3}{2} - \frac{1}{2}\sum_{n=0}^{\infty} \frac{-1}{2n-1}\binom{2n}{n} z^n \\ &= \frac{3}{2} + \sum_{n=0}^{\infty} \frac{1}{2(2n-1)}\binom{2n}{n} z^n = 1 + \sum_{n=1}^{\infty} \frac{1}{2(2n-1)}\binom{2n}{n} z^n. \end{aligned}$$

Innen

$$c_n = \frac{1}{2(2n-1)}\binom{2n}{n}, \ \ n \geq 1.$$

Mivel $b_n^{(1)} = 2^{n-1}$, ha $n \geq 1$, könnyen ellenőrizhető, hogy $B^{(1)} = \dfrac{z}{1-2z}$. Tehát

$$B^{(k)}(z) = \frac{1}{2(2k-1)}\binom{2k}{k} \frac{z^{2k-1}}{(1-2z)^{2k-1}} \ .$$

Mivel azonban

$$\frac{1}{(1-z)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{n} z^n,$$

a következő eredményhez jutunk:

$$\begin{aligned} B^{(k)}(z) &= \frac{1}{2(2k-1)}\binom{2k}{k}\sum_{n=0}^{\infty}\binom{2k+n-2}{n}2^n z^{2k+n-1} \\ &= \frac{1}{2(2k-1)}\binom{2k}{k}\sum_{n\geq 2k-1}\binom{n-1}{n-2k+1}2^{n-2k+1}z^n. \end{aligned}$$

Innen pedig

$$b_n^{(k)} = \frac{1}{2k-1}\binom{2k}{k}\binom{n-1}{2k-2}2^{n-2k}$$

vagy

$$b_n^{(k)} = \frac{1}{n}\binom{2k}{k}\binom{n}{2k-1}2^{n-2k}.$$

1.4. Azonosságok bizonyítása

A generátorfüggvényeket jól lehet használni azonosságok bizonyítására.

Alapötletünk az, hogy egy függvényt kétféleképpen fejtjük sorba, majd azonosítjuk z^n együtthatóit a két kifejtésben.

Tekintsük a következő generátorfüggvényt:

$$\frac{1}{\sqrt{1-4z}} = (1-4z)^{-\frac{1}{2}} = \sum_{n=0}^{\infty}\binom{-\frac{1}{2}}{n}(-4z)^n =$$

$$= \sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}2^{2n}z^n = \sum_{n=0}^{\infty}\binom{2n}{n}z^n$$

Felhasználva ezt a $A(z) = \dfrac{z}{\sqrt{1-4z}}$ függvény kétféle sorba fejtésében egy érdekes azonosságot kapunk.

A fenti képlet alapján:

$$A(z) = \sum_{n=0}^{\infty}a_n z^n = \frac{z}{\sqrt{1-4z}} = \sum_{n=0}^{\infty}\binom{2n}{n}z^{n+1} = \sum_{n=1}^{\infty}\binom{2n-2}{n-1}z^n,$$

ahonnan $a_n = \binom{2n-2}{n-1}$.

Másfelől

$$A(z) = \frac{z}{\sqrt{1-4z}} = \frac{z\sqrt{1-4z}}{1-4z} = \frac{z}{1-4z}\sqrt{1-4z}$$

De tudjuk, hogy

$$\frac{z}{1-4z} = z\sum_{n=0}^{\infty}(4z)^n = \sum_{n=0}^{\infty}4^n z^{n+1} = \sum_{n=1}^{\infty}4^{n-1}z^n \tag{1.15}$$

és

$$\sqrt{1-4z} = \sum_{n=0}^{\infty} \frac{-1}{2n-1}\binom{2n}{n} z^n \tag{1.16}$$

A (1.15) és (1.16) képletek függvényeit összeszorozva, azt kapjuk, hogy:

$$A(z) = \left(\sum_{n=1}^{\infty} 4^{n-1} z^n\right)\left(\sum_{n=0}^{\infty} \frac{-1}{2n-1}\binom{2n}{n} z^n\right)$$

Innen következik, figyelembe véve a generátorfüggvények szorzását:

$$a_n = \sum_{k=0}^{n-1} 4^{n-1-k} \cdot \frac{-1}{2k-1}\binom{2k}{k}$$

Egyenlővé téve a_n két kifejezését, azt kapjuk, hogy:

$$-4^{n-1}\sum_{k=0}^{n-1} \frac{1}{4^k(2k-1)}\binom{2k}{k} = \binom{2n-2}{n-1},$$

amely még a következő alakban is felírható ($n-1$ helyébe n-t írva):

$$\sum_{k=1}^{n} \frac{4^{n-k}}{2k-1}\binom{2k}{k} = 4^n - \binom{2n}{n}, \qquad n \geq 1.$$

1.5. Bernoulli-számok és -polinomok

Az exponenciális generátorfüggvények alkalmazásaként bemutatjuk a Bernoulli-számok és polinomok néhány tulajdonságát. Ezeknek a polinomoknak nagyon nagy szerepük van a később bevezetendő, Riemann-féle zeta függvény vizsgálatában, az analitikus számelméletben, kombinatorikában de az approximációelméletben is.

1.3. értelmezés. *Azon $B_n(x)$ polinomokat, amelyeknek exponenciális generátorfüggvénye $\dfrac{z\,e^{xz}}{e^z-1}$, vagyis*

$$\frac{z\,e^{xz}}{e^z-1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n, \tag{1.17}$$

***Bernoulli-polinomoknak**, valamint a $B_n(0) = B(n)$ értékeket **Bernoulli-számoknak** nevezzük.*

1.4. tétel. *A $B_n(x)$ polinom általános alakja*

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B(k) x^{n-k}.$$

Bizonyítás. A (1.17) és

$$e^{xz} = \sum_{n=0}^{\infty} \frac{x^n z^n}{n!}, \tag{1.18}$$

képletek alapján

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n = \frac{z}{e^z - 1} \cdot e^{xz} = \left(\sum_{n=0}^{\infty} \frac{B(n)}{n!} z^n \right) \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n \right).$$

z^n együtthatóit kifejezve,

$$\frac{B_n(x)}{n!} = \sum_{k=0}^{n} \frac{B(k)}{k!} \frac{x^{n-k}}{(n-k)!},$$

ahonnan következik a kért azonosság.

□

1.5. tétel. *A Bernoulli-polinomok a következő differenciaegyenlet megoldásai:*

$$B_n(x+1) - B_n(x) = nx^{n-1}, \quad n \geq 1.$$

Bizonyítás. A következő azonosságokat írhatjuk fel:

$$e^{(x+1)z} - e^{xz} = e^{xz}(e^z - 1),$$

$$z\frac{e^{(x+1)z}}{e^z - 1} - z\frac{e^{xz}}{e^z - 1} = ze^{xz}.$$

Az (1.17) és (1.18) alapján

$$\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} z^n = \sum_{n=0}^{\infty} \frac{x^n}{n!} z^{n+1}.$$

Egyenlővé téve a z^n együtthatóját, kapjuk a kért egyenletet. □

Következmény. A differenciaegyenletbe 0-t helyettesítve

$$B(n) = B_n(0) = B_n(1),\ n \geq 2.$$

Ha a 1.4 tétel következtetését $x = 1$-re írjuk fel, és használjuk az előbbi következményt, akkor a Bernoulli-számokra a következő differenciaegyenletet kapjuk.

1.6. tétel. *Ha $n \geq 2$, akkor*

$$B(n) = \sum_{k=0}^{n} \binom{n}{k} B(k), \tag{1.19}$$

vagy

$$\sum_{k=0}^{n-1} \binom{n}{k} B(k) = 0,\ n \geq 2.$$

Megjegyzések.
1. A fenti differenciaegyenlet nem tekinthető lineáris egyenletnek, mivel a rendje nem határozható meg pontosan.

2. Az értelmezésből adódik, hogy $B(0) = 1$ és az (1.19) összefüggés alapján a Bernoulli-számok értékei:

n	0	1	2	3	4	5	6	7	8	9	10	11
$B(n)$	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0

3. A 1.4 tételből kiszámíthatjuk a Bernoulli-polinomok néhány értékét

$$\begin{aligned} B_0(x) &= 1, \\ B_1(x) &= x - \frac{1}{2}, \\ B_2(x) &= x^2 - x + \frac{1}{6}, \\ B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, \\ B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30} \end{aligned}$$

Formálisan a következőképpen írhatjuk fel a Bernoulli-polinomokra, illetve Bernoulli-számokra vonatkozó képleteket

$$B_n(x) = (B + x)^n,$$

$$B(n) = (B + 1)^n.$$

1.6. Dirichlet-sorok

Ebben a részben egy más típusú generátorfüggvénnyel, a számelméletben használatos Dirichlet-sorokkal foglalkozunk. Minden u_n sorozat tulajdonképpen egy számelméleti függvény. Ebben a részben inkább a számelméleti függvény elnevezést és jelölést használjuk, mert ez közelebb áll a Dirichlet-sorok számelméleti vagy kombinatorikai alkalmazásához. A következőkben általában olyan függvényekkel foglalkozunk, melyek értelmezési tartománya az $\mathbb{N}^*$.

Bevezetünk néhány gyakran használt számelméleti függvényt és azok alapvető tulajdonságait is felsoroljuk.

1. A Möbius-függvény
A Möbius-függvény értelmezése

$$\mu(n) = \begin{cases} 1, & \text{ha} \quad n = 1 \\ (-1)^k, & \text{ha} \quad n = p_1 \cdot p_2 \cdots p_k \\ 0, & \text{ha} \quad \exists\, p:\ p^2 \mid n, \end{cases}$$

ahol $p_1,\ p_2, \cdots, p_k$ különböző prímszámok.
A Möbius-függvényre érvényesek a következő tulajdonságok.
1. Adott $n \geq 1$ természetes számra:

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = I(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases} . \tag{1.20}$$

Az $I(n)$ függvénynek fontos szerepe van a Dirichlet-féle konvolúciós szorzat vizsgálatában.

2. Az Euler-féle φ függvény
Az Euler-féle φ függvényt úgy értelmezzük, mint az n-nél kisebb és n-nel relatív prím természetes számok száma.
Alapvető tulajdonságai:
1. Adott $n \geq 1$ természetes számra:

$$\sum_{d|n} \varphi(d) = n. \tag{1.21}$$

2. Adott $n \geq 1$ természetes számra:

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}. \tag{1.22}$$

3. Adott $n \in N^*$-ra:

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{1.23}$$

Az osztók száma és az osztók összege
Értelmezzük az osztók száma és egy általánosítása, az osztók összege számelméleti függvényeket, valamint ezek egy közös általánosítását.
Adott $n \geq 1$ természetes számra legyen $\tau(n)$ az n szám osztóinak a száma:

$$\tau(n) = \sum_{d|n} 1.$$

Legyen $\tau_\ell(n)$ az n természetes szám ℓ darab ($l \geq 2$) rendezett szám ℓ -esekre való felbontásainak a száma:

$$\tau_l(n) = \sum_{\substack{n = d_1 d_2 \cdots d_\ell \\ d_1 \leq d_2 \leq \ldots \leq d_\ell.}} 1$$

Adott $n \geq 1$ természetes számra legyen $\sigma(n)$ az n szám osztóinak az összege:

$$\sigma(n) = \sum_{d|n} d.$$

Adott s valós számra legyen $\sigma_s(n)$ az n osztói s-edik hatványának az összege:

$$\sigma_s(n) = \sum_{d|n} d^s.$$

A fenti osztófüggvényekre érvényesek a következő tulajdonságok:
1. Ha $n = 1$, akkor $\tau(n) = 1$, ha pedig $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, ahol $p_1, p_2, \ldots, p_k$ különböző prímszámok, akkor

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1).$$

2. Bármely $n \geq 1$ természetes számra

$$\tau_\ell(n) = \prod_{p^\alpha || n} \binom{\alpha + \ell - 1}{\ell - 1}$$

3. Ha $n = 1$, akkor $\sigma(n) = 1$, ha pedig $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, akkor

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1-1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

4. Adott s valós számra, ha $n = 1$, akkor $\sigma_s(n) = 1$, ha pedig $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, akkor

$$\sigma_s(n) = \frac{p_1^{s(\alpha_1+1)} - 1}{p_1^s - 1} \cdot \frac{p_2^{s(\alpha_2+1)} - 1}{p_2^s - 1} \cdots \frac{p_k^{s(\alpha_k+1)} - 1}{p_k^s - 1}.$$

Az osztók szorzata
Egy olyan számelméleti függvényt is értelmezzünk, melynek a tulajdonságait az

utóbbi időben kezdték tanulmányozni.
Legyen $T(n)$ az n természetes szám osztóinak a szorzata:

$$T(n) = \prod_{d|n} d.$$

Ekkor bizonyítható a következő képlet:

$$T(n) = n^{\frac{\tau(n)}{2}}.$$

Ramanujan-összeg
Először bevezetjük a következő jelölést:

$$e(t) = e^{2\pi i t}, \quad t \in \mathbb{R}.$$

Az $e(t)$ függvényt általában racionális értékekre fogjuk használni. Bevezetjük a Ramanujan-összeg fogalmát.
Adott $n \geq 2$ természetes számra, a következő összeget Ramanujan-összegnek nevezzük:

$$c_n(m) = \sum_{\substack{k \leq n \\ (k,n)=1}} e\left(\frac{k \cdot m}{n}\right).$$

A Ramanujan-összegre érvényes a következő tulajdonság:
1. Adott $n \geq 2$ természetes számra és tetszőleges $m \in \mathbb{N}^*$-ra

$$c_n(m) = \sum_{\substack{d \mid m \\ d \mid n}} d \cdot \mu\left(\frac{n}{d}\right).$$

Mivel a később bevezetendő Dirichlet-sorok elméletében nagy jelentősége van a multiplikatív számelméleti függvényeknek és a Dirichlet-féle konvolúciós szorzatnak, először ezeket értelmezzük.

1.7. értelmezés. *Az f számelméleti függvényt **multiplikatívnak** nevezzük, ha*

$$f(mn) = f(m)f(n),$$

minden m és n relatív prím természetes számpárra.
Ha az

$$f(mn) = f(m)f(n)$$

*összefüggés tetszőleges m, n számpárra teljesül, akkor a függvényt **teljesen multiplikatívnak** nevezzük.*

Mivel az f multiplikatív számelméleti függvényre igaz, hogy

$$f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdots f(p_n^{\alpha_n}),$$

ezeket a függvényeket elég prímszám hatványon megadni.
A Möbius-, Euler- és az osztófüggvények multiplikatívak, míg az osztók szorzata nem multiplikatív függvény.

1.8. értelmezés. *Adott f és g számelméleti függvények **Dirichlet konvolúciója**, (vagy Dirichlet-szorzata), az a h számelméleti függvény, amelyre*

$$h(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} g(d) \cdot f\left(\frac{n}{d}\right). \tag{1.24}$$

Jelölés. Röviden a

$$h = f * g$$

jelölést használjuk, ami azt jelenti, hogy

$$h(n) = (f * g)(n), \quad \forall n \in \mathbb{N}^*.$$

Bevezetjük a következő számelméleti függvényeket:

$$e(n) = n, \quad \forall n \in \mathbb{N}^*$$

$$U(n) = 1, \quad \forall n \in \mathbb{N}^*.$$

1. Az előzőleg bevezetett függvények tulajdonságait a következőképpen írhatjuk fel a konvolúció segítségével:

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor \Longleftrightarrow \mu * U = I,$$

$$\sum_{d|n} \varphi(d) = n \Longleftrightarrow \varphi * U = e,$$

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} \Longleftrightarrow \varphi = \mu * e,$$

$$\tau(n) = \sum_{d|n} 1 \Longleftrightarrow \tau = U * U,$$

$$\sigma(n) = \sum_{d|n} d \Longleftrightarrow \sigma = e * U,$$

$$\sigma_s(n) = \sum_{d|n} d^s \Longleftrightarrow \sigma = e^s * U,$$

Bevezetjük a Dirichlet-sor fogalmát.

1.9. értelmezés. *Az $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ számelméleti függvény* ***Dirichlet sora*** *a következő sor:*

$$D(f)(s) = F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},\ s \in \mathcal{D}.$$

$\mathcal{D} \subset \mathbb{C}$ egy olyan tartomány, ahol a sor konvergens.

Megjegyzés. Mi a továbbiakban csak formálisan dolgozunk a Dirichlet-sorokkal, feltételezzük, hogy mindig létezik olyan $s_0 > 0$ valós szám, hogy $|s| > s_0$ esetén a Dirichlet-sor konvergens, és ahol nem mondunk semmit a sorok természetéről, ott ezt feltételeztük. Vannak olyan eredmények, melyeknél nagyon fontos a konvergencia, és azt a bizonyításban is használni kell, ezeknél a kijelentésben is megjelenik a konvergencia.

Ha az $u(n) = 1$ függvény Dirichlet-sorát írjuk fel, akkor a legalapvetőbb generátorfüggvényt, a Riemann-féle zeta függvényt kapjuk.

1.10. értelmezés. *Az $|s| > 1$ komplex számra értelmezett*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

függvényt a ***Riemann-féle zeta függvénynek*** *nevezzük.*

Megjegyzések.

1. A ζ függvény hatványsorba fejtéssel természetes módon kiterjeszthető a teljes komplex síkra. Az így létrejött függvény a prímszámok elméletében és bizonyos aszimptotikus formulák bizonyításában kiemelt fontosságú.

2. A Riemann-féle zeta függvényhez kapcsolódik az egyik leghíresebb és legfontosabb sejtés, a Riemann-sejtés, amely megtalálható a harmadik évezred hét legfontosabb feladata között, és megoldása jelentős pénzdíjjal, egymillió dollárral jár (a Clay Intézet [17], 3. évezred feladatai között szerepel).

A Riemann-sejtés azt állítja, hogy a ζ függvény minden nem triviális $s \in \mathbb{C}$ zérushelyének a valós része $\frac{1}{2}$, vagyis

$$\mathrm{Re}\,(s) = \frac{1}{2}.$$

A triviális zérushelyek a páros egész számok.

Nagyon sok olyan eredmény van a számelméletben, de más matematikai ágakban (például algebrai geometriában, topológiában) is, amelyek ekvivalensek a fenti sejtéssel. Itt két olyan elemi feladatot említünk meg, amelyek ekvivalensek a Riemann-sejtéssel, az elsőben szerepel egy expliciten nem ismert állandó (az Euler-állandó), míg a másodikban egy ilyen állandó sem szerepel.

- **1. feladat.** (G. Robin [62], 1984)
  A

$$\sigma(n) < e^{\gamma} n \log\log n, \quad n \geq 5041,$$

egyenlőtlenség, ahol γ az Euler-féle állandó egyenértékű a Riemann-sejtéssel.

- **2. feladat.** (J. Lagarias [51], 2002) A

$$\sigma(n) \leq H_n + e^{H_n} \log(H_n),$$

egyenlőtlenség, ahol H_n az n-edik harmonikus szám

$$H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n},$$

egyenértékű a Riemann-sejtéssel.

3. A Riemann-féle zeta függvény $s = 2m$, $m \in \mathbb{N}^*$ értékre a következőképpen fejezhető ki a Bernoulli-számok segítségével:

$$\zeta(2m) = \frac{4^m(-1)^{m-1}B(2m)\pi^{2m}}{2(2m)!}. \tag{1.25}$$

Ennek a részletes bizonyítása megtalálható például T. M. Apostol [3] könyvében, . Példaként írjunk fel néhány értéket:

$$\begin{aligned}
\zeta(2) &= \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \\
\zeta(4) &= \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \\
\zeta(6) &= \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}, \\
\zeta(8) &= \sum_{n=1}^{\infty} \frac{1}{n^8} = \frac{\pi^8}{9450}, \\
\zeta(10) &= \sum_{n=1}^{\infty} \frac{1}{n^{10}} = \frac{\pi^{10}}{93555}, \\
\zeta(12) &= \sum_{n=1}^{\infty} \frac{1}{n^{12}} = \frac{\pi^{12}}{638512875}.
\end{aligned}$$

Legtöbbször a $\zeta(2)$-re van szükségünk. Ha megvizsgáljuk a Bernoulli-számokat, akkor a $B(12)$-ig elég "normálisan" viselkednek, de a $B(12) = -\frac{691}{2730}$ számlálójában a 691 prím. Ez a prím terelte helyes irányba Eulert, mert először kiszámított néhány $\zeta(2k)$ értéket anélkül, hogy észrevette volna ezek kapcsolatát a Bernoulli-számokkal. Mivel $\zeta(2m)$ 1-hez tart, ha k tart végtelenhez, a (1.25) képlet alapján a $|B(2m)|$ értékek nagyon gyorsan nőnek.
A zeta függvény páratlan helyen felvett értékeiről nagyon keveset tudunk.

A Dirichlet-sorok egyenlőségéből következik a számelméleti függvények egyenlősége.

1.11. tétel. *Adottak az*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

és

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

Dirichlet-sorok. Ha létezik olyan $(s_k)_{k\geq 1}$ komplex számsorozat, amelynek a Re s_k valós részére igaz, hogy Re $s_k \longrightarrow \infty$ ha $k \longrightarrow \infty$, és $F(s_k) = G(s_k)$ akkor

$$f(n) = g(n), \quad \forall n.$$

A Dirichlet-sorok szorzata fontos művelet, érvényes a következő tétel.

1.12. tétel. *Legyen az f és g számelméleti függvények Dirichlet-sorai*

$$F(s) = \sum_{n+1}^{\infty} \frac{f(n)}{n^s},$$

$$G(s) = \sum_{n+1}^{\infty} \frac{g(n)}{n^s}.$$

A két Dirichlet-sor szorzatára érvényes a következő képlet:

$$F(s) \cdot G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s},$$

ahol

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

vagy

$$D(f) \cdot D(g) = D(f * g). \tag{1.26}$$

Bizonyítás. Az értelmezés alapján a következő formulákat írhatjuk fel:

$$\begin{aligned} D(f)(s) \cdot D(g)(s) &= F(s) \cdot G(s) = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{f(m)g(k)}{(mk)^s} = \\ &= \sum_{n=1}^{\infty} \left(\sum_{mk=n} \frac{f(m)g(k)}{(mk)^s} \right) = \\ &= \sum_{n=1}^{\infty} \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right) \right) \frac{1}{n^s} \\ &= D(f * g)(s). \end{aligned}$$

□

Megjegyzés. A tétel azonnali következménye a következő összefüggés:

$$(D(f))^k = D(\underbrace{f * f * \ldots * f}_{k}). \tag{1.27}$$

Példák.
1. példa. Legyen $f(n) = 1$ és $g(n) = \mu(n)$. Ekkor $h(n) = I(n)$ és a (1.26) képlet alapján

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1,$$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$$

2. példa. Legyen $f(n) = 1$ és $g(n) = \varphi(n)$. Mivel

$$h(n) = \sum_{d|n} \varphi(d) = n,$$

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1),$$

vagy

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

3. példa. Legyen $f(n) = 1$ és $g(n) = n$. Mivel $h(n) = \sum_{d|n} d = \sigma(n)$

$$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}.$$

Jelöljük a prímszámok halmazát $\mathbb{P}$-vel.
A következő, Euler által megtalált formulát a számelmélet alaptétele analitikus alakjának is nevezik.

1.13. tétel. *Adott az f multiplikatív számelméleti függvény, amelyre a*

$$\sum_{n=1}^{\infty} f(n),$$

összeg abszolút konvergens. Ekkor az összeget a következőképpen írhatjuk át egy abszolút konvergens végtelen szorzattá:

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} (1 + f(p) + f(p^2) + \cdots + f(p^k) + \cdots). \tag{1.28}$$

Ha az f függvény teljesen multiplikatív, akkor

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \frac{1}{1-f(p)}. \tag{1.29}$$

Bizonyítás. Jelöljük $P(x)$-szel a következő véges szorzatot:

$$P(x) = \prod_{p\le x}(1+f(p)+f(p^2)+\cdots+f(p^k)+\cdots).$$

Mivel ez a szorzat véges számú abszolút konvergens sor szorzata, a tagokat átrendezhetjük anélkül, hogy az összeg megváltozna. Ha elvégezzük a szorzást, azt kapjuk, hogy egy tag a szorzatból

$$f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_\ell^{\alpha_\ell}) = f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\ell^{\alpha_\ell})$$

alakú (felhasználtuk az f függvény multiplikativitását). Így

$$P(x) = \sum_{n\in A(x)} f(n),$$

ahol $A(x)$ azon természetes számok halmaza, amelyeknek mindegyik p prímosztója $p \le x$.
Ha $B(x)$-szel jelöljük azon természetes számok halmazát, amelyeknek van legalább egy, x-nél nagyobb prímosztója, akkor

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n\in B(x)} f(n),$$

$$\left|\sum_{n=1}^{\infty} f(n) - P(x)\right| \le \sum_{n\in B(x)} |f(n)| \le \sum_{n>x} |f(n)|.$$

Ha $x\to\infty$, az abszolút konvergencia miatt a jobboldali tag 0-hoz tart. Tehát

$$\lim_{x\to\infty}\left|\sum_{n=1}^{\infty} f(n) - P(x)\right| = 0,$$

ami pontosan a (1.28) összefüggést jelenti.
A (1.28) jobboldalának abszolút konvergenciája következik abból a konvergenciakritériumból, hogy ha $\sum_{n=1}^{\infty} a_n$ abszolút konvergens, akkor $\prod_{i=1}^{\infty}(1+a_n)$ is abszolút konvergens.
Ha az f függvény teljesen multiplikatív, akkor $p\in\mathbb{P}$-re

$$f(p^n) = f(p)^n,$$

ahonnan (1.28)-ból

$$\begin{aligned}\sum_{n=1}^{\infty} f(n) &= \prod_{p\in\mathbb{P}}(1+f(p)+f(p^2)+\cdots+f(p^k)+\cdots) = \\ &= \prod_{p\in\mathbb{P}}\left(1+f(p)+f(p)^2+\cdots+f(p)^k+\cdots\right) = \\ &= \prod_{p\in\mathbb{P}}\frac{1}{1-f(p)}.\end{aligned}$$

□

Ezt a tételt alkalmazva abszolút konvergens Dirichlet-sorokra, a következő eredményt kapjuk.

1.14. tétel. *Adott az f multiplikatív számelméleti függvény, amelyre a*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s},$$

Dirichlet-sor abszolút konvergens $Re(s) > s_0$ esetén. Ekkor az összeget a következőképpen írhatjuk át egy abszolút konvergens végtelen szorzattá $Re(s) > s_0$ értékekre

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}}(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\cdots+\frac{f(p^k)}{p^{ks}}+\cdots). \tag{1.30}$$

Ha az f függvény teljesen multiplikatív, akkor

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}}\frac{1}{1-\frac{f(p)}{p^{-s}}}. \tag{1.31}$$

Példák.

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_{p\in\mathbb{P}}\frac{1}{1-\frac{1}{p^s}}, \quad \mathrm{Re}(s) > 1$$

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right), \quad \mathrm{Re}(s) > 1$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \prod_{p\in\mathbb{P}}\frac{1-\frac{1}{p^s}}{1-\frac{1}{p^{s-1}}}, \quad \mathrm{Re}(s) > 2$$

$$\begin{aligned}\zeta(s)\cdot\zeta(s-1) &= \sum_{n=1}^{\infty}\frac{\sigma(n)}{n^s} = \\ &= \prod_{p\in\mathbb{P}}\frac{1}{\left(1-\frac{1}{p^s}\right)\left(1-\frac{1}{p^{s-1}}\right)}, \quad \mathrm{Re}(s) > 2.\end{aligned}$$

Feladatok

1.1. Bizonyítsuk be a generátorfüggvények segítségével, hogy

$$\left\langle {n \atop k} \right\rangle = \binom{n+k-1}{k},$$

ahol $\left\langle {n \atop k} \right\rangle$ n elem k-adrendű ismétléses kombinációját jelöli.

1.2. Számítsuk ki a következő sorozatok generátorfüggvényét, valamint exponenciális generátorfüggvényét:

$$u_n = 2^n + 5^n,$$

$$u_n = 3^n + \sin\frac{n\pi}{2},$$

$$u_n = n2^n + (n^2+1)\cos\frac{n\pi}{2}.$$

1.3. Számítsuk ki a

$$\sum_{k=1}^{n} \frac{1}{k(n-k)}$$

összeget a generátorfüggvény segítségével.

1.4. A generátorfüggvény segítségével oldjuk meg a következő rekurzív egyenleteket:

$$u_{n+2} + 3u_{n+1} + 2u_n = 0,$$
$$u_0 = 1,\ u_1 = -4,$$

$$u_{n+4} + u_{n+3} + 30u_{n+2} + 20u_{n+1} + 24u_n = 0$$
$$u_0 = u_1 = 0, u_2 = 1, u_3 = 10,$$

$$u_{n+2} - 4u_{n+1} + 3u_n = 2^n,$$
$$u_0 = 1,\ u - 1 = 2.$$

1.5. Oldjuk meg generátorfüggvény segítségével az alábbi rekurzív egyenletet.

$$H_n = 2H_{n-1} + 1, \quad H_0 = 0.$$

(H_n itt a Hanoi-tornyai nevű probléma lépésszámát jelenti.)

1.6. Bizonyítsuk be, hogy

$$\sqrt{1-4z} = \sum_{n\geq 0} \frac{-1}{2n-1}\binom{2n}{n} z^n$$

1.7. Bizonyítsuk be, hogy

$$\sum_{k=0}^{n} \binom{2k}{k} \binom{2n-2k}{n-k} = 2^{2n}$$

1.8. Bizonyítsuk be, hogy

$$\sum_{k=0}^{n} \frac{1}{2k-1} \binom{2k}{k} \binom{2n-2k}{n-k} = -\delta_{n0}$$

1.9. Számítsuk ki a

$$\sum_{k=0}^{n} f_k f_{n-k}$$

összeget, ahol f_n a Fibonacci-sorozat n-edik tagja.

1.10. Számítsuk ki, hány olyan n csúcsú bináris fa van, amelynek sem a bal, sem pedig a jobb oldali részfája nem üres.

1.11. Számítsuk ki, hány olyan n csúcsú bináris fa van, amelyben minden levéltől különböző csúcsnak pontosan két leszármazottja van.

1.12. A generátorfüggvény segítségével határozzuk meg, hogy hányféleképpen építhetünk fel egy $2 \times 2 \times n$ méretű oszlopot $2 \times 1 \times 1$-es téglalapokból.

1.13. Hányféleképpen lehet az $\{1, 2, \ldots, 2n\}$ számokat egy $2 \times n$ mátrixba úgy elhelyezni, hogy a számok a sorokban balról jobbra, az oszlopokban pedig fentről lefelé növekedjenek? $n = 5$=re egy példa

$$\begin{pmatrix} 1 & 2 & 4 & 5 & 8 \\ 3 & 6 & 7 & 9 & 10 \end{pmatrix}$$

1.14. Oldjuk meg generátorfüggvény segítségével az alábbi rekurzív egyenletet.

$$\begin{aligned} a_n &= a_{n-1} + 2a_{n-2} + \cdots + na_0, \quad \text{ha } n > 0 \\ a_0 &= 1 \end{aligned}$$

1.15. Oldjuk meg az exponenciális generátorfüggvény segítségével az alábbi rekurzív

egyenletet

$$\begin{aligned} g_n &= -2ng_{n-1} + \sum_{k=0}^{n} \binom{n}{k} g_k g_{n-k}, \quad n > 0 \\ g_0 &= 0 \\ g_1 &= 1 \end{aligned}$$

1.16. Számítsuk ki a

$$T(m,n) = \sum_{k=0}^{n} \binom{k}{m} \frac{1}{n-k}, \quad m,n \geq 0$$

értékét.

1.17. Legyen

$$f_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}.$$

Bizonyítsuk be, hogy

$$f_n(n) > \frac{e^n}{2}.$$

1.18. Tudva, hogy

$$\sum_{n=0}^{\infty} \frac{x^n (x-1)^{2n}}{n!} = \sum_{n=0}^{\infty} a(n) x^n, \ \forall x \in \mathbb{R},$$

bizonyítsuk be, hogy az $a(n)$ sorozat három egymásután következő tagjának mindegyike nem lehet 0.

1.19. Adott az $u \in S$ sorozat generátorfüggvénye:

$$\sum_{n=0}^{\infty} \frac{1}{1-2x-x^2} = \sum_{n=0}^{\infty} u(n) x^n.$$

Bizonyítsuk be, hogy bármely $n \in \mathbb{N}$ természetes szám esetén létezik olyan m természetes szám, amelyre

$$u(n)^2 + u(n+1)^2 = u(m).$$

1.20. Adott az $a \in S$ sorozat, amelyre $a(0) = 1$ és

$$a(n+1) = \frac{1}{n+1} \sum_{k=0}^{n} \frac{a(k)}{n-k+2}.$$

Számítsuk ki a következő határértéket:

$$\lim_{n\to\infty}\sum_{k=0}^{n}\frac{a(k)}{2^k}.$$

1.21. Írjuk fel az alábbi függvények Dirichlet-féle generátorfüggvényét (Dirichlet-sorát)

$$f(n)=\sqrt{n},$$
$$f(n)=\ln n,$$
$$f(n)=\begin{cases}1, & \text{ha } n \text{ négyzetmentes}\\ 0, & \text{ellenkezőleg},\end{cases}$$
$$f(n)=\begin{cases}1, & \text{ha } n \text{ } k \text{ hatványmentes}\\ 0, & \text{ellenkezőleg},\end{cases}$$

1.22. A Liouville-függvényt a következőképpen értelmezzük:

$$\lambda(n)=\begin{cases}1 & n=1\\ (-1)^{\Omega(n)} & n>1,\end{cases}$$

ahol $\Omega(n)$ az n természetes szám összes prímosztóinak a száma.
Bizonyítsuk be, hogy

$$\sum_{d|n}\lambda(d)=k(n)=\begin{cases}1 & n \text{ teljes négyzet}\\ 0 & \text{ellenkezőleg},\end{cases}$$

ahol $k(n)$ a négyzetmentes számok karakterisztikus függvénye.

1.23. Bizonyítsuk be, hogy $t\in(-1,1)$ valós számokra

$$\sum_{i=1}^{\infty}\frac{t^i}{1-t^i}=\sum_{n=1}^{\infty}\tau(n)t^n,$$

ahol $\tau(n)$ az n természetes szám osztóinak az összege

$$\tau(n)=\sum_{d|n}1.$$

1.24. Bizonyítsuk be, hogy $t\in(-1,1)$ valós számokra

$$\sum_{i=1}^{\infty}\frac{it^i}{1-t^i}=\sum_{i=1}^{\infty}\frac{t^i}{(1-t^i)^2}=\sum_{n=1}^{\infty}\sigma(n)t^n,$$

ahol $\sigma(n)$ az osztók összege

$$\sigma(n)=\sum_{d|n}d.$$

2.

Kombinációk, permutációk, variációk generálása

A kombinációk, permutációk, variációk generálására a következő általános eljárást alkalmazhatjuk, amely minden egyes meghíváskor egy $V = (v_1, v_2, \ldots, v_n)$ vektort ad vissza, amelynek elemei a generált elemek vagy azok indexei. Használunk egy *ind* változót, amelynek kezdeti értéke 0, az eljárás első meghívásakor 1-re változik, majd ismét 0-ra vált, ha már minden elemet generáltunk. Az eljárás általános alakja [52]:

```
GENERÁL(V, n, ind):
if ind = 0
  then V := kezdeti érték
       ind := 1
       exit
if létezik következő
  then V := következő
  else ind := 0
```

Megjegyzendő, hogy itt az *ind* bemeneti-kimeneti változó. Az eljárás hívásakor meghatározott értékét a következő hívás felhasználja. Az eljárást a következőképpen hívjuk meg:

```
ind := 0
repeat
    GENERÁL (V, n, ind)
    if ind = 1
      then ÍRD V_1, V_2, ..., V_n
until ind = 0
```

2.1. Kombinációk generálása

Ha n különböző elemből k elemű csoportokat képezünk úgy, hogy a csoportokon belül az elemek sorrendje nem számít, akkor egy ilyen csoportot n elem k-ad osztályú (vagy k-adrendű) *kombinációjának* nevezzük. Az összes ilyen kombináció számát $\binom{n}{k}$ vagy C_n^k jelöli.

Az összes

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

n elemű k-ad osztályú kombináció generálására a $V = (1,2,\ldots,k)$ vektorral kezdünk, amely az első kombinációt jelenti. Ha egy adott lépésnél a $V = (v_1, v_2, \ldots, v_k)$ kombinációból indulunk ki, akkor a következő kombináció meghatározására megkeressük azt a legkisebb i indexet, amelyre $v_i < n-k+i$, és generáljuk a

$$(v_1, v_2, \ldots, v_{i-1}, v_i+1, v_i+2, \ldots, v_i+n-i+1)$$

kombinációt. Az algoritmus akkor ér véget, amikor már nincs egyetlen v_i elem sem, amely a fenti feltételt kielégíti.

Könnyű belátni, hogy ez az algoritmus az összes kombinációt generálja. Kezdetben V vektor elemei növekvő sorrendben vannak, és ez a tulajdonság végig megőrződik, azaz az eljárás minden meghívása után az elemek szintén növekvő sorrendben lesznek, tehát az algoritmus egymástól különböző kombinációkat generál. Ugyanakkor azt is könnyű belátni, hogy az algoritmus minden kombinációt generál.

Az algoritmus következő:

```
KOMBINÁCIÓ (V, n, k, ind)
if ind = 0
  then  for i := 1, 2, ..., k
            do v_i := i
        ind := 1
        exit
for i := k, k-1, ..., 1
    do  if v_i < n-k+i
          then v_i := v_i + 1
               for j := i+1, i+2, ..., k
                   do v_j := v_{j-1} + 1
               exit
ind := 0
```

Az eljárás hívása:

```
ind := 0
```

repeat
  KOMBINÁCIÓ (V,n,k,ind)
  if $ind = 1$
    then ÍRD $V_1,V_2,\ldots,V_k$
until $ind = 0$

Ha alkalmazzuk algoritmusunkat az $n = 6$, $k = 4$ értékekre, a következőket kapjuk:

```
1 2 3 4   1 2 3 5   1 2 3 6   1 2 4 5   1 2 4 6
1 2 5 6   1 3 4 5   1 3 4 6   1 3 5 6   1 4 5 6
2 3 4 5   2 3 4 6   2 3 5 6   2 4 5 6   3 4 5 6
```

2.2. Permutációk generálása

Ha egy n elemű halmaz elemeit különböző sorrendbe helyezzük, akkor azt mondjuk, hogy a halmaz elemeit permutáljuk. Egy ilyen elrendezés neve *permutáció*. Az összes n elemű permutáció száma $P_n = 1 \cdot 2 \cdot 3 \cdots n = n!$.

Három módszert mutatunk be az összes $n!$ permutáció generálására.

1. módszer

A kezdeti vektor $V = (1,2,\ldots,n)$. Meghatározzuk azt a legnagyobb i indexet, amelyre $v_i < v_{i+1}$ és $v_{i+1} > v_{i+2} > \ldots > v_n$, majd azt a legnagyobb k indexet, amelyre $v_k > v_i$. Felcseréljük egymás között a v_i és v_k elemeket, majd az utolsó $n-i$ elemet, azaz v_{i+j}-t felcseréljük v_{n+1-j}-vel minden $j = 1,2,\ldots,\frac{n-i}{2}$ értékekre.

PERMUTÁL$_1$ (V,n,ind)
if $ind = 0$
  then for $i = 1,2,\ldots,n$
      do $v_i := i$
    $ind = 1$
    exit
$i := n-1$
while $v_i > v_{i+1}$
    do $i := i-1$
      if $i = 0$
        then $ind := 0$
          exit
$k := n$
while $v_i > v_k$
    do $k := k-1$
$v_i \leftrightarrow v_k$
for $i := 1,2,\ldots,\lfloor\frac{n-i}{2}\rfloor$
  do $v_{i+j} \leftrightarrow v_{n+1-j}$

Az eljárás meghívása:

```
ind := 0
repeat
    PERMUTÁL1 (V,n,ind)
    if ind = 1
      then ÍRD V1,V2,...,Vn
until ind = 0
```

Példa. Ha $n = 3$, az algoritmus a következő permutációkat generálja:

```
1 2 3   1 3 2   2 1 3   2 3 1   3 1 2   3 2 1
```

2. módszer

A kezdeti vektor $V = (1,2,\ldots,n)$. A vektor elemeit vagy azok egy részét cirkulárisan permutáljuk. Például (1,2,3,4) esetében a cirkuláris permutációk után a következőket kapjuk: (4,1,2,3), (3,4,1,2) és (2,3,4,1). Majd az (1,2,3,4)-ből az utolsó három elem cirkuláris permutációja után az (1,4,2,3)-at kapjuk, amelyet egészében újra permutáljuk cirkulárisan.

```
PERMUTÁL2 (V,n,ind)
if ind = 0
  then for i = 1,2,...,n
            do v_i := i
       ind := 1
       exit
for k := n,n-1,...,2
    do CIRKULÁRIS (V,n,k)
       if V_{n-k+1} ≠ n-k+1
         then exit
ind := 0
```

A CIRKULÁRIS eljárás az utolsó k elemet permutálja cirkulárisan:

```
CIRKULÁRIS(V,n,k)
p := v_n
for i := n,n-1,...,n-k+2
    do v_i := v_{i-1}
v_{n-k+1} := p
```

Az eljárás hívása a következő:

```
ind := 0
repeat
```

PERMUTÁL$_2$ (V,n,ind)
if $ind = 1$
then ÍRD $V_1,V_2,\ldots,V_n$
until $ind = 0$

Példa.

```
1 2 3   3 1 2   2 3 1   1 3 2   2 1 3   3 2 1
```

3. módszer

Ez a módszer rekurzívan generálja a permutációkat „alulról fölfelé”, azaz elindulunk az (a_1) elemmel, amelyből generáljuk a következő csoportokat (a_2,a_1), (a_1,a_2). Általában az $(a_1,a_2,\ldots,a_k)$ csoportból kapjuk a következőket:

$(a_{k+1},a_1,a_2,\ldots,a_k)$,
$(a_1,a_{k+1},a_2,\ldots,a_k)$,
$(a_1,a_2,a_{k+1},\ldots,a_k)$,
$\ldots$ $\ldots$ $\ldots$
$(a_1,a_2,\ldots,a_{k+1},a_k)$,
$(a_1,a_2,\ldots,a_k,a_{k+1})$.

A következő leírásban a $B=(b_1,b_2,\ldots,b_n)$ és $C=(c_1,c_2,\ldots,c_n)$ köztes vektorokat használjuk.

PERMUTÁL$_3$ (k,b)
if $k <= n$
then for $i := 1,2,\ldots,k$
do for $j := 1,2,\ldots,i-1$
do $c_j := b_j$
$c_i := a_k$
for $j := i+1,i+2,\ldots,k$
do $c_j := b_{j-1}$
PERMUTÁL$_3$ $(k+1,c)$
else írd $b_1,b_2,\ldots,b_n$

Hívás:

PERMUTÁL$_3$ $(1,a)$

Három elem esetében az eredmény a következő:

```
3 2 1   2 3 1   2 1 3   3 1 2   1 3 2   1 2 3
```

2.3. Variációk generálása

Ha n különböző elemből k elemű csoportokat képezünk úgy, hogy a csoportokon belül az elemek sorrendje is számít, akkor egy ilyen csoportot n elem k-ad osztályú (vagy k-adrendű) *variációjának* nevezzük. Az összes ilyen variáció számát V_n^k jelöli, ahol $V_n^k = n(n-1)\cdots(n-k+1)$.

Az összes variáció generálására felhasználjuk az előbbi algoritmusokat. Miután generáltunk egy kombinációt, elkészítjük annak összes permutációit.

```
VARIÁCIÓ (V,n,k,ind1)
ind1 := 0
repeat
    KOMBINÁCIÓ (V,n,k,ind1)
    if ind1 = 1
      then ind2 := 0
           for i := 1,2...,k do Wi := Vi
           repeat
                PERMUTÁL (W,k,ind2)
                if ind2 = 1
                  then ÍRDW1,W2,...,Wk
           until ind2 = 0
until ind1 = 0
```

A fenti eljárásban a PERMUTÁL csupán annyiban különbözik PERMUTÁL_1 vagy PERMUTÁL_2 eljárásoktól, hogy hiányzik a kezdeti értékadás, azaz

```
if ind = 0
  then for i = 1,2,...,n
           do vi := i
       ind := 1
       exit
```

rész helyett csupán a következő van:

```
if ind = 0
  then ind := 1
       exit
```

Példa.

Ha alkalmazzuk eljárásunkat az $n = 4$, $k = 3$ értékekre, a következőket kapjuk:

```
1 2 3     1 3 2     2 1 3     2 3 1     3 1 2     3 2 1
1 2 4     1 4 2     2 1 4     2 4 1     4 1 2     4 2 1
1 3 4     1 4 3     3 1 4     3 4 1     4 1 3     4 3 1
2 3 4     2 4 3     3 2 4     3 4 2     4 2 3     4 3 2
```

2.4. Ismétléses kombinációk generálása

Amennyiben a kombinációk esetében minden eleme ismétlődhet akárhányszor, ismétléses kombinációkról beszélünk. Ezek száma

$$\left\langle {n \atop k} \right\rangle = \binom{n+k-1}{k} = \frac{(k+n-1)!}{k!(n-1)!} = \frac{(n+k-1)(n+k-2)\cdots n}{k!}$$

Érvényes a következő képlet is:

$$\left\langle {n \atop k} \right\rangle = \left\langle {n \atop k-1} \right\rangle + \left\langle {n-1 \atop k} \right\rangle$$

Ez az algoritmus az n elemű k-ad osztályú ismétléses kombinációkat generálja. A kezdeti vektor (1,1, ..., 1) (k elemű). Minden lépésben a $(v_1, v_2, \ldots, v_k)$ vektorból a következő szabállyal kapjuk meg a rákövetkezőt: megkeressük azt a legnagyobb i indexet, amelyre $v_i < n$ és innen a $(v_1, v_2, \ldots v_{i-1}, v_i + 1, v_i + 1, \ldots, v_i + 1)$ vektort kapjuk. Nyilvánvaló, hogy megkapjuk az összes ismétléses kombinációt.

ISMÉTLÉSES-KOMBINÁCIÓ (V, n, k, ind)
if $ind = 0$
  then for $i = 1, 2, \ldots, k$
    do $v_i := 1$
  $ind := 1$
  exit
for $i := k, k-1, \ldots, 1$
  do if $v_i \neq n$ **then**
    for $j := i, i+1, \ldots, k$
      do $v_j := v_i + 1$
    exit
$ind := 0$

Hívás:

$ind := 0$
repeat
  ISMÉTLÉSES-KOMBINÁCIÓ (V, n, k, ind)
  if $ind = 1$
    then ÍRD $V_1, V_2, \ldots, V_k$
until $ind = 0$

Ha $n = 4$, $k = 3$ akkor az eredmény:

```
1 1 1      1 1 2      1 1 3      1 1 4      1 2 2
```

```
1 2 3     1 2 4     1 3 3     1 3 4     1 4 4
2 2 2     2 2 3     2 2 4     2 3 3     2 3 4
2 4 4     3 3 3     3 3 4     3 4 4     4 4 4
```

Ha $n = 2$, $k = 3$ akkor az eredmény:

```
1 1 1     1 1 2     1 2 2     2 2 2
```

2.5. Ismétléses variációk generálása

A variációk esetében is ismétlődhetnek elemek. Ha n elemünk van, és k elemű, ismétlődést is megengedő, csoportokat használunk, akkor bármelyik helyre 1-től k-ig bármelyik elem kerülhet (az n közül). Így az n elemű k-adrendű ismétléses variációk száma n_k.

1. módszer

A kezdeti vektor $V = (1,1,\ldots,1)$. A V vektor rákövetkezője a következőképpen határozható meg: megkeressük azt a legnagyobb i indexet, amelyre $v_i < n$, és ha ez az index létezik, akkor a V rákövetkezője: $(v_1, v_2, \ldots, v_{i-1}, v_i + 1, 1, \ldots, 1)$. Ha ilyen i index nem létezik, akkor ez azt jelenti, hogy már minden elemet generáltunk.

ISMÉTLÉSES-VARIÁCIÓ$_1$ (V, n, k, ind)
if $ind = 0$
  then for i:=1,2,...,k
        do $v_i := 1$
     $ind := 1$
     exit
  else for $i := k, k-1, \ldots, 1$
        do if $v_i < n$
           then $v_i := v_i + 1$
              exit
           else $v_i := 1$
$ind := 0$

Hívás:

$ind := 0$
repeat
    ISMÉTLÉSES-VARIÁCIÓ$_1$ (V, n, k, ind)
    if $ind = 1$
      ÍRD $V_1, V_2, \ldots, V_k$
until $ind = 0$

Példa. Ha $n = 2, k = 4$ akkor az eredmény:

```
1 1 1 1    1 1 1 2    1 1 2 1    1 1 2 2
1 2 1 1    1 2 1 2    1 2 2 1    1 2 2 2
2 1 1 1    2 1 1 2    2 1 2 1    2 1 2 2
2 2 1 1    2 2 1 2    2 2 2 1    2 2 2 2
```

2. módszer

Ez a módszer rekurzívan oldja meg a feladatot. Minden esetben, amikor elhelyez egy elemet az *i*-edik helyre, rekurzívan meghívja önmagát, és a következő helyre sorra elhelyezi mind az összes *n* elemet.

