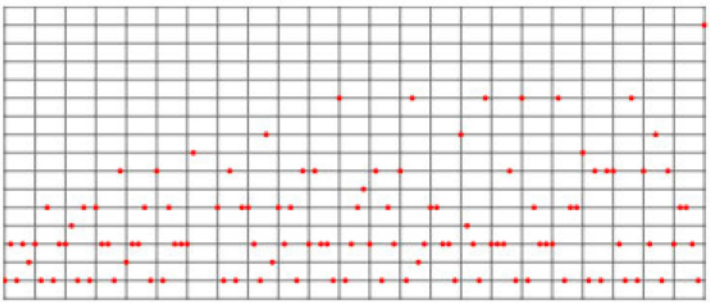
EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR



SZÁMELMÉLET

Fried Katalin
Korándi József
Török Judit

Fried Katalin

Korándi József

Török Judit

Számelmélet

Készült a TÁMOP-4.1.2.A/1-11/1-2011-0073 számú, „E-learning természettudományos tartalomfejlesztés az ELTE TTK-n” című projekt keretében. Konzorciumvezető: Eötvös Loránd Tudományegyetem, konzorciumi tagok: ELTE TTK Hallgatói Alapítvány, ITStudy Hungary Számítástechnikai Oktató- és Kutatóközpont Kft.

Tartalomjegyzék

Bevezetés

Ez a könyv egy háromkötetes elektronikus jegyzet első kötete. A jegyzet a számelmélet és algebra alapjait mutatja be tanárszakos hallgatóknak. Igyekeztünk azokra az alapvető ismeretekre szorítkozni, illetve részletesen kitérni, amelyek a tanítás során (akár burkoltan is) felmerülhetnek. Továbbá igyekeztünk az egyetemi szintű ismereteket összefűzni a korábban tanultakkal, hogy megkönnyítsük az új (fajta) ismeretek feldolgozását.

Munkánkban sokan segítettek, külön köszönettel tartozunk Komjáth Péternek, a könyv korábbi verziójának lektorálásáért, illetve Hermann Péternek és Fried Ervinnek önzetlen segítségükért, amellyel nagyban segítették a munkánkat. Köszönetünk Hraskó Andrásnak, aki a javított, elektronikus kiadást nézte át. A könyv technikai feldolgozásában segítségünkre volt Vásárhelyi János és sok-sok hallgató, különösen Márkus Bence, akinek ezúton is köszönjük a munkáját.

A könyv három részre tagozódik:

Számelmélet: Ez a rész az általános- és középiskolában tanult számelméleti ismereteket kívánja megalapozni, rendszerezni és kiegészíteni. Lényegében az oszthatóság fogalmától elindulva jutunk el a kongruenciákig és a számelméleti függvényekig. Utalás történik a mai modern számelméletnek – ha nem is a módszereire, de – néhány problémájára és eredményére. A feldolgozás során – tekintettel arra, hogy ez a rész kapcsolódik a legközvetlenebbül az általános iskolai anyaghoz – folyamatosan szem előtt tartottuk az iskolai alkalmazásokat, még ha nem is mindig tértünk ki rá.

„Klasszikus" algebra: Ebben a részben megpróbáljuk összefoglalni azokat a (klasszikus) algebrai ismereteket, amelyek meggyőződésünk szerint az algebrai alapműveltség részét képezik, és amelyekre a hallgatóknak egyéb tanulmányaik során is szükségük lehet. Így bevezetjük a komplex számokat, szólunk polinomokról és polinomegyenletekről, valamint még számos olyan dologról, amelyek neve egy ilyen bevezetésben valószínűleg inkább ijesztőek semmint lelkesítőek lennének, így most fel sem soroljuk ezeket. A feldolgozás során folyamatosan használni kezdjük az (absztrakt) algebra kifejezéseit, de ez már igazából a következő részhez tartozik. Íme:

„Modern" algebra: Manapság leginkább ezt szokás algebrának nevezni. Ebben a részben megismerked(het)ünk a mai matematika (és részben fizika, kémia stb.) egészét átható „absztrakt" gondolkodásmód alapfogalmaival, alapvető, illetve elemi tételeivel. Kiderül(het), hogy hol mindenütt fordulnak

elő „algebrai” megfontolások az analízis témaköreiben, hogy miért nem geometriai, hanem algebrai probléma például a „kör négyszögesítése”, de még akár az is megtudható, hogy mik azok a racionális számok.

Megjegyzés

Ez a jegyzet nem könyv. Nem kíván tehát az egykori és mai algebra és számelmélet bármiféle összefoglaló műve lenni.

Ez a jegyzet nem előadásjegyzet. Törekvéseink dacára sem gondoljuk, hogy ez a munka teljesen helyére tudna lépni az előadásokon való jegyzetelésnek.

Ez a jegyzet nem „puska”. Nem pótolja tehát a hallgató egyéni (meg?)barátkozását az anyaggal, a definíciók, tételek, bizonyítások, példák és ellenpéldák végiggondolását, újraalkotását, kiegészítését, megértését, ellenőrzését. Nem titkolt célunk annak elérése, hogy ki-ki képes legyen például saját példákat találni az egyes fogalmakra vagy akár befejezni (más módon) vagy újragondolni saját kútfejéből egy-egy bizonyítást. (Az „*a dolog részletesebb megfontolását az olvasóra bízzuk*” típusú mondatok csábításának mi sem mindig tudtunk ellenállni, de azt azért jó szívvel nem tudjuk javasolni, hogy valaki egy vizsgán csupán arra hivatkozzon, hogy a szóbanforgó dolog „nyilvánvaló”.)

Végezetül: reméljük, hogy ez a jegyzet komoly segítséget jelent mindazoknak, akik értelmesen olvassák-forgatják. Amennyiben így lesz, akkor ebben nagy része van a lektoroknak és mindazon hallgatóknak, akik észrevételeikkel, megjegyzéseikkel és tanácsaikkal támogatták e jegyzet megszületését, amiért ezúton is szeretnénk mindannyiuknak köszönetet mondani.

a szerzők

1. fejezet

Alapok

Számelméletet többféleképpen lehet – illetve esetünkben: lehetne – elkezdeni. Az alábbiakban négy – egyáltalán nem ekvivalens – lehetőséget mutatunk be a *természetes számok* bevezetésére, amelyek közül az utolsót fogjuk választani.

Mindenekelőtt azonban tisztáznunk kell egy látszólag jelentéktelen kérdést, amely gyökeresen megváltoztat egy-egy problémát vagy annak megoldását, és ez a *„Természetes szám-e a nulla?”* kérdése. Ezt illetően a világon sehol sem egyértelmű az álláspont. **A magyar közoktatásban (vagyis az általános és a középiskolákban) a nulla természetes szám, a felsőoktatásban pedig megállapodás kérdése.**

A matematika történetében a nulla nem volt természetes szám. (Mert sokáig szám sem volt.) A XIX. században indult egy olyan törekvés, hogy minden matematikai fogalmat matematikai logikai (ebből következően halmazelméleti) alapokra építsenek. (Lásd a természetes számok második bevezetése.) Ekkor, a természetes számok egységes, halmazelméleten alapuló tárgyalása során merült föl, hogy a nulla ugyanúgy természetes szám lehet, mint az 1, a 2, a 3, a 4 stb.

Ezt persze általában nem lehet törvénybe iktatni, ezért megállapodás kérdése.

Mi a szokásos számelméletet a teljes egész számhalmazon fogjuk tárgyalni, ezért szinte mindegy, hogy a nulla természetes szám-e vagy sem, ezért megengedhetjük magunknak azt a luxust, hogy *általában ne tekintsük annak.*

A természetes számok lehetséges bevezetésekor azonban kivételt teszünk, és a nullát is a természetes számok közé fogjuk sorolni (azért, hogy a termé-

szetes számról az egész számokra való következtetéseink magától értetődőbbek legyenek).