ISMÉTLÉSES-VARIÁCIÓ$_2$ (V,i)
if $i \leq k$
  then for $j = 1,2,\ldots,n$
        do $v_i := j$
          ISMÉTLÉSES-VARIÁCIÓ$_2$ $(V,i+1)$
  else ÍRD $V_1,V_2,\ldots,V_k$

Hívás:

ISMÉTLÉSES-VARIÁCIÓ$_2$ $(V,1)$

2.6. Ismétléses permutációk generálása

Ha egy permutációban az elemek ismétlődhetnek, akkor ismétléses permutációról beszélünk. Ha k elemet akarunk úgy permutálni, hogy az első n_1-szer ismétlődik, a második n_2-ször, és így tovább, a k-adik pedig n_k-szor, akkor az összes lehetséges ilyen permutáció jele $P_{n_1,n_2,\ldots,n_k}$. Ha az ismétlődő elemeket különbözőeknek vennénk, akkor nyilván $(n_1+n_2+\cdots+n_k)!$ lehetőségünk lenne, az ismétlések miatt ezt a számot osztanunk kell $n_1!n_2!\cdots n_k!$ szorzattal. Tehát

$$P_{n_1,n_2,\ldots,n_k} = \frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}$$

Könnyű észrevenni, hogy ez még így is írható:

$$P_{n_1,n_2,\ldots,n_k} = \binom{n_1+n_2+\cdots+n_k}{n_1}\binom{n_2+n_3+\cdots+n_k}{n_2}\cdots\binom{n_{k-1}+n_k}{n_{k-1}}\binom{n_k}{n_k}$$

Ez az utóbbi képlet sugalmazza a generálási megoldást. Először generáljuk az $\binom{n_1+n_2+\cdots+n_k}{n_1}$ kombinációkat, és minden kombináció esetében a megfelelő helyekre (a kombináció elemei az indexek) helyezzük az első elemet (amely n_1-szer ismétlődik). A megmaradt helyekkel ugyanígy járunk el. Az utolsó elemet már csupán a megmaradt n_k helyre lehet helyezni.

Például, ha $n_1 = 2$, $n_2 = 1$, $n_3 = 1$, akkor az eredmény a következő:

```
1123   1213   1321   2113   2131   2311
1132   1312   1231   3112   3121   3211
```

A 4 elemű 2-adrendű kombinációk: `12, 13, 14, 23, 24, 34`. Az első kombináció `12`, ezért kerül az első két helyre `1`, majd a megmaradt helyekre két lehetőség marad (2 elem elsőrendű kombinációja) a `2` számára, így a `3` három már csak a megmaradt helyre kerülhet (első oszlop). A többi esetnek szintén egy-egy oszlop felel meg.

Az alábbi algoritmusban V-ben őrizzük a generált kombinációkat, W-ben a ismétléses kombinációkat, $s = n_1 + n_2 + \cdots + n_k$, i jelenti az i-edik kombinációt a fenti képletből. A KOMBINÁCIÓ a kombinációk generálásánál leírt eljárás.

```
ISMÉTLÉSES-PERMUTÁCIÓ (V,W,s,i)
if i = 1
  then for l := 1,2,...m
          do W_l := 0
if n ≠ 0
  then ind := 0
       repeat
              KOMBINÁCIÓ (V,s,n_i,ind)
              if ind = 1
                then BETESZ (W)
                     ISMÉTLÉSES-PERMUTÁCIÓ (V,W,s−n_i,i+1)
                     KIVESZ (W)
       until ind = 0
  else BETESZ (W)
       ÍRD W_1,W_2,...,W_n
       for l := 1,2,...,n
          do W_l := 0
```

A következő eljárás (amelyben W bemeneti és kimeneti paraméter) beteszi az n_i elemű, éppen generált kombináció adta helyekre az i értéket (a W első n_i nulla értékű komponensébe). A **break** utasítás az aktuális ciklusutasításból való kilépést jelenti.

```
BETESZ (W)
j := 0
l := 1
for p := 1,2,...,n_i
    do while l ≤ n
          do if W_l = 0
               then j := j+1
             if j = V_p
```

then $W_l := i$
break
$l := l + 1$

A következő eljárás (amelyben W bemeneti és kimeneti paraméter) törli W-ből az i értékű elemeket.

KIVESZ (W)
for $l := 1,2,\ldots,n$
do if $W_l = i$
then $W_l := 0$

Hívás:

$s := n_1 + n_2 + \cdots + n_k$
ISMÉTLÉSES-PERMUTÁCIÓ $(V, W, s, 1)$

2.7. Descartes-szorzat elemeinek generálása

Az $A_i = \{1,2,\ldots,n_i\}$ ($i = 1,2,\ldots,m$) halmazok Descartes-szorzata:

$$\prod_{i=1}^{m} A_i = A_1 \times A_2 \times \cdots \times A_m = \{(a_1, a_2, \ldots, a_m) \mid a_1 \in A_1,\ a_2 \in A_2, \ldots, a_m \in A_m\}$$

A következő algoritmus ([52]) (hasonlóan az ismétléses variációk esetében) generálja a Descartes-szorzat minden elemét a $V = (v_1, v_2, \ldots, v_m)$ vektor segítségével. A kezdeti vektor $V = (1,1,\ldots,1)$. A V vektor rákövetkezője a következőképpen határozható meg: megkeressük azt a legnagyobb i indexet, amelyre $v_i < n_i$, és ha ez az index létezik, akkor a V rákövetkezője: $(v_1, v_2, \ldots, v_{i-1}, v_i + 1, 1, \ldots, 1)$. Ha ilyen i index nem létezik, akkor ez azt jelenti, hogy már minden elemet generáltunk. A következő leírásban $N = \{n_1, n_2, \ldots, n_m\}$.

DESCARTES-SZORZAT (V, m, N, ind)
if $ind = 0$
then for i:=1,2,...,m
do $v_i := 1$
$ind := 1$
exit
else for $i := m, m-1, \ldots, 1$
do if $v_i < n_i$
then $v_i := v_i + 1$
exit
else $v_i := 1$
$ind := 0$

Hívás:

```
ind := 0
repeat
    DESCARTES-SZORZAT (V,m,N,ind)
    if ind = 1
      ÍRD V_1,V_2,...,V_m
until ind = 0
```

Ha $m = 3, n_1 = 2, n_2 = 3, n_3 = 2$ a következőket kapjuk:

```
1 1 1    1 1 2    1 2 1    1 2 2    1 3 1    1 3 2
2 1 1    2 1 2    2 2 1    2 2 2    2 3 1    2 3 2
```

2.8. Adott halmaz részhalmazainak generálása

A következő algoritmus ([52]) egy adott halmaz összes részhalmazait generálja a karakterisztikus vektor segítségével. Legyen adott az $X = \{x_1, x_2, \ldots, x_n\}$ halmaz (ahol megadtuk az elemeknek egy sorrendjét is), és legyen Y az X egy részhalmaza. Az X halmaz Y részhalmazának $(c_1, c_2, \ldots, c_n)$ karakterisztikus vektorát a következőképen értelmezzük:

$$c_i = \begin{cases} 1, & \text{ha} \quad x_i \in Y \\ 0, & \text{ha} \quad x_i \notin Y \end{cases} \qquad i = 1, 2, \ldots, n$$

Minden részhalmaznak megfelel egy ilyen karakterisztikus vektor és fordítva, minden karakterisztikus vektornak megfelel egy részhalmaz.

A karakterisztikus vektorok generálása a $\underbrace{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}}_{n}$ Descartes-szorzat generálására redukálódik. Az algoritmus a következő:

```
RÉSZHALMAZ_1 (V,m,ind)
if ind = 0
  then for i:=1,2,...,m
          do v_i := 0
       ind := 1
       exit
  else for i := m,m-1,...,1
         do if v_i < 1
              then v_i := 1
                   exit
              else v_i := 0
ind := 0
```

Hívás:

```
ind := 0
repeat
    RÉSZHALMAZ1 (V,m,N,ind)
    if ind = 1
      then írd (V,m)
until ind = 0
```

Egy háromelemű halmaz esetében az eredmény a következő:

```
∅ {1}  {2}  {1,2}  {3}  {1,3}  {2,3}  {1,2,3}
```

A következő algoritmus a részhalmazokat az elemszámuk növekvő sorrendjében adja meg. A V vektort használjuk, amelynek kezdetben minden eleme 0. A $V = (v_1, v_2, \ldots, v_m)$ rákövetkezője meghatározására megkeressük azt a legnagyobb i indexet, amelyre $v_i < i$ (Ebben az esetben igazak a következők is: $v_{i+1} = i + 1, \ldots, v_{m-1} = m-1, v_m = m$). A következő V vektor pedig $(v_1, v_2 \ldots, v_{i-1}, v_i + 1, v_i + 2, \ldots v_i + m - i + 1)$ lesz. A V vektor értelmezésében eltekintünk a 0 elemektől, például: a $(0,0,1,2)$ vektor az $\{1,2\}$ részhalmazt jelenti.

```
RÉSZHALMAZ2 (V,m,ind)
if ind = 0
  then  for i:=1,2,...,m
              do v_i := 0
        ind := 1
        exit
else for i := m, m-1, ..., 1
        do if v_i < i then
              v_i := v_i + 1
              for j := i+1, i+2, ..., m
                  do v_j := v_{j-1} + 1
              exit
    else v_i := 0
ind := 0
```

Hívás:

```
ind := 0
repeat
    RÉSZHALMAZ2 (V,m,ind)
    if ind = 1
    then írd (V,m)
until ind = 0
```

Egy háromelemű halmaz esetében az eredmény:

```
∅  {1}  {2}  {3}  {1,3}  {2,3}  {1,2,3}
```

2.9. Természetes számok partíciója

Egy természetes szám partícióján (felbontásán) természetes számok összegére bontását értjük. Például az 5 a következőképpen bontható fel természetes számok összegére.

```
5
4+1
3+2
3+1+1
2+2+1
2+1+1+1
1+1+1+1+1
```

Így az 5-nek összesen 7 különböző partíciója van. Egy partícióban nem számít az elemek sorrendje. A következőkben partíciók száma érdekel bennünket.

2.9.1. Természetes szám feltétel nélküli partíciója

A következő algoritmus generálja az n természetes szám összes partícióit, egy $(v_1, v_2, \ldots, v_n)$ vektor segítségével. Az algoritmus ötlete [52], hogy kezdetben $v_n := n$ és $v_i := 0$ minden $i := 1, 2, \ldots, n-1$-re, majd megkeressük azt a legnagyobb i indexet, amelyre $v_i + 1 < v_n$, és minden $v_i, v_{i+1}, \ldots, v_{n-1}$ értéke $v_i + 1$ lesz. A v_n értékét megfelelően módosítjuk, hogy az elemek összege n legyen.

PARTÍCIÓ (V, n, ind)
if $ind = 0$
  then for $i := 1, 2, \ldots, n-1$
        do $v_i := 0$
      $v_n := n$
      $ind := 1$
      exit
$x := v_n$
for $i := n-1, n-2, \ldots, 1$
  do if $v_i + 1 < v_n$
    then $m := v_i + 1$
      for $j := i, i+1, \ldots, n-1$
        do $v_j := m$
      $v_n := x - (n-i-1)m - 1$
      exit
    else $x := x + v_i$
$ind := 0$

Hívás:

$ind := 0$
repeat
  PARTÍCIÓ (V, n, ind)
  if $ind = 1$
    then írd (V, n)
until $ind = 0$

Példa. Ha $n = 4$, akkor az algoritmus eredménye:

```
4
1 3
2 2
1 1 2
1 1 1 1
```

2.9.2. Adott természetes szám felbontása *m*-nél nem nagyobb számok összegére

Olyan partíciók érdekelnek bennünket, amelyekben minden elem legfeljebb m. Jelöljük $P(n,m)$-mel az n szám olyan partícióinak számát, amelyekben minden szám kisebb vagy egyenlő m-mel. Például: $P(5,2)$=3, a partíciók pedig: $2+2+1$, $2+1+1+1$ és $1+1+1+1+1$.

$P(n,m)$-re könnyen találhatunk rekurzív képletet. Felosztjuk a partíciókat két csoportra: egyikbe tartoznak azok, amelyekben nincsenek m-mel egyenlő számok (ezek száma $P(n,m-1)$), a másikba pedig azok, amelyekben van legalább egy m-el egyenlő szám (ezek száma $P(n-m,m)$). A rekurzív képlet a következő:

$$P(n,m) = P(n,m-1) + P(n-m,m), \quad \text{ahol} \quad n > m > 1$$

Figyelembe véve a sajátos eseteket is, a képlet a következő:

$P(n,m) = P(n,m-1) + P(n-m,m)$ ha $n > m > 1$
$P(n,m) = 1 + P(n,n-1)$ ha $1 < n \leq m$
$P(1,m) = P(n,1) = 1$

Az alábbi algoritmus (amelynek alapötlete [44]-ból való) egy $s_1, s_2, \ldots s_{ind}$ vektort használ a partíció elemeinek megőrzésére.

PARTÍCIÓ-REKURZÍVAN (n,m)
if $m = 1$ vagy $n = 1$
  then írd $\underbrace{1,1,\ldots 1}_{n}, s_1, s_2, \ldots, s_{ind}$
  else if $n \leq m$
    then írd $n, s_1, s_2, \ldots, s_{ind}$
      PARTÍCIÓ-REKURZÍVAN $(n, n-1)$
    else PARTÍCIÓ-REKURZÍVAN $(n, m-1)$
      $ind := ind + 1$, $s_{ind} := m$

PARTÍCIÓ-REKURZÍVAN $(n-m,m)$
$ind := ind - 1$

Az eljárás a következőképpen hívható meg:

$ind := 0$
PARTÍCIÓ-REKURZÍVAN (n,m)

Példa. Ha $n = 5, m = 3$, akkor a partíciók:

```
1 1 1 1 1
1 1 1 2
1 2 2
2 3
1 1 3
```

Ez az algoritmus az előbbi feladat megoldására is alkalmas (ahol a partíciók feltétel nélküliek), ha $m := n$. Például, ha $n = 4$ és $m = 4$, akkor az eredmény:

```
4
1 1 1 1
2 2
1 1 2
1 3
```

2.9.3. Adott n természetes szám felbontása m-nél nem nagyobb, egymástól különböző számok összegére

Jelöljük $Q(n,m)$-mel az n természetes szám olyan partícióinak számát, amelyekben m-nél nem nagyobb, különböző számok szerepelnek. Levezethetők a következő rekurzív összefüggések:

$$\begin{array}{ll} Q(n,m) = Q(n,m-1) + Q(n-m,m-1) & \text{ha } n > m > 1 \\ Q(n,m) = 1 + Q(n,n-1) & \text{ha } 1 < n \leq m \\ Q(1,m) = Q(n,1) = 0 & \end{array}$$

A 2.9.2. alfejezetben megadott algoritmushoz hasonlót lehet itt is írni.

Példa. Ha $n = 10$ és $m = 5$, akkor a partíciók:

```
1 4 3 2
2 5 3
1 5 4
```

2.9.4. Adott természetes szám felbontása k darab m-nél nem nagyobb számok összegére

Ha $S(n,m,k)$ jelöli az n olyan felbontásainak a számát, amelyekben k (nem feltétlenül különböző) m-nél nem nagyobb szám szerepel, akkor

$$
\begin{array}{ll}
S(n,m,k) = S(n,m-1,k) + S(n-m,m,k-1) & \text{ha } n > m > 1, k > 1 \\
S(n,m,1) = S(n,m-1,1) + 1 & \text{ha } 1 < n \leq m \\
S(1,n,k) = 1, S(n,1,k) = 0 & \\
S(n,m,1) = 1 & \text{ha } n \leq m \\
S(n,m,1) = 0 & \text{ha } n > m
\end{array}
$$

A 2.9.2. alfejezetben megadott algoritmushoz hasonlót lehet itt is írni.

Példa. Ha $n = 8, m = 4, k = 5$, akkor az eredmény:

```
1 2 2 2 1
1 3 2 1 1
1 4 1 1 1
```

2.9.5. Adott természetes szám felbontása k különböző m-nél nem nagyobb számok összegére

Ha $R(n,m,k)$ jelöli az n olyan felbontásainak a számát, amelyekben k darab, egymástól különböző m-nél nem nagyobb szám szerepel, akkor igazak a következő képletek:

$$
\begin{array}{ll}
R(n,m,k) = R(n,m-1,k) + R(n-m,m-1,k-1) & \text{ha } n > m > 1, k > 1 \\
R(n,m,1) = R(n,m-1,1) + 1 & \text{ha } 1 < n \leq m \\
R(1,n,k) = 1, R(n,1,k) = 0 & \\
R(n,m,1) = 1 & \text{ha } n \leq m \\
R(n,m,1) = 0 & \text{ha } n > m
\end{array}
$$

A 2.9.2. alfejezetben megadott algoritmushoz hasonlót lehet itt is írni.

Példa. Ha $n = 10, m = 5, k = 3$, akkor az eredmény:

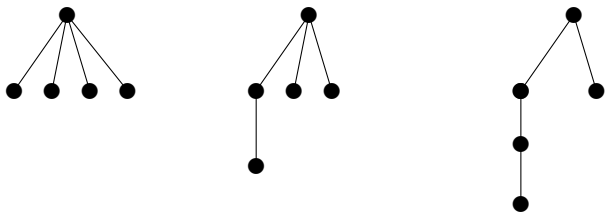
```
2 5 3
1 5 4
```

Alkalmazás. Fák felsorolása. Egy természetes szám partícióját jól lehet használni a fák felsorolásánál (leszámlálásánál). Az n csúcsú fának $n-1$ éle van, tehát a fokszámok összege $2(n-1)$ (az élek kétszerese). A $2(n-1)$ számot felbontjuk $k = n$ nem feltétlenül különböző, de $n-1$-nél nem nagyobb számok összegére. Ezek a számok jelentik a csúcsok fokszámát. Egy ilyen felbontás mindig egy fa fokszámait jelenti.

Például, fel szeretnénk sorolni az összes 5 csúcsú fát.(Cimkézetlen fákkal foglalkozunk.) Ekkor meghatározzuk a 8 felbontásait 5 darab 4-nél nem nagyobb számokra. Ezek a felbontások (amint azt már láttuk az előző alfejezetben):

```
4 1 1 1 1
3 2 1 1 1
2 2 2 1 1
```

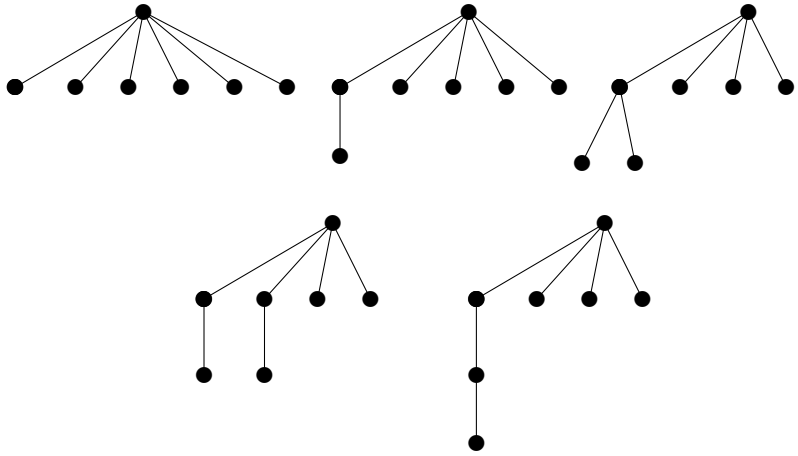
A megfelelő fák a következők:



Hasonlóképpen soroljuk fel azokat a 7 csúcsú fákat, amelyekben a legnagyobb fokszám nagyobb, mint 4. Felosztjuk 12-t 7 darab 6-nál nem nagyobb számok összegére, és kizárjuk azokat a felosztásokat, amelyekben a legnagyobb szám kisebb, mint 4. A felbontások a következők:

```
6 1 1 1 1 1 1     3 3 2 1 1 1 1
5 2 1 1 1 1 1     3 2 2 2 1 1 1
4 3 1 1 1 1 1     2 2 2 2 2 1 1
4 2 2 1 1 1 1
```

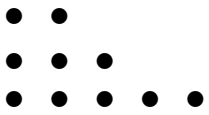
A jobboldali felbontásokat elhagyjuk, a többi négynek a következő fák felelnek meg (a 4 2 2 1 1 1 1 felbontásnak két fa felel meg):



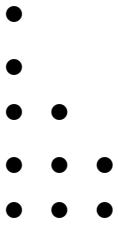
2.9.6. A Ferrers-diagramok

Egy természetes szám felbontása ábrázolható az ún. *Ferrers-diagrammal*. Ha a szám felbontásában a $\pi_1, \pi_2, \ldots, \pi_k$ számok szerepelnek úgy, hogy $\pi_1 \geq \pi_2 \geq \ldots \geq \pi_k$, akkor a Ferrers-diagram a következő pontokból áll: az első sorban π_1 pont, a második sorban π_2 pont, ..., a k-adik sorban pedig π_k pont úgy elrendezve, hogy a pontok

közti távolságok ugyanazok, ezért a diagram oszloposan is rendezett. Például az $(5,3,2)$ felbontásnak a következő diagram felel meg:



Nyilvánvaló, hogy minden felbontáshoz, amely egy adott Ferrers-diagramnak felel meg, hozzárendelhető egy másik felbontás, amely a diagram oszlop szerinti „olvasásából" következik. Így például a fenti felbontás *konjugált felbontása*: $(3,3,2,1,1)$. Ez a felbontás az előbbiből úgy adódik, hogy a sorokat oszlopokká alakítjuk.



Legyen $\pi = (\pi_1, \pi_2, \ldots, \pi_k)$ egy felbontása n-nek, azaz $n = \pi_1 + \pi_2 + \ldots + \pi_k$ és $\pi' = (\pi'_1, \pi'_2, \ldots, \pi'_m)$ a konjugált felbontása (ahol $m = \pi_1$). Értelmezzük a *felbontás súlyát* mint az elemek összegét, tehát $|\pi| = \pi_1 + \pi_2 + \ldots + \pi_k = n$. Egy π felbontás *Durfee-négyzete* a megfelelő Ferrers-diagramnak a legkisebb pontnégyzete. Ennek a négyzetnek a sorszáma megadja a *diagram átmérőjét*. A π felbontás esetében ezt az értéket $d(\pi)$-vel jelöljük. A következő konjugált diagramokban $d(\pi) = d(\pi') = 3$.

$\pi = (6,4,3,1)$ $\pi' = (4,3,3,2,1,1)$

Egy π *felbontás rangja* a következőképpen értelmezhető:

$$r(\pi) = [\pi_1 - \pi'_1, \pi_2 - \pi'_2, \ldots, \pi_{d(\pi)} - \pi'_{d(\pi)}]$$

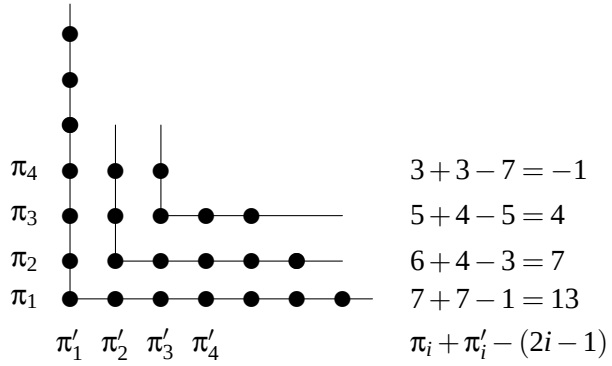
Az előbbi felbontás esetében: $r(\pi) = (2,1,0)$.
A $\pi = (\pi_1, \pi_2, \ldots, \pi_k)$ felbontás $d(\pi)$ átmérőjét a következőképpen számíthatjuk ki:

$i := 0$
while $\pi_{i+1} + \pi'_{i+1} - (2i+1) > 0$
do $i := i+1$
$d(\pi) := i$

vagy matematikai képlettel

$$d(\pi) = \max_{i=1,2,\ldots,k} \left\{ i \;\middle|\; \pi_i + \pi'_i - (2i-1) > 0 \right\}$$

Mivel a fenti algoritmusban (és képletben) π és π' szerepe felcserélhető, következik, hogy $d(\pi) = d(\pi')$.



Az azonos rangú felbontások közül *alapfelbontásnak* nevezzük azt, amelyik a lehető legkisebb súlyú.

Tekintsük az alábbi felbontásokat a konjugáltjukkal együtt:

$\pi = (5,3,3,2,1), \quad |\pi| = 14$
$\pi' = (5,4,3,1,1)$
$r_\pi = (0,-1,0)$

$\rho = (6,4,3,2,2,1), \quad |\rho| = 18$
$\rho' = (6,5,3,2,1,1)$
$r_\rho = (0,-1,0)$

$\tau = (4,4,3,1), \quad |\tau| = 12$
$\tau' = (4,3,3,2)$
$r_\tau = (0,-1,0)$

Ezek közül az utolsó az alapfelbontás.

Egy ranghoz végtelen sok felbontás rendelhető, de ezek közül csupán egy alapfelbontás. A következő tétel [60] megadja a szükséges és elégséges feltételét annak, hogy egy π felbontás, amelynek π' a konjugáltja és d az átmérője, alapfelbontás legyen.

2.1. tétel. *Egy d átmérőjű $\pi = (\pi_1, \pi_2, \ldots, \pi_k)$ felbontás akkor és csakis akkor alapfelbontás, ha a következő kijelentések igazak:*

a) $\pi_d = d$ *vagy* $\pi'_d = d$,
b) Minden $1 \le i < d$ *értékre, ha* $\pi_i > \pi_{i+1}$, *akkor* $\pi'_i = \pi'_{i+1}$.

Az előző példa esetében

$\tau = (4,4,3,1), \quad |\tau| = 12$
$\tau' = (4,3,3,2)$
$r_\tau = (0,-1,0)$
$d = 3$, $\tau_3 = \tau'_3 = 3$ és $\tau_2 > \tau_3 \Rightarrow \tau'_2 = \tau'_3 = 3$.

A következő tételhez, amely hasonlóképpen megadja a szükséges és elégséges feltételét annak, hogy egy π felbontás alapfelbontás legyen, szükségünk van a következőkre.

Egy d átmérőjű π felbontáshoz hozzárendeljük a ρ és σ felbontásokat a következőképpen:

$$\rho = (\pi_1 - d, \pi_2 - d, \ldots, \pi_d - d) \text{ şi } \sigma = (\pi'_1 - d, \pi_2 - d, \ldots, \pi'_d - d)$$

(Ezek megkaphatók a Ferrers-diagramból, miután kitöröljük a Durfee-négyzetet.) A 0 komponenseket kihagyjuk. Így minden π felbontás megadható a következőképpen: $\pi = (d, \rho, \sigma)$.

2.2. tétel. *Egy* $\pi = (d, \rho, \sigma)$ *felbontás akkor és csakis akkor alapfelbontás, ha a konjugált* ρ' *és* σ' *felbontások nem tartalmaznak közös elemeket.*

Példák.

1. $\pi = (6,4,3,2,2,1), \quad |\pi| = 18$
   $\pi' = (6,5,3,2,1,1)$
   $r_\pi = (0,-1,0)$

Ez a π felbontás nem alapfelbontás, mivel $d = 3$ és
$\rho = (3,1,0)$ azaz $\rho = (3,1)$ és $\rho' = (2,1,1)$
$\sigma = (3,2,0)$, azaz $\sigma = (3,2)$ és $\sigma' = (2,2,1)$,
és σ' és ρ' tartalmaznak közös elemeket.

2. A $\tau = (4,4,3,1)$ alapfelbontás. $\tau' = (4,3,3,2)$, $d = 3$, $\rho = (1,1)$, $\sigma = (1)$, a konjugáltak pedig: $\rho' = (2)$, $\sigma' = (1)$, amelyeknek nincs közös elemük.

2.9.7. Felbontások generátorfüggvénnyel

Egy természetes szám felbontása természetes számok összegére generátorfüggvények segítségével is megoldható. Induljunk el a következő generátorfüggvények szorzatából:

$$\frac{1}{1-z} \cdot \frac{1}{1-z^2} \cdot \frac{1}{1-z^3} \cdots \frac{1}{1-z^n}$$

$$= (1 + z + z^2 + z^3 \ldots)(1 + z^2 + z^4 + z^6 \ldots) \ldots (1 + z^n + z^{2n} + z^{3n} \ldots)$$

$$= \sum_{k_1 \ge 0} \sum_{k_2 \ge 0} \cdots \sum_{k_n \ge 0} z^{k_1 + 2k_2 + \ldots nk_n}$$

Ebben a kifejtésben z^n együtthatója éppen n felbontásainak a számát adja meg. A $k_1+2k_2+\ldots nk_n=n$ kitevő azt mutatja, hogy a felbontásban 1 k_1-szer, 2 k_2-ször és í.t. van jelen. Nyilván, ha $k_n=1$, akkor a többi k_i mind 0. Például, ha $n=3$, akkor a következő felbontások lehetségesek: 3, $1+2$, $1+1+1$ (vagyis $3=0\cdot1+0\cdot2+1\cdot3$, $3=1\cdot1+1\cdot2+0\cdot3$, $3=3\cdot1+0\cdot2+0\cdot3$).

Ha a felbontásban minden szám legfeljebb egyszer szerepel, akkor a megfelelő generátorfüggvény:

$$(1+z)(1+z^2)(1+z^3)\ldots(1+z^n).$$

Ha azt szeretnénk, hogy az n felbontásában az $n_1,n_2,\ldots n_k$ számok szerepeljenek, akkor a generátorfüggvény:

$$\frac{1}{1-z^{n_1}}\frac{1}{1-z^{n2}}\cdots\frac{1}{1-z^{n_2}}.$$

Feladatok

2.1. Írjunk algoritmust, amely adott n-re generálja az összes olyan $n\times n$-es mátrixot, amelynek elemei 0 és 1, és minden sorában és oszlopában csak egyetlen egy 1 van. (*Útmutatás.* Az 1,2, $\ldots n$ elemek egy permutációja jelentheti azon sorszámokat, ahol 1 van az illető oszlopban.)

2.2. Írjunk algoritmust, amely az n összegű pénzt az $n_1,n_2,\ldots,n_k$ címletű bankjegyekkel váltja fel. Az algoritmus adja meg az összes lehetséges felváltást. (*Útmutatás.* Ha a felváltások száma $N(n;n_1,n_2,\ldots,n_k)$, akkor $N(n;n_1,n_2,\ldots,n_k)=N(n;n_1,n_2,\ldots,n_{k-1})+N(n-n_k;n_1,n_2,\ldots,n_k)$.)

2.3. Mutassuk meg, hogy egy természetes számot ugyanannyi féleképpen lehet legfeljebb k szám összegére bontani, mint ahányféleképpen legfeljebb k nagyságú számok összegére.

2.4. Mutassuk meg, hogy egy természetes szám olyan felbontásainak a száma, amelyekben páros számú tag van, megegyezik azon felbontások számával, amelyekben minden tag páros számszor fordul elő.

2.5. Mutassuk meg, hogy egy n természetes szám ugyanannyi féleképen lehet legfeljebb k szám összegére bontani, mint ahányféleképpen lehet az $n+k$ számot pontosan k szám összegére.

2.6. Mutassuk meg, hogy egy n természetes szám ugyanannyi féleképen lehet legfeljebb k szám összegére bontani, mint ahányféleképpen lehet az $n+\dfrac{k(k+1)}{2}$ számot pontosan k, páronként különböző szám összegére.

2.7. Bizonyítsuk be, hogy egy n természetes számnak k számú pozitív egész összegére

való felbontásainak a száma (a számok sorrendje nem számít)

$$\binom{n-1}{k-1}.$$

2.8. Adottak az $a_1, a_2, \ldots, a_k$ természetes számok. Jelöljük $f(a_1, a_2, \ldots, a_k; n)$-nel az

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = n$$

megoldásainak számát a nemnegatív egész számok halmazán. Bizonyítsuk be, hogy $|t| < 1$ valós számra

$$\sum_{n=0}^{\infty} f(a_1, a_2, \ldots, a_k)t^n = \prod_{i=1}^{k} \frac{1}{1-t^{a_i}}.$$

2.9. Bizonyítsuk be, hogy az előbbi feladatban értelmezett $f(a_1, a_2, \ldots, a_k; n)$ függvényre, $(a_1, a_2, \ldots, a_k) = 1$ esetén

$$\lim_{n\to\infty} \frac{f(a_1, a_2, \ldots, a_k; n)}{\dfrac{n^{k-1}}{(k-1)!a_1a_2\cdots a_k}} = 1.$$

2.10. Tudva, hogy x és y nemnegatív egész számok határozzuk meg a következő egyenletek megoldásszámát

$$x + 3y = n$$
$$x + 4y = n$$
$$2x + 3y = n.$$

2.11. Legyen $\tau_k(n)$ az

$$n = x_1x_2\cdots x_k$$

egyenlet pozitív egész megoldásainak a száma, úgy, hogy két megoldást különbözőnek tekintünk akkor is, ha a tényezők sorrendjében különböznek. Ekkor ha $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\ell^{\alpha_\ell}$ az n prímtényezős felbontása

$$\tau_k(n) = \prod_{i=1}^{\ell} \binom{\alpha_i + k - 1}{k-1}.$$

2.12. Legyen az

$$x_1 + x_2 + \ldots + x_k = n, \quad x_1 \geq x_2 \geq \ldots \geq x_k \geq 1,$$

feltételeket kielégítő $x_1, x_2, \ldots, x_k$ szám k-asok száma $p(n)$ és legyen $p(0) = 1$. Bizonyítsuk be, hogy $|t| < 1$ esetén

$$\sum_{n=0}^{\infty} p(n)t^n = \prod_{i=1}^{\infty} \frac{1}{1-t^i}.$$

2.13. Bizonyítsuk be a következő azonosságot

$$np(n) = \sum_{k=0}^{n-1} p(k)\sigma(n-k).$$

2.14. Bizonyítsuk be, hogy

$$\lim_{n\to\infty} p(n)^{\frac{1}{n}} = 1.$$

2.15. Legyen az

$$x_1 + x_2 + \ldots + x_k = n, \quad 1 \leq x_1 \geq x_2 \geq \ldots \geq x_k \leq m,$$

feltételeket kielégítő $x_1, x_2, \ldots, x_k$ szám k-asok száma $p(n,m)$ és legyen $p(0,m) = 1$. Bizonyítsuk be, hogy $|t| < 1$ esetén

$$\sum_{n=0}^{\infty} p(n,m)t^n = \prod_{i=1}^{m} \frac{1}{1-t^i}.$$

2.16. Bizonyítsuk be, hogy

$$p(n,3) = \left|\left| \frac{(n+3)^2}{12} \right|\right|,$$

ahol $||x||$ az x-hez legközelebbi egész számot jelenti.

2.17. Bizonyítsuk be, hogy $2 \leq m \leq n$ természetes számokra

$$p(n,m) = p(n,m-1) + p(n-m,m).$$

2.18. Határozzuk meg, az összes $n, x_1, \ldots, x_n \geq 1$ természetes számokat amelyek megoldásai az

$$x_1 + x_2 + \ldots + x_n = 5n - 4$$

egyenletnek és teljesítik az

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = 1,$$

feltételt.

3.

Skatulyaelv

3.1. Skatulyaelv

A skatulyaelv legegyszerűbb megfogalmazása a következő:

Ha n adott dobozba $n+1$ golyót teszünk, valamelyikbe legalább kettő kerül. (Ha mindegyikbe legfeljebb egy jutna, akkor legfeljebb n golyó lenne.)

Egy feladat, amelyben használhatjuk a skatulyaelvet a következő:

3.1. példa. *Bizonyítsuk be, hogy minden társaságban van két olyan ember, akiknek ugyanannyi ismerősük van a jelenlevők között! (Az ismeretségek kölcsönösek.)*

Bizonyítás. Legyen a társaságban n ember. Ekkor ezek ismerőseinek a száma a következő n értéket veheti fel:

$$0, 1, 2, ..., n-2, n-1,$$

de a 0 és $n-1$ nem szerepelhet egyszerre, tehát $n-1$ különböző szám közül kell kiválasszunk n-et, így létezik közöttük két egyenlő. □

Megjegyzések

1. A feladat átfogalmazható a gráfok nyelvére és így egy gráfelméleti tételt kapunk:
Egy egyszerű gráfban van két azonos fokú csúcs.

2. A fenti bizonyítást átfogalmazva a következő számelméleti feladatoknál használható tulajdonságot kapjuk:
Adott $n+1$ természetes szám között mindig létezik kettő, amelyek n-nel osztva ugyanazt a maradékot adják.

Ha a skatulyaelv első kijelentését általánosabban fogalmazzuk meg, akkor:

Ha n tárgyat r dobozba helyezünk el, ahol $r < n$, akkor létezik legalább egy olyan doboz, amely egynél több tárgyat tartalmaz.

Függvényekre átfogalmazva:

Legyen A és B két véges halmaz úgy, hogy

$$|A| = n > r = |B|$$

és $f : A \longrightarrow B$ leképező függvény. Ekkor létezik egy olyan $b \in B$, hogy

$$\left|f^{-1}(b)\right| \geq 2$$

$\left(\left|f^{-1}(y)\right| = \{x \in A \mid f(x) = y\}\right)$.
Ennél több is igaz, nevezetesen:

3.2. tétel. *A fenti jelölésekkel:*

$$\left|f^{-1}(b)\right| \geq \left\lfloor \frac{n}{r} \right\rfloor.$$

Bizonyítás. Ha az egyenlőtlenség nem igaz, akkor

$$\left|f^{-1}(b)\right| < \left\lfloor \frac{n}{r} \right\rfloor, \qquad \forall b \in B$$

és így, mivel a B halmaznak r eleme van

$$n = \sum_{b \in B} \left|f^{-1}(b)\right| < r \cdot \frac{n}{r} = n$$

ami ellentmondás, tehát rossz a feltételezésünk, vagyis létezik $b \in B$, amelyre a kért egyenlőtlenség igaz.

□

A következőkben néhány olyan eredményt mutatunk be, amelyek bizonyításánál kulcsszerepet játszik a skatulyaelv. Először Erdős Pál és Szekeres Gábor [1] egy eredményét mutatjuk be.

3.3. tétel (Erdős-Szekeres tétel). *Adott az $a_1, a_2, ..., a_{m \cdot n+1}$, $m \cdot n + 1$ különböző valós számot tartalmazó sorozat. A sorozatnak van egy $m+1$ elemet tartalmazó növekvő részsorozata:*

$$a_{i_1} < a_{i_2} < ... < a_{i_{m+1}} \quad (i_1 < i_2 < ... < i_{m+1}),$$

vagy egy $n+1$ elemet tartalmazó csökkenő részsorozata:

$$a_{j_1} > a_{j_2} > ... > a_{j_{n+1}} \quad (j_1 < j_2 < ... < j_{n+1}),$$

vagy mindkét típusú részsorozat előfordul.

Bizonyítás. A sorozat mindenik a_i eleméhez hozzárendeljük az (x_i, y_i) elempárt úgy, hogy x_i az a_i-vel kezdődő növekvő részsor maximális hosszúsága, y_i pedig az a_i-vel kezdődő leghosszabb csökkenő sorozat hosszúsága (egy sorozat hosszúságán az elemeinek a számát értjük).

Feltételezzük, hogy a feladat állítása nem igaz, így az összes $x_i \leq m$ és az összes $y_i \leq n$. Ekkor az (x_i, y_i) számpárok

$$|\{x_i \mid 1 \leq x_i \leq m\}| \cdot |\{y_j \mid 1 \leq y_j \leq n\}| = mn$$

különböző értékeket vehetik fel.

Mivel a szorzat $mn+1$ tagot tartalmaz, létezik két olyan tag, a_i és a_j, amelyre az (x_i, y_i) és (x_j, y_j) elempárok azonosak $(x_i = x_j,\ y_i = y_j)$, de ez lehetetlen, mivel akkor a két tag megegyezik (mert ha nem, akkor az egyik benne található a másikkal kezdődő növekvő vagy csökkenő maximális hosszúságú sorozatban).

Így létezik legalább egy $m+1$ elemből álló növekvő, vagy $n+1$ tagból álló csökkenő részsorozat. □

A következőkben egy érdekes alkalmazást mutatunk be az Erdős-Szekeres tételre. Jelöljük N-nel az $\{1, 2, \ldots, n\}$ halmazt, ahol $n \geq 3$ és legyen $\pi_1, \ldots \pi_m$ m darab permutációja az N-nek.

3.4. értelmezés. *Legyen K_n azon $\{\pi_1, \ldots, \pi_m\}$ permutáció rendszerek halmaza, amelyre bármely (i, j, k) különböző számhármas esetén létezik olyan π permutáció a K_n-ből, amelyre a k az i és a j után következik. A $\{\pi_1, \ldots \pi_m\}$ rendszert a K_n* **reprezentatív rendszerének** *nevezzük.*

3.5. értelmezés. *A legkevesebb permutációt tartalmazó rendszer (K_n-ből) permutációinak száma (m) a K_n* **dimenziója**.

Példa. $\dim(K_3) = 3$. A

$$\pi_1 = (1,2,3),\ \pi_2 = (2,3,1),\ \pi_3 = (3,1,2)$$

rendszer teljesíti a feltételt és két permutációval nem érhetjük el ezt. $\dim(K_4) = 3$. Az (3.5) értelmezést teljesítő permutáció rendszer a következő:

$$\pi_1 = (1,2,3,4),\ \pi_2 = (2,4,3,1),\ \pi_3 = (1,4,3,2).$$

Megjegyzés. Könnyen bizonyíthatjuk, hogy $\dim(K_5) = 4$ és $\dim(K_n) = 4$, $5 \leq n \leq 12$, valamint $\dim(K_{13}) = 5$. Felmerül az a kérdés, hogy hogyan változik a K_n dimenziója az n függvényében? Erre ad feleletet a következő tétel.

3.6. tétel. *$n \geq 2$ esetén*

$$\dim(K_n) \geq \log_2 \log_2 n. \tag{3.1}$$

Bizonyítás. A $\dim(K_n)$ növekvő sorozat, mivel ha a K_{n+1}-ből töröljük az $n+1$-et, akkor a fennmaradt n számból álló permutációk rendszere beletartozik a K_n-be. Így

$$\dim(K_n) \leq \dim(K_{n+1}).$$

Így elégséges az (3.1) egyenlőtlenséget $n = 2^{2^\ell} + 1$-re igazolni, mivel $\lfloor \log_2 \log_2 n \rfloor = \ell$ és az egészrész a következő értéket ($\ell+1$-et) $2^{2^{\ell+1}} + 1$-re veszi fel. Feltételezzük, hogy

$$\dim(K_n) \leq \ell.$$

Legyen $N = \{1, 2, \ldots, 2^{2^l} + 1\}$ és $\{\pi_1, \pi_2, \ldots, \pi_\ell\}$ egy reprezentatív rendszere K_n-nek. Az 3.3 tétel szerint a π_1-ben van egy $2^{2^\ell} + 1$ hosszúságú monoton A_1 sorozat ($m = n = 2^{2^{\ell-1}}$), amely vagy szigorúan növekvő vagy szigorúan csökkenő.
Tekintsük most ezt az A_1 halmazt a π_2-ben. Újra alkalmazva az 3.3 tételt ($m = n = 2^{2^{\ell-2}}$) találunk egy A_2 szigorúan monoton sorozatot a π_2-ben (az A_1 elemei között), amely $2^{2^{\ell-2}} + 1$ elemet tartalmaz.

Ezt az eljárást folytatva az ℓ-edik lépésben találunk egy A_ℓ, $2^{2^0} + 1 = 3$ elemű sorozatot amely szigorúan monoton lesz az összes π_i, $i \in \{1, 2, \ldots \ell\}$ permutációban. Legyen $A_\ell = \{a, b, c\}$. A monotonitás miatt $a < b < c$, vagy $a > b > c$ mindenik permutációban, de ez ellentmond a $\{\pi_1, \pi_2, \ldots, \pi_\ell\}$ rendszer kiválasztásának, mert kellene léteznie olyan permutációnak a rendszerben, amelyben a b az a és a c után következik. Így tehát

$$\dim(K_n) \geq \ell + 1,$$

de mivel $\ell + 1$ a $\log_2 \log_2 n$ után következő legkisebb természetes szám és a $\dim(K_n)$ mindig természetes szám, azt írhatjuk, hogy

$$\dim(K_n) \geq \log_2 \log_2 n.$$

□

Megjegyzések. Erdős, Szemerédi és Trotter [1] bizonyították, hogy:

$$\lim_{n \to \infty} \frac{\dim(K_n)}{\log_2 \log_2 n + \left(\frac{1}{2} + o(1)\right) \log_2 \log_2 \log_2 n} = 1.$$

Morris és Hoşten 1998-ban [43] meghatározták a K_n pontos értékét.

A következőkben egy érdekes sorozattal, az ún. Sidon-sorozattal foglalkozunk, és olyan eredményeket mutatunk be, amelyeknél a skatulyaelvet használjuk.

3.7. értelmezés. *Természetes számok egy $a_1 < a_2 < \ldots < a_k$ sorozatát **Sidon-sorozatnak** nevezzük, ha az $a_i + a_j$ $(1 \leq i \leq j \leq k)$ számok mind különbözőek.*

Az általános feladat a következő:

3.8. feladat. *Egy adott korlátig $(a_1 < a_2 < \ldots < a_k \leq n)$ határozzuk meg a leghosszabb Sidon-sorozatot (k legnagyobb értékét).*

Egy egyszerű példa Sidon-sorozatra a 2 hatványaiból álló sorozat. de ennél sokkal sűrűbb Sidon-sorozatot is megadhatunk.

Legyen például $n = 100$. Egy Sidon-sorozat megszerkesztéséhez próbálkozhatunk a "mohó algoritmussal", amely szerint mindig kiválasztjuk a legkisebb olyan számot, amely nagyobb az előzőleg kiválasztott számoknál, és amely teljesíti az 3.7 definícióbeli tulajdonságot. Így 100-ig az

$$1,\ 2,\ 4,\ 8,\ 13,\ 21,\ 31,\ 45,\ 66,\ 81,\ 97$$

számokat kapjuk.

Felmerül a kérdés, hogy ez lesz-e a leghosszabb Sidon-sorozat 100-ig? Erre a válasz nem, mivel az

$$1,\ 3,\ 7,\ 25,\ 30,\ 41,\ 44,\ 56,\ 69,\ 76,\ 77,\ 86$$

sorozat hosszabb. Így tehát a "mohó algoritmussal" nem kapjuk meg a leghosszabb Sidon-sorozatot egy bizonyos korlátig, de bármilyen hosszú Sidon-sorozatot megszerkeszthetünk a segítségével.

3.9. értelmezés. *Jelölje $s(n)$ a leghosszabb olyan Sidon-sorozatot, amelyben a legnagyobb tag legfeljebb n.*

A fentiek szerint $s(100) \geq 12$ és meg lehet mutatni számítógép segítségével, hogy $s(100) = 12$.

Általánosan az $s(n)$ pontos értéke nem ismert, ezért a nagyságrendjét próbáljuk meghatározni a skatulya-elv felhasználásával.

A következő tulajdonság alapvető a Sidon-sorozatra vonatkozó eredmények bizonyításában:

3.10. lemma. *Egy Sidon-sorozat elemeiből képezett különbségek mind különbözőek.*

Bizonyítás. Legyen $a_1 < a_2 < \ldots < a_k$ egy Sidon-sorozat. Ha két különbség egyenlő, akkor

$$a_i - a_j = a_k - a_l, \quad (i \neq k)$$

ami azt jelenti, hogy

$$a_i + a_l = a_j + a_k,$$

de ez ellentmond a Sidon-sorozat értelmezésének. □

A skatulyaelv segítségével a következő eredményt bizonyítjuk ([50]).

3.11. tétel. *Adott n természetes számra*

$$s(n) < 2\sqrt{n}.$$

Bizonyítás. Legyen $a_1 < a_2 < \ldots < a_k$ egy olyan Sidon-sorozat, amelyben $a_k \leq n$. Azon (i, j) indexpárok száma, amelyekre $1 \leq i \leq j \leq k$

$$\binom{k}{2} + k$$

(itt $\binom{k}{2}$ a különböző $i,\ j$ számokból álló számpárok száma, míg k az $i=j$ elempárok száma). Mivel

$$2 \leq a_i + a_j \leq 2n,$$

legyenek a tárgyak az $a_i + a_j$ számok, a skatulyák pedig a lehetséges $2, \ldots, 2n$ értékek. Ha $\binom{k}{2} + k > 2n-1$ lenne, az azt jelentené, hogy a tárgyak száma nagyobb a skatulyák számánál, tehát létezne olyan doboz, amely legalább két tárgyat tartalmazna, vagyis két $a_i + a_j$ összeg azonos lenne, ami ellentmond a Sidon-sorozat értelmezésének. Így a skatulya-elv szerint ahhoz, hogy a sorozat Sidon-sorozat legyen

$$\binom{k}{2} + k \leq 2n-1.$$

Innen

$$k^2 + k + 2 \leq 4n,$$

$$k^2 < 4n, \quad k < 2\sqrt{n},$$

ami azt jelenti, hogy $s(n) < 2\sqrt{n}$. □

A fenti gondolatmenetet és az 3.10. lemmát alkalmazva jobb becslést kaphatunk.