Az egyik lehetőség a természetes számok bevezetésére az **axiomatikus út**. Ez azt jelenti, hogy elfogadunk bizonyos állításokat a természetes számok halmazára, és ezeket nevezzük axiómáknak. A számelmélet axiómarendszerét először Peano (1858–1932) alkotta meg. Egy lehetséges *Peano-féle axiómarendszer:*[1][2]

1. A 0 természetes szám ($0 \in \mathbb{N}$).
2. Minden n természetes számnak van *rákövetkezője* – amelyet n' jelöl –, és az is természetes szám.
3. A 0 nem rákövetkezője egyik természetes számnak sem.
4. Ha két természetes szám rákövetkezője ugyanaz a természetes szám, akkor a két természetes szám is egyenlő.
5. Ha
   – a 0 rendelkezik valamilyen T tulajdonsággal, továbbá
   – valahányszor egy n természetes szám rendelkezik ezzel a T tulajdonsággal, mindannyiszor n' is rendelkezik a T tulajdonsággal,
   akkor minden természetes szám rendelkezik a T tulajdonsággal. (A teljes indukció axiómája.)

Az axiómákban nem szerepel az a kijelentés, hogy ezek és csak ezek a természetes számok, de úgy kell érteni.

Ezek után – mint ahogyan az egy axiomatikus felépítéshez illik – el lehetne kezdeni építkezni: helyesnek tartott következtetési sémákkal újabb állításokat létrehozni; új fogalmakat definiálni (például negatív egész számok) stb. A természetes számok összeadását és szorzását például a következőképpen definiálnánk:

1.1. Definíció. $n + 0 := n$ és $n + k' := (n + k)'$, illetve $n \cdot 0 := 0$ és $n \cdot k' = n \cdot k + n$.

[1] Peano eredetileg nem tekintette természetes számnak a nullát, így nála a legkisebb természetes szám az 1 volt.

[2] Giuseppe Peano (1858–1932) olasz matematikus volt. A 19. század végén a matematika tárgyalását precíz alapokra kívánták helyezni a kor matematikusai; axiómákkal és alapfogalmakból kiindulva precíz fogalmakkal és logikai levezetésekkel akarták megfogalmazni az addigi ismereteket. Peano a természetes számok axiomatikus tárgyalásának egy képviselője volt.

Az út hosszadalmas, és az általa nyújtott precizitásra – jelen pillanatban – nincs sem szükségünk, sem lehetőségünk.

Van azonban egy nagyon fontos, a természetes számokra vonatkozó következmény, amelytől nem tekinthetünk el, és amelyet használni is fogunk, nevezetesen az egyszerűrítési szabály.

1.1. Következmény. *Ha* $a+b=c+b$*, akkor* $a=c$*.*

Bizonyítás. $a+b$ pontos jelentése: a 0-nak $(a+b)$-edik rákövetkezője. $c+b$ jelentése hasonlóan a 0-nak $(c+b)$-edik rákövetkezője. Mivel $a+b$ és $c+b$ egymással egyenlő, 0-tól különböző természetes számok, ezért ők rákövetkezőik valamely – szintén egyenlő – természetes számoknak. Ezt a gondolatmenetet folytatva, b lépésben arra jutunk, hogy a és c egyaránt ugyanannyiadik rákövetkezője a 0-nak, és mivel a rákövetkező egyértelmű, így csak $a=c$ lehet. □

Megjegyzés. A matematikában többféle indukció létezik, és a teljes indukciót is többféle – egymással ekvivalens – módon ki lehet mondani. Az előző bizonyításban látott „visszafelé lépegetés", vagyis a *visszafelé történő indukció* is működik a természetes számokon. A lényege az – ha működik –, hogy megkíséreljük visszavezetni egy tulajdonság teljesülését a megelőző természetes számokra, és olyankor ezt véges sok lépésben el tudjuk végezni.

Megjegyzés. Ebből a típusú felépítésből következik egy nagyságrendi összehasonlítás is: mondhatjuk, hogy minden n esetén az $n<n'$, és ez a rendezés rendelkezzék a szokásos tulajdonságokkal. Most ezt sem vezetjük le.

A másik választható út az, hogyha az új fogalmakat – már meglévő – **halmazelméleti fogalmakkal** vezetjük be. A *számosság* fogalmának ismeretében a természetes szám fogalma már egyszerűen definiálható:

1.2. Definíció. A véges halmazok számosságait *természetes számoknak* nevezzük.

A természetes számok közötti műveleteket halmazműveletekre vezethetjük vissza. Például két természetes szám szorzatának (1.3.), illetve összegének (1.4.) definíciója:

Legyen a és b természetes szám. Ekkor az 1.2. Definíció értelmében léteznek A és B véges halmazok, amelyek számossága a, illetve b.

1.3. Definíció. Az a *és* b *természetes számok szorzatán* értsük az $A\times B$ halmaz számosságát!

A $\times$ halmazszorzás művelet meghatározása a 1.5. definícióban található.

Megmutatható, hogy ha A és B véges, akkor $A \times B$ is az, illetve az is, hogy $A \times B$ számossága nem függ attól, hogy mi az A és a B, hanem csak azok számosságától.

Ha az a, illetve b számosságú A és B halmazok diszjunktak is – minden a, b természetes számhoz található ilyen A és B –, akkor segítségükkel definiálhatjuk a és b összegét is:

1.4. Definíció. Legyen $a, b \in \mathbb{N}$, valamint $|A| = a$ és $|B| = b$, továbbá $A \cap B = \emptyset$. Ekkor az *a és b természetes számok összegén* értsük az $A \cup B$ számosságát!

Hasonló módokon lehetne definiálni például két természetes szám különbségét, a hatványozást stb. De például a negatív számok bevezetése már jóval keményebb dió lenne.

Egészen más jellegű a harmadik, az **absztrakt bevezetési mód.** Itt ugyan hosszú ideig szó sem esne a természetes számokról – még ha közben szinte állandóan arra gondolnánk, hogy azokat akarjuk előállítani, de annál sokkal többről szól.

Először az egész számokat állítjuk elő – amelyet $\mathbb{Z}$-vel szokás jelölni –, egyelőre jelöljük Z-vel a kiinduló halmazt: legyen tehát Z egy nem üres halmaz, amelyen értelmezve van két kétváltozós művelet, a kereszt $(+)$ és a pötty $(\cdot)$, és

1. legyen a $+$ és a $\cdot$ művelet is *kommutatív,* azaz $\forall a, b (\in Z)$-re $a+b = b+a$ és $a \cdot b = b \cdot a$, és
2. legyen a $+$ és a $\cdot$ művelet is *asszociatív,* azaz $\forall a, b, c (\in Z)$-re $(a+b)+c = a + (b + c)$ és $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, valamint
3. legyen a $\cdot$ a $+$-ra nézvést *disztributív,* azaz $\forall a, b, c (\in Z)$-re $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, és
4. *létezzék* olyan $n (\in Z)$, hogy *minden* $a (\in Z)$-re $a + n = a$, és
5. *minden* $a (\in Z)$-hoz *létezzék* olyan $a' (\in Z)$ elem, amelyre $a + a' = n$, és
6. *létezzék* olyan $e (\in Z)$, hogy *minden* $a (\in Z)$-ra $a \cdot e = a$, és
7. *ne legyen olyan* $a, b (\in Z)$, hogy $a \neq n \neq b$ és $a \cdot b = n$ (n a 4. pontban rögzített elem)!

Nos, ha mindez teljesül $(Z, +, \cdot)$-re, akkor ezt egységelemes, nullosztómentes kommutatív gyűrűnek vagy más néven *egységelemes integritási tartománynak* (vagy integritástartománynak) nevezzük. Ilyen például $(\mathbb{Z}, +, \cdot)$ is, vagyis az egész számok halmaza az összeadással és a szorzással. E néhány alaptulajdonságból szinte meglepően sok dolog következik, amelyek minden integritástartományra igazak, így $(\mathbb{Z}, +, \cdot)$-ra is. Mindezekről – valamint az egész számok számos további általánosítható tulajdonságáról – jóval később, a harmadik kötetben lesz szó.

Végül az egész számoknak egy alkalmas részhalmaza lesz a természetes számok halmaza, amelyen persze a definiált műveletek tulajdonságai nem pont ugyanazok.

E megemlített három út helyett mi egy negyediket követünk, amely matematikailag az előzők bármelyikénél kevésbé korrekt, de céljainknak azért megfelel: összegyűjtjük az egész számoknak néhány, többé-kevésbé már ismert tulajdonságát, amelyeket nem bizonyítunk (de axiómáknak sem tekintjük őket!), és a továbbiakban igyekszünk maximálisan ezekre építkezni. (Többnyire sikerülni fog.)

Tehát a természetes számok halmazára $\mathbb{N}$ és az ezen értelmezett összeadásra $(+)$ és szorzásra $(\cdot)$ igazak:

1. $\mathbb{N}$ elemei: (0), 1, 2, 3, 4, 5, ...
2. Teljesülnek rá a Peano-axiómák
3. Teljesülnek rá a szokásos műveleti tulajdonságok
4. $\mathbb{N}$-ben érvényes az összeadásra vonatkozó egyszerűsítési szabály.
5. $\mathbb{N} \subset \mathbb{Z}$
6. A $\mathbb{N}$ és $\mathbb{Z}$ számossága is megszámlálhatóan végtelen $(\aleph_0)$
7. $\mathbb{Z}$ (és $\mathbb{N}$) a kisebb-egyenlő $(\leq)$ reláció szerint teljesen rendezett (azaz bármely két eleme összehasonlítható a $\leq$ relációval)
8. $\mathbb{Z}$-ben csak úgy lehet két elem szorzata 0, ha legalább az egyik elem 0 ($\mathbb{Z}$ és így $\mathbb{N}$ is nullosztómentes)
9. $\forall a, b, c (\in \mathbb{Z})$-re $a < b \Rightarrow a + c < b + c$ ($\mathbb{N}$-ben is teljesül)
10. $\forall a, b, c (\in \mathbb{Z})$-re, ha $c > 0$, akkor $a \leq b \Rightarrow a \cdot c \leq b \cdot c$ ($\mathbb{N}$-ben is teljesül)
11. $\forall a (\in \mathbb{Z})$-re $|a| = a$, ha $a \geq 0$, és $|a| = -a$, ha $a < 0$ ($\mathbb{N}$-ben is teljesül)
12. $\forall a, b (\in \mathbb{Z})$-re $|a \cdot b| = |a| \cdot |b|$ ($\mathbb{N}$-ben is teljesül)

13. $\forall a, b(\in \mathbb{Z})$-re $|a+b| \leq |a| + |b|$ ($\mathbb{N}$-ben is teljesül)

14. $\forall a, b(\in \mathbb{Z})$-re $|a-b| \geq \big||a| - |b|\big|$ ($\mathbb{N}$-ben is teljesül)

15. stb. (Ha az előzőek valamihez mégsem bizonyulnának elegendőnek, akkor erre fogunk hivatkozni.)

A továbbiakban – hacsak mást nem mondunk – az egész számok halmazára vonatkozó megállapításokat fogunk tenni. Ez egyáltalán nem jelenti azt, hogy más számkörben ne lehetne hasonló fogalmakat alkotni, összefüggéseket felállítani.

Megjegyzés. A természetes számok jelölésére az $\mathbb{N}$ jelet szokás használni, amely a „naturalis" (természetes) latin eredetű szó kezdőbetűje. Az egész számokra a német „szám" (Zahl) szó kezdőbetűje miatt a $\mathbb{Z}$ jel a használatos.

Néhány alapvető fontosságú fogalom és összefüggés

Az alábbiakban néhány fontos alapfogalmat tekintünk át a teljesség igénye nélkül.

1.5. Definíció. Legyen H nem üres halmaz. A H elemeiből álló rendezett számpárok halmazát, azaz a $\{(h_1, h_2) \mid h_1, h_2 \in H\}$ halmazt, amelyet $H \times H$-val jelölünk a halmaz önmagával vett *Descartes-szorzatának* nevezzük.

1.6. Definíció. Egy halmaz elempárjainak egy S nem üres részhalmazát *kétváltozós* (vagy *binér*) *relációnak* nevezünk.

Megjegyzés. A reláció szó kapcsolatot jelent. Úgy kell gondolnunk a relációra, hogy a relációban lévő párok első tagja kapcsolatban áll a második taggal. Megfordítva: a kapcsolatban álló elemek első és második tagja (ebben a sorrendben) a reláció eleme. Az összes relációban álló elempár alkotja a relációt (ez részhalmaza az összes elempárok halmazának).

Reláció például a valós számok halmazán a $<$, az $=$, de ugyanígy reláció a $\{(1,2),(2,1)\}$ elempár halmaz, hiszen valós számpárok egy részhalmaza.

Az $S \subset H \times H$ binér relációk tulajdonságait a következők szerint szokás csoportosítani:

1.7. Definíció.

1. Ha a H halmaz minden eleme relációban áll önmagával, akkor a relációt *reflexívnek* nevezik.

Ha nem minden elemre teljesül ez a tulajdonság, akkor azt mondjuk, hogy *nem reflexív.*

Ha semelyik elem sem áll relációban önmagával, akkor *irreflexív.*

2. Ha minden $a, b \in H$ esetén amennyiben $(a, b) \in S$, akkor $(b, a) \in S$ is fennáll, akkor a relációt *szimmetrikusna*k nevezzük.

   Ha nem minden $a, b \in H$ esetén teljesül a tulajdonság, akkor azt mondjuk, hogy *nem szimmetrikus.*

   Ha minden $(a, b) \in S$ esetén a $(b, a) \notin S$, akkor azt mondjuk, hogy a reláció *aszimmetrikus.*

   Ha abból, hogy $(a, b) \in S$ és $(b, a) \in S$ minden esetben következik, hogy $a = b$, akkor a relációt *antiszimmetrikusnak* nevezzük.

   Ha minden $a, b \in H$ elempárra az $(a, b) \in S$, a $(b, a) \in S$ és $a = b$ tulajdonságok közül pontosan egy teljesül, akkor a relációt *trichotómnak* nevezzük.

3. Ha minden $a, b, c \in H$ esetén abból, hogy $(a, b) \in S$ és $(b, c) \in S$ következik, hogy $(a, c) \in S$, akkor a relációt *tranzitívnak* nevezzük.

1.1. Megjegyzés. Az egyenlőség reláció reflexív, szimmetrikus és tranzitív. A $<$ reláció irreflexív, trichotóm és tranzitív. A $\leq$ reláció reflexív, antiszimmetrikus és tranzitív.

1.8. Definíció. A reflexív, szimmetrikus és tranzitív relációk neve: *ekvivalencia reláció.*

A reflexív, antiszimmetrikus és tranzitív relációk neve: *rendezési reláció.*

1.9. Definíció. Ha a H nem üres halmazt diszjunkt részhalmazai egyesítéseként írjuk fel, akkor ezt a *H halmaz egy osztályozásának* nevezzük: $H = \bigcup_{i=1}^{n} H_i$ és $H_i \cap H_j = \emptyset$, hacsak $i \neq j$.