3.12. tétel. *$n \geq 1$ természetes számra*

$$s(n) \leq \frac{\sqrt{8n-7}+1}{2}.$$

Bizonyítás. Az adott $a_1 < a_2 < \ldots < a_k$ Sidon-sorozat esetén ($s(n) = k$), az 3.10. lemma alapján az $a_i - a_j$ számok különbözőek kell legyenek, így

$$1 \leq a_j - a_i \leq n-1,\ i < j.$$

A skatulyaelv szerint

$$\binom{k}{2} \leq n-1,$$

vagy

$$(2k-1)^2 \leq 8n-7,$$

$$s(n) = k \leq \frac{\sqrt{8n-7}+1}{2}.$$

□

Megjegyzés. Ennél jobb becslés is igaz ([26]):

$$s(n) < \sqrt{n} + \sqrt[4]{n} + 1. \tag{3.2}$$

Felmerül a kérdés, hogy tudunk-e alsó korlátot adni az $s(n)$-re? Megadható egy olyan Sidon-sorozat amelyre

$$s(n) > \sqrt{n} - n^{\frac{5}{16}}. \tag{3.3}$$

Az (3.2) és (3.3)-ból következik, hogy

$$\lim_{n\to\infty} \frac{s(n)}{\sqrt{n}} = 1.$$

3.2. Logikai szita

A logikai szita formula is számlálással foglalkozik, nevezetesen bizonyos halmazok elemeinek a számára kapunk képletet. A logikai szitát nevezzük még a bennfoglalás és kizárás elvének is, ez az elnevezés jobban mutatja az elv lényegét.

A továbbiakban egy A halmaz elemeinek a számát $|A|$-val jelöljük. Adott az S véges halmaz és az $A, B \subset S$ az S részhalmazai. Az $S \setminus (A \cup B)$ elemeinek a számára érvényes a következő képlet:

$$|S \setminus (A \cup B)| = |S| - |A| - |B| + |A \cap B|.$$

A magyarázat a fenti képletre az, hogy ha az S elemeiből elvesszük az A és B elemeit, akkor az $A \cap B$ elemeit kétszer vettük el, és így egyszer még vissza is kell tegyük.
Az elvet általánosabban megfogalmazva:

3.13. tétel (Logikai szita). *Legyen S egy N elemű halmaz, $A_1, A_2, \ldots, A_k$ pedig nem szükségképpen különböző nem üres részhalmazai az S-nek. Bármely $M \subseteq \{1, 2, \ldots, k\}$ esetén legyen:*

$$\begin{aligned} N(M) &= |\{s \in S \mid s \in \bigcap_{i \in M} A_i\}| \\ N_j &= \sum_{|M|=j} N(M), \quad 0 \le j \le k. \end{aligned}$$

Azon S-beli elemek száma, amelyek egyetlen A_i-ben sem találhatók:

$$N - N_1 + N_2 - N_3 + \cdots + (-1)^k N_k.$$

Bizonyítás. Két esetet különböztetünk meg:
– ha $x \in S$ és x nem eleme egyetlen A_i-nek sem, akkor az x-et csak egyszer az N-ben számoljuk;
– ha $x \in S$ és x pontosan ℓ darab A_i halmazban található, akkor az N-ben 1-szer számoljuk, N_1-ben $\binom{\ell}{1}$-szer, N_2-ben $\binom{\ell}{2}$-szer,…,N_ℓ-ben $\binom{\ell}{\ell}$-szer. Így az x-et

$$1 - \binom{\ell}{1} + \binom{\ell}{2} - \cdots + (-1)^l \binom{\ell}{\ell} = (1-1)^\ell = 0\text{-szor}$$

számoljuk, tehát nem számoltuk az $S \setminus (\bigcup_{i=1}^{k} A_i)$ elemei közé. □

Megjegyzés A binomiális képletet használtuk

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n}y^n$$

$x = 1$ és $y = -1$-re.

A logikai szita formulát még a következő alakban is felírhatjuk:

3.14. tétel. *$A_1, A_2, \ldots, A_n$ véges nem üres halmazokra*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \ldots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|, \tag{3.4}$$

$$|\bigcap_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cup A_j| + \ldots + (-1)^{n+1} \left|\bigcup_{i=1}^{n} A_i\right|, \tag{3.5}$$

ahol

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n, \quad \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n.$$

1. bizonyítás. (Indukcióval.)
$n = 2$ esetén igaz a következő képlet:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|. \tag{3.6}$$

Feltételezzük, hogy az összefüggés fennáll $n-1$-re:

$$|\bigcup_{i=1}^{n-1} A_i| = \sum_{i=1}^{n-1} |A_i| - \sum_{1\le i<j\le n-1} |A_i \cap A_j| + \ldots + (-1)^n |\bigcap_{i=1}^{n-1} A_i|.$$

Az alábbi formula $\bigcup_{i=1}^{n} A_i = \left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n$ és az (3.6) képletet alkalmazva az indukciós feltevés alapján:

$$|\bigcup_{i=1}^{n} A_i| = \left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| =$$

$$= \sum_{i=1}^{n-1} |A_i| - \sum_{1\le i<j\le n-1} |A_i \cap A_j| + \ldots + (-1)^n \left|\bigcap_{i=1}^{n-1} A_i\right| +$$

$$+ |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| \tag{3.7}$$

Az (3.7) képletet még a következő alakban írhatjuk fel:

$$\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n),$$

amit behelyettesítve kapjuk a kért (3.4) összefüggést. Az (3.5) bizonyítása teljesen hasonlóan történik, elégséges felcserélni az $\cup$ és $\cap$ műveleteket.

□

2. bizonyítás.
A karakterisztikus függvény segítségével bizonyítunk.

A következő, könnyen ellenőrizhető képletet használjuk:

$$(1+x_1)(1+x_2)\cdot\ldots\cdot(1+x_n) = \sum_{I\subseteq\{1,2,\ldots,n\}} \left(\prod_{i\in I} x_i\right). \tag{3.8}$$

Legyen $A = A_1 \cup \ldots \cup A_n$, $f_i : A \longrightarrow \{0,1\}$ az A_i halmaz karakterisztikus függvénye $(i \in \{1,2,\ldots,n\})$:

$$f_i(a) = \begin{cases} 1, & a \in A_i \\ 0, & a \notin A_i \end{cases}.$$

Mivel az A_i halmaz nem üres halmaz,

$$\prod_{i=1}^{n}(1 - f_i(a)) = 0.$$

Az (3.8) összefüggésbe $x_i = -f_i(a)$-t helyettesítve, azt kapjuk, hogy:

$$\sum_{a\in A}\left(\sum_{I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|}\prod_{i\in I} f_i(a)\right) = 0$$

A fenti összefüggést felírva minden $a \in A$-ra és összeadva, majd az összegzést felcserélve kapjuk, hogy

$$\begin{aligned} 0 &= \sum_{a\in A}\left(\sum_{I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|}\prod_{i\in I} f_i(a)\right) \\ &= \sum_{I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|}\left(\sum_{a\in A}\prod_{i\in I} f_i(a)\right). \end{aligned} \tag{3.9}$$

Mivel a $\prod_{i\in I} f_i(a)$ a $\bigcap_{i\in I} A_i$ halmaz karakterisztikus függvénye

$$\sum_{a\in A}\prod_{i\in I} f_i(a) = |\bigcap_{i\in I} A_i|.$$

Ha $I = \emptyset$, akkor legyen $\prod_{i\in\emptyset} f_i(a) = 1$ értelmezés szerint. Innen következik, hogy

$$\sum_{a\in A}\prod_{i\in\emptyset} f_i(a) = \sum_{a\in a} 1 = |A|.$$

Így (3.9)-ből következik, hogy

$$|A| + \sum_{\emptyset\neq I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|} \left|\bigcap_{i\in I} A_i\right| = 0$$

éppen az (3.4) képlet.
Az (3.5) képletet hasonlóan bizonyíthatjuk a $\cap$ és $\cup$ felcserélésével.

□

Egyes esetekben megtörténhet, hogy legtöbb $m < n$ halmaz metszetét ismerjük, de m-nél több halmazét nem. Ekkor használhatjuk a következő Bonferoni egyenlőtlenséget.

3.15. tétel. *Adott $A_1, A_2, \ldots, A_n$ véges nem üres halmaz esetén,*
ha m páros és $m < n$

$$\sum_{i=1}^{m} |A_i| - \sum_{1\le i<j\le m} |A_i\cap A_j| + \ldots + (-1)^{m+1} \left|\bigcap_{i=1}^{m} A_i\right| \le \left|\bigcup_{i=1}^{n} A_i\right|; \tag{3.10}$$

ha pedig az m páratlan és $m < n$

$$\sum_{i=1}^{m} |A_i| - \sum_{1\le i<j\le m} |A_i\cap A_j| + \ldots + (-1)^{m+1} \left|\bigcap_{i=1}^{m} A_i\right| \ge \left|\bigcup_{i=1}^{n} A_i\right|. \tag{3.11}$$

A bizonyítás hasonló az előző tétel bizonyításához.

A következőkben néhány alkalmazást mutatunk be.

A szürjektív leképezések száma

3.16. tétel. *Adottak az $X = \{x_1, x_2, \ldots x_m\}$ és $Y = \{y_1, y_2, \ldots, y_n\}$ halmazok, ahol $n \ge m$. Jelöljük az $f : X \to Y$ szürjektív függvények számát $S(m,n)$-nel. Ekkor ezen függvények számára érvényes a következő összefüggés:*

$$\begin{aligned} S(m,n) &= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m + \ldots + (-1)^{n-1}\binom{n}{n-1} \\ &= \begin{cases} n!, & n = m \\ 0, & n > m \end{cases}. \end{aligned} \tag{3.12}$$

Bizonyítás. Legyen S az összes $f : X \to Y$ függvények száma, vagyis

$$S = \{f \mid f : X \to Y\}.$$

Legyen A_i azon függvények halmaza, amelyek egyetlen x értékre sem veszik fel az y_i értéket

$$A_i = \{f \mid f : X \to Y, y_i \notin f(X)\}.$$

Így a szürjektív függvények száma:

$$S(m,n) = |S| - |\bigcup_{i=1}^{n} A_i|.$$

A logikai szita formulát (3.13) használva azt kapjuk, hogy

$$S(m,n) = |S| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j| - \ldots + (-1)^n |\bigcap_{i=1}^{n} A_i|. \tag{3.13}$$

Könnyen belátható, hogy $|S| = n^m$, mivel mindenik X-beli elemhez akárhányszor hozzárendelhetjük az Y tetszőleges elemét. Mivel az A_i-ben az y_i-t nem használhatjuk, ezért az A_I azon függvények halmaza, amelyeknek az értékkészletében $n-1$ elem van, valamint az értelmezési tartománya m elemet tartalmaz. Ez az előbbiek szerint azt jelenti, hogy

$$|A_i| = (n-1)^m.$$

Hasonlóan az $A_i \cap A_j$-be azon függvények tartoznak, amelyek nem veszik fel az y_i valamint az y_j értékeket, tehát

$$|A_i \cap A_j| = (n-2)^m,$$

valamint általánosan

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)^m.$$

Az Y halmazból k elemet $\binom{n}{k}$ féleképpen választhatunk ki, így

$$\sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} |\bigcap_{j=1}^{k} A_{i_j}| = \binom{n}{k}(n-k)^m.$$

Behelyettesítve az (3.13)-be:

$$S(m,n) = n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m + \ldots + (-1)^{n-1}\binom{n}{n-1}$$

(Mivel $A_1 \cap A_2 \cap \ldots \cap A_n = \emptyset$, nem létezik olyan függvény, amelynek az értékkészlete egyetlen elemet sem tartalmaz, vagyis az utolsó tag hiányzik).
$m = n$ esetén a szürjektív függvények száma megegyezik az $\{1, 2, \ldots, n\}$ halmaz permutációinak a számával, vagyis $S(n,n) = n!$.
Ha pedig $m > n$, akkor nincs szürjektív függvényünk.

□

Megjegyzés. $m = n$ esetén a következőképpen néz ki a képlet:

$$\sum_{k=0}^{n-1} (-1)^k \binom{n}{k} (n-k)^n = n!. \tag{3.14}$$

Felmerül az a kérdés, hogy másképpen igazolható-e a fenti képlet?
Egy lehetséges bizonyítás, hogy tekintjük a $P(x) = x^n$ polinomot. Képezzük a

$$P(1) - P(0),\ P(2) - P(1), \ldots$$

különbségeket, amelyek tulajdonképpen a $Q_{n-1}(x) := P(x+1) - P(x)$ $n-1$-ed fokú polinom behelyettesítési értékei. Az x^{n-1}-ed fokú tag együtthatója n. Most képezzük a

$$Q_{n-1}(1) - Q_{n-1}(0),\ Q_{n-1}(2) - Q_{n-1}(1), \ldots$$

különbségeket, amelyek tulajdonképpen a $Q_{n-2}(x) := Q_{n-1}(x+1) - Q_{n-1}(x) = P(x+2) - 2P(x+1) + P(x)$ $n-2$-ed fokú polinom behelyettesítési értékei. Az x^{n-2}-ed fokú tag együtthatója $n(n-1)$.
Az eljárást tovább folytatva, a $k+1$-edik lépésben a

$$\begin{aligned} Q_{n-k}(x): &= Q_{n-k+1}(x+1) - Q_{n-k+1}(x) = \\ &= \sum_{i=0}^{k} (-1)^i \binom{k}{i} P(x+k-i) \end{aligned}$$

$n-k$-ad fokú polinomot kapjuk, amelyben az x^{n-k}-ad fokú tag együtthatója $n(n-1) \cdot \ldots \cdot (n-k+1)$.
Ha $k = n$-et választunk, akkor pontosan az (3.14) képletet kapjuk, mivel $Q_0(x)$ pontosan $n!$-sal egyenlő.

A fenti megjegyzés alapján felmerül a kérdés, hogy bizonyos kombinációs képletek bizonyítására használható-e a logikai szita? Erre adunk feleletet a következő részben.

Kombinációs formula bizonyítása

Bizonyítjuk a következő kombinációs képletet:

3.17. tétel.

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{m+n-i}{k-i} = \begin{cases} \binom{m}{k}, & m \geq k \\ \\ 0, & m < k. \end{cases}$$

Bizonyítás. Az $X = \{x_1, x_2, \ldots, x_n\}$ n elemű halmaz elemeit színezzük kékre, az Y m elemű halmaz elemeit színezzük pirosra. Legyen $Z = X \cup Y$.

Kétféleképpen fogjuk megszámolni Z azon részhalmazainak a számát, amelyek k darab piros elemet tartalmaznak.

Mivel piros elemet csak az Y halmaz tartalmaz, így egyfelől ez a szám $\binom{m}{k}$, ha $k \leq m$ és természetesen 0, ha $k > m$.

Legyen S az összes k elemű részhalmaza Z-nek, ezek száma $\binom{m+n}{k}$, valamint legyenek A_i-k azon részhalmazai a Z-nek, amelyek tartalmazzák az x_i piros elemet. Ekkor a logikai szita, (3.13) alapján a Z halmaz k darab piros elemet tartalmazó részhalmazok száma:

$$\binom{m+n}{k} - N_1 + N_2 + \ldots + (-1)^k N_k, \tag{3.15}$$

ahol N_ℓ ℓ darab A_I metszete, vagyis

$$N_\ell = \sum_{|M|=\ell} N(M) = \binom{n}{\ell}\binom{m+n-\ell}{k-\ell}.$$

Így (3.15) az igazolandó azonosság bal oldala.

□

Az Euler-féle φ függvény

Itt egy olyan alkalmazást mutatunk be, amellyel egy bizonyos számmal relatív prím természetes számok számát számoljuk ki.

3.18. értelmezés. *Legyen $N_m(x)$ az x valós számnál nem nagyobb, m-mel relatív prím természetes számok száma,*

$$N_m(x) = \sum_{\substack{k \leq x \\ (k,m)=1}} 1.$$

Bizonyítjuk a következő eredményt:

3.19. tétel. *Bármely $m \geq 1$ természetes szám, és bármely $x \geq 1$ valós szám esetén*

$$N_m(x) = \sum_{d|m} (-1)^{\omega(d)} \left\lfloor \frac{x}{d} \right\rfloor, \tag{3.16}$$

ahol $\omega(d)$ a d különböző prímosztóinak a számát jelöli.

Bizonyítás. Legyen m prímtényezős felbontása $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, ahol $p_1, p_2, \ldots, p_k$ különböző prímszámok és $\alpha_i \geq 1$, $i \in \{1, 2, \ldots k\}$. Legyen S az összes x-nél kisebb természetes számok száma

$$S = \lfloor x \rfloor.$$

Legyen A_i azon x-nél nem nagyobb természetes számok száma, amelyek oszthatók p_i-vel

$$A_i = \{k \mid k \leq x,\ p_i \mid k\}.$$

Így az x-nél nem nagyobb m-mel relatív prím természetes számok száma:

$$N_M(x) = |S| - |\bigcup_{i=1}^{n} A_i|.$$

A logikai szita formula, (3.13) alapján

$$N_m(x) = |S| - \sum_{i=1}^{n} |A_i| + \sum_{1\leq i<j\leq n} |A_i \cap A_j| - \ldots + (-1)^k |\bigcap_{i=1}^{k} A_i|. \tag{3.17}$$

Könnyen belátható, hogy

$$|A_i| = \left\lfloor \frac{x}{p_i} \right\rfloor,$$

hasonlóan az $A_i \cap A_j$-re

$$|A_i \cap A_j| = \left\lfloor \frac{x}{p_i p_j} \right\rfloor,$$

valamint általánosan

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = \left\lfloor \frac{x}{p_1 p_2 \cdots p_k} \right\rfloor.$$

Behelyettesítve az (3.17)-be:

$$\begin{aligned} N_m(x) &= \lfloor x \rfloor - \sum \left\lfloor \frac{x}{p_i} \right\rfloor + \ldots + (-1)^k \left\lfloor \frac{x}{p_1 p_2 \cdots p_k} \right\rfloor = \\ &= \sum_{d|m} (-1)^{\omega(d)} \left\lfloor \frac{x}{d} \right\rfloor. \end{aligned}$$

□

Ha bevezetjük a Möbius-féle függvényt (amellyel a későbbiekben részletesen foglalkozunk),

$$\mu(n) = \begin{cases} 1 & \text{, ha} \quad n = 1 \\ (-1)^k & \text{, ha} \quad n = p_1 \cdot p_2 \cdots p_k \\ 0 & \text{, ha} \quad \exists\, p:\ p^2 \mid n, \end{cases}$$

ahol $p_1,\ p_2, \ldots, p_k$ különböző prímszámok, akkor az 3.19 tételt még a következő alakban írhatjuk:

3.20. tétel. *Bármely $m \geq 1$ természetes szám, és bármely $x \geq 1$ valós szám esetén*

$$N_m(x) = \sum_{d|m} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor. \tag{3.18}$$

Az Euler-féle függvény sajátos esete az $N_m(x)$ függvénynek.

3.21. értelmezés. *Az **Euler-féle** φ **függvény** ($\varphi(n)$) az n-nel relatív prím, n-nél kisebb pozitív egész számok száma, vagyis*

$$\varphi(n) = \sum_{\substack{d \le n \\ (d,n)=1}} 1.$$

Az (3.18)-ban $x = m = n$-t választva kapjuk, hogy $N_m(n) = \varphi(n)$ és érvényes a következő képlet

3.22. tétel. *Adott $n \ge 1$ természetes számra:*

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{3.19}$$

Bizonyítás. Megjegyezzük, hogy ha $n = 1$, akkor a szorzat egyetlen tagot sem tartalmaz, és éppen ezért az értékét 1-nek tekintjük. Így $\varphi(1) = 1$, ami valóban igaz.
Így az (3.19)-beli szorzat a következő alakban írható fel:

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) =$$

$$= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i \cdot p_j} - \sum \frac{1}{p_i \cdot p_j \cdot p_l} + \cdots + \frac{(-1)^k}{p_1 \cdot p_2 \cdots p_k}. \tag{3.20}$$

Az (3.20)-ban az olyan $\frac{1}{d}$ tagok szerepelnek, amelyek csak prímszámok első hatványával oszthatók és előjelük pontosan $\mu(d)$. Mivel $\mu(d) = 0$, ha d osztható valamely p_i prímszám négyzetével, az (3.20) bal oldala pontosan

$$\sum_{d|n} \frac{\mu(d)}{d}.$$

Így

$$n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \sum_{d|n} \frac{\mu(d)}{d} = \varphi(n).$$

□

A következőkben a logikai szita egy általános változatát fogalmazzuk meg.

3.23. tétel. *Adott az $\mathbb{F}$ test és az S N elemű halmaz. Legyenek $E_1, E_2, \cdots, E_r$ az S nem üres részhalmazai és $W : S \longrightarrow \mathbb{F}$ egy súlyfüggvény.*

Bármely $M \subseteq \{1,2,\ldots,k\}$ esetén legyen:

$$\begin{aligned} W(M) &= \sum_{a \in \bigcap_{i \in M} E_i} w(a), \\ W_j &= \sum_{|M|=j} W(M), \quad 0 < j \leq r \\ W_0 &= \sum_{a \in S} w(a). \end{aligned}$$

Legyen $E(m)$ azon w súlyok összege, amelyek pontosan m darab E_i halmazban fordulnak elő. Ekkor

$$E(m) = \sum_{i=0}^{r-m} (-1)^i \binom{m+i}{i} W_{m+i}.$$

Bizonyítás. Két esetet különböztetünk meg:
– ha $x \in S$ és x pontosan m E_i halmaznak eleme, akkor mindkét oldalhoz $w(x)$-et kell hozzáadjunk;
– ha $x \in S$ és x pontosan $m+k$ darab E_i halmazban található , akkor a W_{m+i}-beli hozzájárulása

$$w(x)\binom{m+i}{i},$$

ami azt jelenti, hogy a jobboldali összeghez

$$w(x)\sum_{i=0}^{k}(-1)^i\binom{m+i}{i}\binom{m+k}{m+i} =$$

$$\begin{aligned} &= w(x)\sum_{i=0}^{k}(-1)^i\frac{(m+k)!}{i!m!(k-i)!} = \\ &= w(x)\binom{m+k}{k}\sum_{i=0}^{k}(-1)^i\binom{k}{i} = 0 - \text{t} \end{aligned}$$

kell hozzáadjunk. □

Ennek a tételnek egy következménye az 3.13 tétel általánosítása, amire egy érdekes bizonyítást adunk.

3.24. tétel. *Legyen S egy N elemű halmaz, A_1, A_2, …,A_k pedig nem szükségképpen különböző nem üres részhalmazai az S-nek. Bármely $M \subseteq \{1,2,\ldots,k\}$ esetén legyen:*

$$\begin{aligned} N(M) &= |\{s \in S \mid s \in \bigcap_{i \in M} A_i\}| \\ N_j &= \sum_{|M|=j} N(M), \quad 0 \leq j \leq k. \end{aligned}$$

Legyen $E(m)$ azon S-beli elemek száma, amelyek pontosan m darab A_i halmazban fordulnak elő. Ekkor

$$E(m) = \sum_{i=m}^{n} (-1)^{i-m} \binom{i}{m} N_k.$$

Bizonyítás. Mivel azt az elemet, amely pontosan r A_j-be tartozik, az N_k-ban $\binom{r}{k}$-szor számoljuk

$$N_k = \sum_{r=k} n \binom{n}{k} E_r.$$

Képezzük a következő polinomokat

$$N(x) = \sum_{k=0}^{n} N_k x^k,$$

$$E(x) = \sum_{r=0}^{n} E_r x^r.$$

Így az $M(x)$-et a binomiális tétel segítségével, a következőképpen írhatjuk fel:

$$N(x) = \sum_{k=0}^{n} \sum_{r=k}^{n} \binom{r}{k} E_r x^k = \sum_{r=0}^{n} E_r \sum_{k=0}^{r} \binom{r}{k} x^k = \sum_{r=0}^{n} E_r (x+1)^r = E(x+1).$$

Innen következik, hogy

$$\begin{aligned} E(x) &= N(x-1) = \sum_{k=0}^{n} N_k (x-1)^k = \sum_{k=0}^{n} N_k \sum_{r=0}^{k} \binom{k}{r} x^r (-1)^{k-r} = \\ &= \sum r = 0^n x^r \sum_{i=m}^{n} (-1)^{i-m} \binom{i}{m} N_k. \end{aligned}$$

Az együtthatók egyenlőségéből következik a kért formula. □

Feladatok

3.1. Egy iskolában 732 tanuló van. Bizonyítsuk be, hogy van 3 olyan tanuló, akiknek az év ugyanazon a napján van a születésnapja.

3.2. Egy matematika versenyen 40 tanuló vesz részt. Tudva, hogy 25 tanuló oldotta meg az első feladatot, 30 tanuló a másodikat, 35 tanuló a harmadikat és 33 a negyediket, bizonyítsuk be, hogy legalább 3 tanuló megoldotta mind a négy feladatot.

3.3. Legyen $a_1, a_2, ..., a_9$ az $1, 2, ..., 9$ számok egy permutációja. Bizonyítsuk be,

hogy:

$$(a_1-1)\cdot(a_2-2)\cdot\ldots\cdot(a_9-9)$$

páros szám.

3.4. a) Válasszunk ki az $1,2,3,\ldots,2n$ halmazból $n+1$ számot. Bizonyítsuk be, hogy létezik közöttük kettő, melyek relatív prímek.

b) Megadhatók-e $a_1,a_2,\ldots,a_n$ természetes számok úgy, hogy

$$1\le a_1\le a_2\le\ldots\le a_n\le 2n$$

és $1\le i\le j\le n$ esetén

$$(a_i,a_j)>1$$

legyen.

3.5. Bizonyítsuk be, hogy bármely természetes számnak van olyan többszöröse, melyet a 0 és 1 számjegyek segítségével írunk fel.

3.6. Bizonyítsuk be, hogy bármely páratlan a esetén létezik egy $b>1$ természetes szám, amelyre a

$$2^b-1$$

osztható a-val.

3.7. Legyen A az $\{1,2,\ldots,2n\}$ halmaz egy $n+1$ elemű részhalmaza $(|A|=n+1)$. Ekkor létezik két olyan szám az A-ból, amelyek közül az egyik osztója a másiknak. Igaz-e az állítás egy n elemű részhalmazra?

3.8. Bizonyítsuk be, hogy bármely $2^{k+1}-1$ egész szám közül kiválasztható 2^k darab, amelyek összege osztható n-nel.

3.9. Adott n darab 0-tól különböző természetes szám. Tudva, hogy páronként különbözőek és kisebbek mint $2n$, bizonyítsuk be, hogy vagy közöttük van az n, vagy van két olyan szám közöttük, amelyek összege $2n$.

3.10. Bizonyítsuk be, hogy $n+1$ darab $2n$-nél nem nagyobb és 0-val nem egyenlő, páronként különböző természetes szám közül kiválasztható 3 úgy (nem kötelező hogy különbözőek legyenek), hogy 2 összege egyenlő legyen a harmadik számmal.

3.11. Adott az $A=\{a_1,a_2,\ldots,a_n\}$ egész számokból álló halmaz. Bizonyítsuk be, hogy létezik A-nek egy nem üres részhalmaza úgy, hogy elemeinek összege osztható n-nel.

3.12. Adott a következő, p egyenletet és $q=2\cdot p$ ismeretlent tartalmazó egyenletrendszer

$$\begin{cases} a_{11}\cdot x_1+a_{12}\cdot x_2+\ldots+a_{1q}\cdot x_q=0\\ a_{21}\cdot x_1+a_{22}\cdot x_2+\ldots+a_{2q}\cdot x_q=0\\ \ldots\\ a_{p1}\cdot x_1+a_{p2}\cdot x2+\ldots+a_{pq}\cdot x_q=0 \end{cases}$$

ahol az a_{ij} a $\{-1,0,1\}$ halmaz elemeinek egyike. Bizonyítsuk be, hogy az egyenletrendszernek van olyan $x_1, x_2, ..., x_q$ megoldása, amely a következő tulajdonságokkal rendelkezik:
a) az x_i-k egészek
b) nem minden x_i szám 0
c) minden x_i-re $|x_i| \leq p$.

3.13. Bizonyítsuk be, hogy a fixpont nélküli n-ed rendű permutációk száma

$$D_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}.$$

3.14. Bizonyítsuk be, hogy a fixpont nélküli n-ed rendű permutációk számára érvényesek a következő rekurzív összefüggések:

$$D_n = n! - nD_{n-1} - \binom{n}{2} D_{n-2} - \ldots - \binom{n}{n-1} D_1 - 1,$$

$$D_n = (n-1)\big(D_{n-1} + D_{n-2}\big).$$

3.15. Legyen a páros fixpont nélküli n-ed rendű permutációk száma $E(n)$ és a páratlan fixpont nélküli n-ed rendű permutációk száma $O(n)$. Bizonyítsuk be, hogy

$$E(n) - O(n) = (-1)^{n-1}(n-1).$$

3.16. Legyen D_n egy n elemű halmaz fixpont nélküli permutációinak a száma és legyen G_n a pontosan egy fixponttal rendelkező permutációk száma. Bizonyítsuk be, hogy $|D_n - G_n| = 1$.

3.17. Legyen S_n az n-ed rendű permutációk halmaza. Ha $\pi \in S_n$ akkor $\sigma(\pi) = 1$ ha π páros permutáció és $\sigma(\pi) = -1$ ha π páratlan permutáció. Legyen $v(\pi)$ a π permutáció fixpontjainak a száma. Bizonyítsuk be, hogy

$$\sum_{\pi \in S_n} \frac{\sigma(\pi)}{v(\pi)+1} = (-1)^{n+1} \frac{n}{n+1}.$$

3.18. Egy 8×8-as sakktábla minden mezőjén búzaszemek vannak. Egz lépésben kiválasztunk egy olyan sort, amelynek minden mezőjén van búzaszem, és a sor minden mezőjéről elveszünk egy-egy búzaszemet, vagy egy tetszőlegesen kiválasztott oszlop minden egyes mezőjén megkétszerezzük a búzaszemek számát. Elérhető-e mindig,

hogy véges sok lépés után egyetlen búzaszem se maradjon a sakktáblán?

3.19. Egy táblára felírtuk a természetes számokat 1-től $4n$-ig, ahol $n \geq 1$ páratlan természetes szám. Egy lépésben a táblán levő számok közül letörlünk egy a és egy b számot, és helyettük vagy az $a - 3b$ vagy a $b - 3a$ különbséget írjuk. Lehetséges-e, hogy néhány lépés után a táblán szereplő összes szám 0 legyen?

3.20. Három urnánk van, és mindegyikben néhány golyó. Ha az A urnában legalább annyi golyó van, mint a B urnában, akkor a B urna tartalmát megduplázhatjuk az A-ból kivett golyókkal, és ez a lépés bármely két urna között elvégezhető. Bizonyítsuk be, hogy ilyen lépések sorozatával a három urna valamelyike kiüríthető.

4.

Szókombinatorika

4.1. Fibonacci-reprezentáció

Leonardo Fibonacci 1202-ben vezette be ezt a számsorozatot, majd a matematikusok egyre több érdekes összefüggést fedeztek fel velük kapcsolatban.

A Fibonacci-sorozat értelmezése:

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2}, \qquad \forall n \geq 2 \end{aligned} \tag{4.1}$$

A sorozat néhány tagja:

n	0	1	2	3	4	5	6	7	8	9	10
f_n	0	1	1	2	3	5	8	13	21	34	55

Megjegyzés.
A Fibonacci-számok gyakran fordulnak elő a természetben:
1.
Egy tipikus napraforgó tányérján például a szorosan egymás mellett levő kis virágok spirálisokban rendeződnek el, amelyek általában 34 teljes „körből” állnak az egyik, 55-ből a másik forgási irányban. Kisebb tányérok esetén ez a szám 21 és 34, vagy 13 és 21. Egyszer Angliában kiállítottak egy gigantikus méretű napraforgót, amelyben 89 és 144 spirális volt. Ezek mind Fibonacci-számok.
2.
Hasonló elrendezés figyelhető meg a fenyőtobozokon is.

3. Helyezzünk két üvegtáblát egymásra. Hányféle módon haladhat át, vagy

verődhet vissza egy fénysugár, ha közben pontosan n-szer változtat irányt? A megoldás a Fibonacci-sorozat.

A Fibonacci-sorozat a következő tulajdonságokkal rendelkezik ([8]):

1.

$$f_n = \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right], \tag{4.2}$$

Ez a Fibonacci-sorozat zárt alakja, és Binét-formulának is nevezik.

2.
Igazolható, hogy

$$\lim_{k \to \infty} \frac{f_{k+1}}{f_k} = \frac{1+\sqrt{5}}{2} = \phi,$$

ami pontosan az **aranymetszési állandó.**
3.
Az

$$f_n = \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

képlet egyik érdekes következménye, hogy az f_n elég nagy n természetes szám esetén közel van a

$$\frac{\phi^n}{\sqrt{5}}$$

irracionális számhoz.
Például $f_{10} = 55$ és $f_{11} = 89$, nagyon közel vannak a

$$\frac{\phi^{10}}{\sqrt{5}} \approx 55.00364$$
$$\frac{\phi^{11}}{\sqrt{5}} \approx 88.99775$$

számokhoz.

4.
A fentiekből és a

$$\left| \frac{\left(\frac{1-\sqrt{5}}{2} \right)^n}{\sqrt{5}} \right| < \frac{1}{2}$$

egyenlőtlenségből következik, hogy

$$f_n = \left\lfloor \frac{\phi^n}{\sqrt{5}} + \frac{1}{2} \right\rfloor.$$

Ha n páros, akkor f_n egy kicsit kisebb, mint $\frac{\phi^n}{\sqrt{5}}$, ha pedig n páratlan, akkor egy kicsit nagyobb.

5.

$$f_{n+1} = \phi \cdot f_n + \phi^n$$

A következő tétel a Fibonacci-számok egy fontos tulajdonságát mutatja be.

4.1. tétel. *(Zeckendorf tétele) Bármely, $n \geq 1$ természetes szám egyértelműen írható fel nem egymásutáni Fibonacci-számok összegeként:*

$$\exists\, k \geq 1,\ m_1 \gg m_2 \gg \ldots \gg m_k \geq 2,$$

$$n = f_{m_1} + f_{m_2} + \ldots + f_{m_k},$$

ahol $m \gg n$ azt jelenti, hogy $m - n \geq 2$.

Bizonyítás. Indukcióval bizonyítunk. n kis értékeire a következő egyértelmű felírások vannak:

$$\begin{aligned} 1 &= f_2 \\ 2 &= f_3 \\ 3 &= f_4 \\ 4 &= f_4 + f_2 \\ 5 &= f_5 \\ 6 &= f_5 + f_2 \end{aligned}$$

Feltételezzük, hogy minden $\ell < n$ természetes szám egyértelműen felírható Fibonacci-számok összegeként a tétel feltételeinek megfelelően, és bizonyítjuk, hogy az n természetes számra is igaz lesz az állítás.
Az n természetes számra létezik olyan m index, hogy

$$f_m \leq n < f_{m+1}.$$

Ekkor az indukciós feltevés alapján egyetlen olyan $m_1, m_2, \ldots m_k$ sorozat létezik, amelyre

$$m_1 \gg m_2 \gg \ldots \gg m_k \geq 2,$$

és

$$n - f_m = f_{m_1} + f_{m_2} + \ldots + f_{m_k},$$

vagy

$$n = f_m + f_{m_1} + f_{m_2} + \ldots + f_{m_k}.$$

Igazolnunk kell, hogy $m \gg m_1$. Mivel $f_m \leq n < f_{m+1}$, következik, hogy

$$n - f_m < f_{m+1} - f_m = f_{m-1},$$

ami azt jelenti, hogy $m_1 < m-1$, $m_1 - 2 \leq m$, vagy másképpen $m \gg m_1$. Az $m_1, m_2, \ldots m_k$ sorozat egyértelműsége miatt az m is egyértelműen van meghatározva, ami az n egyértelmű felírását jelenti.

□

Megjegyzés.
1. A felírást a „mohó" algoritmus segítségével kaphatjuk meg úgy, hogy mindig keressük a számnál kisebb, legközelebbi Fibonacci-számot. Például $n = 50$ esetén a legközelebbi Fibonacci-szám a 34, $50 - 34 = 16$, a 16-hoz legközelebbi a 13, $16 - 13 = 3$, ami Fibonacci-szám. Így

$$50 = 34 + 13 + 3 = f_9 + f_7 + f_4.$$

Ez az észrevétel program írás esetén is nagyon hasznos.
2. Ha nem kérjük, hogy a Fibonacci-számok ne legyenek egymásutániak, akkor a különböző Fibonacci-számok segítségével történő felírás nem lesz egyértelmű. Például az $n = 50$ esetén

$$\begin{aligned} 50 &= f_9 + f_7 + f_4 = \\ &= f_9 + f_7 + f_3 + f_2 = \\ &= f_9 + f_6 + f_5 + f_4 = \\ &= f_9 + f_6 + f_5 + f_3 + f_2 = \\ &= f_8 + f_7 + f_6 + f_5 + f_4 = \\ &= f_8 + f_7 + f_6 + f_5 + f_3 + f_2. \end{aligned}$$

Ezek alapján bevezethetjük a következő értelmezést.

4.2. értelmezés. *Ha tekintünk egy w, 0-ból és 1-ből álló sorozatot (szót):*

$$w = w_1 w_2 \ldots w_k,\ w_i \in \{0,1\}$$

és hozzárendeljük az n_w természetes számot

$$w \to n_w = w_1 f_{k+1} + w_2 f_k + \ldots + w_k f_2,$$

akkor a w-t az n_w ***Fibonacci-reprezentációjának*** *nevezzük.*

4.3. értelmezés. *Az n természetes szám Zeckendorf-tételbeli felírásának megfelelő w szót* ***Zeckendorf-féle reprezentációnak*** *nevezzük.*

A Zeckendorf-féle reprezentációt $< n >$-nel jelöljük.
Megjegyzések.
1. A Zeckendorf-féle felírásban nem szerepel két egymásutáni 1-es, mivel Fibonacci számok indexei legalább 2-vel különböznek egymástól.

2. A Zeckendorf-reprezentációból úgy kapunk különböző Fibonacci-reprezentációt, hogy minden 100 helyett 011-et írunk:

$$100 \to 011.$$

Például $n = 50$ esetén

$$\begin{aligned} < 50 > \;\; = \;\; & 10100\underline{100} \\ & 10\underline{100}011 \\ & 10011\underline{100} \\ & \underline{100}11011 \\ & 1111\underline{100} \\ & 1111011 \end{aligned}$$

3. Mivel minden n természetes számra létezik olyan k természetes szám, hogy $f_k \leq n < f_{k+1}$, következik, hogy a két különböző Fibonacci reprezentáció esetén az egyikben csak egy számjeggyel lehet több vagy kevesebb.
Felmerül az a kérdés, hogy hányféleképpen írható fel egy n természetes szám különböző Fibonacci-számok összegeként?

A következőkben erre próbálunk feleletet adni. Először bevezetjük a következő függvényeket.

4.4. értelmezés. *Legyen $R(n)$ az n különböző Fibonacci-számok összegeként való felírásainak a száma (vagy a különböző Fibonacci-reprezentációk száma); $G(n)$ az n különböző Fibonacci-számok „hosszú” összegeként való felírásainak a száma (a Zeckendorf-reprezentációval azonos számú számjegyet tartalmazó különböző Fibonacci-reprezentációk száma) és $P(n)$ az n különböző Fibonacci-számok „rövid” összegeként való felírásainak a száma (vagy a Zeckendorf-reprezentációnál kevesebb számjegyet tartalmazó különböző Fibonacci-reprezentációk száma).*

Például

$$G(50) = 4;\ P(50) = 2$$

$$R(50) = G(50) + P(50) = 6.$$

Általánosan is érvényes, hogy

$$R(n) = G(n) + P(n).$$

Ha egy szám Fibonacci-reprezentációjában nem találunk 100-at, akkor azt jelenti, hogy egyetlen reprezentációja van, nevezetesen a Zeckendorf-féle reprezentáció, vagyis érvényes a következő eredmény.

4.5. lemma.

$$R(n) = 1 \Longleftrightarrow n = f_k - 1,\ k \geq 3,$$

vagy

$$< n >= 1010\ldots10.$$

Mivel egy Fibonacci-szám Zeckendorf-féle reprezentációja

$$f_d = 1\underbrace{00\ldots00}_{d},$$

mindig csak egy 100 kombináció található a felírásban, és ezt sorban cserélve kapjuk a következő eredményt.

4.6. lemma.

$$R(f_d) = 1 + \left\lfloor \frac{d}{2} \right\rfloor,$$

$$G(f_d) = 1,\ P(f_d) = \left\lfloor \frac{d}{2} \right\rfloor.$$

Ha az n Zeckendorf tétele szerinti felírása

$$n = f_{m_1} + f_{m_2} + \ldots + f_{m_k},$$

akkor az n Zeckendorf-féle reprezentációját még a következőképpen is írhatjuk:

$$< n >= 10^{d_1}10^{d_2}\cdots10^{d_k},$$

ahol

$$d_i = m_i - m_{i+1} - 1,\ d_k = m_k.$$

Például:

$$< 50 >= 10100100 = 10^1 10^2 10^2.$$

Legyen

$$M(d) = \begin{pmatrix} 1 & 1 \\ \lfloor \frac{d}{2} \rfloor & \lceil \frac{d}{2} \rceil \end{pmatrix}.$$

Sajátos esetben

$$M(0) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ M(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Most kijelentjük J. Berstel eredményét az $R(n)$-re vonatkozóan (lásd [11], [24]).

4.7. tétel. *(J. Berstel, 2001) Ha az n Zeckendorf reprezentációja*

$$< n >= 10^{d_1}10^{d_2}\cdots10^{d_k},$$

akkor

$$R(n) = (1\ \ 1)M(d_1)M(d_2)\cdot\ldots\cdot M(d_k)\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Példa.

$$< 50 >= 10^1 10^2 10^2$$

$$\begin{aligned} R(50) &= (1\ 1)M(1)M(2)M(2)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \\ &= (1\ 1)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \\ &= 6 \end{aligned}$$

4.2. Véges szavak

Legyen A egy véges, nem üres halmaz, amelyet *ábécének* nevezünk. Elemei *betűk* vagy *szimbólumok*. Az A ábécé betűiből képzett $a_1a_2\ldots a_n$ sorozatot *szónak* nevezzük. Az $u = a_1a_2\ldots a_n$ szó hossza n, jelölése $|u|$. Azt a szót, amely egyetlen betűt sem tartalmaz, üres szónak nevezzük, és ε-nal jelöljük (néha λ-val). Az A ábécé betűiből képezhető összes véges szó halmazának jelölése: A^*. Használjuk még a következő jelöléseket is:

$$A^+ = A^* \setminus \{\varepsilon\}, \qquad A^n = \Big\{u \in A^* \;\Big|\; |u| = n\Big\} = \Big\{a_1a_2\ldots a_n \mid a_i \in A\Big\},$$

azaz A^+ az A fölötti összes véges és nem üres szavak halmaza, míg A^n az n hosszúságú szavak halmaza. Nyilván $A^0 = \{\varepsilon\}$.

Az A^* halmazban bevezetjük a *konkatenáció* vagy *szorzat* műveletet. Ha $u = a_1a_2\ldots a_n$ és $v = b_1b_2\ldots b_m$, akkor

$$w = uv = a_1a_2\ldots a_nb_1b_2\ldots b_m, \qquad |w| = |u| + |v|.$$

Ez a művelet asszociatív, de nem kommutatív. Semleges eleme az üres szó: $\varepsilon u = u\varepsilon = u$. Az A^* halmaz ezzel a művelettel monoid. Felhasználva a szorzatot, egy u szó hatványát a következőképpen értelmezzük:

- $u^0 = \varepsilon$
- $u^n = u^{n-1}u$, ha $n \geq 1$.

Egy szó *primitív*, ha nem hatványa egyetlen szónak sem, azaz u primitív, ha

$$u = v^n,\ v \neq \varepsilon \quad \Rightarrow \quad n = 1.$$

Az $u = abcab$ szó primitív, míg a $v = abcabc = (abc)^2$ nem az.

Két u és v szó egymás *konjugáltjai*, ha léteznek a p és q szavak úgy, hogy $u = pq$ és $v = qp$. Ebben az esetben az u megkapható v-ből cirkuláris permutációval. A konjugálás nyilvánvalóan ekvivalencia reláció. Az $u = abcda$ és $v = cdaab$ szavak konjugáltak.

Az $u = a_1a_2\ldots a_n$ szó *periodikus,* ha létezik $p \geq 1$ úgy, hogy

$$a_i = a_{i+p}, \text{ minden } i = 1,2\ldots n-p \text{ értékre.}$$

p a szó periódusa. A legkisebb ilyen tulajdonságú p-t a szó *legkisebb periódusának* nevezzük. Az $u = abcabca$ szó periodikus, és legkisebb periódusa $p = 3$.

Jelöljük az a és b számok legnagyobb közös osztóját a szokásos módon (a,b)-vel. A következő állítás nyilvánvaló.

4.8. állítás. *Ha u periodikus és p és q is periódusa, akkor* (p,q) *is periódusa.*

Bevezetjük a *tükrözés* műveletet. Ha $u = a_1a_2\ldots a_n$, akkor $u^R = a_na_{n-1}\ldots a_1$, azaz u^R az u szó *tükörképe.* Nyilván $\left(u^R\right)^R = u$. Ha $u = u^R$, akkor az u *palindromszó.*

Az A^* és az A^+ halmazok megszámlálhatóan végtelenek. Az A^* szavai (és A^+ szavai is) sorba rendezhetők például a hosszúságuk szerint, azon belül pedig ábécé-sorrendbe, ha A betűi között is van sorrend.

Az u szó *részszava* a v szónak, ha léteznek a p és q szavak úgy, hogy $v = puq$. Ha $pq \neq \varepsilon$, akkor az u valódi részszava v-nek. Ha $p = \varepsilon$, akkor u *kezdőszelete* vagy *prefixuma* v-nek, ha pedig $q = \varepsilon$, akkor u *végszelete* vagy *szuffixuma* v-nek. Az u szó n hosszúságú részszavainak halmazát $F_n(u)$ jelöli. $F(u)$ az u összes részszavainak a halmaza. Tehát

$$F(u) = \bigcup_{n=1}^{|u|} F_n(u).$$

Például, ha $u = abaab$, akkor

$F_1(u) = \{a,b\}$, $F_2(u) = \{ab,ba,aa\}$, $F_3(u) = \{aba,baa,aab\}$,
$F_4(u) = \{abaa,baab\}$, $F_5(u) = \{abaab\}$.

Az $u = a_1a_2\ldots a_m$ és $v = b_1b_2\ldots b_n$ szavak akkor egyenlőek, ha

- $m = n$ és
- $a_i = b_i$, ha $i = 1,2,\ldots,n$.

4.9. tétel (Fine–Wilf). *Adottak az n, illetve m hosszúságú u és v szavak. Ha létezik p és q úgy, hogy az* u^p *és* v^q *szavaknak van egy* $n+m-(n,m)$ *hosszúságú közös kezdőszelete, akkor u és v ugyanannak a szónak hatványai.*

Bizonyítás. A bizonyítást elég arra az esetre elvégeznünk, ha $(n,m) = 1$. Ebben az esetben mindkét szó egy betűnek a hatványa. Ha $(n,m) = d \neq 1$, akkor az A ábécé helyett A^d-t vesszük, és a bizonyítás érvényes erre az esetre is. Legyen $u = a_1a_2\ldots a_n$, $v = b_1b_2\ldots b_m$, $n < m$. Két esetet különböztetünk meg:

1) $\frac{m}{2} < n < m$
2) $n < \frac{m}{2}$.

Egyenlőség nem lehet, mivel $(m,n) = 1$.

1. eset. $\frac{m}{2} < n < m$. Ekkor a következő helyzet érvényes:

$$\begin{array}{llllllllll} x = u^p = a_1 & a_2 & \ldots & a_n & a_1 & a_2 & \ldots & a_{m-n} & a_{m-n+1}\ldots \\ y = v^q = b_1 & b_2 & \ldots & b_n & b_{n+1} & b_{n+2} & \ldots & b_m & b_1\ldots \end{array}$$

Innen

$$\begin{aligned} &a_1 = b_{n+1} = b_1 \\ &a_2 = b_{n+2} = b_2 \\ &\ldots \\ &a_{m-n} = b_{n+(m-n)} = b_m = b_{m-n}, \end{aligned}$$

tehát a $b_1b_2\ldots b_m$ szó periodikus n periódussal. Folytatva

$$\begin{aligned} &a_{m-n+1} = b_1 = b_{m-n+1} \\ &a_{m-n+2} = b_2 = b_{m-n+2} \\ &\ldots \\ &a_{m-n+(2n-m)} = b_{2n-m} = b_{m-n+(2n-m)} = b_n \end{aligned}$$

Tehát a $b_1b_2\ldots b_n$ szó periodikus $m-n$ periódussal, de $(m,n) = (m,m-n) = 1$, így a szó periódusa 1, azaz minden betű azonos. Ebben az esetben az u-nak mind az n betűje azonos, tehát a v szó betűi is, az $m+n-1$ hosszúságú közös kezdőszelet miatt.