1.1. Tétel. *1. Ha H-nak megadjuk egy osztályozását, akkor az a reláció, hogy „egy osztályba tartoznak" egy H-n értelmezett ekvivalenciareláció.*

2. Ha H-n adott egy ekvivalenciareláció, akkor az egy-egy osztályba sorolt elemek mint H részhalmazai a H-nak egy osztályozását adják meg.

Bizonyítás. 1. Az adott reláció reflexív (mert minden elem egy osztályban van saját magával), szimmetrikus (mert ha a egy osztályban van b-vel, akkor b egy osztályban van a-val) és tranzitív (mert ha a és b egy osztályba esnek

és b és c is egy osztályba esnek, akkor a és c is egy osztályba esik). Ez a reláció tehát ekvivalenciareláció.

2. Minden elemet besoroltunk valamely részhalmazba, mert minden elem relációban áll önmagával. Minden elem pontosan egy részhalmazba esik bele, mert ha az a elem relációban áll egy b-vel (vagyis egy halmazban vannak), és relációban áll c-vel (vagyis vele is egy halmazban van), akkor a tranzitivitás miatt b is egy halmazba esik c-vel. □

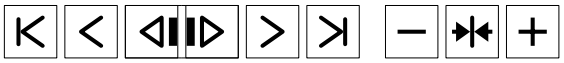
Például: A természetes számok halmazán legyen ekvivalens két szám, ha a felírásukban szereplő számjegyek összege egyenlő.

Eszerint az 1 ekvivalens a 10-zel, a 100-zal, az 1000-rel stb. Sőt, 10 bármelyik két hatványa ekvivalens egymással: ezek egy részhalmazba esnek.

A 2 ekvivalens a 11-gyel, a 20-szal, a 101-gyel stb., sőt, bármely két olyan szám ekvivalens egymással, amelyek felírásához egyetlen 2-est vagy két 1-est, illetve tetszőleges számú 0-t használunk: ezek is egy részhalmazba esnek.

És így tovább.

Mivel minden természetes szám felírásában meghatározható a számjegyei összege, ezért minden számot besorolunk valahova, és mivel minden természetes szám felírásában a számjegyek összege egyértelműen meghatározott, így minden szám pontosan egy részhalmazhoz tartozik, vagyis osztályozást kaptunk (1.1. ábra – animáció).



1.1. ábra. Legyen két szám akkor ekvivalens, ha számjegyeik összege ugyanannyi. Az ábrán az egy osztályba tartozó elemeket ugyanazzal a színnel színeztük (animáció).

Sokszor fogunk azonos algebrai átalakításokat végezni. Legtöbbjükkel középiskolában mindenki találkozhatott. Néhányat – a nem triviálisak közül a legfontosabbakat – összegyűjtöttünk, és ehelyt bebizonyítjuk.

1.1. Állítás. *Ha $q \neq 1$, akkor a q hányadosú (latin eredetű szóval: kvóciensű – innen a q jelölés) mértani sorozat első n tagjának az összege*

$$a_0 + a_0q + a_0q^2 + \ldots + a_0q^{n-1} = a_0\frac{1-q^n}{1-q} = a_0\frac{q^n-1}{q-1}$$

Bizonyítás. Ha $a_0 = 0$, akkor az állítás nyilvánvaló – mindkét oldalon 0 áll.

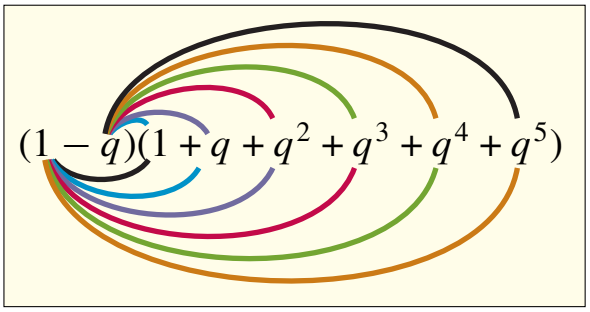
Ha $a_0 \neq 0$, akkor mindkét oldalt oszthatjuk vele.

$$1 + q + q^2 + \ldots + q^{n-1} = \frac{1-q^n}{1-q}$$

Ezután a bal oldalon álló kifejezést megszorozva $(1-q)$-val éppen a jobb oldali tört számlálóját kapjuk.

$$\begin{aligned}&(1+q+q^2+\ldots+q^{n-1})(1-q) = \\ &= 1\cdot 1 \underbrace{-1\cdot q + q\cdot 1}_{0} \underbrace{-q\cdot q + q^2\cdot 1}_{0} - q^2\cdot q + \cdots + q^{n-1}\cdot 1 - q^{n-1}\cdot q = \\ &= 1\cdot 1 - q^{n-1}\cdot q = 1 - q^n\end{aligned}$$

Az ilyen típusú összegeket – ahol az egymás utáni tagok éppen kiejtik egymást – *teleszkopikus összegnek* szokás nevezni. Ezt $n = 6$-ra az 1.2. ábra szemlélteti. □



1.2. ábra. A színes, azonos színnel jelzett szorzatok összege nulla. Végül csak a feketével jelölt szorzatok maradnak.

1.2. Állítás.

$$(a+b)^n = a^n + na^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-2}a^2b^{n-2} + nab^{n-1} + b^n$$

Speciálisan például ($a = b = 1$ esetben):

$$(1+1)^n = 1 + n + \binom{n}{2} + \ldots + \binom{n}{n-2} + n + 1 = 2^n$$

Bizonyítás. Sokféle bizonyítás létezik, például a teljes indukció módszere. Mi most egy kombinatorikus bizonyítást adunk.

Az n-tényezős szorzatot a zárójelek felbontásával számíthatjuk ki.

$$(a+b)^n = (a+b) \cdot (a+b) \cdot \ldots \cdot (a+b) \cdot (a+b),$$

ahol n tényező szerepel a szorzatban. A zárójelek felbontásakor minden tényezőből vagy az a, vagy a b tagot választjuk ki. Olyan eset, amikor mindegyikből az a-t választjuk ki, egyféle van, és az a^n szorzatot kapjuk: a^n.

Abban az esetben, amikor $n-1$ tényezőből az a tagot, 1-ből pedig a b-t választjuk, n-féle lehetőség van a kiválasztásra, és minden esetben az $a^{n-1}b$ szorzatot kapjuk: $na^{n-1}b$.

Általában, ha – tetszőleges $0 \leq k \leq n$ esetén – k tényezőből választjuk a b tagot (a többiből az a-t), akkor ezt $\binom{n}{k}$-féleképpen tehetjük meg, és mindannyiszor az $a^{n-k}b^k$ szorzatot kapjuk, így adódik a $\binom{n}{k}a^{n-k}b^k$ tag.

Az összes ilyen szorzatot összeadva a tétel állítása szerinti összeget kapjuk. □

1.3. Állítás. *Egyszerűen bizonyítható, hogy $a_1, a_2, \ldots, a_k$; $b_1, b_2, \ldots, b_n$ számokra az*

$$(a_1 + a_2 + \ldots + a_k)(b_1 + b_2 + \ldots + b_n)$$

szorzat kifejtve olyan a_ib_j szorzatok összege, amelyekben minden lehetséges i és j index szerepel. Másképp csoportosítva a szorzatokat a következőkkel is egyenlő még:

$$\begin{gathered} a_1(b_1 + b_2 + \ldots + b_n) + a_2(b_1 + b_2 + \ldots + b_n) + \ldots \\ \ldots + a_{k-1}(b_1 + b_2 + \ldots + b_n) + a_k(b_1 + b_2 + \ldots + b_n), \end{gathered}$$

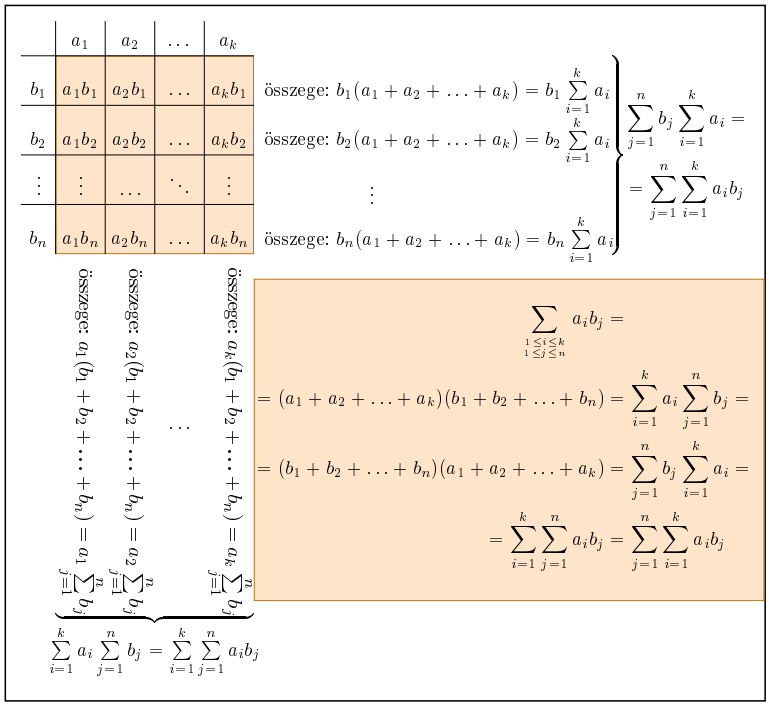
illetve

$$\begin{gathered} b_1(a_1 + a_2 + \ldots + a_k) + b_2(a_1 + a_2 + \ldots + a_k) + \ldots \\ \ldots + b_{n-1}(a_1 + a_2 + \ldots + a_k) + b_n(a_1 + a_2 + \ldots + a_k) \end{gathered}$$

Ezt az átalakítást (hogy a későbbiekben ebben az alakjában is felismerjük) $\sum$ alakban is felírjuk:

$$\sum_{\substack{1\le i\le k\\ 1\le j\le n}} a_i b_j = \sum_{1\le i\le k} a_i \left(\sum_{1\le j\le n} b_j\right) = \sum_{1\le j\le n} b_j \left(\sum_{1\le i\le k} a_i\right) = \sum_{1\le j\le n} b_j \sum_{1\le i\le k} a_i$$

Ezeket az összegzéseket az 1.3. ábrán szemléltetjük.



1.3. ábra.

Feladatok

1. Határozza meg azon mértani sorozat első 100 tagjának összegét, amelynek kezdőeleme 1, a hányadosa a következő!
   $\frac{1}{3}$; $-\frac{1}{2}$; 2; -1; 1
2. Igazolja, hogy ha a természetes számok halmazán két számot akkor tekintünk relációban állónak, ha a tízes helyiértéken álló számjegyük egyenlő, akkor ez ekvivalenciareláció. Hány ekvivalenciaosztály keletkezik? Határozza meg az ekvivalenciaosztályokat!

3. Igazolja, hogy ha a természetes számok halmazán két számot akkor tekintünk relációban állónak, ha ugyanannyi számjegyel írhatók fel, akkor ez ekvivalenciareláció. Hány ekvivalenciaosztály keletkezik? Határozza meg az ekvivalenciaosztályokat!

4. A nagyság szerint rendezett, 1-től induló természetes számokat úgy soroljuk osztályokba, hogy az elsőbe az első 9 számot, a másodikba a következő 90-et, a harmadikba a soronkövetkező 900-at és így tovább, a k-adikba a következő $9 \cdot 10^{k-1}$-et soroljuk, akkor adjon meg egy ekvivalenciarelációt, amely ezt az osztályozást indukálja!

5. Írja fel a $\sum_{i=1}^{3} \sum_{j=11}^{13} (i + j)$ összeg tagjait. Írja át ezt a szummát más formába!

6. Írja fel a $\sum_{i=1}^{3} \sum_{j=11}^{13} (i \cdot j)$ összeg tagjait. Írja át ezt a szummát más formába!

2. fejezet

Oszthatóság, maradékos osztás

Az egész számok körében az összeadás és a szorzás minden számpáron elvégezhető. Az $a + x = b$ (a és b adott egész számok, x az ismeretlen, amelyet az egész számok körében keresünk) egyenlet is mindig megoldható.

Nem mindig oldható meg viszont az $ax = b$ egyenlet (a szorzás nem invertálható). Vannak azonban olyan speciális a, b számpárok, amelyekre igen.

Ha viszont adott a, b egész számokra létezik olyan x egész szám, hogy $ax = b$, akkor azt szoktuk mondani, hogy b többszöröse (valahányszorosa) az a-nak. Ezt a tulajdonságot úgy is megfogalmazhatjuk, hogy van olyan egész szám az a-hoz, amellyel megszorozva b-t kapjuk:

2.1. Definíció. Egy a egész szám *osztója* a b egész számnak, ha létezik olyan q egész szám, amelyre $aq = b$. Ilyenkor azt is mondhatjuk, hogy b *többszöröse* a-nak.

2.1. Jelölés. $a \mid b$, (a osztója b-nek, b többszöröse a-nak, b osztható a-val), illetve ha ez nem áll fenn köztük, akkor $a \nmid b$ (a nem osztója b-nek).

Például: $2 \mid 6$, mert $q = 3$-ra teljesül, hogy $2 \cdot q = 6$.

$-3 \mid 6$, mert $q = -2$-re teljesül, hogy $(-3) \cdot q = 6$.

$2 \mid 0$, mert $q = 0$-ra teljesül, hogy $2 \cdot q = 0$.

$0 \mid 0$, mert tetszőleges q esetén $O \cdot q = 0$. (Sőt, mivel q tetszőleges egész szám lehet, végtelen sok ilyen q szám van. Egyébként ha az oszthatóságra úgy gondolnánk, hogy b-t maradékosan osztva a-val a maradék 0, vagyis az oszthatóságot osztással definiálnánk, akkor persze nem lenne értelme a 0-val való *oszthatóságról* beszélni. Ez is ok arra, hogy *ne osztással definiáljuk az oszthatóságot*, hiszen így kicsit általánosabb a definíció.)

$4 \nmid 6$, mert nincs olyan egész q, amelyre $4 \cdot q = 6$ lenne.

$0 \nmid 6$, mert nincs olyan egész q, amelyre $0 \cdot q = 6$ lenne.

Megjegyzés. Egy halmazon, ahol értelmes a szorzás, felmerül a kérdés: mivel szoroztam meg az a számot, hogy c-t kapjam, vagyis lehet-e osztani is. Keressük, hogy a c szám „hányszorosa" valamely a számnak. Van-e olyan szám, amellyel megszorozva az a-t a c-t kapjuk. Ha csak az egész számok halmazán vagyunk, akkor tudjuk, hogy ez nem mindig teljesül: 5-öt bármilyen egész számmal is szorozzuk meg, soha nem kapunk 2-t. A racionális számok körében azonban van ilyen szám, a $\frac{2}{5}$.

Ha nincs is minden a és c esetén alkalmas szorzó, akkor is van értelme megkérdezni, hogy egyes konkrét esetekben többszöröse-e a c az a-nak.

Oszthatósági szempontból vannak különlegesen viselkedő számok: van olyan, amelyik minden számnak osztója, és van olyan is, amely minden számnak többszöröse (azaz minden szám osztója).