2. eset. $n < \frac{m}{2}$. Ekkor

$$\begin{array}{llllllll} x = u^p = a_1\ldots a_n & a_1 & \ldots a_n & a_1\ldots & a_n & a_1\ldots & a_{m-ln} \\ y = v^q = b_1\ldots b_n & b_{n+1} & \ldots b_{2n} & b_{2n+1}\ldots & b_{3n} & b_{3n+1}\ldots & b_m \end{array}$$

A bizonyítás hasonló, de a második részben

$$\begin{aligned} &b_{ln+1} = a_1 = b_1 \\ &b_{ln+2} = a_2 = b_2 \\ &\ldots \\ &b_{ln+(m-ln)} = a_{m-ln} = b_m, \end{aligned}$$

tehát a $b_1b_2\ldots b_m$ szó periodikus, méghozzá $m-n$ periódussal, de $(m,ln) = (m,m-nl) = 1$, és mivel n is periódus, periódus lesz az 1 is, így minden betű azonos. □

A tételben megadott $n+m-(n,m)$ érték éles. Ezt a következő példával illusztráljuk. Itt a két szónak van $n+m-(n,m)-1$ hosszúságú közös kezdőszelete, és u és v nem hatványai ugyanannak a szónak. Legyenek

$$\begin{array}{lll} u = abaab, & m = |u| = 5, & u^2 = abaababaab \\ v = aba, & n = |v| = 3, & v^3 = abaabaaba \end{array}$$

A tétel szerint egy 7 hosszúságú közös kezdőszelet biztosítaná, hogy a két szó ugyanannak a szónak a hatványai legyenek. Látszik, hogy u^2 és v^3 szavaknak van egy 6 hosszúságú kezdőszelete: (*abaaba*), és nincs olyan x szó, hogy u és v az x-nek hatványai lennének. Tehát a közös kezdőszelet megadott hossza éles.

4.3. Végtelen szavak

A véges szavak mellett *végtelen* (pontosabban jobbról végtelen) szavakat is vizsgálunk:

$$u = u_1u_2\ldots u_n\ldots$$

Az A ábécé feletti végtelen szavak halmazát A^ω jelöli. Néha a véges és végtelen szavakat együtt vizsgáljuk, ilyenkor hasznos a következő jelölés:

$$A^\infty = A^* \cup A^\omega.$$

Ebben az esetben is értelmezzük a részszó, kezdőszelet, végszelet fogalmakat, hasonlóan a véges szavakhoz.

Legyen $u \in A^\omega$. A $v \in A^+$ szó részszava u-nak, ha léteznek a $p \in A^*$, $q \in A^\omega$ szavak úgy, hogy $u = pvq$. Ha $p \neq \varepsilon$, akkor p az u szó kezdőszelete, míg q a végszelete. Ugyanúgy $F_n(u)$ az u szó n hosszúságú részszavainak halmazát jelöli.

Példa végtelen szavakra:

1) A ***hatványszó*** értelmezése:

$$p = 010011000111\ldots\underbrace{0\ldots0}_{n}\underbrace{1\ldots1}_{n}\ldots = 010^2 1^2 0^3 1^3 \ldots 0^n 1^n \ldots$$

Látható, hogy

$F_1(p) = \{0,1\}$, $F_2(p) = \{01,10,00,11\}$,
$F_3(p) = \{010,100,001,011,110,000,111\},\ldots$

2) A véges ***Fibonacci-szavak*** a következőképpen értelmezhetők:

$f_0 = 0,\ f_1 = 01$
$f_n = f_{n-1} f_{n-2}$ ha $n \geq 2$

A következő szavakat kapjuk:

$f_0 = 1$
$f_1 = 01$
$f_2 = 010$
$f_3 = 01001$
$f_4 = 01001010$
$f_5 = 0100101001001$
$f_6 = 010010100100101001010$
$f_7 = 01001010010010100101001001010010$

A végtelen Fibonacci-szó a véges Fibonacci-szavak sorozatának határértéke:

$$f = \lim_{n\to\infty} f_n.$$

Ennek a szónak a részszavai a következők:

$F_1(f) = \{0,1\}$, $F_2(f) = \{01,10,00\}$, $F_3(f) = \{010,100,001,101\}$,
$F_4(f) = \{0100,1001,0010,0101,1010\},\ldots$

Az elnevezés onnan ered, hogy a véges Fibonacci-számok képzése és azok hossza kapcsolatba hozható a Fibonacci-számokkal: $|f_n| = F_{n+2}$, azaz az n-edik f_n Fibonacci-szó hossza egyenlő az $(n+2)$-edik Fibonacci-számmal.

A végtelen Fibonacci-szónak sok érdekes tulajdonsága van. A szó képzéséből látható, hogy nem tartalmazhat egyetlen olyan részszót sem, amelyben két 1-es lenne egymás mellett. (Mindig olyan szavakat illesztünk egymás mellé, amelyek 0-val kezdődnek).

Egy x szó 1-eseinek számát jelöljük $h(x)$-szel. Egy végtelen u szó *kiegyensúlyozott*, ha tetszőleges x és y, ugyanolyan hosszúságú részszavaira mindig fennáll $|h(x)-h(y)| \leq 1$, azaz

$$x,y \in F_n(u) \;\Rightarrow\; |h(x)-h(y)| \leq 1.$$

4.10. tétel. *Az f Fibonacci-szó kiegyensúlyozott.*

Bizonyítás. A részszavak hosszára vonatkozó teljes indukcióval bizonyítunk. Ha $n=1$, a tétel kijelentése nyilván igaz. Feltételezzük, hogy a tétel igaz bármely n-nél rövidebb részszóra.

Egy n hosszúságú részszó végződése 00, 01 vagy 10 lehet. A következő eseteket vizsgáljuk:

1) $x = u00$ és $y = v10$.
Az x részszó csupán 1-gyel folytatható, tehát $x' = u001$, az y részszó folytatható 0-val és 1-gyel is: $y' = v100$, $y'' = v101$. Ekkor

$h(x')-h(y') = h(x)+1-h(y) = h(x)-h(y)+1$, de $h(x)-h(y) \neq 1$, mivel különben $h(u)-h(v) = 2$ lenne, amely ellentmond az indukciós feltételnek. Tehát $|h(x')-h(y')| \leq 1$.

$h(x')-h(y'') = h(x)+1-h(y)-1 = h(x)-h(y)$, tehát az indukciós feltétel szerint $|h(x')-h(y'')| \leq 1$.

2) $x = u00$ és $y = v01$.
Ebben az esetben mindkét részszó egyféleképpen folytatódhat, tehát $x' = u001$, $y' = v010$. Ekkor:

$h(x')-h(y') = h(x)+1-h(y)$, de $h(x)-h(y) \neq 1$, mert különben $h(u)-h(v) = 2$, amely nem lehetséges az indukciós feltételből. Tehát $|h(x')-h(y')| \leq 1$.

3) $x = u10$ és $y = v01$.
Itt is $x' = u100$ és $x'' = u101$, míg $y' = v010$. A következő esetek lehetségesek:

$h(x')-h(y') = h(x)-h(y)$

$h(x'')-h(y') = h(x)+1-h(y)$, de ha $h(x)-h(y) = 1$, akkor $h(u1)-h(v0) = 2$, ami ellentmondás. Tehát:

$|h(x')-h(y')| \leq 1$ és $|h(x'')-h(y')| \leq 1$,
és ezzel a tétel bebizonyítottuk. □

4.11. tétel. *$F_n(f)$-nek $n+1$ eleme van.*

Bizonyítás. Láttuk az előbbi bizonyításban, hogy minden részszó 00, 01 vagy 10-ban végződik. Ezek közül azok, amelyeknek végződése 00 vagy 01, csak egyféleképpen folytathatók, míg azok, amelyek 10-ban végződnek kétféleképpen folytathatók.

Tehát $\#F_{n+1}(f) \leq \#F_n(f)+1$. Ezek a szavak mind részszavai f-nek, ezért $\#F_{n+1}(f) = \#F_n(f)+1$, ahonnan $\#F_n(f) = n+1$. □

Ha az u véges szót önmagával szorozzuk végtelenszer, akkor ennek jelölése: u^ω.

Az u végtelen szót *periodikusnak* mondjuk, ha létezik egy v véges szó úgy, hogy $u = v^\omega$. Ez a fogalom általánosítja a véges szavaknál használt periodikusságot. Az u szó *végperiodikus*, ha léteznek a v és w véges szavak, amelyekre $u = vw^\omega$.

A Fibonacci-szó generálható egy homomorfizmus segítségével. A homomorfizmus értelmezése:

$$h : A^* \to A^*, \quad h(uv) = h(u)h(v), \quad \forall u, v \in A^*.$$

Ennek alapján elegendő, ha a h függvényt csak betűkre értelmezzük. Egy homomorfizmus kiterjeszthető végtelen szavakra is a következőképpen:

$$h : A^\omega \to A^\omega, \quad h(uv) = h(u)h(v), \quad \forall u \in A^*, v \in A^\omega.$$

Az f_n Fibonacci-szót generálhatjuk a következő homomorfizmussal:

$$\sigma(0) = 01,\ \sigma(1) = 0.$$

Ebben az esetben érvényes a következő tétel.

4.12. tétel. $f_{n+1} = \sigma(f_n)$

Bizonyítás. A bizonyítást matematikai indukcióval végezzük. Nyilvánvaló, hogy $f_1 = \sigma(f_0)$. Feltételezzük, hogy $f_k = \sigma(f_{k-1})$ minden $k \leq n$ értékre. Mivel

$$f_{n+1} = f_n f_{n-1},$$

az indukciós feltevésünk szerint

$$f_{n+1} = \sigma(f_{n-1})\sigma(f_{n-2}) = \sigma(f_{n-1} f_{n-2}) = \sigma(f_n).$$

□

Innen azonnal következik egy újabb tétel.

4.13. tétel. $f_n = \sigma^n(0)$

Az f végtelen Fibonacci-szó a σ homomorfizmus fixpontja.

$$f = \sigma(f).$$

4.4. Szógráfok

Legyen $X \subseteq A^m$ az m hosszúságú szavak egy halmaza az A ábécé fölött, és $E \subseteq AX \cap XA$. Értelmezünk egy olyan irányított gráfot, amelynek csúcsai X halmazból, éleik pedig az E halmazból valók. Van él az $a_1a_2\ldots a_m$ csúcsból a $b_1b_2\ldots b_m$ csúcsba, ha

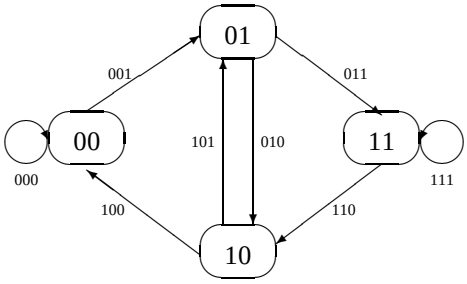
$$a_2 = b_1,\ a_3 = b_2,\ \ldots,\ a_m = b_{m-1} \text{ és } a_1a_2\ldots a_mb_m \in E,$$

azaz az első szó utolsó $m-1$ betűje azonos a második szó első $m-1$ betűjével. Ezt a élt az $a_1a_2\ldots a_mb_m$ szóval címkézzük meg (amely azonos a következővel $a_1b_1\ldots b_m$).

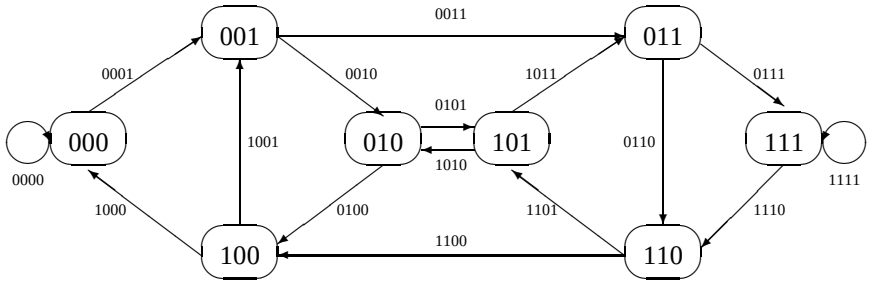
De Bruijn-gráfok

Ha $X = A^m$ és $E = A^{m+1}$, ahol $A = \{a_1, a_2, \ldots a_n\}$, akkor a gráf neve *De Bruijn-gráf*, jelölése: $B(n,m)$.

A $B(2,2)$ és $B(2,3)$ De Bruijn-gráfok a 4.1. és 4.2. ábrákon láthatók. A 4.3. ábrán a $B(3,2)$ gráfot láthatjuk.



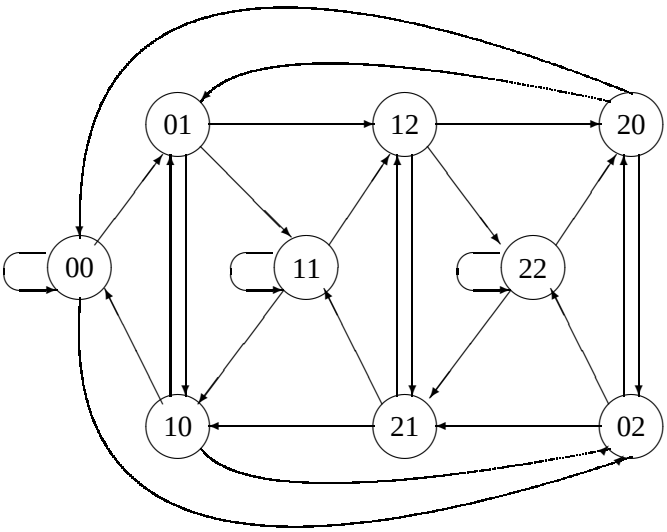
4.1. ábra. A $B(2,2)$ De Bruijn-gráf.



4.2. ábra. A $B(2,3)$ De Bruijn-gráf.

A De Bruijn-gráf egy $x_1x_2\ldots x_m,\ x_2x_3\ldots x_mx_{m+1},\ \ldots,\ z_1z_2\ldots z_m$ sétájához[1] hozzárendeljük az $x_1x_2\ldots z_{m-1}z_m$ szót, amelyet a csúcsokat jelképező szavak maximális átfedéséből kapunk. A 4.2. ábra $B(2,3)$ gráfjában a $001,011,111,110$ sétának (egyben útnak) megfelelő szó 001110. A $B(n,m)$ gráf egy Hamilton-útjának (amely a gráf minden csúcsát tartalmazza) megfelelő szót (n,m) típusú *De Bruijn-szónak* nevezzük. Például a 0001110100 és 0001011100 szavak $(2,3)$-típusú De Bruijn-szavak. Egy (n,m) típusú De Bruijn-szó tartalmazza az összes m hosszúságú szót.

Egy irányított összefüggő gráf[2] Euler-gráf,[3] ha minden csúcsába ugyanannyi él fut be, mint amennyi ki.



4.3. ábra. A $B(3,2)$ De Bruijn-gráf.

4.14. tétel. *A $B(n,m)$ de Bruijn-gráf Euler-gráf.*

Bizonyítás. a) A gráf összefüggő, mivel bármely $x_1x_2\ldots x_m$ és $z_1z_2\ldots z_m$ csúcsa között létezik irányított út. Az $x_1x_2\ldots x_m$ csúcsból n él fut ki az összes olyan szóba,

[1] Emlékeztetőül: Egy gráfban a séta egymásutáni élek sorozata: Amennyiben a séta egyetlen éle sem ismétlődik, vonalról, ha pedig egyetlen csúcsa sem, akkor útról beszélünk.

[2] Egy irányított gráf összefüggő, ha bármely két csúcsa között létezik legalább egyik irányba irányított út.

[3] Egy irányított gráf Euler-gráf, ha tartalmaz a gráf minden élén átmenő zárt irányított vonalat.

amelynek első $m-1$ betűje $x_2x_3\ldots x_m$, az utolsó pedig mind különböző. Ezért létezik az $x_1x_2\ldots x_m,\ x_2x_3\ldots x_mz_1,\ \ldots,\ x_mz_1\ldots z_{m-1},\ z_1z_2\ldots z_m$ út.

b) Az $x_1x_2\ldots x_m$ csúcsba az $yx_1\ldots x_{m-1}$ csúcsokból futnak be élek, ahol $y\in A$ (A a gráf ábécéje, azaz $X=A^m$). Az $x_1x_2\ldots x_m$ csúcsból kifutó élek végpontja $x_2x_3\ldots x_my$, ahol $y\in A$. Tehát a gráf Euler-gráf. □

Innen azonnali következő tétel:

4.15. tétel. *A $B(n,m)$-gráf egy Euler-vonalának (amely a gráf minden élét tartalmazza) megfelel ugyanabban a sorrendben a $B(n,m+1)$ gráf egy Hamilton-útja.*

Például $B(2,2)$-ben a 000, 001, 010, 101, 011, 111, 110, 100 élsorozat egy Euler-vonalnak felel meg. Ugyanakkor, ezek a szavak a $B(2,3)$-ben egy Hamilton-út csúcsai.

Algoritmus egy De Bruijn-szó generálására

A De Bruijn-szavak generálására több módszer is létezik. Ezek közül a Martin-algoritmust [56] mutatjuk be. Legyen $A=\{a_1,a_2,\ldots,a_n\}$ egy ábécé. Egy (n,m) típusú De Bruijn-szót akarunk generálni az A ábécé felett.

Az $\underbrace{a_1a_1\ldots a_1}_{m-\text{szer}}$ szóból indulunk ki, és jobbról hozzáillesztünk egy-egy betűt a következők szerint: az olyan legnagyobb indexű a_k-val folytatjuk a szót, amelyre fennáll az, hogy az utolsó m betűből alkotott részszó (beleértve az a_k-t is) még nem szerepel a szóban. Addig folytatjuk, ameddig csak lehetséges. Be lehet bizonyítani, hogy csak akkor nem lehet már folytatni, amikor minden m hosszúságú szó már szerepel pontosan egyszer a szóban. Természetesen, ekkor a szó hossza n^m+m-1. Az algoritmus leírásában A az n-betűs ábécé, b pedig az eredmény, az (n,m)-típusú De Bruijn-szó.

```
MARTIN(A,b)
for i := 1,2...m
    do b_i := a_1
i := m
repeat
    megáll := true
    k := n
    while k > 1
        do if b_{i-m+2}b_{i-m+3}...b_ia_k nem részszava b_1b_2...b_i-nek
            then i := i+1
                 b_i := a_k
                 megáll:= false
                 exit while
            else k := k-1
until megáll
```

Példa. Legyen $A=\{0,1\}$. Keresünk egy $(2,3)$ típusú De Bruijn-szót.

000-val kezdünk.
Hozzáilleszthetjük az 1-est. A kapott szó: 0001.
Hozzáilleszthetjük az 1-est. A kapott szó: 00011.
Hozzáilleszthetjük az 1-est. A kapott szó: 000111.
Most már csak a 0-t illeszthetjük, mivel 111 már szerepel (átfedéssel). A kapott szó: 0001110.
Hozzáilleszthetjük az 1-est. A kapott szó: 00011101.
Ismét csak a 0-t illeszthetjük, mert 011 már szerepel a szóban. A kapott szó: 000111010.
Ismét csak a 0-t illeszthetjük, mert 101 már szerepel (átfedéssel). A kapott szó: 0001110100. Nem lehet folyatni sem 1-gyel, sem 0-val. Tehát, a keresett szó 0001110100.

Megfigyelhető, hogy 0001011100 is ugyanolyan típusú De Bruijn-szó. Ebből a kettőből, cirkuláris permutációval, minden (2,3) típusú De Bruijn-szó megkapható.

Az algoritmus alapján kijelenthetjük a következő tételt.

4.16. tétel. *Egy (n,m) típusú De Bruijn-szó az összes m hosszúságú és n betűt tartalmazó szó közül a legrövidebb.*

Algoritmus az összes De Bruijn-szó generálására

Az összes (q,k) típusú De Bruijn-szó generálására a következő rekurzív algoritmust használjuk.

Az ábécé $a_1,a_2,\ldots,a_q$ betűi helyett vegyük az $a_i = i-1$ ($i = 1,2,\ldots,q$) értékeket, amelyek egy q-alapú számrendszer számjegyei. Az algoritmusban az $S = (S_1,S_2,\ldots)$ vektor a De Bruijn-szó betűit tartalmazza. A $B = (B_1,B_2,\ldots)$ vektor komponensei jelzik, hogy egy adott részszó szerepel már (a komponens 1), vagy még nem (a komponens 0) a De Bruijn-szóban. Az aktuális betűnek a szóhoz való illesztése után kiszámítjuk az utolsó k betűből képzett $S_{i-k}S_{i-1}\ldots S_{i-1}$ részszónak megfelelő számot (val($S_{i-k}S_{i-1}\ldots S_{i-1}$)), ha ezt r-rel jelöljük, akkor B_r-t 1-re állítjuk, amennyiben 0 volt. Kezdetben:

$S_i := 0$ ha $i = 1,2,\ldots,k$

$B_0 := 1$, és minden más i-re $B_i := 0$.

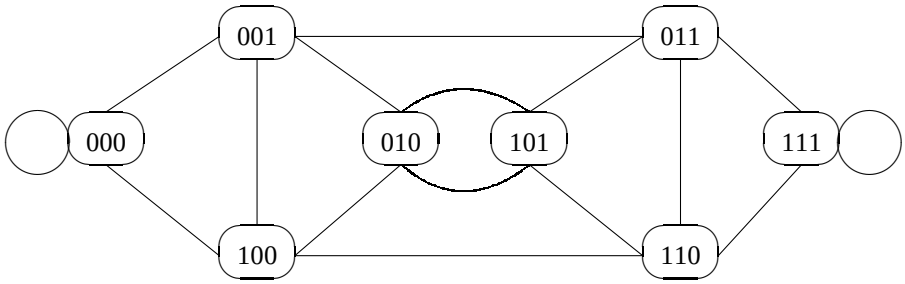
```
DEBRUIJN (S,i,k,B)
for j := 1,2,...,q
   do S_i := a_j
      r := val(S_{i-k}S_{i-1}...S_{i-1})
      if B_r = 0
        then B_r := 1
             DEBRUIJN(S,i+1,k,B)
             B_r := 0
        else if length(S) = q^k + k - 1
               then írd S
```

exit for

Az eljárás hívása:

for $i = 1,2,\ldots,k$
  do $S_i := 0$
$B_0 := 1$
for $i = 1,2,\ldots,2^k - 1$
  do $B_i := 0$
DEBRUIJN $(S, k+1, k, B)$.

Alkalmazás. Számítógép-hálózatok. A De Bruijn-gráfok nem irányított változata (4.4. ábra) jól modellezi a számítógép-hálózatokat. Ez a gráf többszörösen összefüggő, azaz minden él (a hurokélektől eltekintve) több élfüggetlen körön található, és kitörlésekor a gráf még összefüggő marad. A gráf átmérője m, azaz bármely csúcsból bármely másikba el lehet jutni egy legfeljebb m hosszúságú úton. Természetesen, hálózatok esetében a hurokéleket és többszörös (párhuzamos) éleket kihagyjuk.



4.4. ábra. A $B^*(2,3)$. nem irányított De Bruijn-gráf

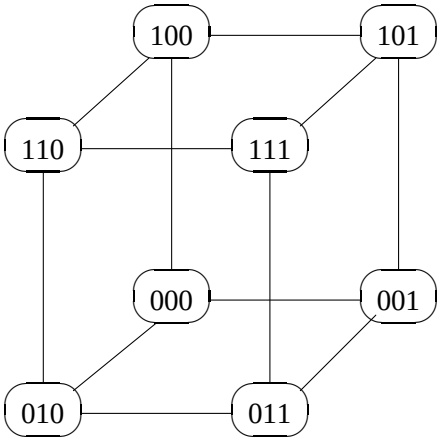
Egy másik hasznos modell a számítógép-hálózatokra a hiperkocka (4.5., 4.6. ábrák).

Rauzy-gráfok

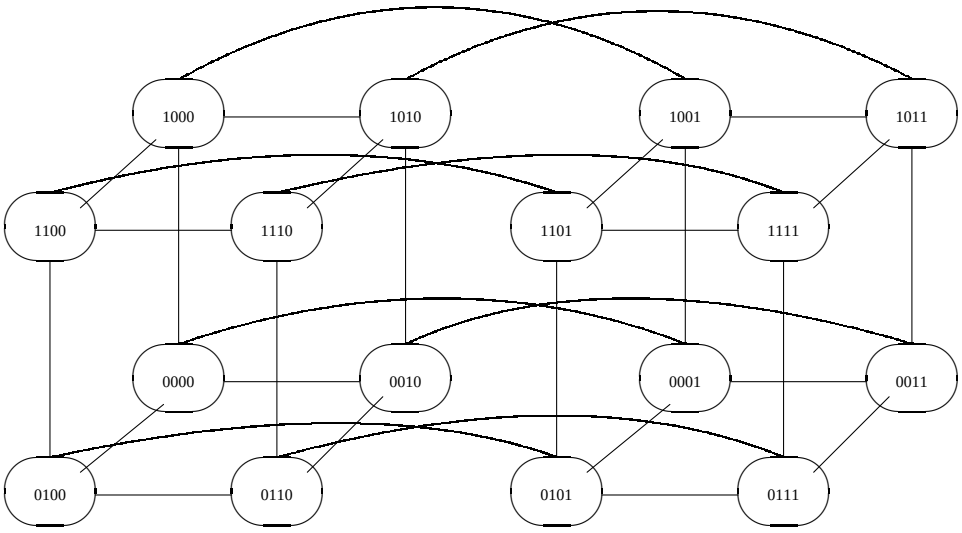
Ha az u szó végtelen, és $X = F_n(u)$, $E = F_{n+1}(u)$, akkor az ezeken értelmezett szógráf neve *Rauzy-gráf* (vagy *részszó*-gráf). A 4.7. ábrán a a Fibonacci-szó Rauzy-gráfjai láthatók $n = 1,2,3,4,5$ értékekre. Amint már láttuk, a végtelen Fibonacci-szó

$$f = 01001010010010100 1010\ldots,$$

és $F_1(f) = \{0,1\}$, $F_2(f) = \{01,10,00\}$,
$F_3(f) = \{010,100,001,101\}$, $F_4(f) = \{0100,1001,0010,0101,1010\}$,
$F_5(f) = \{01001,10010,00101,01010,10100,00100\}$.



4.5. ábra. Kocka („háromdimenziós hiperkocka”).



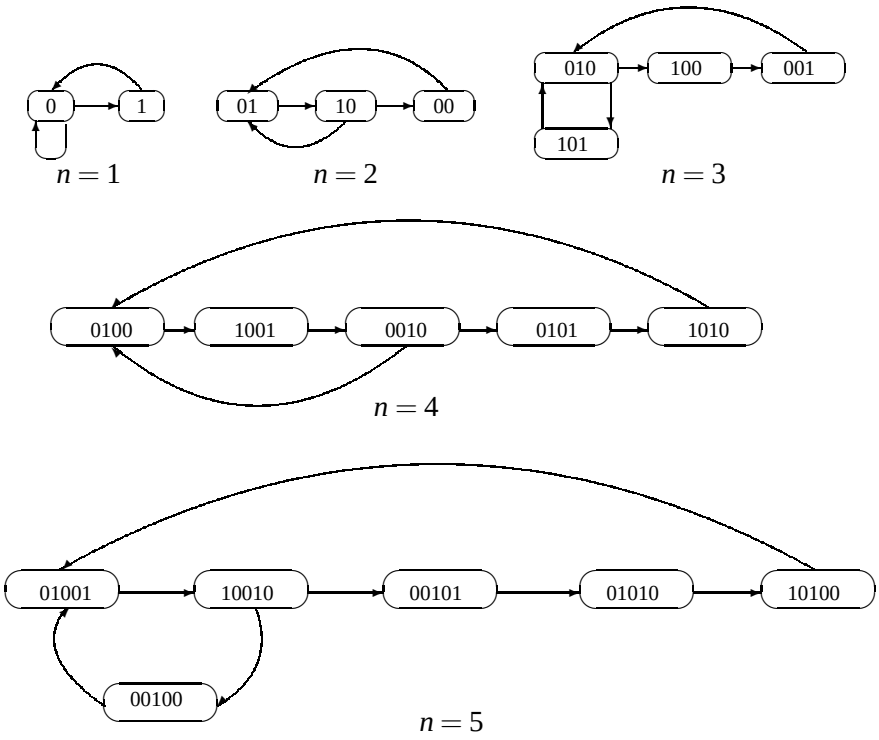
4.6. ábra. Négydimenziós hiperkocka.

A

$$p = 0100110001110000111100000111111\ldots\underbrace{0\ldots0}_{n}\underbrace{1\ldots1}_{n}\ldots$$

hatványszó esetében

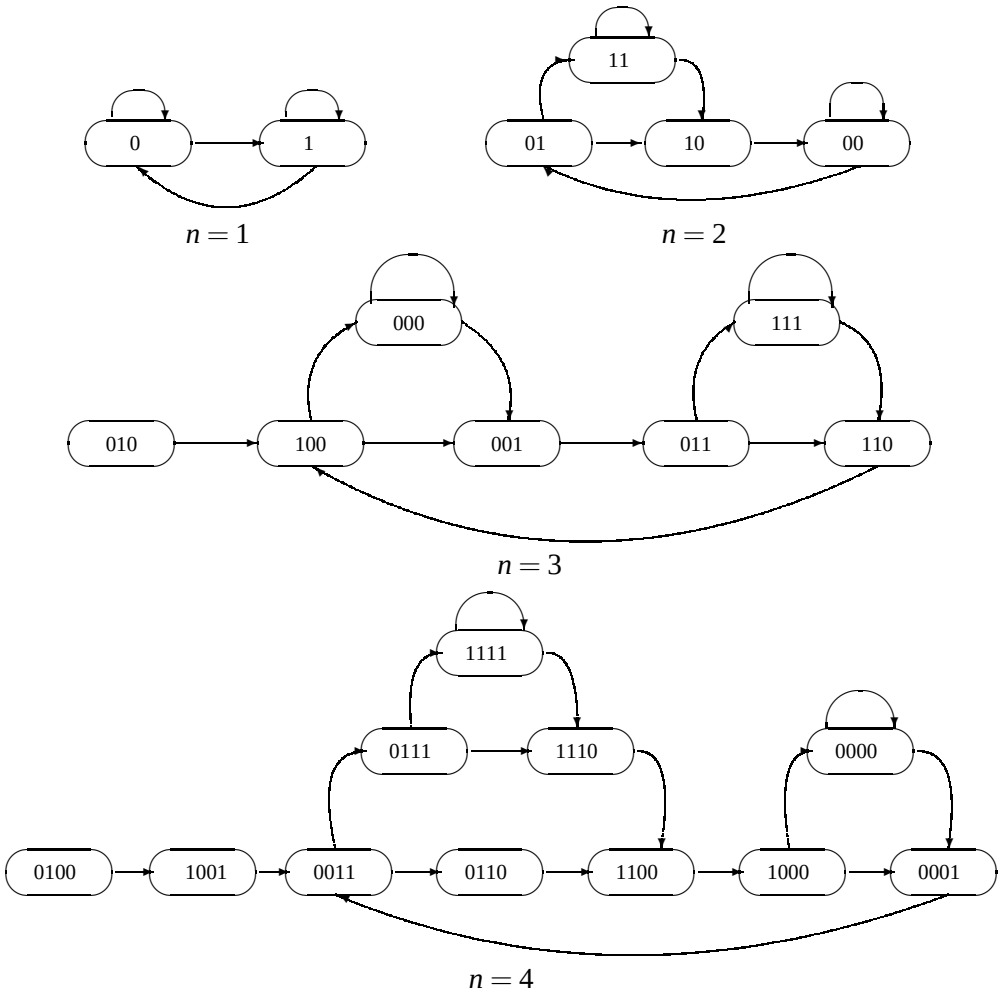
$F_1(p) = \{0,1\}, \quad F_2(p) = \{01,10,00,11\},$
$F_3(p) = \{010,100,000,001,011,111,110\},$



4.7. ábra. Fibonacci-szó Rauzy-gráfjai

$F_4(p) = \{0100, 1001, 0011, 0110, 1100, 1000, 0000, 0001, 0111, 1110, 1111\}$,
a megfelelő Rauzy-gráfok a 4.8. ábrán láthatók.

Amint a 4.7. és 4.8. ábrákon láthatjuk, vannak olyan n hosszúságú részszavak, amelyek csak egyféleképpen folytathatók egy betű hozzáadásával (ezekből az ábrákon egy-egy él fut ki), és vannak olyanok, amelyekből két-két él fut ki, azaz kétféleképpen is folytathatók. Ez utóbbiakat *speciális* szavaknak nevezzük. A $v \in F_n(u)$ *jobbról speciális részszó*, ha létezik legalább két olyan $a \in A$ betű, amelyre $va \in F_{n+1}(u)$. Hasonlóképpen, $v \in F_n(u)$ *balról speciális részszó*, ha létezik legalább két olyan $a \in A$ betű, amelyre $av \in F_{n+1}(u)$. Egy részszó *bispeciális*, ha egyben balról is és jobbról is speciális. Néhány speciális részszó a 4.7. és 4.8. ábrákon látható:
balról speciális részszavak: 0100, 01001 (*4.7. ábra*), 10, 110, 1110, 0001 (*4.8. ábra*)
jobbról speciális részszavak: 0010, 10010 (*4.7. ábra*), 01, 011, 0111 (*4.8. ábra*)
bispeciális: 010, 00100 (*4.7.* ábra), 000, 111, 1111, 0011 (*4.8.* ábra)



4.8. ábra. A hatványszó Rauzy-gráfjai.

4.5. Szavak bonyolultsága

A szavak bonyolultsága olyan mérték, amely a részszavak változatosságát jellemzi. A következő bonyolultságokat értelmezzük.

1) Egy szó *részszóbonyolultsága* vagy egyszerűen csak *bonyolultsága* a szó azonos hosszúságú különböző részszavainak a száma. Az u szó n-hosszúságú részszavainak a száma $f_u(n)$.

$$f_u(n) = \#F_n(u), \quad u \in A^\infty$$

Igaz a következő is: $f_u(n) = 0$, ha $n > |u|$ vagy $n = 0$.

2) *Maximális bonyolultság* csak véges szavakra értelmezhető.

$$C(u) = \max\{ f_u(n) \mid n \geq 1\}, \quad u \in A^*$$

Végtelen szavakra értelmezzük a $C_u^-(n)$ *alsó maximális bonyolultságot* valamint a $C_u^+(n)$ *felső maximális bonyolultságot*.

$$C_u^-(n) = \min_i C(u_i u_{i+1} \dots u_{i+n-1}), \quad C_u^+(n) = \max_i C(u_i u_{i+1} \dots u_{i+n-1})$$

3) *Globális maximális bonyolultság.* Ezt a bonyolultságot az A^n halmazban értelmezzük mint az összes maximális bonyolultság közül a legnagyobb.

$$G(n) = \max\{C(u) \mid u \in A^n\}$$

4) A *teljes bonyolultság* egy szó összes nem üres különböző részszavainak a számát jelenti.

$$K(u) = \sum_{i=1}^{|u|} f_u(i), \quad u \in A^*$$

Végtelen szavakra értelmezzük a $K_u^-(n)$ *alsó teljes bonyolultságot,* valamint a $K_u^+(n)$ *felső teljes bonyolultságot*.

$$K_u^-(n) = \min_i K(u_i u_{i+1} \dots u_{i+n-1}), \quad K_u^+(n) = \max_i K(u_i u_{i+1} \dots u_{i+n-1})$$

5) *d-bonyolultság*

A d-bonyolultság [45] értelmezéséhez előbb értelmezzük a részszó általánosítását, a *d-részszót*. Legyenek $d,k,s \in \mathbf{N}$, $u = a_1 a_2 \dots a_k \in A^k$. A $v = a_{i_1} a_{i_2} \dots a_{i_s}$ szó u-nak *d-részszava*, ha

$$\begin{aligned} &i_1 \geq 1, \\ &1 \leq i_{j+1} - i_j \leq d, \qquad \text{ha } j = 1,2,\dots,s-1 \\ &i_s \leq k. \end{aligned}$$

Az $u = abab$ szó 2-részszavai:

1 hosszúságúak: *a*, *b*
2 hosszúságúak: *ab*, *aa*, *ba*, *bb*
3 hosszúságúak: *aba*, *abb*, *aab*, *bab*
4 hosszúságú: *abab*.

Az előbbi bonyolultságok értelmezhetők d-részszavakra is. Itt csak a véges szavakra értelmezzük ezeket.

– *d-részszóbonyolultság* vagy egyszerűen *d-bonyolultság* egy adott szó meghatározott hosszúságú különböző d-részszavainak a száma. Ezt a bonyolultságot $f_{u,d}(n)$-nel jelöljük adott u szóra, ha a d-részszavak hossza n. Itt is $f_{u,d}(n) = 0$, ha $n > |u|$ vagy $n = 0$.

– *maximális d-bonyolultság*:

$$C_d(u) = \max\{ f_{u,d}(n) \mid n \geq 1\}$$

– *globális maximális d-bonyolultság*:

$$G_d(n) = \max\{C_d(u) \mid u \in A^n\}$$

– *teljes d-bonyolultság*:

$$K_d(u) = \sum_{i=1}^{|u|} f_{u,d}(i)$$

4.5.1. Részszóbonyolultság

Amint már láttuk

$$f_u(n) = \#F_n(u), \quad \forall u \in A^\infty,\ n \in \mathbf{N}.$$

$f_u(n) = 0$, ha $n > |u|$ vagy $n = 0$.

Például, az $u = abacab$ szó esetében:

$$f_u(1) = 3,\ f_u(2) = 4,\ f_u(3) = 4,\ f_u(4) = 3, f_u(5) = 2,\ f_u(6) = 1.$$

A Fibonacci-szó esetében, amint azt már láttuk a 4.11. tételben:

$$f_f(n) = n+1$$

A $p = 010011\ldots0^k1^k\ldots$ hatványszó esetében a bonyolultság

$$f_p(n) = \frac{n(n+1)}{2} + 1.$$

Ezt be lehet bizonyítani, ha kiszámítjuk az $f_p(n+1) - f_p(n)$ különbséget, amely azon n hosszúságú részszavak száma, amelyeket kétféleképpen lehet folytatni, hogy $n+1$ hosszúságú részszót kapjunk. Ha $k \leq n-k$, akkor csupán a 0^k1^{n-k} alakú szavakat lehet kétféleképpen folytatni, míg ha $k < n-k$, akkor csak az 1^k0^{n-k} alakúakat. Külön megvizsgálva, amikor n páros és páratlan, könnyen adódik, hogy

$$f_p(n+1) - f_p(n) = n+1,$$

ahonnan

$$\begin{aligned} f_p(n) &= n + f_p(n-1) = n + (n-1) + f_p(n-2) = \ldots \\ &= n + (n+1) + \ldots + 2 + f_p(1) = \frac{n(n+1)}{2} + 1. \end{aligned}$$

A következő szóban a pontok csupán az egyes részszavak elhatárolására szolgálnak, egyéb szerepük nincs.

$$\begin{aligned} u_C = u_0u_1\dots u_n\dots &= 0.1.10.11.100.101.110.111.1000\dots \\ &= 0110111001011101111000\dots, \end{aligned}$$

Itt minden u_i az i bináris ábrázolása minimális számjeggyel. Ez a végtelen szó a ún. *Champernowne-szó*, amelynek bonyolultsága nyilván $f_{u_C}(n) = 2^n$.

4.17. tétel. *Ha az $u \in A^\omega$ végtelen szó esetében létezik egy $n \in \mathbf{N}$ úgy, hogy $f_u(n) \le n$, akkor az u végperiodikus.*

Bizonyítás. $f_u(1) \ge 2$, különben a szó triviális (egyetlen betűt tartalmaz). Tehát léteznie kell egy $k \le n$ értéknek, amelyre $f_u(k) = f_u(k+1)$. De

$$f_u(k+1) - f_u(k) = \sum_{v \in F_k(u)} \Big(\#\big\{ a \in \Sigma \mid va \in F_{k+1}(u) \big\} - 1 \Big).$$

Tehát bármely $v \in F_k(u)$ részszó csak egyféleképpen folytatható, hogy $va \in F_{k+1}(u)$ részszót kapjunk. Így, ha $v = u_iu_{i+1}\dots u_{i+k-1} = u_ju_{j+1}\dots u_{j+k-1}$, akkor $u_{i+k} = u_{j+k}$ is. Mivel $F_k(u)$ véges halmaz és u végtelen, léteznek az i és j ($i < j$) indexek, amelyekre $u_iu_{i+1}\dots u_{i+k-1} = u_ju_{j+1}\dots u_{j+k-1}$, de akkor $u_{i+k} = u_{j+k}$ is igaz. De akkor $u_{i+1}u_{i+2}\dots u_{i+k} = u_{j+1}u_{j+2}\dots u_{j+k}$ egyenlőségből következik $u_{i+k*1} = u_{j+k+1}$, tehát $u_{i+l} = u_{j+l}$ minden $l \ge 0$ értékre. Ekkor pedig az u szó végperiodikus. □

4.18. értelmezés. *Az $u \in A^\omega$ szót Sturm-típusú szónak nevezzük, ha $f_u(n) = n+1$ bármely $n \ge 1$-re.*

A Sturm-típusú szavak azok a végtelen nem periodikus szavak, amelyek a lehető legkisebb bonyolultságúak. A Fibonacci-szó nyilvánvalóan Sturm-típusú. Abból, hogy $f_u(1) = 2$ következik, hogy ezek a szavak mind kétbetűsek.

A 4.17. tételből következik, hogy minden végtelen, nem végperiodikus szó bonyolultsága legalább $n+1$, azaz

$$u \in A^\omega, u \text{ nem végperiodikus } \Rightarrow\ f_u(n) \ge n+1.$$

Egyenlőség a Sturm-típusú szavak esetében van.

A végtelen szavakat hasonló módon lehet jellemezni a felső maximális és a felső teljes bonyolultság segítségével is.

4.19. tétel. *Ha a végtelen u szó nem végperiodikus és $n \ge 1$, akkor*

$$C_u^+(n) \ge \left\lceil \frac{n}{2} \right\rceil + 1, \quad K_u^+(n) \ge \left\lceil \frac{n^2}{4} + n \right\rceil.$$

A Sturm-típusú szavak esetében egyenlőség áll fenn.

Jelölje $\{x\}$ az x szám egész részét. Nyilvánvaló, hogy $x = \lfloor x \rfloor + \{x\}$. Az R függvény n-szeres összetételét önmagával R^n-nel jelöljük, tehát $R^n = R \circ R \circ \ldots \circ R$ (n-szer). A Sturm-szavakat a következőképen jellemezhetjük:

4.20. tétel. *Az u szó Sturm-típusú akkor és csakis akkor, ha létezik egy α irracionális szám és egy z valós szám úgy, hogy $R(x) = \{x+\alpha\}$ esetében*

$$u_n = \begin{cases} 0, \text{ ha } R^n(z) \in (0, 1-\alpha) \\ 1, \text{ ha } R^n(z) \in [1-\alpha, 1) \end{cases}$$

vagy

$$u_n = \begin{cases} 1, \text{ ha } R^n(z) \in (0, 1-\alpha) \\ 0, \text{ ha } R^n(z) \in [1-\alpha, 1) \end{cases}$$

A Fibonacci-szó esetében ezek a számok: $\alpha = z = \dfrac{\sqrt{5}-1}{2}$ (aranymetszési állandó).

A Sturm-típusú szavak a következőképpen is származtathatók. Egy billiárdgolyót elindítunk egy billiárdasztal egyik szélétől irracionális szög alatt, és súrlódás nélküli mozgást feltételezve a golyó végtelen mozgásba kezd. Amikor a golyó valamelyik egymással párhuzamos oldalról verődik vissza 0-t írunk a végtelen szóba, amikor pedig a másik két párhuzamos oldal valamelyikét érinti, akkor 1-et. Ily módon kétbetűs végtelen szavakat generálhatunk. Ezt általánosítani lehet $(s+1)$ betűs ábécére, amikor $(s+1)$-dimenziós hiperkockában vizsgáljuk a billiárdgolyó pályáját. Ebben az esetben a bonyolultság

$$f_u(n, s+1) = \sum_{i=0}^{\min(n,x)} \frac{n!s!}{(n-i)!i!(s-i)!}$$

Ha $s = 1$, akkor $f_u(n,2) = f_u(n) = n+1$, ha pedig $s = 2$, akkor $f_u(n,3) = n^2 + n + 1$.

4.5.2. Maximális bonyolultság

Egy véges u szó esetében

$$C(u) = \max\{ f_u(n) \mid n \geq 1\}$$

a maximális bonyolultság. Az alábbi táblázatban néhány szó bonyolultsága található minden lehetséges hosszúságra. Innen látszik például, hogy $C(11211122) = 5$, $C(11211211) = 3$ stb.

u	$f_u(1)$	$f_u(2)$	$f_u(3)$	$f_u(4)$	$f_u(5)$	$f_u(6)$	$f_u(7)$	$f_u(8)$
11211122	2	4	5	5	4	3	2	1
11211211	2	3	3	3	3	3	2	1
11211212	2	3	4	4	4	3	2	1
11211221	2	4	5	5	4	3	2	1
11211222	2	4	5	5	4	3	2	1
11212111	2	3	5	5	4	3	2	1
11212112	2	3	4	5	4	3	2	1
11212122	2	4	4	4	4	3	2	1

A bonyolultságra érvényes a következő tétel.

4.21. tétel. *Ha w véges szó, $f_w(n)$ a bonyolultsága, akkor léteznek az m és M természetes számok, amelyekre $1 \leq m \leq M \leq |w|$ úgy, hogy*

- $f_w(n+1) > f_w(n)$ *ha* $1 \leq n < m$,
- $f_w(n+1) = f_w(n)$ *ha* $m \leq n < M$,
- $f_w(n+1) = f_w(n) - 1$ *ha* $M \leq n \leq |w|$.

Az előbbi táblázatból látszik, hogy ha
$w = 11211122$, akkor $m = 3$, $M = 4$,
$w = 11212112$, akkor $m = 4$, $M = 4$,
$w = 11212122$, akkor $m = 2$, $M = 5$.

4.5.3. Globális maximális bonyolultság

A globális maximális bonyolultság

$$G(n) = \max\{C(u) \mid u \in A^n\},$$

azaz a legnagyobb (részszó)bonyolultság az adott ábécé fölötti összes n hosszúságú szavak halmazában. A következő kérdések adódnak:

– milyen hosszúságúak azok a részszavak, amelyekre a globális maximális bonyolultság egybeesik a maximális bonyolultsággal?

– hány ilyen szó van?

Példák.

Az $A = \{0,1\}$ ábécére az alábbi táblázatok az összes 3 és 4 hosszúságú szavak esetében tartalmazzák a (részszó)bonyolultságot.

	$f_u(i)$		
u	$i=1$	$i=2$	$i=3$
000	1	1	1
001	2	2	1
010	2	2	1
011	2	2	1
100	2	2	1
101	2	2	1
110	2	2	1
111	1	1	1

A 3 hosszúságú szavak esetében a globális maximális bonyolultság 2, és ez az 1 és 2 hosszúságú részszavakéval azonos. A globális maximális bonyolultságot 6 szó éri el.

	$f_u(i)$			
u	$i=1$	$i=2$	$i=3$	$i=4$
0000	1	1	1	1
0001	2	2	2	1
0010	2	3	2	1
0011	2	3	2	1
0100	2	3	2	1
0101	2	2	2	1
0110	2	3	2	1
0111	2	2	2	1
1000	2	2	2	1
1001	2	3	2	1
1010	2	2	2	1
1011	2	3	2	1
1100	2	3	2	1
1101	2	3	2	1
1110	2	2	2	1
1111	1	1	1	1

A 4 hosszúságú szavak esetében a globális maximális bonyolultság 3, és a 2 hosszúságú részszavakra kapjuk. Ezen szavak száma 8.

Az előbbi két feladat megoldásához a következő jelöléseket használjuk:

$$R(n) = \{i \in \{1,2,\ldots,n\} \mid \exists u \in A^n : f_u(i) = G(n)\}$$

$$M(n) = \#\{u \in A^n : C(u) = G(n)\}$$

A 4.9. táblázatban megtaláljuk a $G(n)$, $R(n)$, $M(n)$ értékeket 20 hosszúságig egy kétbetűs ábécé fölött.

4.22. tétel. *Ha* $\#A = q$ *és* $q^k + k \leq n \leq q^{k+1} + k$, *akkor* $G(n) = n - k$.

4.23. tétel. *Ha* $\#A = q$ *és* $q^k + k < n \leq q^{k+1} + k$, *akkor* $R(n) = \{k+1\}$, *és ha* $n = q^k + k$, *akkor* $R(n) = \{k, k+1\}$.

4.24. tétel. *Ha* $\#A = q$ *és* $q^k + k \leq n \leq q^{k+1} + k$, *akkor* $M(n)$ *egyenlő a* $B(q, k+1)$ *De Bruijn-gráf* $n-k+1$ *hosszúságú különböző útjainak számával.*

4.25. tétel. *Ha* $n = 2^k + k - 1$, *akkor* $M(n) = 2^{2^{k-1}}$.

Bizonyítás. A $B(2,k)$ De Bruijn-gráfban $2^{2^{k-1}-k}$ Hamilton-kör van [12]. A Hamilton-kör minden csúcsával kezdődik egy De Bruijn-szó, amely tartalmazza az összes k hosszúságú részszót, és amelynek maximális a bonyolultsága, tehát $M(n) = 2^k \cdot 2^{2^{k-1}-k} = 2^{2^{k-1}}$. □

Ez a tétel általánosítható $q \geq 2$ betűjű ábécére.

4.26. tétel. *Ha* $n = q^k + k - 1$, *akkor* $M(n) = (q!)^{q^{k-1}}$.

n	$G(n)$	$R(n)$	$M(n)$
1	1	1	2
2	2	1	2
3	2	1, 2	6
4	3	2	8
5	4	2	4
6	4	2, 3	36
7	5	3	42
8	6	3	48
9	7	3	40
10	8	3	16
11	8	3, 4	558
12	9	4	718
13	10	4	854
14	11	4	920
15	12	4	956
16	13	4	960
17	14	4	912
18	15	4	704
19	16	4	256
20	16	4, 5	79006

4.9. ábra. A globális maximális bonyolultság, amely $R(n)$ hosszúságú szavakra egyenlő a maximális bonyolultsággal. $M(n)$ azon szavak száma, amelyekre a maximális bonyolultság egyenlő a globális maximális bonyolultsággal.

4.5.4. Teljes bonyolultság

Teljes bonyolultság alatt egy szó összes nem üres, különböző részszavainak a számát értjük.

$$K(u) = \sum_{i=1}^{|u|} f_u(i)$$

Egy $\underbrace{a \ldots a}_{k}$ szót ($k > 1$) *triviális szónak* nevezünk (csak egy betűt használ). Egy ilyen k hosszúságú szónak a teljes bonyolultsága k (minden hosszúságból csupán egyetlen szót tartalmaz).

A következő kérdések merülnek fel:

1. Keressünk adott teljes bonyolultságú legrövidebb szót.

Ennek a feladatnak mindig van megoldása, hisz legrosszabb esetben egy triviális szó a megoldás.

2. Keressünk adott hosszúságú és adott teljes bonyolultságú legrövidebb szót, ha létezik.

A következő rekurzív algoritmus megoldja a feladatot, ha van megoldása. Megkeresi az összes k hosszúságú szót, amelynek teljes bonyolultsága C. Az $a_1, a_2, \ldots, a_k$ betűkből álló ábécét használjuk, a $+$ jel pedig összeillesztést (szorzást) jelent. Az eljárás hívásakor a w szó üres.

SZÓT-GENERÁL(w):
if $K(w) < C$ és $|w| < k$
  then for $i = 1, 2, \ldots, k$
    do SZÓT-GENERÁL $(w + a_i)$
  else if $K(w) = C$ és $|w| = k$
    then írd w

Az algoritmus alkalmas az első feladat megoldására is, ha lemondunk a szó hosszának a korlátozásáról. A kérdés az, hogy létezik-e mindig nem triviális szó, amelynek C a teljes bonyolultsága. A választ a következő tétel adja meg.

4.27. tétel. *Ha C 2-től és 4-től különböző természetes szám, akkor létezik nem triviális szó, amelynek bonyolultsága C.*

Bizonyítás. Tekintsük a következő k hosszúságú szavakat, és azok teljes bonyolultságát, amelyek egyszerű számítással megkaphatók.

$K(a^{k-1}b) = 2k-1$, ha $k \geq 1$,
$K(ab^{k-3}aa) = 4k-8$, ha $k \geq 4$,
$K(abcd^{k-3}) = 4k-6$, ha $k \geq 3$.

1. Ha C páratlan szám, akkor felírható $C = 2k-1$ alakban. Innen $k = \frac{C+1}{2}$ és az $a^{k-1}b$ szó teljes bonyolultsága C.

2. Ha C páros szám, akkor felírható $C = 2\ell$ alakban. A következő eseteket különböztetjük meg:

2.1. Ha $\ell = 2h$, akkor $4k-8 = C$ egyenlőségből következik $4k-8 = 4h$, vagyis $k = h+2$. Ekkor az $ab^{k-3}aa$ szónak a teljes bonyolultsága C (ha $k \geq 4$).

2.2. Ha $l = 2h+1$, akkor $4k-6 = C$ egyenlőségből következik $4k-6 = 4h+2$. Ebből pedig $k = h+2$ következik, és az $abcd^{k-3}$ szónak a teljes bonyolultsága C (ha $k \geq 3$). □

Érvényes a következő tétel is.

4.28. tétel. *Ha C olyan természetes szám, amely különbözik az 1, 2, 4, 6, 10, 18 és 22 számoktól, akkor létezik kétbetűs szó, amelynek teljes bonyolultsága C.*

Bizonyítás. Az előbbi tétel bizonyításában csupán a 2.2. esetben használtunk kettőnél több betűt. Tehát elég a bizonyítást arra az esetre elvégezni, amelyre C $4h+2$ alakú. Ha $C = 4h+2$ és $C \geq 34$, akkor

$K(ab^{k-7}abbabb) = 8k-46$, ha $k \geq 10$,
$K(ab^{k-7}ababba) = 8k-42$, ha $k \geq 10$,

Ha $h = 2s$, akkor $8k - 46 = 4h + 2$, vagyis $k = s + 6$ és az $ab^{k-7}abbabb$ szó teljes bonyolultsága $4h+2$.

Ha $h = 2s+1$, akkor $8k - 42 = 4h + 2$, vagyis $k = s + 6$ és az $ab^{k-7}ababba$ szó teljes bonyolultsága $4h+2$.

Ha $C < 34$, akkor csak a 14, 26 és 30 számokra létezik megoldás: $K(ab^4a) = 14$, $K(ab^6a) = 26$, $K(ab^5aba) = 30$. □

4.5.5. Teljes d-bonyolultság

A d-részszó a részszó általánosítása.

4.29. értelmezés. *Legyenek d, k és s természetes számok, és $p = x_1x_2\cdots x_k \in X^k$. $q = x_{i_1}x_{i_2}\cdots x_{i_s}$ a p szó d-részszava, ha*

$$\begin{aligned} &i_1 \geq 1, \\ &1 \leq i_{j+1} - i_j \leq d, \qquad ha \quad j = 1,2,\cdots,s-1, \\ &i_s \leq k. \end{aligned}$$

Jelölés: $q \subseteq_d p$. Ha $q \subseteq_d p$ és $q \neq p$, akkor q valódi d-részszava p-nek és ennek jelölése $q \subset_d p$.

A p szó teljes *d-bonyolultságát* $K_d(p)$-vel jelöljük ([45]), és ez egyenlő a p szó összes különböző d-részszavának a számával.

Megfigyelhető, hogy $K_1(p) = K(p)$.

Példa. Legyen $X = \{a,b\}$ és $p = abab$. Ebben a szóban van két 1 hosszúságú 2-részszó (a,b), négy 2 hosszúságú 2-részszó (ab,aa,ba,bb), négy 3 hosszúságú 2-részszó (aba,abb,aab,bab), és egyetlen 4 hosszúságú 2-részszó $(abab)$. Ezért $K_2(p) = 2+4+4+1 = 11$.

Ha egy k hosszúságú szóban a betűk különbözőek, akkor a teljes d-bonyolultságot $N(k,d)$-vel jelöljük. Ha $|X| \geq 2$, $k \geq 1$, $d \geq 1$ és $p \in X^k$, akkor

$$k \leq K_d(p) \leq 2^k - 1.$$

Ha a p szóban különböző betűk vannak, d természetes szám, $a_{i,d}(p)$-vel jelöljük a p szó azon d-részszavainak a számát, amelyek az i-edik helyen végződnek. Ha $k \geq 1$ és $p \in X^k$ különböző betűkből áll, akkor

$$a_{i,d}(p) = 1 + a_{i-1,d}(p) + a_{i-2,d}(p) + \ldots + a_{i-d,d}(p), \qquad i = 1,2,\ldots,k \tag{4.3}$$

Egy k hosszúságú, különböző betűkből álló p szó teljes d-bonyolultsága a következő képlettel kapható meg:

$$N(k,d) = \sum_{i=1}^{k} a_{i,d}(p).$$

A (4.3) képlet alapján, $d \geq 2$ esetében felírhatjuk, hogy

$$a_{i,d} + \frac{1}{d-1} = \left(a_{i-1,d} + \frac{1}{d-1}\right) + \cdots + \left(a_{i-d,d} + \frac{1}{d-1}\right).$$

Legyen

$$b_{i,d} = a_{i,d} + \frac{1}{d-1}, \qquad \text{és} \qquad c_{i,d} = (d-1)b_{i,d},$$

akkor

$$c_{i,d} = c_{i-1,d} + c_{i-2,d} + \ldots + c_{i-d,d},$$

így a $c_{i,d}$ számok Fibonacci típusúak. Bármely d-re $a_{1,d} = 1$ és innen $c_{1,d} = d$. A $c_{i,d}$ számokat a következő rekurzív képlettel értelmezhetjük.

$$\begin{array}{ll} c_{n,d} = c_{n-1,d} + c_{n-2,d} + \ldots + c_{n-d,d}, & \text{ha} \quad n > 0, \\ c_{n,d} = 1, & \text{ha} \quad n \leq 0. \end{array}$$

Ezek a számok megkaphatók generátorfüggvény segítségével is, ahogy az következő tételből következik.

4.30. tétel.

$$F_d(z) = \sum_{n\geq 0} c_{n,d} z^n = \frac{1 + (d-3)z - (d-1)z^2 + z^{d+1}}{(1-z)(1-2z+z^{d+1})}.$$

Bizonyítás. A $c_{n,d}$ számok generátorfüggvénye

$$F_d(z) = \sum_{n\geq 0} c_{n,d} z^n.$$

A (4.3) képlet alapján

$$F_d(z) = c_{0,d} + c_{1,d}z + \cdots + c_{d-1,d}z^{d-1} + z\sum_{n\geq d} c_{n-1,d}z^{n-1} +$$

$$+ z^2 \sum_{n\geq d} c_{n-2,d} z^{n-2} + \cdots + z^n \sum_{n\geq d} c_{n-d,d} z^{n-d} =$$

$$= \sum_{n=0}^{d-1} c_{n,d} z^n + z\left(F_d(z) - \sum_{n=0}^{d-2} c_{n,d} z^n\right) + z^2\left(F_d(z) - \sum_{n=0}^{d-3} c_{n,d} z^n\right) +$$

$$+ \cdots + z^{d-1}(F_d(z) - c_{0,d}) + z^d F_d(z).$$

Ekkor

$$F_d(z)(1 - z - z^2 - \cdots - z^d) = c_{0,d} + z(c_{1,d} - c_{0,d}) + z^2(c_{2,d} - c_{1,d} - c_{0,d}) +$$

$$+ \cdots + z^{d-1}(c_{d-1,d} - c_{d-2,d} - \cdots - c_{0,d}).$$

De $c_{0,d} = 1$, $c_{1,d} = d$, $c_{2,d} = c_{1,d} + c_{0,d} + c_{-1,d} + \ldots + c_{2-d,d} = 2d - 1$ stb., tehát

$$F_d(z) = \frac{1 + (d-1)z + (d-2)z^2 + \cdots 2z^{d-2} + z^{d-1}}{1 - z - z^2 - \cdots - z^d}.$$

Mivel

$$(1-z-z^2-\cdots z^d)(1-z)=1-2z+z^{d+1},$$

a következőt kapjuk:

$$F_d(z)=\frac{1+(d-2)z-z^2-\cdots-z^d}{1-2z+z^{d+1}}=\frac{1+(d-3)z-(d-1)z^2+z^{d+1}}{(1-z)(1-2z+z^{d+1})},$$

ami bizonyítja a tételt. □

Az $N(k,d)$ teljes d-bonyolultságot ki lehet fejezni ezekkel a $c_{n,d}$ számokkal is:

$$N(k,d)=\frac{1}{d-1}\left(\sum_{i=1}^{k}c_{i,d}-k\right), \qquad \text{ha } d>1$$

és

$$N(k,1)=\frac{k(k+1)}{2}$$

vagy

$$N(k,d)=N(k-1,d)+\frac{1}{d-1}(c_{k,d}-1), \qquad \text{ha} \quad d>1,\ k>1.$$

Ha $d=2$, akkor

$$F_2(z)=\frac{1-z^2}{1-2z+z^3}=\frac{1+z}{1-z-z^2}=\frac{F(z)}{z}+F(z),$$

ahol $F(z)$ az F_n Fibonacci-számok generátorfüggvénye (ahol $F_0=0$, $F_1=1$). Akkor, innen

$$c_{n,2}=F_{n+1}+F_n=F_{n+2}$$

és

$$N(k,2)=\sum_{i=1}^{k}F_{i+2}-k=F_{k+4}-k-3.$$

Az 1. táblázat $N(k,d)$ értékeit tartalmazza, ha $k\leq 10$ és $d\leq 10$.

$k \setminus d$	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	3	3	3	3	3	3	3	3	3	3
3	6	7	7	7	7	7	7	7	7	7
4	10	14	15	15	15	15	15	15	15	15
5	15	26	30	31	31	31	31	31	31	31
6	21	46	58	62	63	63	63	63	63	63
7	28	79	110	122	126	127	127	127	127	127
8	36	133	206	238	250	254	255	255	255	255
9	45	221	383	464	494	506	510	511	511	511
10	55	364	709	894	974	1006	1018	1022	1023	1023

1. táblázat

A d-részszó értelmezéséből következik, hogy

$$N(k,d) = N(k,d+1), \qquad \text{ha} \quad d \geq k-1$$

de

$$N(k,k-1) = 2^k - 1$$

és akkor

$$N(k,d) = 2^k - 1, \qquad \text{ha} \quad d \geq k-1.$$

A következő tétel $N(k,d)$ értékét adja meg nagyon sok esetben.

4.31. tétel. *Ha $k \geq 2d-2$, akkor*

$$N(k,k-d) = 2^k - (d-2)\cdot 2^{d-1} - 2.$$

Bizonyítás. Legyen $k \geq 2d-2$. Akkor $N(k,k-d-1)$ a következőképpen számítható ki. Az összes $N(k,k-d)$ részszó között pontosan $d \cdot 2^{d-1}$ van, amelyekre $i_{j+1} - i_j = k-d$ egy adott j-re, mivel d lehetőség van arra, hogy $k-d$ távolságú helyeket válasszunk, és 2^{d-1} lehetőség, hogy kiválasszuk a többi betűt. (Ezek a távolságok a betűk között kisebbek kell, hogy legyenek, mint $k-d$, tehát $k-d+1 \geq d-1$, vagyis $k \geq 2d-2$), tehát

$$N(k,k-d-1) = N(k,k-d) - d\cdot 2^{d-1}.$$

Ha $d = 1,2,\ldots,$ akkor:

$$N(k,k-2) = N(k,k-1) - 1$$

$$N(k,k-3) = N(k,k-2) - 2\cdot 2^1$$

$$N(k,k-4) = N(k,k-3) - 3\cdot 2^2$$

$$\ldots$$

$$N(k,k-d) = N(k,k-d-+1) - (d-1)\cdot 2^{d-2},$$

és ehhez adódik még a nyilvánvaló

$$N(k,k-1) = 2^k - 1$$

összefüggés. Összeadva ezeket, az eredmény

$$N(k,k-d) = 2^k - 1 - \left(1 + 2\cdot 2^1 + 3\cdot 2^2 + \ldots + (d-1)\cdot 2^{d-2}\right),$$

ahonnan, egyszerű számítással kapjuk, hogy

$$N(k,k-d) = 2^k - (d-2)2^{d-1} - 2,$$

amit éppen bizonyítani kellett. □

Az $N(k,d)$ értéke kiszámítható úgy is, hogy megszámoljuk azokat a 0-ból és 1-ből álló k hosszúságú szavakat, amelyekben legfeljebb $d-1$ nulla lehet egymás mellett. Egy ilyen szóban 1 jelenti a megfelelő helyű betű jelenlétét a d-részszóban, 0 pedig annak a hiányát. Legyen $b_{k,d}$ azon 0-t és 1-et tartalmazó k hosszúságú szavak száma, amelyekben az első és utolsó helyen 1 van, és legfeljebb $d-1$ 0 van egymás mellett. Könnyű belátni, hogy

$$\begin{aligned} b_{k,d} &= b_{k-1,d} + b_{k-2,d} + \ldots + b_{k-d,d}, \qquad \text{ha} \quad k > 1 \\ b_{1,d} &= 1, \\ b_{k,d} &= 0, \qquad\qquad\qquad\qquad \text{ha} \quad k \leq 0, \end{aligned}$$

mert a $k-i$ ($i = 1,2,...,d$) hosszúságú részszavakat csak egyféleképpen lehet folytatni, hogy hasonló k hosszúságú szót kapjunk (jobbról $0^{i-1}1$ alakú részszóval folytatva). $b_{k,d}$-re a következő képlet is fennáll:

$$b_{k,d} = 2b_{k-1,d} - b_{k-1-d,d}.$$

A következő tétel megadja a $b_{n,d}$ számok generátorfüggvényét.

4.32. tétel.

$$B_d(z) = \sum_{n\geq 0} b_{n,d} z^n = \frac{z}{1-z-\cdots-z^d} = \frac{z(1-z)}{1-2z+z^{d+1}}.$$

Megjegyzés. A $b_{n,2}$ számok azonosak az ismert Fibonacci-számokkal.

Ezen szavakhoz balról vagy/és jobbról nullákat ragasztva, megkaphatjuk az $N(k,d)$-t mint ezeknek a számát. Így

$$N(k,d) = b_{k,d} + 2b_{k-1,d} + 3b_{k-2,d} + \cdots + kb_{1,d}.$$

(i nullát $i+1$ módon adhatunk hozzá: egyet sem balról és i-t jobbról, egyet balról és $(i-1)$-et jobbról, ás így tovább).

A fenti képletből megkaphatjuk az $N(k,d)$ számok $N_d(z)$ generátorfüggvényét mint két generátorfüggvény szorzatát. Az egyik $B_d(z)$, a másik pedig

$$A(z) = \sum_{n\geq 0} (n+1) z^n = \frac{1}{(1-z)^2},$$

amelyből kapjuk a következő tételt.

4.33. tétel.

$$N_d(z) = \sum_{n\geq 0} N(n,d) z^n = \frac{z}{(1-z)(1-2z+z^{d+1})}.$$

Ha $d = 1$, akkor

$$N(k,1) = \frac{k(k+1)}{2},$$

és

$$N_1(z) = \sum_{n\geq 0} \frac{n(n+1)}{2} z^n = \frac{z}{(1-z)^3}.$$

Ha $d = 2$, akkor

$$N(k,2) = F_{k+4} - k - 3,$$

és a megfelelő generátorfüggvény a következő:

$$N_2(z) = \sum_{n\geq 0} (F_{n+4} - n - 3) z^n = \frac{z}{(1-z)^2(1-z+z^2)}.$$

4.5.6. Dyck-szavak

$2n$ hosszúságú Dyck-szavaknak nevezzük az olyan $\{0,1\}$ fölötti szavakat, amelyekben pontosan n darab 0, és n darab 1 van, és balról jobbra vizsgálva, az 1-esek száma soha nem haladja meg a 0-k számát. A $2n$ hosszúságú Dyck-szavak számát C_n-nel jelöljük, és Catalan-számoknak nevezzük[4]. Ilyen Dyck-szó például $n = 4$-re: 00101101.

4.34. tétel.

$$C_n = \frac{1}{n+1}\binom{2n}{n}, \quad n \geq 0$$

Bizonyítás. ([69]) Tekintsük az m darab 1-ből és k darab 0-ból álló összes szót. Ezek ismétléses permutációk, és számuk

$$P_{m,k} = \frac{(m+k)!}{m!k!} = \binom{m+k}{m}.$$

Nevezzük *jónak* azokat a szavakat, amelyekben balról jobbra haladva egyetlen helyen sem haladja meg az 1-esek száma a 0-két, és legyenek *rosszak*, amelyekre ez nem áll. Jó szavak esetén nyilván $m \leq k$ kell, hogy legyen. Ha $m = k$, akkor a jó szavak éppen Dyck-szavak. Számoljuk meg a rossz szavakat.

Vegyünk egy olyan x szót, amelyben m darab 1 és k darab 0 van, és amely egy adott $2i+1$ helyen elromlik, azaz a $2i$ helyig ugyanannyi 0 van mint 1, és előtte egyetlen helyig sincs több 1, mint 0. Ha most elébe teszünk egy 0-t, akkor a $0x$ szó első $2i$ helye jó szót képez, és összesen m darab 1 és $(k+1)$ darab 0 van benne, és az első $2i+2$ helyen az 1-esek és 0-k száma megegyezik. Cseréljük fel a $0x$ első $2i+2$ helyén a 0-kat és 1-eket, legyen ez $1x'$, ekkor az x'-ben $(m-1)$ 1-es és $(k+1)$ 0-s van. Tehát egy rossz szó ilyen alakú szóhoz vezetett.

[4] Eugène Charles Catalan (1814–1894) francia matematikusról. A Dyck-szavakat is nevezhetnénk Catalan-szavaknak

Fordítva, minden $1x$ alakú szó, amelyben m darab 1 és $(k+1)$ darab 0 van, egy rossz szóhoz vezet a következőképpen. Mivel $m \leq k$, ennek a szónak egy kezdőszeletében ugyanannyi 1 van, mint 0. Cseréljük fel ebben a kezdőszeletben az 1-eseket és 0-sokat, majd hagyjuk el az első 0-t, ekkor egy rossz szóhoz jutunk.

Tehát a rossz szavak száma egyenlő az $(m-1)$ darab 1-est és $(k+1)$ darab 0-t tartalmazó ismétléses permutációk számával, azaz

$$P_{m-1,k+1} = \frac{(m+k)!}{(m-1)!(k+1)!} = \binom{m+k}{m-1}.$$

Innen a jó szavak száma

$$P_{m,k} - P_{m-1,k+1} = \binom{m+k}{m} - \binom{m+k}{m-1} = \frac{k-m+1}{k+1}\binom{m+k}{m}.$$

Ha $m = k$, akkor $C_n = \dfrac{1}{n+1}\binom{2n}{n}$. □

Algoritmus Dyck-szavak generálására

Az algoritmus alapötlete az, hogy egy Dyck-szóban az első 10 szekvenciát 01-re cseréljük, és ezáltal újabb Dyck-szót kapunk. A következő eljárásokat használjuk.

A KERES(x,i) függvényeljárás az x-ben a i-edik pozíciótól kezdődően megkeresi az első 10 szekvenciát, és visszaadja annak a pozícióját. Ha nincs ilyen szekvencia, akkor a visszatérített érték 0 lesz.

```
KERES(x, i)
j := i
while j < length(x)
      do if x_j = 1 és x_{j+1} = 0
            then return j
            else j := j + 1
return 0
```

A CSERÉL(x,i) eljárás felcseréli x_i-t x_{i+1}-gyel (ezzel cseréljük ki 10-t 01-re)

```
CSERÉL(x, i)
z     := x_i
x_i   := x_{i+1}
x_{i+1} := z
```

A DYCK-SZÓ(x,k) eljárás az x Dyck-szó k-adik pozíciójától kezdődően generál újabb Dyck-szavakat.

```
DYCK-SZÓ(x,k)
i := k
while i < length(x)
      do j := KERES(x,i)
      if j > 0
        then y := CSERÉL(x, j)
             írd y
             DYCK-SZÓ(y, j − 1)
             i := j + 2
```

Az eljárás hívása: DYCK-SZÓ$(x,1)$, ahol $x = 0101\ldots01$

Példa. Ha kezdetben $x = 01010101$, akkor az eredmény:

```
01010101
00110101
00101101
00011101
00011011
00010111
00001111
00101011
00100111
00110011
01001101
01001011
01000111
01010011
```

4.5.7. Catalan-számok

A $C_n = \dfrac{1}{n+1}\binom{2n}{n}$ Catalan-számoknak nagyon sokféle alkalmazása van. Ezek a számok nemcsak a Dyck-szavak számát jelentik, hanem sok más egyebet is. Lássunk ezek közül néhányat!

Adott n-re a C_n Catalan-szám

- az n-csúcsú bináris fák száma,
- azon módok száma, ahányféleképpen lehet zárójelezni $n+1$, adott sorrendű számot, hogy kettesével összeszorozzuk őket,
- az n műveletet és $n+1$ operandust tartalmazó (fordított) lengyel alakban felírt helyes kifejezések száma,
- egy rács $(0,0)$ és (n,n) pontjai között húzható, főátlót át nem lépő, csak vízszintes és függőleges rácséleken haladó utak száma,

- a sík $2n$ pontját összekötő, egymást nem metsző szakaszok száma,
- azon $(x_1, x_2, \ldots, x_{2n})$ sorozatok száma, amelyekre $x_i \in \{1, -1\}$ és $x_1 \geq 0$, $x_1 + x_2 \geq 0$, $\ldots$, $x_1 + x_2 + \cdots + x_{2n-1} \geq 0$, $x_1 + x_2 + \cdots + +x_{2n} = 0$,
- egy $n+2$ csúcsú sokszög n háromszögre való felosztásainak száma.

Ezeket könnyen lehet bizonyítani, ha minden esetben megadunk egy olyan módot, amellyel a fenti objektumokat Dyck-szavakkal kódoljuk.

A Catalan-számokra többféle rekurzív képlet létezik. Például:

$$C_{n+1} = C_0 C_n + C_1 C_{n-1} + \cdots + C_n C_0, \text{ ha } n \geq 0,$$

ahol $C_0 = 1$.

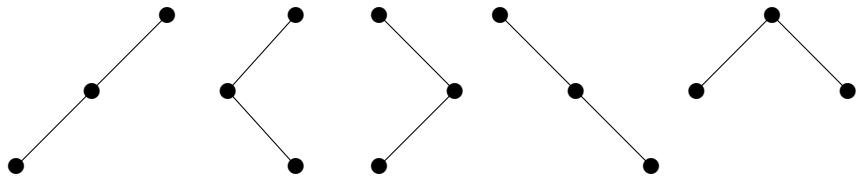
Ugyanakkor: $(n+2)C_{n+1} = (4n+2)C_n$, ha $n \geq 0$ (és $C_0 = 1$).

A C_n számok generátorfüggvénye:

$$\sum_{n \geq 0} C_n x^n = \frac{1 - \sqrt{1-4x}}{2x}.$$

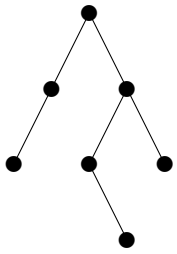
Bináris fák kódolása

A gyökérből kiindulva, előbb a bal, majd a jobb oldali részfát kódoljuk. Ha egy csúcsból kiindulva mindkét leszármazott létezik, akkor a bal oldali él kódja 00, a jobb élé pedig 11; egy bal oldali él kódja 01, és egy jobb oldali él kódja 10, amennyiben hiányzik az él párja. A kapott kód elejére 0-t, a végére pedig 1-et teszünk. Az így kapott szó Dyck-szó. Egy n csúcsú bináris fa kódja egy $2n$ hosszúságú Dyck-szó. Az alábbi 3-csúcsú bináris fa kódja:



0 01 01 1 0 01 10 1 0 10 01 1 0 10 10 1 0 00 11 1

Egy bonyolultabb példa:



0 00 01 11 00 10 11 1

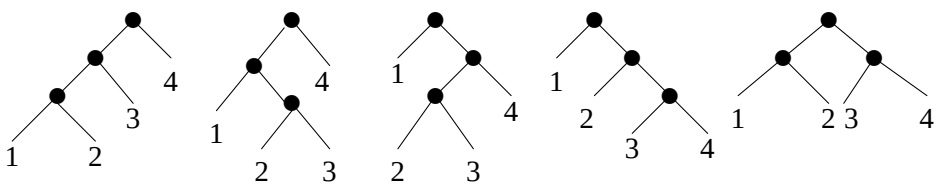
Bináris fa kódolási algoritmusa

BINÁRIS-FA-KÓDOLÁS(B)
Legyen B-ben B_L a bal, B_R pedig a jobb oldali részfa
if $B_L \neq \emptyset$ és $B_R = \emptyset$
  then írd 01
    BINÁRIS-FA-KÓDOLÁS(B_L)
if $B_L = \emptyset$ és $B_R \neq \emptyset$
  then írd 10
    BINÁRIS-FA-KÓDOLÁS(B_R)
if $B_L \neq \emptyset$ és $B_R \neq \emptyset$
  then írd 00
    BINÁRIS-FA-KÓDOLÁS(B_L)
    írd 11
    BINÁRIS-FA-KÓDOLÁS(B_R)

Az eljárás hívása
írd 0
BINÁRIS-FA-KÓDOLÁS(B)
írd 1

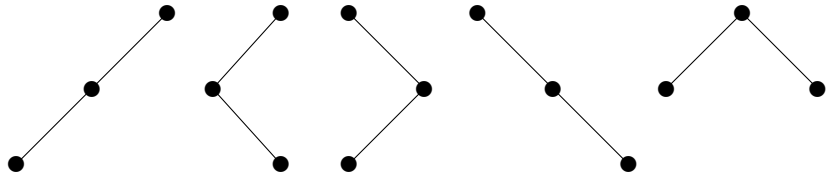
Szorzat kódolása

A szorzat kódolására először hozzárendelünk az n szám egy adott szorzási módjához egy bináris fát a következőképpen: ha a-t szorozzuk b-vel, akkor ez a bináris fa egy részfájának felel meg, amelynek a gyökere a szorzási művelet, a két részfája pedig a két operandus. Az eredmény egy reguláris bináris fa (minden belső csúcsnak két leszármazottja van). Aztán kitöröljük a fa leveleit és az így kapott bináris fát kódoljuk. Például $n = 4$ esetében a következő szorzási módok lehetnek:



(((1 2) 3) 4) ((1 (2 3)) 4) (1 ((2 3) 4)) (1 (2 (3 4))) ((1 2) (3 4))

Miután kitöröljük a leveleket, az eredmény:



Fordított lengyel forma kódolása

Minden operandus kódja 0, minden műveleté pedig 1, majd 1-et írunk a végére. Például az $abc\times d\times\times$ kifejezés — amely az $(a\times((b\times c)\times d))$ kifejezés lengyel formája — kódja 00010111.

Sorozatok kódolása

A kódolás egyszerű: az 1-et 0-val, a -1-et pedig 1-gyel kódoljuk. Ha $n=3$, akkor a következő kódolások lehetségesek:

`1, 1, 1, -1, -1, -1` kódja: 000111

`1, 1, -1, 1, -1, -1` kódja: 001011

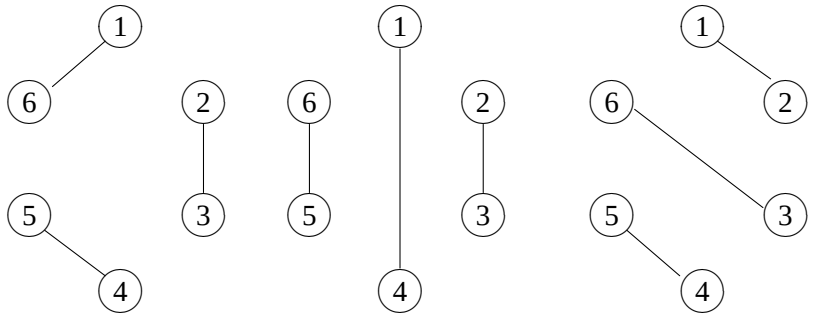
`1, 1, -1, -1, 1, -1` kódja: 001101

`1, -1, 1, 1, -1, -1` kódja: 010011

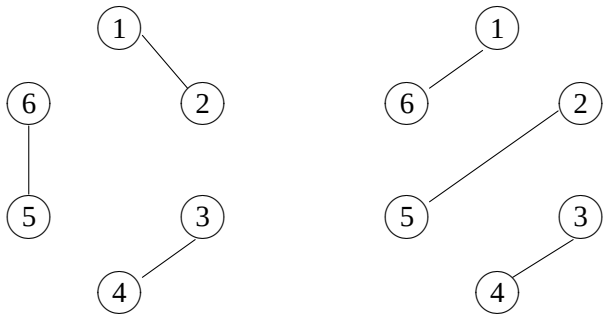
`1, -1, 1, -1, 1, -1` kódja: 010101

Szakaszok kódolása

Ha a síkban $2n$ pontot n szakasszal kötjük össze úgy, hogy nem metszik egymást, akkor a következő kódolást használjuk: megszámozzuk a pontokat 1-től $2n$-ig, majd egy szakaszra, amely az i és j ($i<j$) pontokat köti össze, a kód i-dik pozíciójába 0-t, a j-dikbe pedig 1-et írunk. $n=3$ esetében a következő ábrák és kódok lehetségesek:



001011 001101 010011

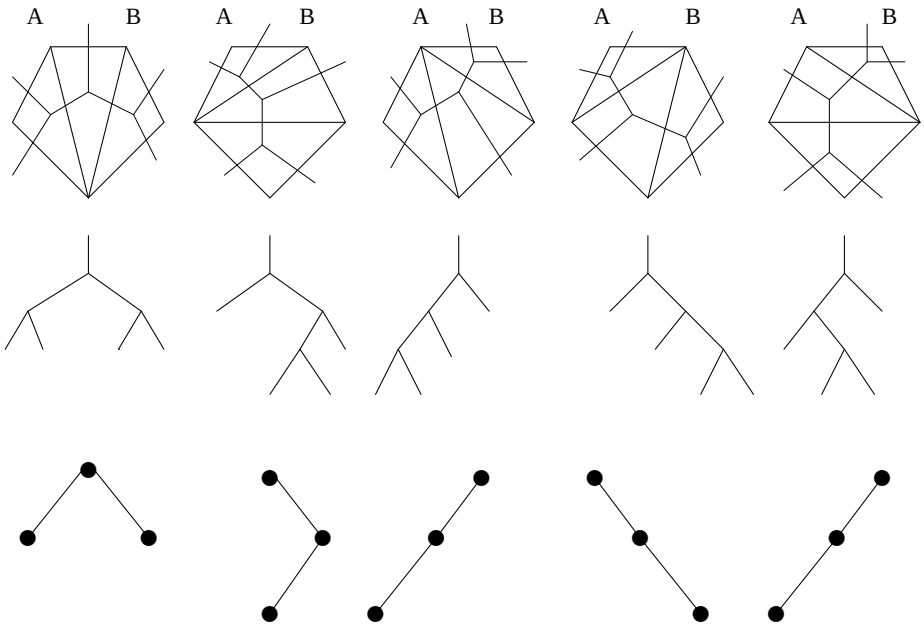


010101 000111

Sokszögek felbontásának kódolása

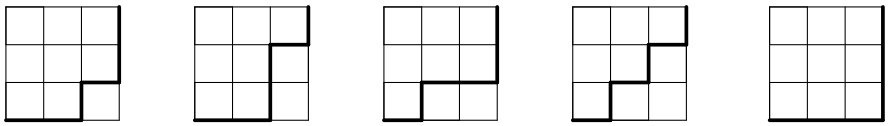
Miután felosztottuk a sokszöget háromszögekre, hozzárendelünk egy bináris fát a következőképpen. Minden háromszögben felveszünk egy csúcsot, majd a sokszög minden oldala mellett kívül is egyet-egyet. Egy éllel kötünk össze két csúcsot, ha azok egy oldal (a sokszög vagy a háromszög oldala) két oldalán találhatók. Az így kapott fában kiválasztunk egy (kijelölt oldalnak megfelelő) gyökeret. Az így kapott bináris fákból kitöröljük a leveleket, majd kódoljuk őket.

$n = 3$ esetében ötszöget $(n+2)$ kell felosztanunk háromszögekre. A példában az *AB* oldalt választjuk a gyökér megjelölésére.



Rácsutak kódolása

A kódolás egyszerű, 0-t írunk egy vízszintes egységnyi szakasz esetében, és 1 egy vertikális egységnyi szakasz esetében. Egy 3×3 rács esetében a kódolások a következők:



001011 001101 010011 010101 000111

Visszakódolás

A Dyck-szavak visszakódolása a legtöbb esetben nyilvánvaló. A visszakódolást a bináris fák esetében mutatjuk be. Példaként a 00010111 Dyck-szót használjuk.

Ha egy Dyck-szónak megfelelő bináris fát keressük, először kitöröljük a szó első és utolsó jegyét. A 00 szekvencia azt jelenti, hogy egy bal oldali élt rajzolunk, amelynek lesz egy jobb oldali megfelelője (egy veremben megőrizzük a pozícióját), következik egy 10 szekvencia, amely egy jobb oldali élnek felel meg, majd 11, amely a 00 élnek megfelelő jobb oldali él. A megfelelő fa az alábbi ábrán látható (a) ábra).

Dyck-szó visszakódolása bináris fává

Ha egy aktuális csúcsból élt húzunk egy másik csúcsba, akkor ez utóbbi aktuális csúccsá válik.

VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)
olvasd ab
töröld ab-t c-ből
if $ab = 01$
  then rajzolj egy bal élt az aktuális csúcsból
  VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)
if $ab = 10$
  then rajzolj egy jobb élt az aktuális csúcsból
  VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)
if $ab = 00$
  írd be a verembe az aktuális csúcs helyét
  then rajzolj egy bal élt az aktuális csúcsból
  VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)
if $ab = 11$
  olvasd ki a veremből az aktuális csúcs helyét, ez lesz aktuális csúcs
  then rajzolj egy jobb élt az aktuális csúcsból
  VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)

Az eljárás hívása:

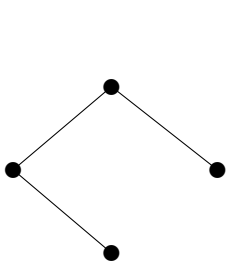
kitöröljük c Dyck-szóból az első 0-t és utolsó 1-et.
VISSZAKÓDOLÁS-BINÁRIS-FÁVÁ(c)

Ha szakaszokat szeretnénk visszakapni, akkor először megkeressük az első 01 szekvenciát, megrajzoljuk a neki megfelelő szakaszt (a 3 és 4 pontok között), majd kitöröljük ezeket a szóból, és folytatjuk újabb 01 szekvencia keresésével (megőrizve az eredeti pozíciókat). Eredmény-l a b) ábrán levő szakaszokat kapjuk.

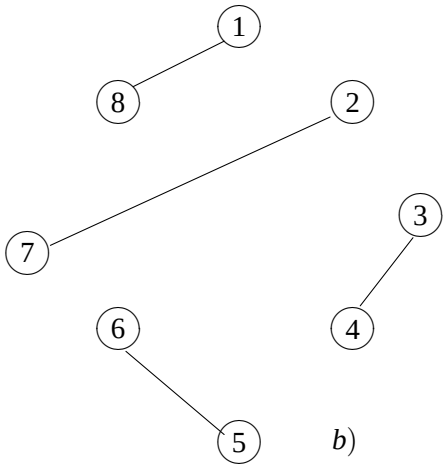
Ha szorzatot szeretnénk kapni, akkor előbb felépítjük a bináris fát (ld. a). ábra), majd kipótoljuk újabb csúcsokkal úgy, hogy minden csúcsnak pontosan két leszármazottja legyen. Az eredmény a c). ábrán látható.

A rácsban az utat egyből felírhatjuk, hiszen a 0 egy vízszintes, az 1 pedig egy függőleges szakasznak felel meg (ld. d) ábra).

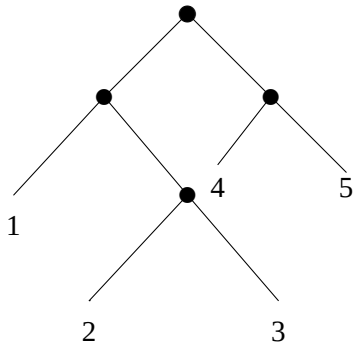
A sorozatok és sokszögek visszakódolása szintén azonnali.



a)

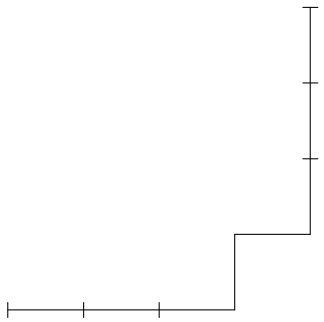


b)



((1 (2 3)) (4 5))

c)



d)

A Catalan-számokat lehet általánosítani [19]. Értelmezhetjük például a $C_n^{(k)}$ számokat, amelyek a $(0,0,\ldots,0)$ és $(n,n,\ldots,n)$ közötti utak száma egy k-dimenziós rácsban, ha $(x_1,x_2,\ldots,x_k)$ pontra igaz, hogy $x_1 \geq x_2 \geq \ldots \geq x_k$. Ennek a számnak az értéke:

$$C_n^{(k)} = \frac{1}{\binom{n+1}{1}} \cdot \frac{1}{\binom{n+2}{2}} \cdots \frac{1}{\binom{n+k-1}{k-1}} \cdot \frac{(kn)!}{n!n!\cdots n!},$$

(itt $n!$ k-szor szerepel). Ha $k = 2$, akkor visszakapjuk az ismert Catalan-számokat.

Feladatok

4.1. Tekintsük a $\sigma(0) = 01$, $\sigma(1) = 02$, $\sigma(2) = 0$ homomorfizmust, és 0-ból indulunk a szavak képzésében. Legyen r az a végtelen szó, amely ennek a homomorfizmusnak

a fixpontja, azaz $\sigma(r) = r$. Bizonyítsuk be, hogy $f_r(n) = 2n+1$.

4.2. Legyenek adottak a következő szavak: $w_0 = 0$ és $w_1 = 12$, és a $w_n = w_{n-1}^2 w_{n-2}$ szabály, ha $n \geq 2$. Bizonyítsuk be, hogy ha $w = \lim_{n\to\infty} w_n$ akkor $f_w(n) = n+2$.

4.3. Adott a $\sigma(0) = 0010,\ \sigma(1) = 1$ homomorfizmus, és 0-val kezdjük a szavak generálását. Ha $s = \sigma(s)$ (Chacon-szó), bizonyítsuk be, hogy $f_s(n) = 2n-1$ ha $n \geq 2$.

4.4. Bizonyítsuk be, hogy tetszőleges u Sturm-szóra a balról speciális n hosszúságú részszavak száma megegyezik a jobbról speciális n hosszúságú részszavak számával és ez a szám éppen $f_u(n+1) - f_u(n)$.

4.5. Bizonyítsuk be, hogy a Sturm-szavak esetében minden bispeciális részszó palindrom szó (azonos a tükörképével), és bármely balról speciális részszó tükörképe jobbról speciális.

4.6. Bizonyítsuk be, hogy ha a

$$c = 0.1.10.11.100.101.110.111.1000.1001.1010.1011.1100\ldots$$

Champernowne-szó n hosszúságú palindrom részszavait $pal_c(n)$-nel jelöljük, akkor

$$pal_c(n) = 2^{\lfloor \frac{n}{2} \rfloor + \varepsilon}$$

ahol

$$\varepsilon = \begin{cases} 0, & \text{ha } n \text{ páros} \\ 1, & \text{ha } n \text{ páratlan} \end{cases}$$

4.7. Bizonyítsuk be, hogy a

$$p = 01001100011100001111\ldots \underbrace{0\ldots0}_{n}\underbrace{1\ldots1}_{n}\ldots$$

hatványszó esetében a palindrom részszavak száma

$$pal_p(n) = 2\left\lfloor \frac{n}{3} \right\rfloor + 1 + \varepsilon$$

ahol

$$\varepsilon = \begin{cases} 0, & \text{if } n \text{ osztható 3-mal} \\ 1, & \text{különben} \end{cases}$$

4.8. Bizonyítsuk be, hogy az olyan monoton növekvő $f : \{1,2,\ldots,n\} \longrightarrow \{1,2,\ldots,n\}$ függvények száma, amelyekre $f(k) < k$ $(1 \leq k \leq n)$, egyenlő a C_n Catalan-számmal.

4.9. Legyen $H(n)$ egy olyan $n \times n$-es mátrix, amelynek (i,j) eleme egyenlő a C_{i+j}

Catalan-számmal minden $0 \leq i \leq n-1,\ 0 \leq j \leq n-1$ indexre. (Hankel-mátrix). Bizonyítsuk be, hogy a $H(n)$ mátrix determinánsa bármilyen $n > 1$-re egyenlő 1-gyel.

4.10. Bizonyítsuk be, hogy a $C_n,\ n > 0$ Catalan-szám akkor és csakis akkor páratlan ha az n Mersenn-szám ($n = 2^p - 1,\ p \in \mathbb{P}$).

4.11. Bizonyítsuk be, hogy a Catalan-számok között csak két prímszám van, a C_2 és C_3.

5.

Euklidészi algoritmusok

5.1. Euklidészi algoritmusok

5.1. értelmezés. *Az a és b természetes számok* ***legnagyobb közös osztójának*** *nevezzük azt a d természetes számot, amely teljesíti a következő feltételeket:*
a) $d \mid a$ *és* $d \mid b$
b) *d a legnagyobb olyan természetes szám, amely teljesíti az a*) *feltételt.*

Jelölés. $(a,b) = d$.

Megjegyzés. Az 3.9 definícióbeli b) tulajdonság egyenértékű a következő tulajdonsággal:
b$_1$)

$$d_1 \mid a \text{ és } d_1 \mid b \Longrightarrow d_1 \mid d.$$

Valóban, mivel d, $d_1 \in \mathbb{N}^*$, a $d_1 \mid d$ azt jelenti, hogy $d_1 \leq d$, vagyis d a legnagyobb olyan természetes szám, amely teljesíti az **a)** feltételt.
Bármely két 0-tól különböző természetes számnak van legnagyobb közös osztója és ezt kiszámíthatjuk az euklidészi algoritmus segítségével:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\
&\dots \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}, \quad (r_{n+1} = 0).
\end{aligned} \tag{5.1}$$

Először osztjuk az a-t a b-vel, majd a b-t az r_1-gyel, r_1-et az r_2-vel, és addig folytatjuk az osztást, míg valamelyik maradék 0 lesz (a mi esetünkben az r_{n+1}). Ez szükségképpen bekövetkezik, mivel az $(r_n)_{n\in\mathbb{N}^*}$ egy szigorúan csökkenő természetes számokból álló sorozat, amelynek a legnagyobb tagja kisebb mint b.

Az a és b természetes számok legnagyobb közös osztója az r_n (az utolsó 0-tól különböző maradék). Valóban, $r_n \mid r_{n-1}$ és visszafelé haladva a felírt összefüggésekből következik, hogy $r_n \mid a$ és $r_n \mid b$. Ezzel igazoltuk az **a)** tulajdonságot és, ha feltételezzük, hogy $r \mid a$ és $r \mid b$ és elölről haladunk végig az összefüggéseken, azt kapjuk, hogy $r \mid r_n$ és így bebizonyítottuk a $\mathbf{b_1}$**)** tulajdonságot is.

Az így felírt algoritmus $n+1$ osztási lépésből áll. A lépések számára bevezetjük a következő jelölést:

5.2. értelmezés. *Az a és b természetes számokra az euklidészi algoritmusban elvégzett osztások számát jelöljük $E(a,b)$-vel.*

Példa. Számítsuk ki az euklidészi algoritmus segítségével $(1626,954)$ és $E(1626,954)$ értékét.

$$\begin{aligned} 1626 &= 954\cdot 1+672\\ 954 &= 672\cdot 1+282\\ 672 &= 282\cdot 2+108\\ 282 &= 108\cdot 2+66\\ 108 &= 66\cdot 1+24\\ 66 &= 24\cdot 2+18\\ 24 &= 18\cdot 1+6\\ 18 &= 6\cdot 3+0 \end{aligned}$$

Tehát $(1626,954)=6$ és $E(1626,954)=8$.

Tehát s fentiek alapján a következő algoritmust adhatjuk meg a legnagyobb közös osztó kiszámítására:

EUKLIDÉSZI$((a,b))$:
if $b=0$
  then
    return (a)
  else
    return EUKLIDÉSZI$((b, a \bmod b))$

Ha ismerjük a lépések számát az euklidészi algoritmusban, akkor az eredeti természetes számok nagyságára érvényes a következő eredmény:

5.3. tétel. *Adottak az $a>b>0$ természetes számok, amelyekre $E(a,b)=n$. Az a-ra és b-re érvényes a következő egyenlőtlenség:*

$$a \geq F_{n+2}, \quad b \geq F_{n+1},$$

ahol F_n a Fibonacci sorozat n-edik tagja.

Bizonyítás. Legyen $a = r_0$, $b = r_1$ és az euklidészi algoritmus lépései:

$$\begin{aligned}
r_0 &= r_1q_1 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, \quad 0 < r_3 < r_2 \\
r_2 &= r_3q_3 + r_4, \quad 0 < r_4 < r_3 \\
&\dots \\
r_{n-3} &= r_{n-2}q_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_n, \quad (r_{n+1} = 0).
\end{aligned}$$

Indukcióval bizonyítjuk, hogy $r_0 \geq F_{n+1}$ és $r_1 \geq F_{n+1}$.
$n = 1$ azt jelenti, hogy az euklidészi algoritmus egy lépésből áll,

$$r_0 = q_0r_1.$$

Mivel $r_0 > r_1$, a legkisebb értékek $r_0 = 2$ és $r_1 = 1$.
Feltételezzük, hogy a tétel állítása igaz $i < n$-re. Az első lépésben

$$r_0 = q_1r_1 + r_2,$$

de $E(u_1,u_2) = n-1$, így az indukciós feltevés alapján

$$r_1 \geq F_{n+1} \text{ és } r_2 \geq F_n.$$

Innen következik, hogy

$$r_0 = q_1r_1 + r_2 \geq r_1 + r_2 \geq F_{n+1} + F_n = F_{n+2}.$$

□

Ahhoz, hogy a „legkisebb” (a,b) számpárt megtaláljuk, bevezetjük a következő rendezést:

5.4. értelmezés. *Az (a,b) számpár **lexikografikusan kisebb**, mint az (a',b') számpár, ha*

$$a < a'$$

vagy

$$a = a' \text{ és } b < b'.$$

A lexikografikus rendezés segítségével a 5.3 tételből a következő pontosabb eredményt fogalmazhatjuk meg.