Ha egy szám többszöröse minden természetes számnak, akkor a 0-nak is többszöröse – ez csak maga a 0 lehet. Ezért azt kell eldöntenünk, hogy a 0 minden számnak többszöröse-e. Mivel minden a egész számhoz létezik olyan q – nevezetesen a $q = 0$ –, amelyre $aq = 0$, így ez is teljesül.

Arról is könnyen meggyőződhetünk, hogy több ilyen tulajdonságú szám nincs, sőt ennél több is igaz, a 0-n kívül egyetlen egész számnak sincs végtelen sok osztója. Igaz ugyanis a következő:

2.1. Tétel. *Ha $a \mid b$ és $b \neq 0$, akkor $|a| \leq |b|$.*

Bizonyítás. Ha $a \mid b$, akkor $\exists q$, amelyre $aq = b$. Ekkor nyilván $|aq| = |b|$, így $|a||q| = |b|$. Ha $b \neq 0$, akkor q sem lehet 0, vagyis $|q| \geq 1$. Ekkor azonban $|a||q| \geq |a|$, vagyis $|b| \geq |a|$. □

(Egyébként egyenlőség is csak $|a| = |b|$ esetben lehet.)

Ez viszont azt jelenti, hogy ha $b \neq 0$, akkor b összes osztója a $[-|b|; |b|]$ intervallumból kerül ki, márpedig ebben az intervallumban csak véges sok egész szám van (szám szerint pontosan $2|b|+1$ darab). Ezért igaz a következő:

2.2. Tétel. *A 0-n kívül minden számnak véges sok osztója van.*

Bizonyítás. Az előző tételből következik. □

Azzal a kérdéssel, hogy melyik számnak pontosan hány osztója van, majd később foglalkozunk, azt azonban már most érdemes megjegyezni, hogy olyan b szám, amelynek pontosan $2 \cdot |b| + 1$ osztója lenne, nincs. A $-|b|$ és $|b|$ közötti

$2|b|+1$ számból ugyanis az egyik a 0, ami saját magán kívül nem osztója semelyik egész számnak sem. (A $b=0$-nak viszont végtelen sok osztója van.) Így egy $b \neq 0$ számnak legfeljebb $2|b|$ darab osztója lehet. Könnyen belátható, hogy éppen $2|b|$ osztója csak a $b = 1$, -1, 2, -2 számoknak van.

Most térjünk rá annak a kérdésnek a vizsgálatára, hogy melyek azok a számok, amelyek minden számnak osztói. Azonnal eszünkbe ötlik az 1, de azt nem tudhatjuk, hogy nincs-e más ilyen szám. Ezt vizsgáljuk most meg.

2.2. Definíció. *ε egység,* ha $\forall a$-ra $\varepsilon \mid a$.

2.3. Tétel. *Az egész számok körében pontosan két egység van:* 1 *és* (-1).

Bizonyítás. Tetszőleges a számnak osztója az 1, mert van olyan szám (maga az a), amellyel az 1-et megszorozva az a-t kapjuk, vagyis az 1 minden számnak osztója, tehát egység: $1 \mid a$.

Tetszőleges a számnak osztója a -1, mert van olyan szám (nevezetesen a $(-a)$), amellyel a (-1)-et megszorozva az a-t kapjuk, vagyis a -1 is osztója minden számnak, tehát egység: $(-1) \mid a$.

Hátravan még annak a bizonyítása, hogy más egység nincs. Ha ε egység, akkor minden számnak, így az 1-nek is osztója. Ez a 2.1. Tétel értelmében azt jelenti, hogy $|\varepsilon| \leq 1$. Ennek a feltételnek három egész szám tesz eleget: a -1, a 0 és az 1.

A 0 azonban nyilván nem egység, mert saját magán kívül semelyik egész számnak sem osztója. Emiatt csak $\varepsilon = 1$ vagy $\varepsilon = -1$ lehet. □

Megjegyzés. A tétel bizonyításából az is kiderül, hogy minden szám osztható saját magával (mert $a \cdot 1 = a$) és saját ellentettjével (mert $(-a) \cdot (-1) = a$). A definíciója alapján minden egész szám osztható az egységekkel is. Eszerint az minden egységtől és 0-tól különböző egész számnak van legalább négy osztója. Az egységeknek két osztójuk van, a 0-nak pedig végtelen sok.

2.3. Definíció. Az a egységszereseit az a szám *asszociáltjainak* nevezzük.

Például: a 2 asszociáltjai a 2 és a -2, a -2 asszociáltjai a -2 és a 2, általában az a szám asszociáltjai az a és $-a$. Minden nem 0 egész számnak két asszociáltja van, mert az egész számok körében két egység van.

Mivel az egységekkel és saját asszociáltjaival minden szám osztható, megkülönböztetjük a nyilvánvaló osztókat a többi osztótól (ha van):

2.4. Definíció. Ha $a \neq 0$, akkor az 1-et, a -1-et, az a-t és a $-a$-t az a *triviális osztóinak,* a többi osztóját – ha van – *valódi osztóknak* nevezzük. A triviális osztót másképpen *nem valódi osztónak* is szoktuk nevezni.

Oszthatósági szempontból egy szám és az asszociáltjai megkülönböztethetetlenek:

2.4. Tétel. *Ha $a \mid b$, akkor $-a \mid b$, $a \mid -b$, $-a \mid -b$.*

Általában: $\varepsilon_1 a \mid \varepsilon_2 b$ (ε_1 és ε_2 egységek).

Bizonyítás. Ha $a \mid b$, akkor $\exists q$, amelyre $aq = b$. Ekkor viszont $(-a)(-q) = b$, $a(-q) = -b$, $(-a)(q) = -b$. Ezekből már következik a tétel összes állítása.

Általában ha $\varepsilon_1 \mid 1$, akkor van olyan ε_1', amelyre $\varepsilon_1 \cdot \varepsilon_1' = 1$. Ha $a \mid b$, akkor valamilyen q-ra $aq = b$, amiből következik, hogy $(\varepsilon_1 a)(\varepsilon_1' q) = b$, így $(\varepsilon_1 a)(\varepsilon_2 \varepsilon_1' q) = (\varepsilon_2 b)$. Ez pedig az általánosan kimondott állítást igazolja. □

2.1. Következmény. *Az oszthatóság definíciójából közvetlenül következik, hogy ha $a \mid b$ és c tetszőleges egész szám, akkor $ac \mid bc$.*

$c \neq 0$ esetén a megfordítás is igaz: ha $ac \mid bc$, akkor $a \mid b$.

Bizonyítás. Ha $a \mid b$, akkor van olyan q egész szám, amelyre $aq = b$. Ekkor tetszőleges c egész számra $acq = bc$, vagyis $ac \mid bc$.

Ha $ac \mid bc$, akkor van olyan q egész szám, amelyre $acq = bc$. Ha $c \neq 0$, akkor ebből $aq = b$ (hiszen $acq - bc = 0$ miatt $(aq - b)c = 0$, azaz vagy c nulla – amit kizártunk –, vagy $aq = b$). Ebből viszont $a \mid b$ következik. □

Az „$a \mid b$” reláció tulajdonságairól szól a következő tétel:

2.5. Tétel. *1. $\forall a \in \mathbb{Z}$ esetén $a \mid a$ (az oszthatóság reflexív).*

2. $\forall a, b \in \mathbb{Z}$ esetén ha $a \mid b$ és $b \mid a$, akkor $|a| = |b|$.

3. $\forall a, b, c \in \mathbb{Z}$ esetén ha $a \mid b$ és $b \mid c$, akkor $a \mid c$ (az oszthatóság tranzitív).