5.5. tétel (Lamé, 1844). *Tudva, hogy $a > b > 0$, az $(a,b) = (F_{n+2},F_{n+1})$, a lexikografikusan legkisebb (a,b) számpár, amelyre $E(a,b) = n$.*

Ha egy adott (a,b) számpárra akarjuk meghatározni a lépések számát, akkor a következő eredményt írhatjuk fel.

5.6. tétel. *Az $a > b > 0$ természetes számokra*

$$E(a,b) < c_1 \log a + c_2 - 2 + c_3 \frac{1}{a},$$

$$E(a,b) < c_1 \log b + c_2 - 1 + c_3 \frac{1}{b},$$

ahol

$$c_1 = \frac{1}{\log \alpha},\ c_2 = \frac{\log \sqrt{5}}{\log \alpha},\ c_3 = \frac{1}{\sqrt{5}\log \alpha}.$$

$$\alpha = \frac{1+\sqrt{5}}{2},\ \beta = \frac{1-\sqrt{5}}{2}.$$

Bizonyítás. A Binét-formula alapján:

$$F_{n+2} = \frac{1}{\sqrt{5}}(\alpha^{n+2} - \beta^{n+2}).$$

Feltételezzük, hogy $E(a,b) = n$, ahonnan a 5.3 tétel alapján $a \geq F_{n+2}$. Mivel $|\beta| < 1$

$$a \geq \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}} > \frac{\alpha^{n+2} - 1}{\sqrt{5}},$$

$$(n+2)\log \alpha \leq \log(1 + a\sqrt{5}).$$

De

$$\log(x+1) = \log x + \log\left(1 + \frac{1}{x}\right) < \log x + \frac{1}{x}, \quad \forall x > 0,$$

ahonnan $x = a\sqrt{5}$-re

$$(n+2)\log \alpha < \log\left(a\sqrt{5}\right) + \frac{1}{a\sqrt{5}},$$

$$n = E(a,b) < c_1 \log a + c_2 + c_3 \frac{1}{a}.$$

Hasonlóan bizonyítható a $b \geq F_{n+1}$ egyenlőtlenségből az

$$E(a,b) < c_1 \log b + c_2 - 1 + c_3 \frac{1}{b}$$

egyenlőtlenség. □

Az $E(a,b)$ átlagértékére érvényes a következő aszimptotikus képlet, amelyet Porter bizonyított 1975-ben [61].

5.7. tétel. *$n \geq 1$-re*

$$\sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} E(n,k) = \frac{12\log 2}{\pi^2}\log n\varphi(n) + C\varphi(n) + O\left(\varphi(n)n^{-\frac{1}{6}+\varepsilon}\right),$$

ahol C egy n-től független állandó és $\varepsilon > 0$.

A legnagyobb közös osztó egy fontos tulajdonsága, hogy felírható a számok lineáris kombinációjaként. A következőkben először bizonyítjuk az euklidészi algoritmus segítségével, majd ezt a bizonyítást átírjuk mátrixok segítségével és erre az átírásra szerkesztünk egy algoritmust.

5.8. tétel. *Ha $a,b \in \mathbb{N}^*$, akkor az a és b legnagyobb közös osztója a következőképpen írható fel:*

$$(a,b) = ax + by,$$

ahol x és y alkalmasan kiválasztott egész számok.

Bizonyítás. A 5.1 euklidészi algoritmusból következik, hogy $(a,b) = r_n$. Az euklideszi algoritmus összefüggéseit használva, fordított sorrendben azt kapjuk, hogy

$$r_n = (a,b) = r_{n-2} - r_{n-1}\cdot q_n = r_{n-1}\cdot x_1 + r_{n-2}\cdot y_1.$$

Mivel $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, következik, hogy

$$(a,b) = r_{n-2}(1+q_{n-1}q_n) - r_{n-3}\cdot q_n = r_{n-2}\cdot x_2 + r_{n-3}\cdot y_2.$$

A behelyettesítést folytatva, n lépés után kapjuk, hogy

$$(a,b) = x_n a + y_n b,$$

ahol $x_n = x$ és $y_n = y$.

□

Legyen $r_0 = a$ és $r_1 = b$. Ha az euklidészi algoritmus lépéseit mátrixos alakban írjuk, akkor:

$$\begin{aligned}
\begin{bmatrix} r_0 \\ r_1 \end{bmatrix} &= \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \\
\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} &= \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_2 \\ r_3 \end{bmatrix} \\
&\vdots \\
\begin{bmatrix} r_{n-2} \\ r_{n-1} \end{bmatrix} &= \begin{bmatrix} q_{n-2} & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} \\
\begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} &= \begin{bmatrix} q_{n-1} & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_n \\ r_{n+1} \end{bmatrix},
\end{aligned}$$

ahol $d = r_n = (r_0, r_1)$ és $r_{n+1} = 0$.
A fenti egyenleteket összeszorozva:

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

Legyen

$$M_k := \begin{bmatrix} b_k & c_k \\ d_k & e_k \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix}.$$

Így írhatjuk, hogy

$$M_{n-1}^{-1} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

Mivel $\det M_{n-1} = (-1)^n$,

$$M_{n-1}^{-1} = (-1)^n \begin{bmatrix} e_{n-1} & -c_{n-1} \\ -d_{n-1} & b_{n-1} \end{bmatrix}.$$

Tehát

$$e_{n-1}a - c_{n-1}b = (-1)^n d,$$

vagyis $x = (-1)^{n-1}e_{n-1}$, $y = (-1)^{n+1}c_{n-1}$.
A fenti leíráshoz tartozó algoritmus a következő:

KITERJESZTETT EUKLIDÉSZI (a,b)
az (a,b) kiszámítása és azon x,y meghatározása, amelyre $ax+by=d$
$M =: \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$n := 0$
while $(b \neq 0)$
  do $q := \lfloor \frac{a}{b} \rfloor$
    $M := M \begin{bmatrix} q & 1 \\ 1 & 0 \end{bmatrix}$
    $a := b$, $b := a - qb$
    $n := n + 1$
return $(d := a,\ x := (-1)^n M_{22},\ y := (-1)^{n+1} M_{12})$,

ahol

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix}.$$

J. Stein egy olyan nem euklidészi algoritmust szerkesztett, amely a következő tulajdonságokon alapul:

1. Ha a és b páros természetes számok, akkor

$$(a,b) = 2\left(\frac{a}{2},\frac{b}{2}\right).$$

2. Ha a páros és b páratlan természetes szám, akkor

$$(a,b) = \left(\frac{a}{2},b\right).$$

3. Ha a és b páratlan természetes számok, akkor

$$(a,b) = \left(\frac{|a-b|}{2},b\right).$$

BINÁRIS-LNKO (a,b)
$g := 1$
while $(a \bmod 2 = 0)$ **and** $(b \bmod 2 = 0)$
    do $a := \frac{a}{2}$
    $b := \frac{b}{2}$
    $g := 2g$
while $(a \neq 0)$
    do if $(a \bmod 2 = 0)$
        then $a := \frac{a}{2}$
      else if $(b \bmod 2 = 0)$
            then $b := \frac{b}{2}$
      else $t := \frac{|a-b|}{2}$
          if $a \geq b$
            then $a := t$
            else $b := t$
return $(g \cdot b)$

5.2. Lánctörtek

5.9. értelmezés. *Az*

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cdots + \cfrac{1}{x_n}}}$$

kifejezést ***lánctörtnek*** *nevezzük.*

Jelölés. A fenti lánctörtet a következőképpen jelölhetjük:

$$[x_0, x_1, \ldots, x_n].$$

Ebben a felírásban az $x_i \in \mathbb{Z}$.

Ha az x_0 egész szám és x_i, $i \geq 1$ természetes számok, akkor ***egyszerű lánctörtről*** beszélünk.

Ha adott egy x (nem egész) valós szám, akkor a következőképpen szerkeszthetjük meg a hozzá tartozó lánctörtet. Legyen x_0 az x valós szám alsó egészrésze, $x_0 = \lfloor x \rfloor$ és legyen

$$x = x_0 + \frac{1}{\alpha_1}.$$

Az eljárást folytatva

$$\alpha_k = x_k + \frac{1}{\alpha_{k+1}},$$

vagy

$$\alpha_{k+1} = \frac{1}{x_k - \alpha_k}$$

adódik, ahol $x_k = \lfloor x \rfloor$.

Ha x irracionális szám, akkor α_k irracionális és akkor az előbbi lánctörtbe fejtés soha sem áll le, és

$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots + \cfrac{1}{x_n + \cfrac{1}{\alpha_{n+1}}}}}}.$$

Az α_n számról csak annyit tudunk, hogy $x_{n+1} \leq \alpha_{n+1} < x_{n+1} + 1$. Ezért az x irracionális számot úgy közelíthetjük, hogy az $\dfrac{1}{\alpha_{n+1}}$ tagot elhagyjuk, az így adódó racionális számot pedig $\dfrac{P_n}{Q_n}$-nel jelöljük:

$$[x_0, x_1, \ldots, x_n] = \frac{P_n}{Q_n}.$$

Ebben az esetben az is érdekel, hogy a közelítés mennyire pontos. Ennek a meghatározása érdekében szükségünk van egy lemmára.

5.10. lemma (Dirichlet). *Legyen x egy valós szám. Ekkor léteznek p, q egész számok úgy, hogy*

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Bizonyítás. Osszuk fel a $[0,1)$ intervallumot q részre:

$$I_k = \left[\frac{k}{q}, \frac{k+1}{q}\right], \quad k \in \{0,1,\ldots,q-1\}.$$

Tekintsük az

$$\{x\},\ \{2x\},\ \ldots\{(q-1)x\}$$

számokat, ahol $\{a\}$ az a szám törtrészét jelöli. Ha ezek közül valamelyik I_0-ba, vagy I_{q-1}-be esik, akkor az állítás igaz. Egyébként a skatulya elv alapján létezik olyan k, amelyre valamely $r_1 \neq r_2$-re, $\{r_1x\}, \{r_2x\} \in I_k$. Legyen

$$r_1x = s_1 + \{r_1x\},\ r_2x = s_2 + \{r_2x\},$$

ahol $s-1$ és s_2 az $r-1x$ illetve r_2x egészrésze. Így

$$|(r_1x - s_1) - (r_2x - s_2)| \leq \frac{1}{q}.$$

Ha $r_1 > r_2$, $p = s_1 - s_2$, mivel $r_1 - r_2 = q_1 < q$

$$|xq_1 - p| \leq \frac{1}{q},$$

$$\left|x - \frac{p}{q_1}\right| \leq \frac{1}{qq_1} < \frac{1}{q_1^2}.$$

□

Megjegyzés. Ha x irracionális szám, akkor végtelen sok olyan q egész létezik, amelyre alkalmas p esetén

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}.$$

A 5.10 lemmából következik, hogy az x valós szám esetén

$$|x - [x_0, x_1, \ldots x_n]| = \left|x - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}.$$

Megjegyezzük, hogy a $Q_0, Q_1, \ldots Q_n$ sorozat exponenciálisan tart a végtelenhez (létezik olyan $c > 1$ állandó, hogy $Q_n > c^n$). Így az x valós szám lánctörtekkel való közelítés hibája n növekedésével igen gyorsan csökken.
Ha az x valós szám racionális, akkor véges lánctörtet tudunk felírni

$$x = [x_0, x_1, \ldots, x_n].$$

Az x valós szám estén a következő algoritmust írhatjuk fel amellyel az $\{x_0, x_1, \ldots x_n \ldots\}$ sorozatot szerkesszük meg.

LÁNCTÖRT (x)
$i := 0$
$a_0 := x$
$x_0 := \lfloor a_0 \rfloor$
output (x_0)
while $(a_i \neq x_i)$
do $a_{i+1} := \dfrac{1}{a_i - x_i}$
$i := i + 1$
$x_i := \lfloor a_i \rfloor$
output (x_i)

Az algoritmus helyességét racionális számra bizonyítjuk.

5.11. tétel. *A* LÁNCTÖRT *(x) algoritmus akkor és csakis akkor generál egy véges* $(x_0, x_1, \ldots, x_n)$ *vektort, ha x racionális szám, és ekkor* $x = [x_0, x_1, \ldots, x_n]$.

Bizonyítás. Feltételezzük, az algoritmus az $(x_0, x_1, \ldots, x_n)$ vektort generálja, és bizonyítjuk, hogy $x = [x_0, x_1, \ldots, x_n]$, tehát racionális.

Az algoritmusból indukcióval következik, hogy

$$a_0 = [x_0, x_1, \ldots, x_{i-1}, a_i].$$

Mivel az algoritmus eredménye $(x_0, x_1, \ldots, x_n)$, $a_n = x_n$ és

$$x = a_0 = [x_0, x_1, \ldots, x_n],$$

vagyis x racionális.

Feltételezzük, hogy $x = a_0$ racionális. Indukcióval igazolható, hogy a_i racionális és feltételezzük, hogy $a_i = \frac{u_i}{u_{i+1}}$. Így

$$x_i = \lfloor a_i \rfloor,$$

$$\begin{aligned} a_{i+1} &= \frac{1}{a_i - x_i} = \frac{1}{\frac{u_i}{u_{i+1}} - \left\lfloor \frac{u_i}{u_{i+1}} \right\rfloor} = \\ &= \frac{u_{i+1}}{u_i - u_{i+1} \left\lfloor \frac{u_i}{u_{i+1}} \right\rfloor} = \\ &= \frac{u_{i+1}}{u_i \bmod u_{i+1}}. \end{aligned}$$

Ha az $\frac{u}{v}$ törtet az (u,v) számpárral jelöljük akkor az a_{i+1}-et az a_i-ből a következőképpen kapjuk meg:

$$(u_i,u_{i+1}) \to (u_{i+1},u_i \bmod u_{i+1}).$$

Ez pontosan az euklidészi algoritmus egy lépését jelenti, mivel az euklidészi algoritmus véges lépésből áll, ez;rt LÁNCTÖRT (x) algoritmus is véges lépésből áll, és akkor lesz vége, ha $u_i \bmod u_{i+1} = 0$, ahonnan

$$\frac{u_i}{u_{i+1}} = \left\lfloor \frac{u_i}{u_{i+1}} \right\rfloor,$$

ami annyit jelent, hogy $a_i = x_i$ a befejezés feltétele. □

Megjegyzés. Az LÁNCTÖRT (x) algoritmus utolsó lépésében az $a_n \geq 2$, ha $n \geq 1$.

A bizonyítás alapján a következő tételt jelenthetjük ki.

5.12. tétel. LÁNCTÖRT *(x)-ben* $x = (x_0,x_1,\ldots,x_{n-1})$ *akkor és csakis akkor, ha az* (a,b) *euklidészi algoritmusa n lépésből áll (*$E(a,b) = n$*).*

A következőkben a legkisebb maradékos euklidészi algoritmussal foglalkozzunk. Az euklidészi algoritmusban az (a,b) számpárt a $(b,a \bmod b)$ számpárral helyettesítjük. Ha a maradék függvényében az (a,b) számpár helyett a

$$\begin{array}{lll} (b,a \bmod b) & \text{ha} & |a \bmod b| \leq \frac{|b|}{2} \\ (b,a \bmod b-b) & \text{ha} & |a \bmod b| > \frac{|b|}{2} \end{array}$$

számpárokat írjuk, akkor a legkisebb maradékos algoritmust kapjuk.
Bevezetjük a következő egész függvényt:

$$\rho(x) := \left\lceil x - \frac{1}{2} \right\rceil$$

és a

$$a \operatorname{rmod} n := \begin{cases} a, & \text{ha } n = 0 \\ a - \rho\left(\frac{a}{n}\right), & \text{ha } n \neq 0. \end{cases}$$

„maradék” függvényt. Ennek a függvénynek a segítségével az euklidészi algoritmusnak a következő változatát írhatjuk fel:

LEGKISEBB MARADÉKOS-EUKLIDÉSZI$((a,b))$:
if $b = 0$
  then
    return (a)
  else
    return LEGKISEBB MARADÉKOS-EUKLIDÉSZI$((b,a \operatorname{rmod} b))$

Mivel az előbbiek szerint az euklidészi algoritmus szoros kapcsolatban van a lánctörtekkel, felmerül a kérdés, hogy az előbbi észrevétellel módosítva a LÁNCTÖRT (x) algoritmust, milyen lánctörtet kapunk eredményül.

Az algoritmust legközelebbi egész lánctört algoritmusnak nevezzük és LE-LÁNCTÖRT (x)-szel jelöljük, és az alsó egészrész helyett a $ro(x)$ egész függvényt használjuk.

LE-LÁNCTÖRT (x)
$i := 0$
$a_0 := x$
$x_0 := ro(a_0)$
output (x_0)
while $(a_i \neq x_i)$
do $a_{i+1} := \dfrac{1}{a_i - x_i}$
$i := i+1$
$x_i := ro(a_i)$
output (x_i)

Például, ha kiszámítjuk $\dfrac{7}{19}$-et mindkét algoritmussal akkor

$$\text{LÁNCTÖRT}\left(\frac{7}{19}\right) = (0,2,1,2,2),$$

$$0+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}$$

$$\text{LE-LÁNCTÖRT}\left(\frac{7}{16}\right) = (0,3,-4,2),$$

$$0+\cfrac{1}{3+\cfrac{1}{-4+\cfrac{1}{2}}}$$

Megjegyzés.
1. A LE-LÁNCTÖRT (x) algoritmus eredményében negatív egész számok is szerepelhetnek, ezért az eredmény nem egy egyszerű lánctört.
2. Bármely racionális szám egyértelműen írható fel véges szám] lépésben a LE-LÁNCTÖRT (x) segítségével és ha $x = [x_1, x_2, \ldots, x_n]$ akkor
a) $|x_i| \geq 2, \quad i \in \{1,2,\ldots,n\}$,
b) $x_n \neq -2$,

c) ha $x_i = -2$ valamely $i < n$ értékre, akkor $x_{i+1} \leq -2$,
d) ha $x_i = 2$ valamely $i < n$ értékre, akkor $x_{i+1} \geq 2$.

A LE-LÁNCTÖRT (x) algoritmus lépéseinek a számára bevezetjük a következő jelölést:

5.13. értelmezés. *Az a és b természetes számokra a legkisebb-egész euklidészi algoritmusban elvégzett osztások számát jelöljük $\lambda(a,b)$-vel.*

Ha ismerjük a lépések számát a LE-LÁNCTÖRT (x) algoritmusban, akkor az eredeti természetes számok nagyságára érvényes a következő eredmény:

5.14. tétel. *Adottak az $a > b > 0$ természetes számok, amelyekre $\lambda(a,b) = n$. Az a-ra és b-re érvényes a következő egyenlőtlenség:*

$$a \geq a_{n-1} + a_n, \quad b \geq a_n,$$

ahol a_n az $a_0 = 0$ és $a_1 = 1$

$$a_n = 2a_{n-1} + a_{n-2}, \quad n \geq 2,$$

rekurzív sorozat n-edik tagja.
A lexikografikusan legkisebb (a,b) számpár $(a,b) = (a_{n-1} + a_n, a_n)$.

A bizonyítás hasonló a 5.3 illetve 5.2 tételek bizonyításához.
Az (a_n) sorozat általános tagjára érvényes a következő képlet:

$$a_n = \frac{1}{2\sqrt{2}} \left((1+\sqrt{2})^n - (1-\sqrt{2})^n \right).$$

Ennek alapján, ha egy adott (a,b) számpárra akarjuk meghatározni a lépések számát, akkor a következő eredményt írhatjuk fel.

5.15. tétel. *Az $a \geq b > 0$ természetes számokra*

$$\lambda(a,b) < d_1 \log a + d_2 - 2 + d_3 \frac{1}{a},$$

ahol

$$d_1 = \frac{1}{\log \alpha} = 1.13, \; d_2 = 1 + \frac{\log(2\sqrt{2}) - \log(\alpha+1)}{\log \alpha} = 0.79,$$

$$d_3 = \frac{1}{2\sqrt{2} \log \alpha} = 0.40.$$

$$\alpha = 1 + \sqrt{2}.$$

A LE-LÁNCTÖRT (x) algoritmus azzal a tulajdonsággal rendelkezik, hogy a lépéseinek a száma kevesebb, mint minden más euklidészi algoritmusnak, így a következő eredményt fogalmazhatjuk meg:

5.16. tétel (Kroncker-Vahlen). *Az $a \geq b > 0$ természetes számokra*

$$\lambda(a,b) \leq K(a,b),$$

ahol $k(a,b)$ egy Euklidész típusú algoritmus lépéseinek a száma.

Feladatok

5.1. Tudva, hogy az a és b számokra alkalmazott euklidészi algoritmusban a hányadosok $q_0, q_1, \ldots q_{n-1}$, bizonyítsuk be, hogy

$$q_0 q_1 \cdots q_{n-1} \leq a,$$

$$q_1 \cdots q_{n-1} \leq b.$$

5.2. Bizonyítsuk be, hogy nem létezik olyan kétváltozós $f(x,y)$ polinom, amelyre

$$f(m,n) = (m,n), \quad \forall m,n \in \mathbb{N}^*.$$

5.3. Hány lépéssel határozható meg az

$$a = \frac{2^n - (-1)^n}{3},\ b = \frac{2(2^{n-1} - (-1)^{n-1}}{3}$$

számok legnagyobb közös osztója a BINÁRIS-LNKO algoritmussal?

5.4. Feltételezzük, hogy

$$\begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}.$$

Bizonyítsuk be, hogy

$$\frac{p_n}{q_n} = \langle a_0, a_1 \ldots, a_n \rangle.$$

5.5. Adottak az a és b relatív prím természetes számok. Bizonyítsuk be, hogy bármely $n > ab$ természetes szám felírható

$$n = xa + yb$$

alakban, ahol x és y pozitív természetes számok.

5.6. Adott n természetes szám osztóinak az összege

$$\sigma(n) = \sum_{d|n} d.$$

Az n számot *bővelkedőnek* nevezzük, ha

$$\sigma(n) > 2n.$$

Bizonyítsuk be, hogy egy bővelkedő szám többszöröse is bővelkedő.

5.7. Bizonyítsuk be, hogy minden 20161-nél nagyobb természetes szám felírható két bővelkedő szám összegeként.

5.8. Bizonyítsuk be, hogy minden 11-nél nagyobb természetes szám felírható két összetett szám összegeként.

5.9. Legyen f_i az i-edik Fibonacci-szám és

$$A_n = \sum_{k=0}^{n} \frac{1}{f_{2^k}}.$$

Bizonyítsuk be, hogy $n \geq 3$-ra az A_n lánctörtes alakja

$$A_n\langle 2, 2, \underbrace{1, \ldots, 1}_{2^n-5}, 2\rangle,$$

és

$$\lim_{n\to\infty} A_n = \frac{7-\sqrt{5}}{2}.$$

5.10. Adott az $a \geq 3$ természetes szám. Határozzuk meg

$$\sum_{k=0}^{\infty} \frac{1}{a^{2^k}}$$

lánctörtes alakját.

5.11. Bizonyítsuk be, hogy

$$\sum_{1\leq i,j\leq n} (i,j) = \frac{1}{\zeta(2)} n^2 \log n + O(n^2),$$

ahol

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

a Riemann-féle zeta függvény és (a,b) az a és b természetes számok legnagyobb közös osztója.

5.12. Bizonyítsuk be, hogy

$$\sum_{1\le i,j\le n} [i,j] = \frac{\zeta(3)}{4\zeta(2)} n^4 + O(n^3 \log n),$$

ahol $[a,b]$ az a,b számok legkisebb közös többszöröse.

6.

Prímszámok

6.1. Alapfogalmak

6.1. értelmezés. *A p természetes számot **prímszámnak** nevezzük, ha:*
a) $p > 1$*;*
b) *p-nek csupán az* 1 *és a p az osztója* $(az\ \mathbb{N}^*\text{-}ban)$.

Megjegyzés. A prímszámok értelmezésére még használatos a következő tulajdonság is: *a* $q \in \mathbb{N}^*$, $q \neq 1$ *természetes szám prímszám, ha*

$$q \mid ab \Longrightarrow q \mid a \text{ vagy } q \mid b.$$

6.2. értelmezés. *Az $n > 1$ természetes számot, amely nem prímszám,* összetett számnak *nevezzük.*

6.3. tétel. *Bármely 1-nél nagyobb természetes szám felbontható prímszámok szorzatára.*

Megjegyezzük, hogy ha az n természetes számot különböző prímek segítségével írjuk fel, akkor azt kapjuk, hogy

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{6.1}$$

ahol $\alpha_1 > 0,\ \alpha_2 > 0, \cdots, \alpha_k > 0$.

6.4. értelmezés. *Az n természetes szám* (6.1) *képlettel felírt alakját az n **kanonikus alakjának** nevezzük.*

A továbbiakban kijelentjük a számelmélet alaptételét.

6.5. tétel (a számelmélet alaptétele). *Az adott $n > 1$ természetes szám kanonikus alakjának a felírása*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{6.2}$$

egyértelmű (eltekintve a prímtényezők sorrendjétől).

6.6. lemma. *Az n összetett szám legkisebb prímosztója nem lehet nagyobb $\sqrt{n}$-nél.*

Bizonyítás. Legyen p az n összetett szám legkisebb prímosztója. Ekkor:

$$n = pn_0, \quad n_0 > 1.$$

Mivel p a legkisebb prímosztó, következik, hogy

$$p \leq n_0,$$

ahonnan

$$p^2 \leq n \Longrightarrow p \leq \sqrt{n}.$$

□

Ennek a felhasználásával egy olyan algoritmust mutatunk be, amellyel megadjuk egy természetes szám összes osztóját (egy prímszám annyiszor fog szerepelni a multihalmazban, ahányszor a prímtényezős felbontásban).

PRÍMOSZTÓK (n)
$O := \{\ \}$
$N := n$
while $2 \mid N$
  do $N := \frac{N}{2}$
    $O := O \cup \{2\}$
$d := 3$
while $d^2 \leq N$
  while $d \mid N$
    do $N := \frac{N}{d}$
      $O := O \cup \{d\}$
    $d := d + 2$
if $N = 1$
  return O
return $O := O \cup \{N\}$

6.2. A prímszámok száma és nagysága

Ebben a részben először a prímszámok számával foglalkozunk. A számelmélet alaptételéből arra a következtetésre jutunk, hogy a prímszámok száma valószínűleg végtelen. Ezt a sejtést fogja alátámasztani a prímszámok meghatározására adott nagyon egyszerű módszer is. Először meghatározunk egy felső korlátot az adott természetes számot osztó prímszámra, amit használni fogunk az alábbiakban leírt módszernél.

Az első néhány prímszám a következő

$$2,3,5,7,11,13,17,19,23,29,31,37,41,\cdots$$

Ha adott egy N természetes szám, akkor Eratoszthenész szitájának a segítségével meghatározhatjuk az N-nél kisebb vagy vele egyenlő prímszámokat.

Leírjuk az összes természetes számot N-ig

$$2,3,4,5,6,\cdots,N,$$

és sorozatosan kihúzzuk az összetett számokat a következőképpen:
a) a 4, 6, 8,... számokat, vagyis 2^2-t és minden utána következő páros számot;
b) a 9, 15, 27,... számokat, vagyis 3^2-t és minden utána következő 3-mal osztható számot;
c) a 25, 35, 55, 65,... számokat, 5^2-t és minden fennmaradó 5^2-nél nagyobb 5-tel osztható számot.
...

Folytatjuk az eljárást a megmaradó számok közül, a legkisebbel mindaddig, míg elérünk az első $\sqrt{N}$-nél nagyobb természetes számig. A ki nem húzott számok az N-nél nem nagyobb prímszámok.

Erre az egyszerű szitára (Eratoszthenész szitája) a következő algoritmust adhatjuk meg. Ezzel az algoritmussal az (L,R) intervallumbeli prímeket határozzuk meg, ahol L és R páros számok. Feltételezzük, hogy $B \mid R-L$, $L > P = \lceil \sqrt{R} \rceil$ valamint, hogy ismerjük a P-nél kisebb prímszámokat ($p_k < P$).
A prímszámok számára bevezetjük a következő függvényt:

6.7. értelmezés. *Legyen $\pi(x)$ az x-nél nem nagyobb prímek száma,*

$$\pi(x) = \sum_{p \le x} 1, \tag{6.3}$$

ERATOSZTHENÉSZ $((L,R))$
for $(k \in [2,\pi(P)])$
  do $q_k := \left(-\frac{1}{2}(L+1+p_k)\right) \pmod{p_k}$
$T := L$
while $(T < R)$
  for $(j \in [0,B-1])$
    do $b_j := 1$
  for $(k \in [2,\pi(P)])$
    for $(j = q_k;\ j < B;\ j := j + p_k)$
      do $b_j := 0$
    $q_k := q_k - B \pmod{p_k}$
  for $(j \in [0,B-1])$

```
    if (b_j = 1)
      return T + 2j + 1
  T := T + 2B
```

Az Eratoszthenész szitájában a lépések mind összeadások. Mivel egy p prímszámra a $2p,\ 3p,\ 4p,\ldots$ számokat húzzuk ki, az összes lépés száma arányos a

$$\sum_{p\le N}\frac{N}{p}$$

összeggel. De

$$\sum_{p\le N}\frac{N}{p}=N\log\log N+O(N),$$

ahonnan következik, hogy a lépések száma arányos $\log\log N$-nel (ha 1-től N-ig keressük a prímszámokat).

Megjegyezzük, hogy $\log\log N$ tart a végtelenhez, ha N tart a végtelenhez, de a növekedés lassú. Például, ha $N\le 10^{9565}$, akkor $\log\log N<10$.

6.2.1. Euklidész-számok

Az Eratoszthenész szitája arra enged következtetni, hogy a prímszámok száma végtelen. Azt tudjuk, hogy az 1 000 000 000-nál kisebb prímek száma 50 847 478, de ezek mindegyike nem ismert.

A prímek meghatározása külön feladat, és ezeket legtöbbször 2^p-1 alakban keressük. Az ilyen prímeket Mersenne-prímeknek nevezzük, és még foglalkozunk velük a későbbiekben.

A továbbiakban bebizonyítjuk, hogy a prímek száma végtelen. Erre több bizonyítást adunk, melyek közül egyesek algebrai vagy topológiai segédeszközöket igényelnek. Ezen bizonyítások segítségével vezetjük be a Euklidész, Fermat és Mersenne számokat és prímeket is. Az első bizonyítás magától Euklidésztől származik.

6.8. tétel (Euklidész második tétele). *A prímszámok száma végtelen.*

Először bemutatjuk Euklidész bizonyítását.

1. bizonyítás. Adott a prímszámok egy véges halmaza, $\{p_1,p_2,\cdots,p_k\}$, és képezzük az

$$n=p_1p_2\cdots p_k+1$$

számot. Ennek a számnak a 6.3 tétel alapján van egy prímosztója. Ez a p nem lehet a $p_i,\ i\in\{1,2,\cdots,k\}$ egyike sem, mert akkor kellene osztania az

$$n-p_1p_2\cdots p_k=1$$

számot is, ami ellentmondás. Tehát van még egy prímszámunk a $\{p_1,p_2,\cdots p_k\}$ halmazon kívül. Ez azt jelenti, hogy egyetlen véges prímszámhalmaz sem tartalmazhatja

az összes prímszámot. □

Megjegyzés. A tétel szerint

$$\lim_{x\to\infty} \pi(x) = \infty.$$

Valójában a $\pi(x)$ függvényre sokkal jobb becsléseket lehet adni, amelyeket a későbbiekben fogunk tárgyalni.

Az Euklidész bizonyítása alapján bevezetjük az Euklidész-számokat.

6.9. értelmezés. *Jelöljük az első n prímszám szorzatát p_n#-nel:*

$$p_n\# = \prod_{k=1}^{n} p_k.$$

Az

$$E_n = 1 + p_n\# = 1 + \prod_{k=1}^{n} p_k,$$

*számokat **Euklidész-számoknak** nevezzük.*

Az első euklideszi számok a következők:

$$E_1 = 3,\ E_2 = 7,\ E_3 = 31,\ E_4 = 211,\ E_5 = 2311,\ E_6 = 300031.$$

A legnagyobb ismert euklideszi-szám az E_{13494}.
Az alábbi feladatok még nincsenek megoldva.

6.10. feladat. *Létezik-e végtelen Euklidész-szám, amely prím?*

6.11. feladat. *Az E_n Euklidész-szám négyzetmentes-e (nem osztható egyetlen prímszám négyzetével)?*

6.12. feladat. *Legyen q_k az E_k számnál nagyobb, legközelebbi prím*

$$q_k = p_{1+\pi(E_k)}.$$

Igaz-e, hogy az

$$r_k = q_k - E_k + 1$$

számok prímszámok bármely k-ra?

Eddig igazolták, hogy $k \leq 1000$-re igaz az előbbi állítás.

Az Euklidész-számokhoz hasonlóan a következő sorozatokat vezetjük be:
1. R. Guy és R. Novakowski [37] a következő $(a_k)_{k\geq 1}$ sorozatot vezették be:
$a_1 = 2$ és a_{k+1} az $a_1a_2\ldots a_k + 1$ legkisebb prímosztója,

$$a_{k+1} = \min\{p \mid p \in \mathbb{P},\ a_1a_2\cdots a_k + 1 \equiv 0 \pmod{p}\}.$$

Az első 10 tagja a sorozatnak:

$$a_1 = 2,\ a_2 = 3,\ a_3 = 7,\ a_4 = 43,\ a_5 = 13,\ a_6 = 53,\ a_7 = 5,\ a_8 = 6221671,$$

$$a_9 = 38709183810571,\ a_{10} = 139.$$

A sorozatnak az első 43 tagja ismert. Még megoldatlan a következő feladat:

6.13. feladat. *Az $(a_n)_{n\geq 1}$ tartalmazza az összes prímszámot?*

2. Értelmezzük a $(b_n)_{n\geq 1}$ szigorúan növekvő sorozatot. $b_1 = 2$ és b_{k+1} a legkisebb olyan prímszám, amely osztja valamely $d+1$ számot, ahol d a $b_1 b_2 \cdots b_k$ egy osztója,

$$b_{k+1} = \min\{p \mid p \in \mathbb{P},\ p > b_k,\ d+1 \equiv 0 \pmod{p},\ d \mid b_1 b_2 \cdots b_k\}.$$

C. Pomerance [22] bizonyította, hogy a sorozat tartalmazza az összes prímszámot, de a bizonyítás nyomtatásban nem jelent meg.

3. A következő sorozatot M. Newman szerkesztette. $c_1 = 2,\ c_2 = 3$ és c_{k+1} a legkisebb prímszám, amely osztja a $c_i c_j + 1,\ 1 \leq i < j \leq k$ valamelyikét,

$$c_{k+1} = \min\{p \mid p \in \mathbb{P},\ p > b_k,\ \exists i, j,\ 1 \leq i < j \leq k,\ c_i c_j + 1 \equiv 0 \pmod{p}\}.$$

A következő feladatra még nem ismert a megoldás.

6.14. feladat.
a) *Növekvő-e a $(c_n)_{n\geq 1}$ sorozat?*
b) *A $(c_n)_{n\geq 1}$ tartalmazza az összes prímszámot?*

6.2.2. Fermat-számok

A következő bizonyításban az úgynevezett Fermat-számokat fogjuk használni, ezért külön is foglalkozunk a tulajdonságaival.

6.15. értelmezés. *Az*

$$F_n = 2^{2^n} + 1, \quad n \geq 0$$

*számot az n-edik **Fermat-számnak** nevezzük.*

Fermat azt hitte, hogy ezen számok mindegyike prím, mivel az első ötöt kiszámolva azt találta, hogy mindegyik prím ($F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65537$). Ha tovább vizsgáljuk a számokat, akkor már a hatodik Fermat-szám (F_5) nem lesz prím (ezt először Euler bizonyította 1732-ben). Ennek a bizonyítását mutatjuk be a következőkben, mivel a bizonyítás nem az F_5 kiszámolásával történik.

6.16. tétel. *Az*

$$F_5 = 2^{32} + 1$$

szám egy osztója a 641.

Bizonyítás. A 641 számot a következő alakokban írhatjuk fel:

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1.$$

Így

$$F_5 = 2^{32} + 1 = (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1).$$

De

$$641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32}$$

és

$$641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7)^4 - 1 = 5^4 \cdot 2^{28} - 1,$$

ahonnan következik, hogy 641 osztja a két szám különbségét, így az F_5-öt is. □

A további Fermat-számokra vonatkozóan 1880-ban Landau bebizonyította, hogy F_6 összetett szám és jelenleg ismert, hogy a

$$7 \leq n \leq 25, \text{ illetve } n = 36, 39, 55, 63, 73$$

értékekre az F_n összetett szám. F_4 utáni prímszámot az $(F_n)_{n\geq 0}$ sorozatban nem találtak. Így valószínűleg igaz a következő sejtés:

6.17. sejtés. *Az F_n, $n \geq 0$ Fermat-számok között véges számú prímszám van.*

Megjegyzés. Ha a prímszámok számára egy „jó” becslést használunk, akkor valószínűségszámítási megfontolások alapján igaznak tűnik a sejtés.

6.18. tétel. *A Fermat-számok páronként relatív prímek, vagyis*

$$(F_n, F_m) = 1, \quad \forall n \neq m.$$

Bizonyítás. Felírhatjuk, hogy

$$\begin{aligned} \prod_{k=0}^{n-1} F_k &= (2^{2^0}+1)(2^{2^1}+1)\cdots(2^{2^{n-1}}+1) = \\ &= (2^{2^0}-1)(2^{2^0}+1)(2^{2^1}+1)\cdots(2^{2^{n-1}}+1) = \\ &= 2^{2^n} - 1 = F_n - 2. \end{aligned} \tag{6.4}$$

Tudjuk, hogy $(F_0, F_1) = 1$. Feltételezzük, hogy $F_1, \ldots, F_{n-1}$ páronként relatív prímek, és bizonyítjuk, hogy F_n relatív prím az $F_1, \ldots, F_{n-1}$ számok mindegyikével. Valóban, ha létezik $k < n$ úgy, hogy

$$(F_k, F_n) = d,$$

(6.4)-ből következik, hogy $d \mid 2$, de d páratlan kell legyen, mivel az F_k számok mind páratlanok, így $d = 1$. Tehát bármely két F_n, F_m relatív prím, $n \neq m$ esetén. □

A Fermat-számokra igazak a következő eredmények.

6.19. tétel. *Adott n természetes szám esetén, az F_n Fermat-szám p prímosztójára*

$$p \equiv \pmod{2^{n+2}}.$$

6.20. tétel (Pepin-teszt). *Adott n természetes szám esetén az $F_n = 2^{2^n} + 1$ Fermat-szám akkor és csakis akkor prím, ha*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

A Pepin-teszttel vizsgálhatjuk a Fermat-számok összetettségét. Például az F_{14} és az F_{20} összetettségét a Pepin-teszt segítségével bizonyította J. Selfridge és A. Hurwitz [65] illetve D. Buell és J. Young [14].

6.8 tétel 2. bizonyítása.

A 6.18 tételből is következik, hogy a prímszámok száma végtelen, mert ha véges számú prím létezne, $p_1, p_2, \ldots, p_k$, akkor az $F_1, F_2, \ldots, F_{k+1}$ közül legalább kettő ugyanazzal a prímszámmal kellene osztható legyen, ami ellentmond annak, hogy a Fermat-számok páronként relatív prímek. □

6.2.3. Mersenne-számok

Bevezetjük a Mersenne-számokat és a Mersenne-prímeket, és majd segítségükkel bizonyítjuk a 6.8 tételt.

6.21. értelmezés. ***Mersenne-számoknak*** *nevezzük a*

$$2^p - 1$$

típusú számokat, ahol p prímszám. Ha a Mersenne szám prímszám, akkor ***Mersenne-prímnek*** *nevezzük. Az n-edik Mersenne-prímet M_n-nel jelöljük.*

A Mersenne-számokat és prímeket nagyon sokan vizsgálták, pillanatnyilag (2006. április) 43 Mersenne-prímet ismerünk. A következőkben bemutatunk egy táblázatot, amely a Mersenne-számok történetét szemlélteti

1536,	*Hudabicus Regius*	$2^{11} - 1 = 28 \cdot 39$
1588,	*Pietri Cataldi*	$2^{17} - 1 \in \mathbb{P}$
1603,	*Pietri Cataldi*	$2^{19} - 1 \in \mathbb{P}$
1772,	*Euler*	$2^{31} - 1 \in \mathbb{P}$
1882,	*Lucas*	$2^{127} - 1 \in \mathbb{P}$
...		
1963,	*Gillies*	$M_{23} = 2^{11213} - 1$
...		
2003,	*Shafer*	M_{40}
2004,	*Findley*	M_{41}
2005,	*Nowak*, *Woltman*, *Kurowski*	M_{42}
2005,	*Cooper*, *Boone*	M_{43}

Megjegyzések.

1. Az

$$M_{23} = 2^{11213} - 1$$

Mersenne prímet az Illinois T.E.-en találták meg és Bateman javaslatára megjelent bélyegen is, amit 1976-ig használtak, amikor a négyszámtétel került a bélyegre.

2. A legnagyobb Mersenne-prímet 2005 decemberében C. Cooper és S. Boone találták meg. A szám

$$M_{43} = 2^{30402457} - 1,$$

és 9.152.052 számjegyből áll.
3. Az első legalább 10^7 számjegyű prímszám megtalálására 100,000 $ pénzdíj van kitűzve (GIMPS, „The great Internet Mersenne prime search” [33])
4. A Mersenne-prímek fontosak a tökéletes számok vizsgálatában. Egy számot tökéletesnek nevezünk, ha valódi osztóinak az összege egyenlő a számmal, vagy ha

$$\sigma(n) = \sum_{d|n} d,$$

akkor

$$\sigma(n) = 2n.$$

Euler bizonyította, hogy a páros tökéletes számok

$$n = 2^{p-1}(2^p - 1)$$

alakúak, ahol $p \in \mathbb{P}$ és $2^p - 1$ Mersenne-prím. Innen következik, hogy 43 páros tökéletes számot ismerünk. Megjegyezzük, hogy egyetlen páratlan tökéletes szám sem ismert.

A Mersenne-prímekre érvényes a következő eredmény.

6.22. tétel. *A $2^p - 1$-nek minden prímosztója nagyobb, mint p.*

Bizonyítás. Ha q osztója a $2^p - 1$-nek, akkor azt jelenti, hogy a 2 rendje a $(\mathbb{Z}_q \setminus \{0\}, \cdot)$-ban p. Ennek a csoportnak viszont $q-1$ eleme van. Mivel az

$$\{1, 2, \ldots, 2^{p-1}\}$$

egy alcsoportja a $\mathbb{Z}_q$-nak, Lagrange tételéből következik, hogy $p \mid q-1$, vagyis $p < q$. □

Ennél több is igaz.

6.23. tétel. *Adott $p > 2,\ p \in \mathbb{P}$-re a $2^p - 1$ q prímosztójára*

$$q \equiv 1 \pmod{p}, \quad q \equiv \pm 1 \pmod{8}.$$

6.8 tétel 3. bizonyítása.
Ha a prímek száma véges lenne, akkor létezne egy legnagyobb közöttük, legyen ez p_0, majd, ha ehhez hozzárendeljük a $2^{p_0} - 1$ Mersenne-számot, akkor ennek van egy p_0-nál nagyobb osztója, ami ellentmondás, tehát nem lehet véges számú prímszámunk. □

6.2.4. Egész számok egy topológiája

Megszerkesztünk egy topológiát az egész számok halmazán és ennek a segítségével bizonyítjuk a prímek számának a végtelenségét.
6.8 tétel 4. bizonyítása (topológiai segédeszközökkel).

Ez a bizonyítás H. Fürstenbergtől származik 1955-ből [31]. Az egész számok halmazán értelmezzük a következő topológiát. Adott $a, b \in \mathbb{Z},\ b > 0$-hoz hozzárendeljük az

$$N_{a,b} = \{\, a + nb \mid n \in \mathbb{Z} \}$$

egész számokból álló halmazt, amely tulajdonképpen egy (jobbról is és balról is) végtelen elemből álló számtani sorozat (haladvány).

Az $O \subseteq \mathbb{Z}$ halmazt nyílt halmaznak nevezzük, ha $O = \emptyset$, vagy, ha bármely $a \in \mathbb{Z}$ esetén létezik $b > 0$ úgy, hogy

$$N_{a,b} \subseteq O.$$

Innen következik, hogy nyílt halmazok egyesítése is nyílt halmaz.

Ha $O_1,\ O_2$ nyílt halmazok és $a \in O_1 \cap O_2$, akkor

$$a \in O_1 \Longrightarrow \exists\, b_1 > 0 :\ N_{a,b_1} \subseteq O_1$$

$$a \in O_2 \Longrightarrow \exists\, b_2 > 0 :\ N_{a,b_2} \subseteq O_2$$

$$N_{a,b_1} \subseteq O_1 \Rightarrow a + nb_1 \in O_1,\ \forall n \in \mathbb{Z} \Rightarrow a + kb_1b_2 \in O_1,\ \forall k \in \mathbb{Z} \tag{6.5}$$

$$N_{a,b_2} \subseteq O_2 \Rightarrow a + nb_2 \in O_2,\ \forall n \in \mathbb{Z} \Rightarrow a + kb_1b_2 \in O_2,\ \forall k \in \mathbb{Z}. \tag{6.6}$$

A (6.5) és (6.6)-ból következik, hogy

$$N_{a,b_1b_2} \subseteq O_1 \cap O_2,$$

vagyis az $O_1 \cap O_2$ halmaz is nyílt halmaz.

Indukcióval igazolható, hogy véges számú nyílt halmaz metszete is nyílt. Így egy topológiát szerkesztettünk az egész számok halmazán.

Az értelmezésből következik, hogy bármely nem üres nyílt halmaz végtelen elemet tartalmaz és bármely $N_{a,b}$ halmaz egyfelől nyílt (az értelmezés alapján), másfelől zárt, mivel

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

vagyis $N_{a,b}$ nyílt halmazok egyesítésének a komplementuma.

Most rátérünk a tétel bizonyítására. Mivel bármely n ($n \neq \pm 1$) egész számnak van egy p prím osztója, ezért az n eleme az $N_{0,p}$ halmaznak, vagyis minden -1 és 1-től különböző egész szám beletartozik valamely $N_{0,p}$-be, amit a következőképpen írhatunk fel:

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}, \tag{6.7}$$

ahol $\mathbb{P}$-vel a prímszámok halmazát jelöltük.

Ha feltételezzük, hogy $\mathbb{P}$ véges halmaz, következik, hogy

$$\bigcup_{p \in \mathbb{P}} N_{0,p}$$

zárt halmazok véges egyesítése, tehát zárt halmaz. Így (6.7) alapján a $\{-1,1\}$ halmaz nyílt kell legyen, de ez ellentmond annak, hogy bármely nyílt halmazban végtelen elem van. □

A (6.3) jelölés alapján tudjuk, hogy $\pi(x) \longrightarrow \infty$, ha $x \longrightarrow \infty$. Szeretnénk egy elemi becslést adni a $\pi(x)$-re, ami egy bizonyítás lehetne a prímszámok számának a végtelenségére.

6.24. tétel. *Bármely $x \geq 1$ valós számra igaz a következő egyenlőtlenség:*

$$\pi(x) \geq \log x - 1.$$

Bizonyítás. Ha $n \leq x < n+1$, akkor

$$\log x < \log(n+1) \leq 1 + \frac{1}{2} + \cdots + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m}, \tag{6.8}$$

ahol az összegzést olyan m természetes számokra végezzük, amelyeknek minden prím osztója kisebb vagy egyenlő mint x. Mivel mindegyik ilyen m természetes szám egy és csakis egyféleképpen írható fel

$$\prod_{p \leq x} p^{\alpha_p}$$

kanonikus alakban, azt kapjuk, hogy a (6.8)-beli összeg egyenlő a következő szorzattal:

$$\prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right).$$

Így

$$\begin{aligned} \log x &< \prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right) = \\ &= \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1} = \\ &= \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}. \end{aligned} \tag{6.9}$$

Nyilvánvalóan

$$p_k \geq k+1,$$

és így

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k},$$

amit ha behelyettesítünk (6.8)-ba kapjuk, hogy

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x)+1,$$

vagyis

$$\pi(x) \geq \log x - 1.$$

□

Ennél a becslésnél jobb becslések is igazak, például:

6.25. tétel (Prímszámtétel).

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1. \tag{6.10}$$

Analitikus segédeszközökkel bizonyítható a következő tétel.

6.26. tétel. *Az $x \geq 2$ valós számra*

$$\pi(x) = li(x) + \left(xe^{-A(\log x)^{\frac{1}{2}}}\right),$$

ahol

$$li(x) = \int_2^x \frac{1}{\log t} dt. \tag{6.11}$$

és $A > 0$ egy pozitív állandó.

Megjegyzések.

1. Könnyen meggyőződhetünk, hogy

$$\lim_{x\to\infty} \frac{\mathrm{li}(x)}{\frac{x}{\log x}} = 1,$$

ami annyit jelent, hogy a (6.11)-ből következik (6.10).