Bizonyítás. 1. $\forall a$-ra $a \cdot 1 = a$ (vagyis létezik olyan q, nevezetesen a $q = 1$, amelyre $aq = a$), tehát $a \mid a$.

2. Ha $a \mid b$ és $b \mid a$, akkor vagy $a = b = 0$, vagy egyrészt $|a| \leq |b|$, másrészt $|b| \leq |a|$. Ez csak akkor teljesülhet, ha $|a| = |b|$.

3. Ha $a \mid b$, akkor $\exists q \in \mathbb{Z}$, amelyre $aq = b$. Ha $b \mid c$, akkor $\exists r \in \mathbb{Z}$, amelyre $br = c$. Ekkor viszont $aqr = c$, vagyis $a \mid c$. □

Megjegyzés. Ennek a tételnek a második állítása szerint az oszthatósági reláció „majdnem” (asszociált erejéig) antiszimmetrikus (ami az lenne, hogy $a \sim b$ és $b \sim a$-ból következik, hogy $a = b$). Ha azonban például a természetes számokra (vagy a pozitív egész számokra) szorítkozunk, akkor az

abszolút értékek egyenlősége egyben a számok egyenlőségét is jelenti. Vagyis a természetes számok (vagy a pozitív egész számok) halmazán az oszthatóság reflexív, antiszimmetrikus és tranzitív, tehát rendezési reláció.

Megjegyzés. A természetes számok halmazán az oszthatóság rendezési reláció, de nem teljes rendezési reláció. (A teljes rendezéshez ugyanis az kell, hogy bármely két különböző elem között fennálljon valamelyik irányban a reláció. Az egész számok körében azonban például $9 \nmid 15$ és $15 \nmid 9$.)

Megjegyzés. Az eddigiek során az egész számok körében értelmeztük az oszthatóság fogalmát: azt definiáltuk, hogy mikor mondjuk, hogy egy egész szám osztója egy másiknak. Definíciónkat azonban általánosabban is megfogalmazhatjuk; tetszőleges olyan halmazon beszélhetünk oszthatóságról, ahol értelmezve van egy szorzás művelet:

Tegyük fel, hogy adott egy H halmaz és azon egy $\otimes$ művelet. Tetszőleges $a, b \in H$ esetén azt mondjuk, hogy $a \mid b$, ha létezik olyan $q \in H$, amelyre $a \otimes q = b$.

1. Legyen például H a páros számok halmaza, a művelet pedig a szokásos szorzás. Ezen a halmazon a definíció értelmében a 2 osztója például a 8-nak, hiszen van olyan páros szám (nevezetesen a 4), amellyel a 2-t megszorozva 8-at kapunk, de nem osztója például a 10-nek, hiszen nincs olyan páros szám, amelynek a kétszerese 10 lenne.

   A 0-nak ezen a halmazon is minden szám osztója, és a 0 most is csak saját magának osztója. Az is igaz, hogy a 0-n kívül minden számnak véges sok osztója van (hiszen ha $a \mid b$ és $b \neq 0$, akkor most is igaz, hogy $|a| \leq |b|$). Az azonban már nem igaz, hogy minden számnak lenne osztója: például a 2-nek vagy a 6-nak egyetlen páros szám sem osztója (mert semelyik páros szám páros többszöröse nem lesz 2-vel vagy 6-tal egyenlő – ehhez ugyanis az kellene, hogy a 2 vagy a 6 mint egész szám többszöröse legyen a 4-nek). Emiatt ebben a halmazban nincs olyan szám, amely minden számnak osztója lenne, vagyis nincs egység.

   Az is könnyen meggondolható, hogy a páros számok halmazán az oszthatóság nem reflexív (a 0-n kívül semelyik páros szám sem „páros osztója” saját magának); viszont antiszimmetrikus ($a \mid b$ és $b \mid a$ csak úgy teljesülhet egyszerre, ha $a = b = 0$), továbbá tranzitív is.

2. Vizsgáljuk meg most az oszthatóságot a racionális számok halmazán. Itt azt tapasztaljuk, hogy a 0 kivételével minden szám osztója minden számnak (minden nem 0 racionális számnak többszöröse akármelyik racionális szám). Az $\frac{1}{2}$ például osztója a $\frac{3}{5}$-nek, hiszen van olyan raci-

onális szám (nevezetesen a $\frac{6}{5}$), amelynek az $\frac{1}{2}$-szerese éppen $\frac{3}{5}$. Ez azon múlik, hogy a racionális számok halmazán a szorzás (a 0-tól eltekintve) invertálható művelet, így sem ott, sem más *számtestekben* nem túl érdekes az oszthatósági kérdések vizsgálata. A számtesteken az $ax = b$ egyenlet ugyanis $a \neq 0$ esetén mindig megoldható – ez a test mint algebrai struktúra egyik axiómája. (Természetesen a racionális számok körében sem igaz az, hogy a 0 osztója lenne egy nem 0 számnak; de persze magának a 0-nak igen.)

Az egész számok oszthatóságára vonatkozik a következő egyszerű, gyakran használt tétel:

2.6. Tétel. *Ha $a \mid b$ és $a \mid c$, akkor $a \mid b + c$, $a \mid b - c$, és tetszőleges k-ra $a \mid bk$ (speciálisan $a \mid bc$).*

Általában: $a \mid b$ és $a \mid c$ esetén tetszőleges $k, l (\in \mathbb{Z})$ mellett $a \mid kb + lc$.

Bizonyítás. Ha $a \mid b$, akkor $\exists q$, amelyre $aq = b$. Ha $a \mid c$, akkor $\exists r$, amelyre $ar = c$. Ekkor viszont $a(q+r) = b+c$, $a(q-r) = b-c$, $aqk = bk$ (speciálisan $aqar = bc$).

Általában: $aq = b$ és $ar = c$ esetén $aqk+arl = kb+lc$, vagyis $a(qk+rl) = kb + lc$, amiből következik az állítás. □

Megjegyzés. A tétel semelyik állításának a megfordítása sem igaz.

Abból, hogy $a \mid b+c$, nem következik, hogy a az összeg akármelyik tagját is osztaná, például $3 \mid 2 + 7$, de $3 \nmid 2$ és $3 \nmid 7$. (Azt azonban elmondhatjuk, hogy ha $a \mid b + c$, akkor b és c közül vagy mindkettő, vagy egyik sem osztható a-val. Ha például $a \mid b + c$ és $a \mid b$, akkor a tétel második állítása szerint $a \mid (b + c) - b$, vagyis $a \mid c$.)

Abból, hogy $a \mid b - c$, nem következik, hogy akár b, akár c osztható lenne a-val, például $3 \mid 10-4$, de $3 \nmid 10$ és $3 \nmid 4$. (Azt azonban most is elmondhatjuk, hogy ha $a \mid b-c$, akkor b és c közül vagy mindkettő, vagy egyik sem osztható a-val – a tétel első állítása értelmében –, sőt, mint később látni fogjuk, azt is, hogy ebben az esetben b és c ugyanazt a maradékot adja a-val osztva.)

Abból, hogy $a \mid bc$, nem következik, hogy akár b, akár c osztható lenne a-val, például $6 \mid 3 \cdot 4$, de $6 \nmid 3$ és $6 \nmid 4$. (Később látni fogjuk, hogy ha a oszt egy szorzatot, akkor milyen további feltételnek kell teljesülnie ahhoz, hogy a szorzat valamelyik tényezőjét is ossza.)

És általában: ha $a \mid kb + lc$, akkor – az előzőek alapján nyilvánvalóan – nem feltétlenül teljesül az, hogy $a \mid b$ és $a \mid c$. (Még akkor sem, ha $a \mid b$

vagy $a \mid c$ valamelyike fennáll, hiszen akkor még mindig lehet, hogy a az l-et, illetve a k-t osztja.)