2. A (6.11)-ből következik, hogy

$$|\pi(x) - \mathrm{li}(x)| = O\left(\frac{x}{(\log x)^k}\right).$$

3. A (x) függvény elég jó becslést ad a prímszámok számára. Ezt mutatja a következő számbeli eredmény is:

$$\pi(10^{21}) = 21127269486018731928,$$

$$\mathrm{li}\,(10^{21}) \approx 21127269486616126181.3$$

Ha megvizsgáljuk a $\mathrm{li}(x)-\pi(x)$ különbséget, akkor azt vesszük észre, hogy ez a különbség pozitív és mindig kisebb, mint a $\pi(x)$ négyzetgyöke:

$$0 < \mathrm{li}(x) - \pi(x) < \sqrt{\pi(x)},$$

mint ahogy az alábbi táblázatból is látszik.

x	$\pi(x)$	$\mathrm{li}(x)-\pi(x)$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
$\vdots$		
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
$\vdots$		
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207

$\pi(10^{22})$ értékét X. Gourdon és P. Sebah [36] határozták meg 2004-ben. Így az a sejtés alakult ki, hogy a $\mathrm{li}(x)$ mindig nagyobb, mint a $\pi(x)$. Bár nagy értékekre is igaz az állítás, mégsem igaz. Ezt igazolja J. E. Littlewood 1914-ben bizonyított tétele [42].

6.27. tétel. *Található tetszőlegesen nagy x valós érték, amelyre*

$$\pi(x) > \int_2^x \frac{dt}{\log t}.$$

Felmerül a kérdés, melyik a legkisebb x_1 érték, amelyre $\pi(x) > \mathrm{li}(x)$? Littlewood bizonyításából nem lehet következtetni x_1 nagyságára, mindenesetre az előbbiek alapján egy elég nagy számnak kell lennie. Az eddig ismert legjobb eredmény

$$x_1 < 1.3982 \times 10^{316},$$

amit C. Bays és R. H. Hudson bizonyított 2000-ben [5]. A pontos x_1 érték meghatározása nem könnyű feladat, mert a jelenlegi (2006 április) technikával és az ismert algoritmusokkal csak 10^{22} körüli $\pi(x)$ értékeket lehet meghatározni.

Felmerül a kérdés, hogy mit mondhatunk az $a \bmod d$ maradékosztályban található prímek számáról. Erre a kérdésre ad feleletet Dirichlet tétele.

6.28. tétel. *Ha a és d relatív prím természetes számok ($(a,d)=1$), akkor az*

$$a,\ a+d,\ a+2d,\ldots,\ a+kd,\ldots$$

számtani haladvány végtelen prímszámot tartalmaz.

Pontosabb eredmény is igaz.

6.29. tétel. *Adottak* $1 \le a \le q$, $(a,q) = 1$, $x > 2$. *Legyen*

$$\pi(x;a,q) = \sum_{\substack{p \le x \\ p \equiv a \bmod d}} 1$$

az x-nél kisebb $a+kd$ *alakú prímszámok száma. Erre a függvényre érvényes a következő aszimptotikus képlet:*

$$\pi(x;a,q) = \frac{1}{\varphi(q)} li(x) + O\left(xe^{-A\sqrt{\log x}}\right),$$

ahol az A egy pozitív állandó.

A. Granwille és G. Martin [35] egy érdekes cikket írtak, amely különböző számtani haladványokban található prímek számával foglalkozik.

Eddig bizonyítottunk egy becslést összetett szám prímosztójára, bizonyítottuk a prímszámok számának a végtelenségét, a továbbiakban a prímszámok nagyságára adunk egy becslést, majd megvizsgáljuk, hogyan viselkedik (milyen nagyságú) két egymás utáni prímszám különbsége ($d_n = p_{n+1} - p_n$), vagyis milyen távol esnek a prímszámok egymástól.

6.30. tétel. *Ha* p_n*-nel jelöljük az n-edik prímszámot, akkor*

$$p_n \le 2^{2^{n-1}}, \quad \forall n \ge 1.$$

Bizonyítás. Indukcióval igazoljuk az egyenlőtlenséget.
$n = 1$-re

$$p_1 = 2 \le 2 = 2^{2^0},$$

tehát az állítás igaz.
Feltételezzük, hogy az állítás igaz bármely $n \le k$-ra és igazoljuk $n = k+1$-re.
Tehát igaz, hogy

$$p_n \le 2^{2^{n-1}}, \quad n \in \{1,2,\ldots,k\}, \tag{6.12}$$

és azt kell igazolnunk, hogy

$$p_{k+1} \le 2^{2^k}.$$

Valóban, ha tekintjük az

$$m = p_1 p_2 \cdots p_k + 1$$

számot, akkor, mivel m nem osztható $p_1, p_2, \ldots, p_k$ egyikével sem, következik, hogy van p_k-nál nagyobb prím osztója, de ez biztosan nagyobb vagy egyenlő mint p_{k+1}. Így (6.12)-ből

$$\begin{aligned} p_{k+1} &\leq m = p_1 p_2 \cdots p_k + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{k-1}} + 1 = \\ &= 2^{2^k-1} + 1 \leq 2^{2^k-1} + 2^{2^k-1} = 2^{2^k}. \end{aligned}$$

□

Megjegyzés. Az n-edik prímszám nagyságára jóval erősebb becslések érvényesek, de ezek bizonyítására szükségünk van bizonyos analízisbeli segédeszközökre (például a prímszámtételre (6.10)). Ilyen a következő egyenlőtlenség. Léteznek a $c_1, c_2 > 0$ állandók, úgy, hogy

$$c_1 n \log n < p_n < c_2 n \log n, \tag{6.13}$$

ahol $0 < c_1 < 1$ és $c_2 > 1$.

Igaz a következő tétel:

6.31. tétel. *A p_n n-edik prímszámra*

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

6.2.5. Két egymás utáni prímszám különbsége

Ha megnézzük a prímek eloszlását, észrevehetjük, hogy a prímszámok elég szabálytalanul követik egymást. Ezért felmerül a kérdés, hogy két egymás utáni prímszám között lehet-e akármilyen hosszú távolság. Ha felírjuk a prímszámokat és aláírjuk a különbségeket, azt kapjuk, hogy

p_n	2	3	5	7	11	13	17	19	23	29
d_n		1	2	2	4	2	4	2	4	6	2

p_n	31	37	41	43	47	53	59	61	67	71
d_n		6	4	2	4	6	6	2	6	4	2

p_n	73	79	83	89	97	101	103	107	109	
d_n		6	4	6	8	4	2	4	2	4

p_n	113	127	131	137	139	149
d_n		14	4	6	2	10

Két egymás utáni prímszám közötti távolságra érvényes a következő tétel:

6.32. tétel. *Tetszőleges N pozitív természetes számhoz meg lehet szerkeszteni N számú szomszédos összetett számot.*

Bizonyítás. Legyenek $N+1$-ig a prímszámok sorrendben

$$2 = p_1 < p_2 < \cdots < p_k < N+1 \leq p_{k+1},$$

ahol p_{k+1} az $N+1$, ha $N+1$ prímszám vagy a nála nagyobb legközelebbi prím. Tekintsük az

$$m = p_1 p_2 \cdots p_{k+1}$$

számot. Ekkor minden $(N+1)$-ig terjedő szám a $\{p_1, p_2, \ldots p_{k+1}\}$ prímszámok segítségével írható kanonikus alakban, tehát az

$$a_1 = m+2,\ a_2 = m+3, \ldots,\ a_N = m+(N+1)$$

egymás utáni természetes számokra fennáll, hogy

$$2 \mid a_1,\ 3 \mid a_2, \ldots,$$

vagyis mind összetettek (mivel $a_i > p_j$, $i \in \{1,2,\ldots,N\}$, $j \in \{1,2,\ldots,N+1\}$, vagyis a_i nagyobb az összes prím osztójánál). Tehát $a_1,\ a_2, \ldots,\ a_N$ számsorozat N egymás utáni összetett számból áll. □

Az előbbi tétel szerint, bármilyen nagy „hézagok” találhatók az egymás utáni prímszámok között. Másfelől a 6.30 tétel nem jelenti azt, hogy a prímszámok egyre ritkábban fordulnának elő. Tudjuk, hogy két egymás utáni páratlan prímszám közötti legkisebb különbség a 2. Ilyen párok a 3, 5; 5, 7; 11, 13; 101, 103. Kiszámították, hogy 100 000-ig 1224 ilyen pár létezik.

6.33. értelmezés. *Az olyan prímszámokat, amelyek között a különbség* 2,

$$d_k = p_{k+1} - p_k = 2,$$

***ikerprímeknek** nevezzük.*

Ha megvizsgáljuk az ikerprímek számát, akkor az alábbi, máig bizonyítatlan sejtés alakul ki:

6.34. sejtés. *Végtelen sok ikerprím számpár létezik.*

Az eddig (2006. április) ismert legnagyobb ikerprímeket Járai és munkatársai találták meg 2005-ben [15]:

$$16869987339975 \times 2^{171960} \pm 1.$$

Jelöljük azon p prímszámok halmazát, amelyekre p és $p+2$ ikerprímek $\mathbb{P}_2$-vel és $\mathbb{P}_{2k}$-val azon p prímek halmazát, amelyekre p és $p+2k$ is prímszámok.

A prímszámokhoz hasonlóan bevezetjük az ikerprímekre a következő függvényt.

6.35. értelmezés. *Jelöljük az x-nél nem nagyobb ikerprímek számát $\pi_2(x)$-szel*

$$\pi_2(x) = \sum_{\substack{p \le x \\ p \in \mathbb{P}_2}} 1,$$

és azon x-nél nem nagyobb prímek számát, amelyekre p és $p+2k$ prím $\pi_{2k}(x)$-szel

$$\pi_{2k}(x) = \sum_{\substack{p \le x \\ p \in \mathbb{P}_{2k}}} 1.$$

Az ikerprímek számának végtelenségéhez kapcsolódnak a következő sejtések.

6.36. sejtés. *Az ikerprímek számára*

$$\lim_{x\to\infty} \frac{\pi_2(x)}{li_2(x)} = 2C_2,$$

ahol

$$li_2(x) = \int_2^x \frac{1}{(\log t)^2} dt,$$

és C_2 az úgynevezett ikerprím állandó:

$$C_2 = \prod_{2<p\in\mathbb{P}} \left(1 - \frac{1}{(p-1)^2}\right).$$

Megjegyzések.

1. A tételbeli $\mathrm{li}_2(x)$-et helyettesíthetjük a könnyebben kiszámítható $\frac{x}{(\log x)^2}$ függvénnyel:

$$\lim_{x\to\infty} \frac{\pi_2(x)}{\frac{x}{(\log x)^2}} = 2C_2,$$

2. T. Nicely 2004-ben [59] kiszámította $\pi_2(x)$-et $x = 5.4\times 10^{15}$-re

$$\pi_2\left(5.4\times 10^{15}\right) = 5761178723343.$$

Ezt még nagyon jól megközelíti a $2C_2\mathrm{li}_2(x)$, mivel

$$2C_2\mathrm{li}_2\left(5.4\times 10^{15}\right) \approx 5761176717388.$$

6.37. sejtés. *A $\pi_{2k}(x)$-re*

$$\lim_{x\to\infty} \frac{\pi_{2k}(x)}{li_2(x)} = 2C_2 \prod_{p|k,\ p>2} \frac{p-1}{p-2},$$

ahol C_2 az ikerprím állandó.

A fenti sejtést G. H. Hardy és J. E. Littlewood fogalmazta meg 1922-ben [40].

Ha tovább vizsgáljuk az egymás utáni prímszámokat, láthatjuk, hogy a p, $p+2$, $p+4$ nem lehet egyidejűleg prímszám, mivel az egyik közülük biztosan osztható 3-mal. Léteznek olyan

$$p,\ p+2,\ p+6$$

vagy

$$p,\ p+4,\ p+6$$

alakú számhármasok, melyeknek mindhárom eleme prímszám. Ennek alapján a következő máig megoldatlan feladatok fogalmazódnak meg:

6.38. feladat. *Létezik-e végtelen sok*

$$p,\ p+2,\ p+6$$

prímszámokból álló számhármas?

6.39. feladat. *Létezik-e végtelen sok*

$$p,\ p+4,\ p+6$$

prímszámokból álló számhármas?

Az előbbi vizsgálatot folytathatjuk ebben az irányban, de jelenleg a matematika nem tud egyértelmű választ adni az ilyen jellegű kérdésekre.

Ha a 6.30 tételt átfogalmazzuk, akkor a tétel kijelentése így hangzik. A

$$d_n = p_{n+1} - p_n$$

sorozat (ahol p_n az n-edik prímszám) nem korlátos.
Ezt a tételt is lehet élesíteni, vagyis be lehet bizonyítani, hogy a $(d_n)_{n\geq 1}$ sorozat két szomszédos eleme végtelen sokszor lesz egy akármilyen nagy N_0 korlát fölött. Azaz végtelen sok k-ra

$$p_{k+1} - p_k > N_0$$

$$p_k - p_{k-1} > N_0$$

teljesül, vagyis érvényes a következő Sierpinskitől származó tétel:

6.40. tétel. *Tetszőleges nagy N_0 természetes számhoz található végtelen sok olyan p_k prímszám, hogy a*

$$(p_k - N_0, p_k + N_0)$$

intervallumban a p_k számtól eltekintve minden szám összetett szám. (Vagyis végtelen sok „izolált” prímszám van.)

Lehet igazolni, hogy végtelen n-re $d_{n+1} > d_n$ és végtelen n-re $d_{n+1} < d_n$. A következő feladatnak sem ismerjük a megoldását:

6.41. feladat. *Igaz-e végtelen sok n-re a*

$$d_{n+2} > d_{n+1} > d_n$$

vagy a

$$d_{n+2} < d_{n+1} < d_n$$

egyenlőtlenség?

Valószínűleg a $d_{n+1} \leq d_n$ és a $d_{n+1} \geq d_n$ egyenlőtlenség egy elég nagy N-ig átlagban az esetek közel felében következik be, sőt valószínűleg végtelen sok n-re $d_{n+1} = d_n$. Ez irányban érvényes a következő Erdőstől [25] származó tétel, amelyet bizonyítás nélkül közlünk.

6.42. tétel. *Léteznek olyan $h, c > 0$ valós számok, amelyekre minden elég nagy korlát alatt legalább $c \cdot N$ számú n-re teljesül a*

$$d_{n+1} \geq (1+h)d_n$$

egyenlőtlenség.

6.3. Bertrand posztulátuma és alkalmazásai

6.3.1. A Legendre-formula

A továbbiakban ismertetjük a Legendre-formulát, amely az $n!$ kanonikus alakját adja meg és többször használjuk bizonyításokban (p prímszámot jelöl).

6.43. tétel (Legendre-formula). *Az $n!$ kanonikus alakja*

$$n! = \prod_{p \leq n} p^{\alpha(n,p)},$$

ahol

$$\alpha(n,p) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

(ebben a képletben $\lfloor x \rfloor$ az x valós szám alsó egész részét jelöli).

Bizonyítás. Először megjegyezzük, hogy az $\alpha(n,p)$ képletében előforduló végtelen összeg véges számú tagot tartalmaz, mivel elég nagy k_0-ra $\frac{n}{p^{k_0}} < 1$ és így $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$, $\forall k \geq k_0$-ra.

Most rátérünk tételünk bizonyítására. Rögzítünk egy n-nél nem nagyobb p prímszámot. Ekkor az $n! = 1 \cdot 2 \cdots n$ tényezői közül a

$$p,\ 2p, \ldots,\ \left\lfloor \frac{n}{p} \right\rfloor p \tag{6.14}$$

tényezők azok, melyek oszthatók p-vel. Mivel $n!$ olyan tényezői, melyek p-vel nem oszthatók, a későbbiekben nem játszanak szerepet, jelöljük szorzatukat A_1-gyel. (6.14)-ből következik, hogy

$$n! = p \cdot 2p \cdot \ldots \cdot \left\lfloor \frac{n}{p} \right\rfloor p \cdot A_1 = p^{\left\lfloor \frac{n}{p} \right\rfloor} \cdot 1 \cdot 2 \cdot \ldots \cdot \left\lfloor \frac{n}{p} \right\rfloor \cdot A_1, \tag{6.15}$$

ahol $(A_1, p) = 1$.

Tovább vizsgálva az $n!$ számot, ha $\left\lfloor \frac{n}{p} \right\rfloor \geq p$, akkor az

$$1,\ 2, \ldots,\ \left\lfloor \frac{n}{p} \right\rfloor$$

számok között lesznek olyanok, amelyek p-vel oszthatók, éspedig

$$p,\ 2p, \ldots,\ \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor p. \tag{6.16}$$

Itt ismét a p-vel nem osztható tényezőknek nincs jelentőségük, ezért jelöljük a szorzatukat A_2-vel. Így (6.15) és (6.16) alapján

$$n! = p^{\left\lfloor \frac{n}{p} \right\rfloor} p \cdot 2p \cdots \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor p \cdot A_1 A_2. \tag{6.17}$$

A

$$\left\lfloor \frac{\lfloor x \rfloor}{a} \right\rfloor = \left\lfloor \frac{x}{a} \right\rfloor,$$

képletet alkalmazva kapjuk, hogy

$$\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor. \tag{6.18}$$

A (6.17) és (6.18) képletek alkalmazásával

$$n! = p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor} 1 \cdot 2 \cdots \left\lfloor \frac{n}{p^2} \right\rfloor \cdot A_1 A_2,$$

ahol $(A_1A_2, p) = 1$.
Az eljárást folytatva az

$$n! = p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \left\lfloor \frac{n}{p^k} \right\rfloor + \cdots} \cdot A_1A_2 \cdots A_k \cdots$$

alakot kapjuk, ahol $(A_i, p) = 1$, $i \in \{1, 2, \cdots, k, \cdots\}$.
Ezt nem kell végtelenszer elvégezni, csak mindaddig, míg $\frac{n}{p^k} < 1$ lesz.
Így azt kaptuk, hogy rögzített p-re a p hatványa az $n!$-ban

$$\alpha(n, p) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

□

A következőkben a binomiális együtthatók kanonikus alakját írjuk fel. Mivel a binomiális együtthatók kifejezhetők faktoriálisok segítségével, a Legendre-formulából kapjuk a következő eredményt.

6.44. tétel. *Az* $\binom{n}{j}$ *binomiális együttható kanonikus alakja*

$$\binom{n}{j} = \prod_{p \le n} p^{h_p},$$

ahol

$$h_p = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{j}{p^k} \right\rfloor - \left\lfloor \frac{n-j}{p^k} \right\rfloor \right).$$

Sajátos esetben

$$\binom{2n}{n} = \prod_{p \le 2n} p^{h_p},$$

és

$$h_p = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Bizonyítás. Tudjuk, hogy

$$\binom{n}{j} = \frac{n!}{j! \cdot (n-j)!}.$$

Egy rögzített $p \le n$-re a p hatványkitevője a Legendre-formula alapján

$$h_p = \alpha(n, p) - \alpha(j, p) - \alpha(n-j, p) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{j}{p^k} \right\rfloor - \left\lfloor \frac{n-j}{p^k} \right\rfloor \right).$$

□

6.3.2. Bertrand posztulátuma

Bizonyítottuk az előzőekben, hogy a prímszámok száma végtelen, valamint azt is, hogy két egymás utáni prímszám között tetszőleges „hézagok” találhatók, ami azt jelenti, hogy két egymás utáni prímszám különbsége tetszőlegesen nagy lehet.
Bertrand vette észre először, hogy $n < 3\,000\,000$ esetén n és $2n$ között mindig találunk prímszámot, de bizonyítást először P. Csebisev adott 1850-ben. Egyszerű bizonyítást adott rá még Ramanujan, valamint Erdős is 1932-ben. A következőkben Erdős bizonyítását mutatjuk be.

6.45. tétel (Bertrand posztulátuma). *Bármely $n \geq 1$ természetes szám esetén létezik olyan p prímszám, amelyre*

$$n < p \leq 2n.$$

Bizonyítás. A bizonyítás alapötlete az, hogy becsüljük a $\binom{2n}{n}$ binomiális együttható nagyságát.

• Először igazoljuk a tételt $n < 4000$-re. Ehhez elégséges felírni a következő prímszámokat:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001,$$

amelyeket úgy írtunk fel, hogy mindig az utolsó prím kétszereséhez legközelebb álló, de annál kisebb prímszámot írtuk fel. Így bármely

$$A_n = \{y \mid n < y \leq 2n\}$$

halmaz $n \leq 4000$-re tartalmaz legalább egy prímszámot a fenti 14 közül.

• A következőkben bebizonyítunk három segédtételt, és majd felhasználjuk a tétel bizonyításánál.

6.46. lemma. *$x \geq 2$ valós számra:*

$$\prod_{p \leq x} p \leq 4^{x-1}, \quad \forall x \geq 2. \tag{6.19}$$

Bizonyítás. Legyen q a legnagyobb olyan prím, melyre fennáll, hogy $q \leq x$. Így

$$\prod_{p \leq x} p = \prod_{p \leq q} p$$

és

$$4^{q-1} \leq 4^{x-1},$$

tehát elégséges a (6.19) helyett a

$$\prod_{p\le q} p \le 4^{q-1}$$

egyenlőtlenséget igazolni. Ezt q szerinti indukcióval fogjuk bizonyítani:
$q=2$-re kapjuk, hogy

$$2=\prod_{p\le 2} p \le 4^{2-1}=4,$$

ami nyilvánvalóan igaz.
A továbbiakban feltételezzük, hogy q páratlan prím, vagyis $q=2m+1$ alakú. Ezzel a jelöléssel

$$\prod_{p\le q} p=\prod_{p\le 2m+1} p=\prod_{p\le m+1} p\cdot \prod_{m+1<p\le 2m+1} p \le 4^m\cdot\binom{2m+1}{m}, \tag{6.20}$$

egyrészt, mert az indukciós feltevés szerint

$$\prod_{p\le m+1} p \le 4^m,$$

másrészt, mivel

$$\prod_{m+1<p\le 2m+1} p$$

osztója a

$$\binom{2m+1}{m}=\frac{(2m+1)!}{m!\cdot(m+1)!}$$

binomiális együtthatónak (p osztja a számlálót, de nem osztja a nevezőt).
Így (6.20)-ből következik, hogy

$$\prod_{p\le q} p \le 4^m\cdot\binom{2m+1}{m}\le 4^m\cdot 2^{2m}=4^{2m}=4^{q-1},$$

mivel

$$2\cdot\binom{2m+1}{m}=\binom{2m+1}{m}+\binom{2m+1}{m+1}<\sum_{k=0}^{2m+1}\binom{2m+1}{k}=2^{2m+1}. \tag{6.21}$$

□

6.47. lemma. *Legyen a $\binom{2n}{n}$ binomiális együttható kanonikus alakja:*

$$\binom{2n}{n}=\prod_{p\le 2n} p^{h_p}.$$

Ekkor:

$$h_p \leq \max\{r \mid p^r \leq 2n\};$$

a $p > \sqrt{2n}$ *prímekre* $h_p \leq 1$*;*
ha $\frac{2}{3}n < p \leq n$*, akkor* $h_p = 0$*.*

Bizonyítás. A 6.44 tételt használva azt kapjuk, hogy a $\binom{2n}{n}$ kanonikus alakjában egy p prímszám kitevője

$$h_p = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right). \tag{6.22}$$

Az összegben a zárójel értéke 0, ha $p^k > 2n$ és mindegyik zárójel legnagyobb értéke 1, mert

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1 \right) = 2.$$

Így (6.22)-ban

$$h_p \leq \max\{r \mid p^r \leq 2n\},$$

vagyis az alsó egészrész miatt a p^{h_p} értéke nem haladhatja meg a $2n$-et.
Sajátosan, ha azokat a prímszámokat tekintjük, amelyekre $p > \sqrt{2n}$, akkor azok kitevője csak 1 lehet.
Ha tovább vizsgáljuk a prímszámok kitevőit, akkor azon p prímszámok, amelyekre

$$\frac{2}{3}n < p \leq n,$$

nem osztják a $\binom{2n}{n}$-t. Ez abból következik, hogy

$$\frac{2}{3}n < p \leq n \Longrightarrow 2n < 3p \leq 3n$$

(mivel $n \geq 3$ következik, hogy $p \geq 3$) tehát csak p és $2p$ lehet a

$$\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!}$$

számlálójának egy-egy tényezője, de ugyancsak p második hatványával osztható a nevező is, így valóban ezen p prímszámok nem fordulnak elő $\binom{2n}{n}$ kanonikus alakjában. □

6.48. lemma.

$$\frac{4^n}{(2n)^{1+\sqrt{2n}}} \leq \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p. \tag{6.23}$$

Bizonyítás.

• Becsüljük meg a $\binom{2n}{n}$ nagyságát. Tudjuk, hogy

$$\binom{2n}{0}+\cdots+\binom{2n}{n}+\binom{2n}{n+1}+\cdots+\binom{2n}{2n}=2^{2n},$$

és azt is, hogy a középső binomiális együttható a legnagyobb, vagyis

$$\binom{2n}{k}\le\binom{2n}{n},\quad k\in\{1,2,\cdots,2n\}.$$

Így

$$\begin{aligned}2^{2n} &\le 2n\cdot\binom{2n}{n}\\ \frac{4^n}{2n} &\le \binom{2n}{n}.\end{aligned}$$

• A fenti képlet és az előbbi lemma alapján

$$\frac{4^n}{2n}\le\binom{2n}{n}\le\prod_{p\le\sqrt{2n}}2n\cdot\prod_{\sqrt{2n}<p\le\frac{2}{3}n}p\cdot\prod_{n<p\le2n}p. \tag{6.24}$$

Mivel a $p\le\sqrt{2n}$ prímszámokból $\sqrt{2n}$-nél több nem lehet, a (6.24)-ből kapjuk, hogy $n\ge 3$-ra

$$4^n\le(2n)^{1+\sqrt{2n}}\cdot\prod_{\sqrt{2n}<p\le\frac{2}{3}n}p\cdot\prod_{n<p\le2n}p, \tag{6.25}$$

ahonnan következik (6.23). □

Most a „reductio ad absurdum” módszerének a segítségével bizonyítjuk a Bertrand-posztulátumot:

Feltételezzük, hogy nem létezik olyan p prímszám, amelyre $n<p\le 2n$, tehát a (6.23)-beli utolsó szorzat értéke 1.
Ezt és (6.19)-et behelyettesítve a (6.23)-ba azt kapjuk, hogy

$$4^n\le(2n)^{1+\sqrt{2n}}\cdot\prod_{\sqrt{2n}<p\le\frac{2}{3}n}p\le(2n)^{1+\sqrt{2n}}\cdot\prod_{p\le\frac{2}{3}n}p\le(2n)^{1+\sqrt{2n}}\cdot4^{\frac{2}{3}n},$$

vagy

$$4^{\frac{n}{3}}\le(2n)^{1+\sqrt{2n}}$$

avagy

$$4^n\le(2n)^{3(1+\sqrt{2n})}. \tag{6.26}$$

• A (6.26) egyenlőtlenség elég nagy n-re nem igaz. Mi azt fogjuk igazolni, hogy $n > 4000$-re a (6.26) egyenlőtlenség nem igaz.
Használva az

$$a+1 < 2^a, \quad a \geq 2$$

egyenlőtlenséget, írhatjuk, hogy

$$\begin{aligned} 2n &= \left((2n)^{\frac{1}{6}}\right)^6 < \left(\left\lfloor (2n)^{\frac{1}{6}} \right\rfloor + 1\right)^6 < \\ &< 2^{6\left\lfloor (2n)^{\frac{1}{6}} \right\rfloor} \leq 2^{6(2n)^{\frac{1}{6}}}. \end{aligned} \tag{6.27}$$

$n \geq 50$ esetén $18 < 2\sqrt{2n}$, így a (6.26) és a (6.27) képletből következik, hogy

$$\begin{aligned} 4^n &= 2^{2n} \overset{(6.26)}{\leq} (2n)^{3(1+\sqrt{2n})} \overset{(6.27)}{<} 2^{(2n)^{\frac{1}{6}} \cdot \left(18+18\sqrt{2n}\right)} < \\ &< 2^{(2n)^{\frac{1}{6}} \cdot \left(2\sqrt{2n}+18\sqrt{2n}\right)} = 2^{20(2n)^{\frac{1}{6}} \cdot \sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}. \end{aligned} \tag{6.28}$$

Innen következik, hogy

$$2n < 20(2n)^{\frac{2}{3}} \Longrightarrow n < 4000.$$

Tehát $n \geq 4000$-re a (6.26) egyenlőtlenség nem igaz, ami azt jelenti, hogy kell léteznie egy olyan p prímszámnak, amelyre $n < p \leq 2n$.

□

A 6.45 tétel segítségével becslést kaphatunk az n és $2n$ közötti prímszámok számára.

6.49. tétel. *A* 4000*-nél nagyobb természetes számokra igaz a következő egyenlőtlenség:*

$$\pi(2n) - \pi(n) > \frac{1}{30} \cdot \frac{n}{\log_2 n}.$$

Bizonyítás. A (6.23) egyenlőtlenségből $n \geq 4000$-re következik, hogy

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot \prod_{n<p\leq 2n} p.$$

A fenti egyenlőtlenség és a (6.28) alapján az utolsó szorzat a következőképpen alakul:

$$\prod_{n<p\leq 2n} p \geq 2^{\frac{2}{3}n - 20(2n)^{\frac{2}{3}}} \geq 2^{\frac{1}{30}n}, \tag{6.29}$$

ha $n \geq 4000$. A (6.29) egyenlőtlenséget logaritmáljuk és felhasználjuk a

$$0 < \log_{2n} p < 1$$

egyenlőtlenséget, így

$$\log_{2n}\left(2^{\frac{1}{30}n}\right) \leq \sum_{n<p\leq 2n} \log_{2n} p \leq \pi(2n)-\pi(n),$$

ahonnan

$$\pi(2n)-\pi(n) \geq \frac{1}{30}\frac{n}{\log_2 n+1} > \frac{1}{30}\frac{n}{\log_2 n}.$$

□

A(6.45) tételhez hasonlóan bizonyítjuk a következő tételt:

6.50. tétel. *Elég nagy n természetes számra*

$$\frac{1}{6}\cdot\frac{n}{\log n} < \pi(n) < 3\cdot\frac{n}{\log n}.$$

Bizonyítás. Legyen $m \in \mathbb{N}^*$. Ekkor

$$2^m \leq \binom{2m}{m}.$$

Ezt az egyenlőtlenséget indukcióval igazoljuk.
Ha $m=1$, akkor $2^1 = 2 \leq 2 = \binom{2}{1}$. Feltételezzük, hogy igaz m-re, és igazoljuk $m+1$-re. Így

$$\begin{aligned}\binom{2m+2}{m+1} &= \frac{(2m+2)!}{(m+1)!\cdot(m+1)!} = \frac{(2m+2)(2m+1)}{(m+1)^2}\binom{2m}{m} = \\ &= 2\cdot\frac{2m+1}{m+1}\binom{2m}{m} \geq 2\cdot\binom{2m}{m} \geq 2^{m+1},\end{aligned}$$

amit bizonyítani akartunk.
Az előbbiek és a (6.21) egyenlőtlenség alapján írhatjuk, hogy

$$2^m \leq \binom{2m}{m} < 4^m.$$

Logaritmálva

$$m\cdot\log 2 \leq \log((2m)!) - 2\cdot\log(m!) < m\cdot\log 4. \tag{6.30}$$

Behelyettesítve a Legendre-képletet (6.14 tétel) a középső kifejezésbe

$$\log((2m)!) - 2\cdot\log(m!) = \sum_{p\leq 2m}\sum_{j=1}^{\infty}\left(\left\lfloor\frac{2m}{p^j}\right\rfloor - 2\cdot\left\lfloor\frac{m}{p^j}\right\rfloor\right)\log p. \tag{6.31}$$

A zárójelekbeli alsó egészrészek akkor nem 0-k, ha

$$j \leq \frac{\log(2m)}{\log p},$$

valamint

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0,1\} \quad \forall x \in \mathbb{R}.$$

Így (6.30) és (6.31) alapján

$$m \cdot \log 2 \leq \sum_{p \leq 2m} \left(\sum_{1 \leq j \leq \frac{\log(2m)}{\log p}} 1 \right) \log p \leq \sum_{p \leq 2m} \log(2m) = \pi(2m) \cdot \log 2m.$$

Ha $n = 2m$, akkor

$$\pi(n) \geq \frac{\log 2}{2} \cdot \frac{n}{\log n} > \frac{1}{4} \cdot \frac{n}{\log n},$$

ha pedig $n = 2m+1$, akkor

$$\pi(n) \geq \pi(2m) > \frac{1}{4} \cdot \frac{2m}{\log(2m)} \geq \frac{1}{4} \frac{2m}{2m+1} \cdot \frac{2m+1}{\log(2m+1)} \geq \frac{1}{6} \cdot \frac{n}{\log n},$$

mert $m \geq 1$-re

$$\frac{2m}{2m+1} \geq \frac{2}{3}.$$

A felső korlát bizonyítására induljunk ki az $m < p \leq 2m$ egyenlőtlenségből. Ekkor

$$\left\lfloor \frac{2m}{p^j} \right\rfloor - 2 \cdot \left\lfloor \frac{m}{p^j} \right\rfloor = \begin{cases} 1, & j = 1 \\ 0, & j > 1 \end{cases}.$$

Így (6.30) és (6.31)-ből következik, hogy

$$m \cdot \log 4 \geq \sum_{m < p \leq 2m} \left(\left\lfloor \frac{2m}{p} \right\rfloor - 2 \cdot \left\lfloor \frac{m}{p} \right\rfloor \right) \log p, \tag{6.32}$$

mert a (6.31) összegből csak azokkal a tagokkal foglalkozunk, amelyekre $m < p \leq 2m$, és ezekre a második összegnek (mikor j szerint összegzünk) egyetlen tagja van.

A (6.32)-ből következik, hogy

$$m \cdot \log 4 \geq \sum_{m < p \leq 2m} \log p \geq \sum_{m < p \leq 2m} \log m = (\pi(2m) - \pi(m)) \cdot \log m$$

$$\pi(2m) - \pi(m) \leq \log 4 \cdot \frac{m}{\log m}. \tag{6.33}$$

Legyenek r és s olyan természetes számok, amelyekre teljesülnek a

$$2^r \leq n < 2^{r+1} \text{ és } 2^s \leq n^{\frac{19}{20}} < 2^{s+1}$$

egyenlőtlenségek. Észrevehetjük, hogy

$$r > s,\ n \to \infty \Longleftrightarrow s \to \infty.$$

$m = 2^j$-t helyettesítve (6.33)-ba

$$\pi(2^{j+1}) - \pi(2^j) \leq \log 4 \cdot \frac{2^j}{\log 2^j} \leq \log 4 \cdot \frac{2^j}{\log 2^s},\ j \in \{s, s+1, \cdots, r\}. \qquad (6.34)$$

A (6.34) egyenlőtlenségeket összegezve j szerint

$$\begin{aligned}
\pi(n) - \pi\left(n^{\frac{19}{20}}\right) &\leq \pi\left(2^{r+1}\right) - \pi(2^s) \leq \frac{\log 4}{\log 2^s}\left(2^s + 2^{s+1} + \cdots + 2^r\right) \leq \\
&\leq \frac{\log 4}{\log 2^s}\left(2^{r+1}\right) \leq \frac{2 \cdot \log 4}{s \cdot \log 2} \cdot n = \\
&= 2n \cdot \log 4 \cdot \frac{s+1}{s} \cdot \frac{1}{(s+1)\log 2} \leq \\
&\leq 2n \cdot \log 4 \cdot \frac{s+1}{s} \cdot \frac{1}{\log n^{\frac{19}{20}}} = \frac{40 \log 4}{19} \cdot \frac{s+1}{s} \cdot \frac{n}{\log n} < \\
&< 2{,}92 \cdot \frac{s+1}{s} \cdot \frac{n}{\log n}.
\end{aligned}$$

Így elég nagy s-re (és n-re) azt kapjuk, hogy

$$\begin{aligned}
\pi(n) &< 2{,}95 \cdot \frac{n}{\log n} + \pi\left(n^{\frac{19}{20}}\right) \leq 2{,}95 \cdot \frac{n}{\log n} + n^{\frac{19}{20}} = \\
&= \left(2{,}95 + \frac{\log n}{n^{\frac{1}{20}}}\right) \cdot \frac{n}{\log n} < 3 \cdot \frac{n}{\log n},
\end{aligned}$$

mivel

$$\frac{\log n}{n^{\frac{1}{20}}}, \longrightarrow 0 \text{ ha } n \longrightarrow \infty.$$

□

A prímszámtétel felhasználásával a Bertrand-posztulátumnál erősebb tétel is igazolható.

6.51. tétel. *Tetszőleges $\delta > 0$ valós számhoz létezik $x_0 > 0$ valós szám úgy, hogy $x > x_0$ esetén van legalább egy olyan prímszám, amelyre*

$$x < p < x(1+\delta).$$

Bizonyítás. A prímszám tétel azt jelenti, hogy bármely $\varepsilon > 0$ számhoz létezik $x_1 > 0$ úgy, hogy $\forall x > x_1$-re

$$(1-\varepsilon) \cdot \frac{x}{\log x} < \pi(x) < (1+\varepsilon) \cdot \frac{x}{\log x}. \qquad (6.35)$$

Ha δ rögzített, akkor $x(1+\delta) > x_1$ és (6.35)-ból kapjuk, hogy

$$\pi(x(1+\delta)) > (1-\varepsilon)\cdot\frac{x(1+\delta)}{\log\big(x(1+\delta)\big)}$$

és felhasználjuk a (6.35)-ból a második egyenlőtlenséget.
Ekkor

$$\pi(x(1+\delta))-\pi(x) > (1-\varepsilon)\cdot\frac{x(1+\delta)}{\log(x(1+\delta)}-(1+\varepsilon)\cdot\frac{x}{\log x}.$$

Innen

$$\begin{aligned}\pi(x(1+\delta))-\pi(x) &> \frac{x(1+\delta)}{\log x+\log(1+\delta)}-\frac{x}{\log x}-\frac{\varepsilon\cdot x\cdot(1+\delta)}{\log x+\log(1+\delta)}-\\ &- \frac{\varepsilon\cdot x}{\log x} > \frac{x\cdot(1+\delta)}{\log x+\log(1+\delta)}-\frac{x}{\log x}-\frac{3\cdot\varepsilon\cdot x}{\log x}=\\ &= x\cdot\left(\frac{1}{\log x+\log(1+\delta)}-\frac{1}{\log x}\right)+\\ &+ \delta\cdot\frac{x}{\log x+\log(1+\delta)}-3\cdot\varepsilon\cdot\frac{x}{\log x}.\end{aligned}$$

Felhasználjuk, hogy

$$\log(1+\delta) < \log x,$$

és ezáltal

$$\begin{aligned}\pi(x(1+\delta))-\pi(x) &> x\cdot\left(\frac{-\log(1+\delta)}{\log^2 x+\log x\cdot\log(1+\delta)}\right)+\\ &+ \frac{\delta\cdot x}{2\log x}--3\cdot\varepsilon\cdot\frac{x}{\log x}>\\ &> x\cdot\left(\frac{-\log(1+\delta)}{\log^2 x}\right)+\frac{\delta\cdot x}{2\log x}-\\ &- 3\cdot\varepsilon\cdot\frac{x}{\log x},\end{aligned}$$

de $\log(1+\delta) < \delta$ miatt, $\varepsilon = \dfrac{\delta}{12}$ helyettesítéssel

$$\begin{aligned}\pi(x(1+\delta))-\pi(x) &> x\cdot\left(\frac{-\delta}{\log^2 x}\right)+\frac{\delta\cdot x}{2\log x}-3\cdot\varepsilon\cdot\frac{x}{\log x}=\\ &= \delta\cdot\frac{x}{\log x}\cdot\left(\frac{1}{4}-\frac{1}{\log x}\right).\end{aligned}$$

Így $x > e^4$ értékre

$$\frac{1}{4}-\frac{1}{\log x} > 0,$$

ahonnan következik, hogy

$$\pi(x(1+\delta)) - \pi(x) > 0,$$

de, mivel $\pi(x(1+\delta))$ és $\pi(x)$ is természetes szám, következik, hogy

$$\pi(x(1+\delta)) - \pi(x) \geq 1,$$

vagyis az $(x, x(1+\delta))$ intervallumban van legalább egy prímszám.

□

Megjegyzések.
1. Ha a 6.51 tételt $x = p_n$-re alkalmazzuk, akkor azt kapjuk, hogy $n > n_0$ esetén

$$p_n < p_{n+1} \leq (1+\delta)p_n,$$

vagyis

$$1 < \frac{p_{n+1}}{p_n} \leq 1+\delta. \tag{6.36}$$

2. A Bertrand-posztulátum (6.45 tétel) alapján p_n-re kapjuk, hogy

$$p_n < p_{n+1} \leq 2p_n, \quad \forall n \in N^*.$$

Innen következik, hogy

$$p_n \leq 2p_{n-1} \leq 2^2 p_{n-2} \leq \cdots \leq 2^{n-1} p_1 = 2^n,$$

vagyis

$$p_n \leq 2^n, \tag{6.37}$$

ami egy „jobb" felső korlát, mint a 6.11 tételbeli $2^{2^{n-1}}$.

3. A 6.50 tétel felhasználásával igazolható, hogy p_n, az n-edik prímszám, teljesíti a következő egyenlőtlenségeket:

$$c_1 \cdot n \log n < p_n < c_2 \cdot n \log n, \tag{6.38}$$

ahol $0 < c_1 < 1$ és $c_2 > 1$.

6.3.3. Kombinatorikus Bertrand tulajdonság

A továbbiakban bemutatjuk a Bertrand-posztulátum egy érdekes alkalmazását a kombinatorikus számelméletben.

6.52. tétel. *Az $\{1, 2, \cdots, 2k\}$ halmaz felbontható k darab diszjunkt, két elemből álló halmazra úgy, hogy minden halmazban az elemek összege prímszám.*

Bizonyítás. A bizonyítást indukcióval végezzük.
Legyen $k = 1$, így a halmaz $\{1,2\}$, és elemeinek összege 3. Most feltételezzük, hogy bármely

$$\{1,2,\cdots j\},\ 1 \leq j \leq k-1$$

halmaz felbontható a kívánt módon, és bizonyítjuk, hogy az

$$\{1,2,\cdots,2(k-1),2k-1,2k\}$$

halmaz is felbontható a kért módon.
Először keresünk a $2k$-nak egy párt az $\{1,2,\cdots,2k-1\}$ számok közül úgy, hogy az összegük prímszám legyen. A lehetséges párok $(j,2k)$, $1 \leq j \leq 2k-1$. Ezen számok összege $2k+1$-től $4k-1$-ig az összes természetes számot felveszi. Mivel a Bertrand-posztulátum (6.45 tétel) szerint létezik olyan p prímszám, hogy $2k < p < 4k$, következik, hogy létezik a $2k+1$ és a $4k-1$ között legalább egy olyan szám, a $2k+m$, mely prímszám, ahol m páratlan szám (ellenkező esetben a $2k+m$ páros).
Így, ha tekintjük az

$$\{m,m+1,\cdots,2k-1,2k\}$$

halmazt, ennek a halmaznak páros számú eleme van. Párosítva az elsőt az utolsóval, a másodikat az utolsó előttivel, ..., és végül a két középsőt, azt kapjuk, hogy mindezen párok összege $2k+m$, vagyis prímszám

$$p = m+2k = (m+1)+(2k-1) = \cdots.$$

Az indukciós feltevés alapján az $\{1,2,\cdots,m-1\}$ halmazt fel tudjuk bontani számpárokra úgy, hogy összegük prímszám legyen, azt kapjuk, hogy az egész $\{1,2,\cdots,2k\}$ halmazt fel tudjuk bontani és így az indukció alapján a tételben megfogalmazott tulajdonság igaz bármely $k \geq 1$-re.

□

A fenti tétel alapján bevezethetjük a következő értelmezést:

6.53. értelmezés. *Adott az $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ függvény. Azt mondjuk, hogy az f rendelkezik a **kombinatorikus Bertrand-tulajdonsággal**, ha az*

$$\{f(1), f(2), \cdots, f(2k)\}$$

halmazt felbonthatjuk k darab, olyan kételemű diszjunkt részhalmazra, amelyekben az elemek összege prímszám.

Megjegyzés. Ha $f(n) = n$, akkor a 6.52 tételt kapjuk, így ez a függvény rendelkezik a kombinatorikus Bertrand-tulajdonsággal, de felmerül más ilyen függvények létezése. Még elsőfokú polinomok esetén sincsen egyértelmű válasz.
Ha $f(k) = k^2$, akkor $k = 1000$-ig számítógéppel ellenőrizték, hogy f rendelkezik a kombinatorikus Bertrand-tulajdonsággal, de bizonyítani csupán annyit sikerült, hogy:

6.54. tétel. *Annak a valószínűsége, hogy az*

$$\{1^2, 2^2, \cdots, (2k)^2\}$$

halmaz felbontható legyen k darab diszjunkt, két elemet tartalmazó olyan halmazra, amelyekben az elemek összege prímszám, tart az 1-hez, ha k tart a végtelenhez.

Bizonyítás nélkül közöljük a Sylvester–Schur-tételt, amelynek Erdőstől származó legegyszerűbb bizonyítása is meglehetősen hosszú.

6.55. tétel. *Ha $n \geq 2k$ és $n,k \in \mathbb{N}^*$, akkor a $\binom{n}{k}$ binomiális együtthatónak van k-nál nagyobb prímosztója.*

Megemlíthetjük a máig még megoldatlan alábbi feladatot.

6.56. feladat. *Létezik-e bármely $n \in \mathbb{N}^*$ esetén p prímszám n^2 és $(n+1)^2$ között?*

6.4. Prímszámokra vonatkozó képletek.

Felmerül az a kérdés, hogy lehet-e olyan formulát találni, amely csupa prímeket ad eredményül. Erre a válasz pozitív, ilyen képleteket talált Moser, Mills [58], Wright [70], [71], Sierpinski [66] . Ezek a formulák önmagukban érdekesek, de nem nagyon használhatók segédeszközként.

Legyen p_n az n-edik prímszám.

6.57. tétel. *Ha*

$$\alpha = \sum_{m=1}^{\infty} p_m \cdot 10^{-2^m} = 0,02030005000000070\cdots,$$

akkor

$$p_n = \left\lfloor 10^{2^n}\alpha \right\rfloor - 10^{2^{n-1}} \cdot \left\lfloor 10^{2^{n-1}}\alpha \right\rfloor. \tag{6.39}$$

Bizonyítás. A 6.11 tétel szerint

$$p_m \leq 2^{2^{m-1}} < 2^{2^m} = 4^{2^{m-1}}$$

és ezért a

$$\sum_{m=1}^{\infty} p_m \cdot 10^{-2^m}$$

sor konvergens, így α egy jól meghatározott szám.

A továbbiakban $n \geq 1$-re

$$\begin{aligned} 0 < 10^{2^n} \cdot \sum_{m=n+1}^{\infty} p_m 10^{-2^m} &< \sum_{m=n+1}^{\infty} 4^{2^{m-1}} \cdot 10^{-2^{m-1}} = \\ &= \sum_{m=n+1}^{\infty} \left(\frac{2}{5}\right)^{2^{m-1}} < \left(\frac{2}{5}\right)^{2^n} \cdot \frac{1}{1-\frac{2}{5}} < \\ &< \frac{4}{15} < 1. \end{aligned}$$

Innen következik, hogy

$$\left\lfloor 10^{2^n}\cdot\alpha\right\rfloor = 10^{2^n}\sum_{m=1}^{n} p_m 10^{-2^m} \tag{6.40}$$

$$\left\lfloor 10^{2^{n-1}}\cdot\alpha\right\rfloor = 10^{2^{n-1}}\sum_{m=1}^{n-1} p_m 10^{-2^m}. \tag{6.41}$$

A (6.39) jobb oldalába behelyettesítve a (6.40)-et és (6.41)-t, kapjuk, hogy

$$\left\lfloor 10^{2^n}\cdot\alpha\right\rfloor - 10^{2^{n-1}}\cdot\left\lfloor 10^{2^{n-1}}\cdot\alpha\right\rfloor = 10^{2^n}\left(\sum_{m=1}^{n} p_m 10^{-2^m} - \sum_{m=1}^{n-1} p_m 10^{-2^m}\right) = p_n.$$

□

Megjegyzés. A fenti tételből is látszik, hogy nem igazán hasznos a (6.39) képlet, mivel ahhoz, hogy kiszámítsuk p_n-t, ismerni kell az α-nak 2^n darab tizedesét, vagyis ismerni kell a $p_1, p_2, \cdots p_n$ számokat.

6.58. értelmezés. *Ha p_n az n-edik prímszám, akkor bevezetjük a prímszámok halmazára a következő jelölést:*

$$\mathbb{P} = \{p_k \mid k \in \mathbb{N}^*\}.$$

A fenti jelölés segítségével megfogalmazunk néhány feladatot.

6.59. feladat. *Létezik-e olyan $f : \mathbb{N}^* \longrightarrow \mathbb{P}$ függvény, amelyre*

$$f(k) = p_k?$$

Létezik-e szürjektív $f : \mathbb{N}^* \longrightarrow \mathbb{P}$ függvény?

A Fermat-számok egy ilyen próbálkozást jelentettek a 6.59 feladat megoldására, de mivel F_5 nem prím, ez nem egy megoldás, ahogy a (6.39) formula sem jelent megoldást, mert a képletben szerepelnek a p_n prímek.

6.60. feladat. *Létezik-e olyan rekurzív összefüggés, amellyel a prímszámok mindegyike kifejezhető?*

Megemlíthetjük, hogy több változó esetén lehetséges egy olyan függvény megszerkesztése, amely prímszámot ad eredményül minden pozitív értékre, de itt is ismerni kell a k természetes számig terjedő prímek számát, a $\pi(k)$-t, és éppen ezért nem hasznos a képlet.

6.61. tétel. *Adott az $f : \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{R}$ függvény*

$$f(x,y) = \begin{cases} 0, & ha \quad x = y \\ \frac{1}{2}\left\{1 + \dfrac{x-y}{|x-y|}\right\}, & ha \quad x \neq y. \end{cases} \tag{6.42}$$

Az n-edik prímszámra érvényes a következő képlet:

$$p_n = 1 + \sum_{j=1}^{2^{2^{n-1}}} f(n, \pi(j)). \tag{6.43}$$

Bizonyítás. Az f függvényt még a következőképpen írhatjuk fel:

$$f(x,y) = \begin{cases} 1, & \text{ha} \quad x > y \\ 0, & \text{ha} \quad x = y \\ 0, & \text{ha} \quad x < y. \end{cases}$$

Innen következik, hogy

$$f(n, \pi(j)) = \begin{cases} 1, & \text{ha} \quad n > \pi(j) \\ 0, & \text{ha} \quad n \leq \pi(j). \end{cases}$$

A 6.11 tételből tudjuk, hogy

$$p_n \leq 2^{2^{n-1}}.$$

Mivel az $n > \pi(j)$ egyenlőtlenség ekvivalens a $p_n > j$ egyenlőtlenséggel, és az $n \leq \pi(j)$ ekvivalens a $p_n \leq j$ egyenlőtlenséggel, következik, hogy

$$f(n, \pi(j)) = \begin{cases} 1, & \text{ha} \quad p_n > j \\ 0, & \text{ha} \quad p_n \leq j. \end{cases}$$

Így

$$1 + \sum_{j=1}^{2^{2^{n-1}}} f(n, \pi(j)) = 1 + \sum_{j < p_n} 1 = 1 + (p_n - 1) = p_n.$$

□

Ha csupán azt vizsgáljuk, hogy létezik-e egyszerű $f : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ függvény, úgy, hogy végtelen sok értékre az f értéke prímszám legyen, akkor erre a felelet a prímszámok számának végtelensége miatt egyszerű, mert az $f(n) = n$ függvény megfelel a feltételnek. Vajon más elsőfokú függvényre igaz lesz-e az állítás? Erre ad feleletet a következő tétel.

A Dirichlet tételéből következik, hogy az $f(n) = an + b$ függvény értékei közt $(a,b) = 1$ esetén végtelen számú prímszám van.

Ha emeljük a polinom fokszámát, akkor elég nehéz feladatokat kapunk. Még a mai napig nincs eldöntve, hogy végtelen sok $n^2 + 1$ alakú prímszám létezik-e vagy sem. A sejtés az, hogy végtelen sok ilyen prímszám van.

Ismert viszont néhány olyan tétel, mely negatív eredményt ad bizonyos polinomok létezésére.

6.62. tétel. *Nem létezik olyan egész együtthatós $P \in \mathbb{Z}[x]$ polinom, amely nem állandó és prím értékeket vesz fel az összes, egy n_0-nál nagyobb természetes számra.*

Bizonyítás. Feltételezzük, hogy $P(n)$ legmagasabb fokszámú tagjának az együtthatója pozitív.
Így

$$\lim_{n\to\infty} P(n) = \infty,$$

és létezik olyan $n_0 \in \mathbb{N}^*$, hogy

$$P(n) > 1,\ \forall n > n_0.$$

Legyen $x > n_0$ és

$$P(x) = a_0x^k + \cdots = y > 1.$$

Ha kiszámítjuk a

$$P(ry+x) = a_0(ry+x)^k + \cdots$$

értéket, ahol $r \in \mathbb{N}^*$, akkor ez osztható y-nal, mivel ha minden egyes tagját kifejtjük a binomiális képlettel, akkor azon tagok összege, amelyekben nem szerepel tényezőként az y, éppen

$$a_0x^k + \cdots = y$$

lesz. Ha pedig $r \to \infty$, akkor

$$P(ry+x) \to \infty,$$

így végtelen $P(n)$-nek összetett szám értéke van.

□

6.63. tétel. *Ha P egy egész együtthatós k változós polinom,*

$$f(n) = P(n, 2^n, 3^n, \cdots, k^n),$$

és

$$\lim_{n\to\infty} f(n) = \infty,$$

akkor az $f(n)$ összetett szám végtelen sok n értékre.

Vannak olyan másodfokú polinomok, melyeknek „több" n számra lesz az értékük prímszám. Így például

$$n^2 - n + 41$$

prím értékeket vesz fel $0 \le n \le 41$ esetén, viszont $n = 42$-re osztható 41-gyel.

$$n^2 - 79n + 1601 = (n-40)^2 + (n-40) + 41$$

prímértékű lesz, ha $0 \le n \le 79$, viszont $n = 80$-ra osztható 41-gyel.

6.5. Prímszámok reciprokainak összege

Adott egy természetes számokból álló sorozat. Arra a kérdésre, hogy ezek milyen sűrűn fordulnak elő az összes természetes szám között, részleges választ kapunk, ha megvizsgáljuk, hogy a reciprok értékekből álló összeg a tagok számának növelésével korlátos marad-e vagy sem.
Ha a reciprok értékekből álló összeg nem korlátos, akkor a reciprok értékek lassan csökkennek, vagyis a sorrészlet összegei erősen növekednek, ha pedig a reciprok értékekből álló összeg korlátos, akkor nyilván a reciprok értékek gyorsan csökkennek, tehát a részletösszegek egymás utáni tagjai elég közel vannak egymáshoz.

Ha figyelembe vesszük az összes természetes számot, akkor az un. harmonikus sorra

$$1+\frac{1}{2}+\cdots\frac{1}{n}$$

$$1+\frac{1}{2}+\cdots+\frac{1}{n}>\log n,$$

ami azt jelenti, hogy a harmonikus sor nem korlátos.
Ha például az

$$1+\frac{1}{2^2}+\cdots\frac{1}{n^2}$$

sort tekintjük, akkor ez korlátos, mivel

$$\begin{aligned}1+\frac{1}{2^2}+\cdots+\frac{1}{n^2} &< 1+\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(n-1)\cdot n}= \\ &= 1+\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{n-1}-\frac{1}{n}\right)= \\ &= 2-\frac{1}{n}<2. \qquad (6.44)\end{aligned}$$

Innen következik, hogy ha a prímszámok reciprokai négyzetének összegét vizsgáljuk, akkor azok összege kisebb 2-nél.
Vajon mi történik a prímszámok reciprokaival?
Bizonyítani fogjuk, hogy a prímek reciprokainak összege nem korlátos, ami azt jelenti, hogy a prímszámok az említett szempontból a sűrűbb sorozatok közé tartoznak.

6.64. tétel. *A*

$$\sum_p \frac{1}{p}$$

sor divergens.

Bizonyítás (Erdős Pál bizonyítása).
Tételezzük fel, hogy az állítással ellentétben a

$$\sum_p \frac{1}{p}$$

sor konvergens. Ekkor létezik olyan n_0, hogy

$$\sum_{k=n+1}^{m} \frac{1}{p_k} < \frac{1}{2}, \quad m > n \geq n_0. \tag{6.45}$$

• Legyen n_0 rögzített, és egy elég nagy x természetes számra legyen

$$H_1(x) = \{n \mid n \leq x,\, p \mid n \Rightarrow p = p_i,\, i \in \{1,2,\cdots,n_0\}\},$$

vagyis a $H_1(x)$ azon x -nél nem nagyobb természetes számok halmaza, amelyek prímtényezős felbontásában csupán a $p_1, p_2, \cdots, p_{n_0}$ prímszámok szerepelnek. Jelöljük a $H_1(x)$ elemeinek számát $f(x)$-szel, ($f(x) = |H_1(x)|$). Értelmezzük még a következő halmazt:

$$H_2(x) = \{n \mid n \leq x, \exists p \mid n, p = p_i, i > n_0\},$$

amely azon x-nél nem nagyobb természetes számok halmaza, melyek prímtényezős előállítása legalább egy olyan prímszámot tartalmaz, amely különbözik a $p_1, p_2, \cdots p_{n_0}$ prímektől. Ha x-et elég nagynak választjuk meg, akkor a $H_2(x)$ nem üres halmaz. Jelöljük a $H_2(x)$ elemeinek számát $g(x)$-szel ($g(x) = |H_2(x)|$).

Nyilvánvaló, hogy a $H_1(x)$ és $H_2(x)$ tartalmazza az összes x-nél nem nagyobb természetes számot, vagyis

$$f(x) + g(x) = x. \tag{6.46}$$

• A következőkben felső becslést adunk $f(x)$-re.
Minden természetes szám egyértelműen írható fel egy négyzetszám és egy négyzetmentes szám szorzataként. Valóban, ha

$$n = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k} \cdot p_{k+1}^{2\alpha_{k+1}+1} \cdots p_{k+l}^{2\alpha_{k+l}+1},$$

akkor

$$n = u^2 \cdot v, \quad u = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p_{k+1}^{\alpha_{k+1}} \cdots p_{k+l}^{\alpha_{k+l}}, \quad v = p_{k+1} \cdots p_{k+l}.$$

Ez a felbontás egyértelmű.
Tételezzük fel ugyanis, hogy

$$n = u_1^2 \cdot v_1,$$

ahol v_1 négyzetmentes.
Ha v_1 nem tartalmazza valamelyik p_{k+i}-t, $i \in \{1,2,\cdots,l\}$, akkor $p_{k+i}^{2\alpha_{k+i}+1}$ az u_1^2-ben kell szerepeljen mint tényező, ami ellentmondás, így $v_1 = v$, ahonnan következik, hogy $u = u_1$.

Legyen most $n \in H_1(x)$ és $n = u^2 \cdot v$, ahol v négyzetmentes. Mivel $n \leq x$ következik, hogy

$$u \in \{1,2,\cdots,\lfloor\sqrt{x}\rfloor\} \tag{6.47}$$

és

$$v \in \{1, p_1, p_2, \cdots, p_{n_0}, p_1p_2, \cdots, p_1p_{n_0}, \cdots, p_{n_0-1}p_{n_0}, p_1p_2p_3, \cdots, p_1p_2\cdots p_{n_0}\} \tag{6.48}$$

A (6.47) képletből következik, hogy az u tényező $\lfloor\sqrt{x}\rfloor$ szám közül választható, míg a (6.48) képletből, hogy a v

$$C_{n_0}^0 + C_{n_0}^1 + \cdots + C_{n_0}^{n_0} = 2^{n_0}$$

szám közül kerülhet ki. Így az összes lehetőségek maximális száma

$$f(x) \leq 2^{n_0} \cdot \lfloor\sqrt{x}\rfloor \leq 2^{n_0} \cdot \sqrt{x}. \tag{6.49}$$

• A következőkben alsó becslést keresünk $f(x)$-re. (6.46)-ból következik, hogy

$$f(x) = x - g(x), \tag{6.50}$$

tehát ahhoz, hogy alsó becslést kapjunk $f(x)$-re, a $g(x)$-re fogunk adni egy felső becslést.
Tételezzük fel, hogy p_r a legnagyobb olyan prímszám, amelyre $p_r \leq x$. A $H_2(x)$ halmaz értelmezése szerint az n lehetséges értékei

$$\begin{array}{llll} p_{n_0+1}, & 2p_{n_0+1}, & 3p_{n_0+1}, & \cdots, \quad \left\lfloor \frac{x}{p_{n_0+1}} \right\rfloor p_{n_0+1} \\ p_{n_0+2}, & 2p_{n_0+2}, & 3p_{n_0+2}, & \cdots, \quad \left\lfloor \frac{x}{p_{n_0+2}} \right\rfloor p_{n_0+2} \\ \cdots & & & \\ p_r, & 2p_r, & 3p_r, & \cdots, \quad \left\lfloor \frac{x}{p_r} \right\rfloor p_r. \end{array} \tag{6.51}$$

A fenti számok között lehetnek egyenlők is, így az n szám maximálisan

$$\sum_{i=n_0+1}^{r} \left\lfloor \frac{x}{p_i} \right\rfloor$$

szám közül kerülhet ki, tehát

$$g(x) \leq \sum_{i=n_0+1}^{r} \left\lfloor \frac{x}{p_i} \right\rfloor < x \cdot \sum_{i=n_0+1}^{r} \frac{1}{p_i}. \tag{6.52}$$

A (6.45) és a (6.52)-ból következik, hogy

$$g(x) < x \cdot \frac{1}{2} = \frac{x}{2}.$$

A (6.50) és a fenti egyenlőségből

$$f(x) > x - \frac{x}{2} = \frac{x}{2}, \tag{6.53}$$

vagyis egy alsó korlátot adtunk az $f(x)$-re.

A (6.49) és (6.53) alapján

$$\frac{x}{2} < f(x) \leq 2^{n_0} \cdot \sqrt{x},$$

vagyis

$$\begin{aligned} \frac{x}{2} &< 2^{n_0} \cdot \sqrt{x} \\ x &< 2^{2n_0+2}. \end{aligned}$$

Tehát az $x = 2^{2n_0+2}$ választással ellentmondáshoz jutunk.

□

A következőkben egy olyan bizonyítást ismertetünk, amelyben egy becslést is kapunk a $\sum_{p \leq x} \frac{1}{p}$-re. Ez a bizonyítás Eulertől származik.
Amint láttuk, az előbbi bizonyítás csak a természetes számok szerkezeti felépítését használja, de nem ad semmilyen korlátot, míg a következő tétel bizonyításában kapunk egy alsó korlátot, de ehhez szükségünk lesz néhány analízisből ismert segédeszközre.

6.65. tétel. *Adott $x > 2$ valós számra*

$$\sum_{p \leq x} \frac{1}{p} > \log\log x - 2. \tag{6.54}$$

Bizonyítás. A bizonyításban használni fogjuk a következő egyenlőtlenségeket:

$$\sum_{k \leq x} \frac{1}{k} > \log x, \quad x \geq 2 \tag{6.55}$$

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \leq x + x^2, \quad 0 \leq x \leq \frac{1}{2}, \tag{6.56}$$

valamint a

$$\sum_{k \leq x} \frac{1}{k^2} < 2 \tag{6.57}$$

egyenlőtlenséget (lásd (6.44)-t).
Legyen $x \geq 3$ ($x < 3$-ra könnyen ellenőrizhető a (6.54) egyenlőtlenség) és

$$A_x = \prod_{p \leq x} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{\nu_p}}\right) = \prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{\nu_{p_i}}}\right), \tag{6.58}$$

ahol $p^{\nu_p - 1} \leq x < p^{\nu_p}$.
A második alakja az A_x-nek azt jelenti, hogy pontosan k darab x-nél kisebb prímszám van.

Ha az A_x jobb oldalán elvégezzük a szorzást, akkor a

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} \tag{6.59}$$

számok reciprok értékeit kapjuk, ahol

$$0 \leq \alpha_i \leq \nu_{p_i}, \quad i \in \{1, 2, \cdots, k\}.$$

Mivel (6.59) felírásában az összes prímszámot használjuk, ezek között az összes x-nél kisebb természetes szám megtalálható. Így, (6.55) miatt

$$A_x > 1 + \frac{1}{2} + \cdots + \frac{1}{\lfloor x \rfloor} > \log x. \tag{6.60}$$

Most a (6.58) képletet másképpen próbáljuk felírni. Mivel a bal oldali szorzatban szereplő zárójel egy mértani sor, részletösszege

$$\begin{aligned} A_x &< \prod_{p \leq x} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{\nu_p}} + \frac{1}{p^{\nu_p+1}} + \cdots\right) = \\ &= \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}. \end{aligned}$$

Innen, (6.60) szerint

$$\log x < \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

Mivel $x \geq 3$, a fenti egyenlőtlenség mindkét oldala pozitív, tehát logaritmálhatjuk. Így

$$\log\log x < \sum_{p \leq x} \log \frac{1}{1 - \frac{1}{p}}.$$

Használva (6.56)-et ($x = \dfrac{1}{p}$-re) kapjuk, hogy

$$\log\log x < \sum_{p \leq x} \left(\frac{1}{p} + \frac{1}{p^2}\right) = \sum_{p \leq x} \frac{1}{p} + \sum_{p \leq x} \frac{1}{p^2}, \tag{6.61}$$

de (6.57) alapján

$$\sum_{p \leq x} \frac{1}{p^2} < \sum_{k \leq x} \frac{1}{k^2} < 2,$$

így

$$\sum_{p \leq x} \frac{1}{p} > \log\log x - 2.$$

□

Megjegyzés. Ennél még „jobb" összefüggés is igaz: $\sum_{p\le x}\frac{1}{p}$ aszimptotikusan egyenlő $\log\log x$-szel, vagyis

$$\lim_{x\to\infty}\frac{\sum_{p\le x}\frac{1}{p}}{\log\log x}=1. \tag{6.62}$$

F. Mertens bizonyította, 1874-ben [57] hogy:

6.66. tétel. *$x\ge 2$-re*

$$\sum_{p\le x}\frac{1}{p}=\log\log x+A+O\left(\frac{1}{\log x}\right),$$

ahol $A>0$ egy pozitív állandó.

A továbbiakban igazolunk egy aszimptotikus egyenlőtlenséget, de nem a $\sum_{p\le x}\frac{1}{p}$ összegre, hanem a $\sum_{p\le x}\frac{\log p}{p}$ összegre.

6.67. tétel.

$$\lim_{x\to\infty}\frac{\sum_{p\le x}\frac{\log p}{p}}{\log x}=1. \tag{6.63}$$

Bizonyítás. Itt is használunk néhány segéd összefüggést:

$$n\cdot\log n-n<\sum_{k=1}^{n}\log k<(n+1)\log(n+1)-n \tag{6.64}$$

$$\log(1+x)\le x \tag{6.65}$$

$$\sum_{k=2}^{\infty}\frac{\log k}{k(k-1)}<4. \tag{6.66}$$

A (6.19) alapján

$$\prod_{p\le n}p\le 4^{n-1}<4^n.$$

Ezt logaritmálva kapjuk, hogy

$$\sum_{p\le x}\log p<n\cdot\log 4. \tag{6.67}$$

Emlékeztetünk, hogy $n!$ a Legendre-formula szerint

$$n!=\prod_{p\le n}p^{\alpha(n,p)},$$

ahol

$$\alpha(n,p)=\sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

Ezt logaritmálva kapjuk, hogy

$$\sum_{k=1}^{n}\log k=\sum_{p\le n}\alpha(n,p)\log p=\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\cdots\right)\log p. \tag{6.68}$$

A továbbiakban a $\sum_{p\le x}\frac{\log p}{p}$ sort alulról és felülről fogjuk becsülni, úgy, hogy határértékre térve mindkét becslés határértéke 1 legyen.
A (6.68) és (6.64)-ből következik, hogy

$$\begin{aligned}\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\cdots\right)\cdot\log p &= \sum_{k=1}^{n}\log k=\\ &= \sum_{p\le n}\alpha(n,p)\log p<\\ &< (n+1)\cdot\log(n+1)-n. \end{aligned}\tag{6.69}$$

Az utóbbi kifejezés viszont így is írható:

$$(n+1)\log(n+1)-n=n\cdot\log\left(1+\frac{1}{n}\right)+n\log n+\log(n+1)-n.$$

Alkalmazva (6.65)-ot $x=\frac{1}{n}$-re kapjuk, hogy

$$(n+1)\log(n+1)-n\le 1+n\log n+\log(n+1)-n. \tag{6.70}$$

Ha a (6.69) bal oldalát átírjuk, alkalmazzuk (6.67)-at, akkor

$$\begin{aligned}\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\cdots\right)\log p &\ge \sum_{p\le n}\left\lfloor\frac{n}{p}\right\rfloor\log p\ge\sum_{p\le n}\log p\left(\frac{n}{p}-1\right)=\\ &= n\cdot\sum_{p\le n}\frac{\log p}{p}-\sum_{p\le n}\log p\ge\\ &\ge n\cdot\sum_{p\le n}\frac{\log p}{p}-n\cdot\log 4. \end{aligned}\tag{6.71}$$

A fenti képletben megjelenik a $\sum_{p\le n}\frac{\log p}{p}$, és ez indokolja, hogy a bizonyítást az $n!$ vizsgálatával kezdtük.
A (6.69), (6.70) és (6.71)-ből következik, hogy

$$n\cdot\sum_{p\le n}\frac{\log p}{p}-n\cdot\log 4<1+n\cdot\log n-n+\log(n+1)$$

$$\sum_{p\le n}\frac{\log p}{p} < \log 4 + \log n - 1 + \frac{\log(n+1)}{n} + \frac{1}{n}.$$

Innen

$$\sum_{p\le n}\frac{\log p}{p} < \log n + 2. \tag{6.72}$$

Az n_0-t úgy választjuk meg, hogy

$$\frac{\log(n_0+1)}{n_0} + \frac{1}{n_0} < 3 - \log 4.$$

Ez lehetséges, mivel $3 > \log 4$ és

$$\lim_{n\to\infty}\left(\frac{\log(n+1)}{n} + \frac{1}{n}\right) = 0.$$

Most alsó becslést adunk a $\sum_{p\le n}\frac{\log p}{p}$-re ha $n \ge n_0$.
A (6.68) és (6.64)-ből következik, hogy

$$\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor + \left\lfloor\frac{n}{p^2}\right\rfloor + \cdots\right)\log p = \sum_{k=1}^{n}\log k > n\cdot\log n - n. \tag{6.73}$$

A bal oldali összegre a következő egyenlőtlenségeket írhatjuk fel:

$$\begin{aligned}\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor + \left\lfloor\frac{n}{p^2}\right\rfloor + \cdots\right)\log p &< \sum_{p\le n}\left(\frac{n}{p} + \frac{n}{p^2} + \cdots\right)\log p = \\ &= n\cdot\sum_{p\le n}\frac{\log p}{p} + \\ &+ n\cdot\sum_{p\le n}\left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right)\log p.\end{aligned} \tag{6.74}$$

Használva a végtelen mértani sor összegképletét, majd (6.66)-et

$$\begin{aligned}\sum_{p\le n}\left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right)\log p &= \sum_{p\le n}\log p\cdot\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}} = \\ &= \sum_{p\le n}\log p\frac{1}{p(p-1)} < \\ &< \sum_{k=2}^{\infty}\log k\frac{1}{k(k-1)} < 4.\end{aligned}$$

Ezt behelyettesítve (6.74)-be, kapjuk, hogy

$$\sum_{p\le n}\left(\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\cdots\right)\log p<n\cdot\sum_{p\le n}\frac{\log p}{p}+4\cdot n,$$

majd (6.73) alapján

$$n\cdot\sum_{p\le n}\frac{\log p}{p}+4\cdot n>n\cdot\log n-n,$$

vagy

$$\sum_{p\le n}\frac{\log p}{p}>\log n-5. \tag{6.75}$$

(6.75) és (6.72) alapján

$$\log n-2>\sum_{p\le n}\frac{\log p}{p}>\log n-5.$$

Ezt az egyenlőtlenséget végigosztva $\log n$-nel, majd határértékre térve n szerint, kapjuk, hogy

$$\lim_{x\to\infty}\frac{\sum\limits_{p\le x}\frac{\log p}{p}}{\log x}=1.$$

□

Az ikerprímek reciprokainak összegére érvényes a következő képlet, amelyet először V. Brun bizonyított 1919-ben [13].

6.68. tétel. *$x\ge 2$-re*

$$\sum_{p\in\mathbb{P}_2}\frac{1}{p}=B<\infty,$$

ahol $B=1.9021660583...$ a Brun-féle állandó.

Megjegyzések.

1. A Brun-féle állandó értékét az ikerprímek reciprokainak 10^{16} történő kiszámításával határozták meg [59].

2. A Brun-féle állandóval kapcsolatos számítások során Nicely egy olyan lebegőpontos hibát fedezett fel a Pentium mikrocsipjében, amely az Intel cégnek több millió dollárjába került [22].

6.6. Kutatási feladatok

1. kutatási feladat. A Dirichlet tétel alapján megfogalmazhatjuk azt a kérdést, milyen $a_1,b_1,\ldots,a_k,b_k$ természetes számokra vonatkozó feltételek mellett lesznek egyszerre prímszámok az

$$a_1n+b_1,a_2n+b_2,\ldots a_kn+b_k,$$

számok végtelen n természetes számra.
$k = 1$-re a Dirichlet tétel adja meg a feleletet.
$k-2$, $a_1 = b_1 = 1$, $b-1 = 0$, $b_2 = 2$ esetén az ikerprím sejtés következik innen.
A következő sejtést L. E. Dickson fogalmazta meg 1904-ben [23].

6.69. sejtés. *Adottak az $a_1, b_1, \ldots, a_k, b_k$ egész számok, amelyekre $a_i > 0$, $(a_i, b_i) = 1$, $i \in \{1, 2, \ldots, k\}$, és bármely $p < k$ prímszámra létezik olyan n természetes szám, amelyre az*

$$a_i n + b_i \not\equiv 0 \pmod{p},\ i \in \{1, 2, \ldots, k\}.$$

Ekkor létezik végtelen n természetes szám, amelyre

$$a_i n + b_i \in \mathbb{P},\ i \in \{1, 2, \ldots, k\}.$$

Ennél általánosabb sejtést fogalmazott meg A. Schinzel és W. Sierpinski 1958-ban, [63], [64] amely H-hipotézis néven ismert.

6.70. sejtés (H-hipotézis). *Adottak a $P_1, P_2, \ldots, P_k$ egész együtthatós, irreducibilis polinomok úgy, hogy a főegyütthatójuk pozitív. Tudva, hogy bármely $p \in \mathbb{P}$ prímszámra létezik olyan n természetes szám, amelyre az*

$$P_i(n) \not\equiv 0 \pmod{p},\ i \in \{1, 2, \ldots, k\},$$

létezik végtelen n természetes szám, amelyre a $P_1(n), P_2(n), \ldots, P_k(n)$ mindegyike prímszám.

Keveset tudunk mondani sajátos polinomok esetén is, például egy nagyon híres sajátos esete a fenti sejtésnek az $n^2 + 1$ polinom.

6.71. feladat. *Végtelen $n^2 + 1$ alakú prímszám van?*

Ebhez kapcsolódik a G. H. Hardytól és J. E. Littlewoodtól származó sejtés [40].

6.72. sejtés. *Ha $P(n)$ azon n-nél kisebb prímek száma, amelyek felírhatóak $n^2 + 1$ alakban, akkor*

$$\lim_{n\to\infty} \frac{P(n)}{\frac{\sqrt{n}}{\log n}} = c,$$

ahol

$$c = \prod_{p\in\mathbb{P}} \left(1 - \frac{(-1)^{\frac{p-1}{2}}}{p-1}\right) = 1.3727...$$

Ha a polinom kétváltozós, akkor többet tudunk mondani. J. Friedlander és H. Iwaniec bizonyították, hogy végtelen

$$x^2 + y^4, \quad x, y \in \mathbb{N}$$

alakú prímszám van [30].

Más eredmények és feladatok találhatók a R. Guy [38] könyvében (A1 feladat).

2. kutatási feladat.
A. Schinzel 1958-ban [63] a következő sejtést fogalmazta meg.

6.73. sejtés. *Minden $n \geq 1$ természetes szám felírható*

$$n = \frac{p+1}{q+1}$$

alakban, ahol $p, q \in \mathbb{P}$ prímszámok.

M. M. Conroy 2001 [18] ellenőrizte a sejtést minden $n \leq 10^9$ természetes számra. Könnyen igazolható, hogy ha $q \in \mathbb{P}$ egy rögzített prím, akkor végtelen sok olyan n természetes szám létezik, amelyre

$$n = \frac{p+1}{q+1},$$

ahol $p \in \mathbb{P}$.

Adott $a \in \mathbb{N}^*$-ra és $q \in \mathbb{P}$-re legyen

$$N(q,a) = \left\{ n \mid \exists p \in \mathbb{P},\ n = \frac{p+a}{q+1} \right\}.$$

Bege Antal és Fülöp Péter [9] a következő feladatot fogalmazták meg.

6.74. feladat. *Adottak a $q \in \mathbb{P}$, $q \neq 2$ prímszám, $b \neq c$ természetes számok, amelyek relatív prímek $(q+1)$-gyel. Van-e az $N(q,b)$ és $N(q,c)$ halmazoknak végtelen közös eleme?*

Ha a fenti sejtés igaz $b = 1$ és $c = 3$-ra, akkor következik az ikerprím sejtés helyessége.

Igaz az a tulajdonság is, hogy az

$$M = \left\{ \frac{p+1}{q+1} \mid p, \in \mathbb{P} \right\}$$

halmaz sűrű $\mathbb{R}^+$-ban.

Feladatok

6.1. Tegyük fel, hogy p és $8p-1$ prímszámok. Lehet-e prímszám $8p+1$ is?

6.2. Milyen n egész számokra prímszám

$$n^4 + 4\,?$$

6.3. Bizonyítsuk be, hogy végtelen sok $4n+3$ alakú prímszám létezik.

6.4. Bizonyítsuk be, hogy végtelen sok olyan k páratlan természetes szám létezik, melyre a

$$2^{2^n}+k, \quad (n=1,2,...)$$

számok mind összetettek.

6.5. Melyek azok a p prímszámok, amelyekre a

$$2p+1,\ 3p+2,\ 4p+3,\ 6p+1$$

számok mindegyike prímszám?

6.6. Legyen p_n az n-edik prímszám $(n>1)$ és

$$N = p_n + p_{n+1}.$$

Bizonyítsuk be, hogy N legalább három, nem feltétlenül különböző prímszám szorzata.

6.7. Bizonyítsuk be, hogy tetszőleges k természetes számhoz található olyan n_k természetes szám, hogy $n > n_k$ esetén

$$[1,2,3,\ldots,n] > n^k.$$

6.8. Adott a következő sorozat

$$101,\ 10\,101,\ 1\,010\,101,\ldots$$

Határozzuk meg a sorozat azon elemeit, amelyek prímszámok.

6.9. Bizonyítsuk be, hogy a

$$2^{2^{1999}}-1$$

számnak van 1999 darab különböző prímosztója.

6.10. Adott az

$$a_n = 2^n + 49, \quad n \in \mathbb{N}$$

sorozat. Határozzuk meg azon $a_n,\ a_{n+1}$ egymás utáni tagokat, amelyekre

$$a_n = p\cdot q,\ a_{n+1} = r\cdot s,$$

ahol $p<q,\ r<s$ olyan prímszámok, amelyekre

$$q-p = s-r.$$

6.11. Adott az $n \geq 2$ természetes szám. Bizonyítsuk be, hogy ha

$$k^2 + k + n$$

prímszám bármely $0 \leq k \leq \sqrt{\frac{n}{3}}$ természetes számra, akkor $k^2 + k + n$ prímszám lesz az összes $0 \leq k \leq n-2$ természetes számra is.

6.12. Adott a $p > 2$ prímszám és az $A = \{1, 2, \ldots, 2p\}$ halmaz. Az A-nak hány olyan részhalmaza van, amely p elemet tartalmaz, és amelyben az elemek összege osztható p-vel?

6.13. Létezik-e olyan 14 egymás utáni természetes szám, hogy mindegyik osztható legyen az 1 és 12 közötti prímszámok valamelyikével (egy szám lehet osztható több 1 és 11 közötti prímszámmal is)?

6.14. Bizonyítsuk be, hogy bármely n természetes számra létezik n darab egymás utáni természetes szám, amelyek közül egyik sem prímszám vagy prímszám hatvány.

6.15. Adott a $p > 2$ prímszám. Bizonyítsuk be, hogy a

$$\sum_{n=0}^{p} \binom{p}{n} \cdot \binom{p+n}{n}$$

és

$$2^p + 1$$

p^2-tel való osztási maradéka egyenlő.

6.16. Adott a $p > 3$ prímszám. Legyen $k = \left\lfloor \frac{2p}{3} \right\rfloor$. Bizonyítsuk be, hogy

$$\binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{k}$$

osztható p^2-tel.

6.17. Legyen n tetszőleges természetes szám. Adjunk példát olyan egész együtthatós reducibilis $P(x)$ polinomra, amelynek m különböző természetes számhoz tartozó helyettesítési értéke m különböző prímszám.

6.18. A $P_n(x)$ polinomokat a következőképpen értelmezzük:

$$\begin{aligned} P_0(x) &= 1 \\ P'_{n+1}(x) &= (n+1) \cdot P_n(x+1), \quad \forall n \geq 0, \\ P_{n+1}(0) &= 0 \end{aligned}$$

ahol $P'(x)$ a $P(x)$ deriváltja. Bontsuk prímtényezők szorzatára a $P_{100}(1)$-et.

6.19. Adott az $f(x)$ nem állandó, egész együtthatós polinom. Bizonyítsuk be, hogy végtelen egész számra az $|f(n)|$ összetett.

6.20. 2^n darab prímszámot egymás után írunk. Ha tudjuk, hogy n-nél kevesebb különböző prímszám van a sorban, bizonyítsuk be, hogy kiválasztható egy olyan „kompakt" (egymás utáni tagokból álló) csoport, melyek szorzata teljes négyzet.

6.21. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\left| n \cdot \sum_{p \le n} \frac{\log p}{p} - \log(n!) \right| < 4n.$$

6.22. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\left| \sum_{p \le n} \frac{\log p}{p} - \log n \right| < 5.$$

6.23. Legyen P_n az első n prím szorzata

$$P_n = p_1 p_2 \cdots p_n.$$

Bizonyítsuk be, hogy p_{n+1} az egyetlen olyan m természetes szám, amelyre

$$1 < 2^m \left(\sum_{d \mid P_n} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} \right) < 2,$$

ahol $\mu(d)$ a Möbius-féle függvény.

6.24. $x \ge 2$ valós számra bizonyítsuk be, hogy

$$\pi(x) - \pi(\sqrt{x}) = \lfloor x \rfloor - \sum_{p \le \sqrt{x}} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{p < q \le \sqrt{x}} \left\lfloor \frac{x}{pq} \right\rfloor - \ldots.$$

6.25. Ha igaz a H-hipotézis (6.70 sejtés), bizonyítsuk be, hogy végtelen n természetes számra

$$\sigma\big(\tau(n)\big) = \tau\big(\sigma(n)\big),$$

ahol $\sigma(n)$ az osztók összege és $\tau(n)$ az osztók száma.

Könyvészet

[1] Aigner, Martin–Ziegler, Günter M., *Proofs from THE BOOK*, Springer Verlag, Berlin, 1998. Magyarul: *Bizonyítások a Könyvből*, Typotex, Budapest, 2004.

[2] Anisiu, M-C., Blázsik, Z., Kása, Z., Maximal Complexity of Finite Words, *Pure Math. and Appl.*, **13**, 1–2 (2002) pp. 39–48.

[3] T. M. Apostol, *Introduction to analytic number theory,* Springer Verlag, New York, 1976.

[4] Bach, E.–Shallit, J., *Algorithmic nuber theory, Vol. 1*, MIt Press, Cambridge, 1996.

[5] Bays, C.–Hudson, R. H., A new bound for the smallest x with $\pi(x) < li(x)$, *Math. Comp.*, **69** (2000), 1285–1296.

[6] Bege Antal, *Bevezetés a számelméletbe,* Scientia Kiadó, Kolozsvár, 2002.

[7] Bege Antal–Demeter Albert–Lukács Andor, *Számelméleti feladatgyűjtemény,* Scientia Kiadó, Kolozsvár, 2002.

[8] Bege Antal, *Differenciaegyenletek,* Egyetemi Kiadó, Kolozsvár, 2005.

[9] Bege Antal–Fülöp Péter István, Some results concerning a conjecture of Schinzel, (kézirat)

[10] Bege, A.–Kása, Z., Coding Objects Related to Catalan Numbers, *Studia Universitatis Babeş-Bolyai, Informatica*, **46**, 1 (2001) pp. 31–40.

[11] J. Berstel, An exercise on Fibonacci representations, *Theor. Inform. Appl.*, **35** (2001), 491–498.

[12] Bond, J.–Iványi, A., Modeling of Interconnection Networks Using de Bruijn Graphs, *Third Conference of Program Designers*, July 1–3, 1987, Eötvös Loránd University, Faculty of Natural Sciences, Budapest, 1987, pp. 75-88.

[13] Brun, V., La serie $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\ldots$ ou les denominateurs sont "nombres premiers jumeaux" est convergente ou finite, *Bull Sci. Math.*, **43** (1919), 100–104 and 124–128.

[14] Buell, D–Young, J., The twentieth Fermat number is composite, *Math. Comp.*, **50** 1988, 261–263.

[15] Caldwell, C. K., Twin primes,
`http://primes.utm.edu/top20/page.php?id=1`

[16] Choffrut, C.–Karhumäki, J., Combinatorics of Words, *Handbook of Formal Languages, vol. I–III.*, Springer Verlag, 1997. ed. G. Rozemberg, A. Salomaa.

[17] Clay Mathematics Institute,
`http://www.claymath.org`

[18] Conroy, M. M., A sequence related to a conjecture of Schinzel, *J. Integer Sequences*, **4** 2001, Article 01.1.7.

[19] Cofman, J., Catalan Numbers for the Classroom?, *Elemente der Mathematik*, **52** (1997) pp. 108–117.

[20] Cormen, T. H.–Leiserson, C. E.–Rivest, R. R., *Algoritmusok*, Műszaki Könyvkiadó, Budapest, 2001.

[21] Cormen, T. H.–Leiserson, C. E.–Rivest, R. R.–Stein, C., *Új algoritmusok*, Scolar Kiadó, Budapest, 2003.

[22] Crandall, R.–Pomerance, C., *Prime numbers*, Springer, 2005.

[23] Dickson, L. E., A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.*, **33** (1904), 155–161.

[24] M. Edson, L. Q. Zamboni, On the representations of positive integers in the Fibonacci base, *Theoret. Comput. Sci.*, **326** (2004), 241–260.

[25] Erdős Pál, Problems and results on the difference of consecutive primes, *Publicationes Math. Debrecen*, **1** (1949–50), 33–37.

[26] Erdős Pál–Surányi János, *Válogatott fejezetek a számelméletből*, Polygon, Szeged, 1996.

[27] Ferenczi, S., Les tranformation de Chacon: combinatoire, structure géométrique, lien avec les systèmes de complexité $2n+1$, *Bull. Soc. math. France*, **123** (1995) pp. 271–292.

[28] Ferenczi, S.–Kása, Z., Complexity for Finite Factors of Infinite Sequences, *Theoretical Computer Science*, **218** (1999) pp.l 177–195.

[29] Fogg, N. Pytheas, *Substitutions in Dynamics, Arithmetics and Combinatorics*, Lecture Notes in Mathematics, 1784. Springer, 2002. Eds. V. Berthé, S. Ferenczi, C. Muaduit, A. Siegel.

[30] Friedlander, J.–Iwaniec, H., The polynomial X^2+Y^4 captures its primes, *Ann. of Math.*, **148** (1998), 945–1040.

[31] Fürstenberg, H., On the infinitude of primes, *Amer. Math. Monthly* **62** (1955), 353.

[32] Georgescu, H., A Dirichlet-féle skatulyaelv, *Matematikai Lapok (Kolozsvár)*, **43**, 3 (1995) pp. 161–165.

[33] GIMPS, `http://www.mersenne.org/prime.htm`

[34] Graham, R. L.–Knuth, D. E.–Patashnik, O., *Konkrét matematika*, Műszaki Könyvkiadó, Budapest, 1998.

[35] Granville, A.–Martin, G., Prime number races, *Amer. Math. Monthly,* **113** (2006), 1–33.

[36] Gourdon, X.–Sebah, P, Numbers and constants and computation, 2004 `http://numbers.computation.free.fr/Constants/constants.html`

[37] Guy, R.–Nowakovski, R., Discovering primes with Euclid, *Delta,* **5**(1975), 49–63.

[38] Guy, R. K., *Unsolved problems in number theory,*, (third edition), Springer, New York, 2004.

[39] Hajnal Péter, *Elemi kombinatorikai feladatok*, Polygon, Szeged, 1997.

[40] Hardy, G. H.–Littlewood, J. E., Some problems of partitio numerorum III.: On the expression of a number as a sum of primes, *Acta. Math.,* **44** (1923), 1–70.

[41] Hardy, G. H.–Wright, E. M. *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1998.

[42] Littlewood, J. E., Distribution des nombres premiers, *C. R. Acad. Sci. Paris,* **158** (1914), 1869–1872.

[43] Hoşten, S.–Morris, W. D., The order dimension of the complete graph, *Discrete Math.,* **201** (1999), 133–139.

[44] Iorga, V.–Fătu, I., Asupra partiţiilor unui număr natural, *Gazeta de Informatică*, 1993, nr. 2.

[45] Iványi, A, On the *d*-complexity of Words, *Annales Univ. Sci. Budapest. Sect. Comput.* **8** (1987) pp. 69-90.

[46] Kása Zoltán, *Combinatorică cu aplicaţii*, Presa universitară clujeană, Cluj-Napoca, 2003.

[47] Kása, Z., On the *d*-complexity of Strings, *Pure Math. and Appl.*, **9**, 1–2 (1998) pp. 119–128.

[48] Kása Zoltán–Bege Antal, *Matematică discretă*, Univ. Babeş-Bolyai, Cluj-Napoca, 2002.

[49] Knuth, D. E., *A számítógép-programozás művészete 1., Alapvető algoritmusok*, 2. kiadás, Műszaki Könyvkiadó, Budapest. 1994.

[50] Laczkovich Miklós, *Sejtés és bizonyítás*, Typotex, Budapest, 1998.

[51] J. C. Lagarias, An elementary problem equivalent to the Riemann hypotheis, *Amer. Math. Montly*, **109** (2002), 534–543.

[52] Livovschi, L.–Georgescu, H., *Sinteza şi analiza algoritmilor*, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1986.

[53] Lothaire, M. *Combinatorics on Words*, Addison-Wesley Publishing Company, 1983.

[54] Lothaire, M. *Algebraic Combinatorics on Words*, Cambridge University Press, 2002.

[55] Lovász László, *Kombinatorikai problémák és feladatok*, Typotex Kiadó, Budapest, 1999.

[56] Martin, M. H., A Problem in Arrangements, *Bull. A. M. S.*, **40** (1934) pp. 859–864.

[57] Mertens, F., Ein Beitrag zur analytischen Zahlentheorie, *Crelle's Journal*, **78** (1874), 46–62.

[58] Mills, W. H. A prime representing function, *Bull. American Math. Soc.*, **53** (1947), 604

[59] Nicely, T., Prime constellations project, 2004.
`http://www.trnicely.net/counts.html`

[60] Nolan, J. M.–Savage, C. D.–Wilf, H. S., Basis Partitions, *Discrete Math.*, **179**, 1–3 (1998) pp. 277–283.

[61] Porter, J. W., On a theorem of Heilbronn, *Mathematika*, **22** (1975), 20–28.

[62] G. Robin, Grandes valeurs de la function somme des diviseurs et hypothése de Riemann, *J. Math. Pures Appl.*, **63** (1984), 187–213.

[63] Schinzel, A.–Sierpinski, W., Sur certaines hypothéses concernant les nombres premiers, *Acta Arith.*, **4** (1958), 185–208.

[64] Schinzel, A.–Sierpinski, W., Erratum to "Sur certaines hypothéses concernant les nombres premiers", *Acta Arith.*, **5** (1959), 259.

[65] Selfridge, J.–Hurwitz, A., Fermat numbers and Mersenne numbers, *Math. Comp.*, **18** (1964), 146–148.

[66] Sierpinski, W., Sur une formule donnant tous les nombres premiers, *Comptes Rendus Acad. Sci., Paris*, **235** (1952), 1078–1079.

[67] Tomescu, I., *Introducere în combinatorică*, Editura Tehnică, Bucureşti, 1972.

[68] Turán Pál–Gyarmati Edit, *Számelmélet*, Tankönyvkiadó, Budapest, 1976.

[69] Vilenkin, N. J., *Kombinatorika*, Műszaki Kiadó, Budapest, 1971.

[70] Wright, E. M., A prime representing function, *Amer Math. Monthly,* **58** (1951), 616–618.

[71] Wright, E. M., A class of representing functions, *J. London Math. Soc.*, **29** (1954), 63–71.

Tárgy- és névmutató

alapfelbontás, 64
alappartíció, 64
aranymetszési állandó, 90

Bernoulli
    -polinomok, 27
    -számok, 27
Bernoulli-polinom, 27
Bernoulli-számok, 27
Berstel, J., 94
Bertrand, J. L. F., 172
Bertrand-posztulátum, 172
bináris fák
    levelek megszámolása, 22
    megszámolása, 21
bináris fák kódolása, 125
Binét-formula, 90
binomiális képlet általánosítása, 12
bonyolultság, 108
    d-bonyolultság, 109, 117
    alsó maximális, 109
    alsó teljes, 109
    felső maximális, 109
    globális maximális, 109, 113
    maximális, 108, 112
    részszó-, 110
    teljes, 109, 115
Brun, V., 195
Brun-állandó, 195

Catalan, E. Ch., 122
Catalan-szám, 22
Catalan-számok, 124
Cauchy-szorzat, 10
Csebisev, P., 172

De Bruijn-gráf, 101
De Bruijn-szó, 102
dekódolás, 129
Descartes-szorzat, 55
Dickson, L. E., 196
Dirichlet konvolúció, 33
Dirichlet-sor, 34
Dirichlet-sorok, 29
Durfee-négyzet, 63
Dyck-szó, 122

egyszerű lánctört, 142
Eratoszthenész, 153
eratoszthenészi szita, 153
Erdős Pál, 70, 169, 172, 183, 187
Erdős, Pál, 72
Erdős-Szekeres tétel, 70
Euklidész, 154
Euklidész második tétele, 154
Euklidész-számok, 154
euklidészi algoritmus, 135
    legkisebb maradékos, 145
Euler, L., 156, 190
Euler-féle φ függvény, 30, 83

Fürstenberg, H., 160
fák felsorolása (leszámlálása), 61
felbontás
    rangja, 63
Fermat, 154
Fermat-szám, 156, 157
Ferrers-diagramok, 62
Fibonacci, Leonardo, 89

Fibonacci, Leonardo Pisano, 7, 8, 11, 12
Fibonacci-reprezentáció, 92
Fibonacci-sorozat, 89
Fibonacci-számok, 7
Fibonacci-szó, 105
Friedlander, J., 196

generátorfüggvény, 7
  azonosságok bizonyítása, 26
  bináris fák megszámolása, 21
  egyenletek megoldása, 18
  exponenciális, 14
  gyakran használt, 14
  műveletek, 9
  tulajdonságok, 9
gráf
  De Bruijn, 101
  Rauzy, 105

H-hipotézis, 196
hatványszó, 107
Ho¸sten, S., 72
homomorfizmus, 100

ikerprím, 166
ikerprím állandó, 167
ismétléses kombinációk generálása, 51
ismétléses permutációk generálása, 53
ismétléses variációk generálása, 52
Iwaniec, H., 196

kódolás
  bináris fáké, 125
  fordított lengyel formáé, 127
  rácsutaké, 129
  sokszögeké, 128
  sorozatoké, 127
  szakaszoké, 127
  szorzaté, 126
kanonikus alak, 151
karakterisztikus vektor, 56
kombinációk generálása, 45
kombinatorikus Bertrand-tulajdonság, 182

lánctört, 141
Lagrange-tétel, 159
Landau, E. G. H., 157
Legendre-formula, 169, 171
legnagyobb közös osztó, 135
Liouville-függvény, 43
logikai szita, 75

Möbius-függvény, 30
Mersenne, 154
Mersenne-prím, 158
Mersenne-szám, 158
Mills, W. H., 183
mohó algoritmus, 73
Morris, W. D., 72
Moser L., 183
multiplikatív számelméleti függvény, 32

négyzetmentes szám, 188

osztók összege, 31
osztók száma, 30
osztók szorzata, 32

partíció, 58–61
  rangja, 63
Pepin-teszt, 157
periodikus, 100
permutációk generálása, 45, 47
permutációk reprezentatív rendszere, 71
prím, 151
  Mersenne, 154
  relatív, 157
prímszám tétel, 162

részhalmazok generálása, 56, 57
részszó, 96
  bispeciális, 107
részszóbonyolultság, 108
részszógráf, 105
Ramanujan, S., 172
Ramanujan-összeg, 32
Riemann-féle zeta függvény, 34
Riemann-sejtés, 34

Schinzel, A., 196
Sidon-sorozat, 72
Sierpinski, W., 196
Sierpinski, Waclaw, 168, 183
skatulyaelv, 69
Sturm-szó, 111
Sylvester–Shur-tétel, 183
szám
  összetett, 151
  kanonikus alak, 151
számelmélet alaptétele, 151
szó
  bonyolultsága, 108
  Chacon, 132
  De Bruijn, 102

Fibonacci, 98, 105, 110
hatvány-, 98, 107, 110
kezdőszelete, 96
kiegyensúlyozott, 99
Sturm-típusú, 111
véges, 95
végperiodikus, 100
végszelete, 96
végtelen, 97
szógráfok, 101
Szekeres Gábor, 70
Szemerédi, E., 72

tökéletes szám, 159
teljesen multiplikatív számelméleti függvény, 32
természetes szám partíciója, 58–61
Trotter, W. T., 72

végperiodikus szó, 100
variációk generálása, 45, 50
vektor
karakterisztikus, 56
visszakódolás, 129

Wilf–Fine tétele, 96
Wright, E. M., 183

Zeckendorf tétel, 91
Zeckendorf-reprezentáció, 92