2.7. Tétel. *Minden a, b egész számra*

- $a - b \mid a^n - b^n$, *ha n tetszőleges természetes szám,*
- $a + b \mid a^n + b^n$, *ha n páratlan természetes szám,*
- $a + b \mid a^n - b^n$, *ha n páros természetes szám.*

Bizonyítás. A következő azonosságokból következnek a bizonyítandó állítások;

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}) \tag{2.1}$$

$$a^{2k+1} + b^{2k+1} = (a + b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \ldots + \cdots + b^{2k}) \tag{2.2}$$

$$a^{2k} - b^{2k} = (a + b)(a^{2k-1} - a^{2k-2}b + a^{2k-3}b^2 - \ldots + \ldots - b^{2k-1}) \tag{2.3}$$

A (2.2) és a (2.3) az azonosságok (2.1)-ből levezethetők. Ha ugyanis (2.1)-ben b helyére $-b$-t helyettesítünk, akkor páratlan n-re (2.2)-t, párosra (2.3)-at kapjuk. □

2.2. Következmény. *Tetszőleges n-re $a - b \mid (a^n - b^n)$, illetve páratlan n esetén még $a + b \mid a^n + b^n$ is fennáll, páros n esetén pedig $a + b \mid a^n - b^n$.*

Megjegyzés. A fenti azonosságok közül az $(a+b)$-vel való oszthatóságot könnyebben megjegyezhetjük, ha konkrét példával emlékeztetjük magunkat rá: $a^2 - b^2$ $(n = 1)$ osztható $a + b$-vel, de $a - b$ $(n = 1)$ nem.

Fordítva is érdemes emlékezetbe vésni: a páros kitevőjű hatványkülönbség az alapok összegével és különbségével is osztható: $a^2 - b^2$ osztható $(a+b)$-vel és $(a - b)$-vel is. Ám $a + b$ $(n = 1)$ csak $(a + b)$-vel osztható.

Maradékos osztás

Azt, hogy az egész számok körében b osztója a-nak, szokás úgy is mondani, hogy „b maradék nélkül megvan a-ban”. Ha például 250 Ft-os könyveket

szeretnénk venni összesen 2000 Ft-ért, akkor mivel a 250 osztója a 2000-nek, a kívánt összeget teljes egészében el tudjuk költeni 8 tárgyra.

Sokszor nem is feltétlenül az érdekel minket, hogy egy adott szám osztója-e egy másiknak, hanem az, hogy két adott szám esetén hányszor van meg az egyik a másikban, és mennyi a maradék.

Ha például a 2000 Ft-ért 300 Ft-os könyvekből szeretnénk minél többet venni, akkor ezt is megtehetjük, vehetünk 6-ot, és marad 200 Ft. Amikor ezt kiszámoljuk, úgynezvezett maradékos osztást végzünk.

A maradékos osztás azt jelenti, hogy egy adott (a, b) $(b \neq 0)$ számpárhoz keresünk olyan (q, r) számpárt, amelyre teljesül, hogy $a = bq + r$ (ilyen mindig létezik, például $q = 0$ és $r = a$), ahol – és ez nagyon fontos kitétel – r (a maradék) egy nem negatív, de b-nél (illetve negatív b esetén $|b|$-nél) kisebb szám.

Az, hogy ilyen mindig található (ezt mondja ki – mint majd látni fogjuk – a maradékos osztás tétele (2.8.)), az egész számok fontos tulajdonságai közé tartozik.

Megjegyzés. Az, hogy tetszőleges a-hoz és $b \neq 0$-hoz található olyan q és r, amelyekre $a = bq + r$, önmagában semmitmondó állítás, hiszen ilyen q-t és r-et végtelen sokat találhatunk: bárhogyan választjuk meg q-t, tartozik hozzá egy – az egyenlőséget kielégítő – r. Ha például $a = 8$ és $b = 3$, akkor $8 = 3 \cdot 0 + 8 = 3 \cdot 1 + 5 = 3 \cdot (-1) + 11 = 3 \cdot 2 + 2 = 3 \cdot (-2) + 14 = 3 \cdot 3 + (-1)$ stb.

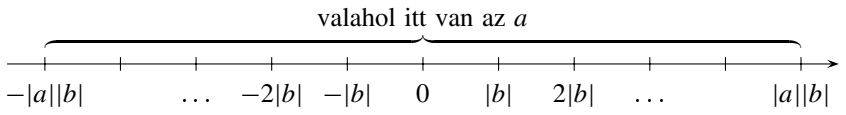
A tétel azt állítja, hogy a *végtelen sok* (q, r) pár között van – méghozzá pontosan egy – olyan, amelyre $0 \leq r < |b|$. (Példánkban ez a $(2, 2)$ pár.)

2.5. Definíció. Az $a = bq + r$ $(0 \leq r < |b|)$ *maradékos osztásban* az a-t szokás *osztandónak,* b-t *osztónak,* q-t *hányadosnak* és r-et *maradéknak* nevezni.

2.8. Tétel. (A maradékos osztás tétele) *Tetszőleges a, b egész számokhoz, ahol $b \neq 0$ egyértelműen léteznek olyan q és r egész számok, amelyekre $a = bq + r$, és $0 \leq r < |b|$.*

Bizonyítás. Először azt fogjuk megmutatni, hogy tetszőleges a és b egész számok esetén léteznek kívánt tulajdonságú q és r számok.

Felosztjuk a számegyenest a b többszörösei segítségével $|b|$ hosszú intervallumokra, és megkeressük, hogy melyikbe esik bele a.



2.1. ábra.

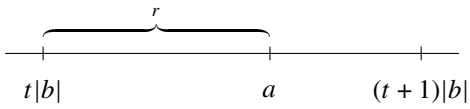
Ehhez keresnünk kell b-nek két olyan többszörösét, amelyek tartalmazzák a $[-|a|; |a|]$ intervallumot.

Jó nagy intervallumot is vehetünk, nem fontos a legkisebbet. Az a lényeg, hogy biztosak lehessünk benne, hogy tartalmazza az a-t.

Mivel $|b| \geq 1$ (hiszen $b \neq 0$), így $-|a||b| \leq -|a| \leq |a| \leq |a||b|$.

Tekintsük most b összes többszörösét $-|a||b|$ és $|a||b|$ között, tehát a $-|a||b|$, $-|a||b| + |b|$, $\ldots$, $|a||b| - |b|$, $|a||b|$ alakú számokat (vagyis $\{k|b| \mid k = -|a|, \ldots, |a|\}$).

Ekkor $-|a||b| \leq a \leq |a||b|$, vagyis a a legkisebb és a legnagyobb felsorolt szám közé esik, így pontosan egy olyan t van, amelyre teljesül, hogy $t \cdot |b| \leq a < (t+1)|b|$.



2.2. ábra.

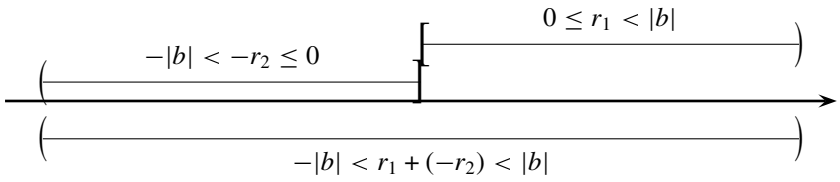
Legyen most $r = a - t|b|$. Az világos, hogy erre az r-re teljesülnek a kirótt feltételek, hiszen nyilván nemnegatív, és mivel $|b|$-nek két egymást követő többszöröse közé esik (de az egyikkel nem lehet egyenlő), így kisebb $|b|$-nél.

Mivel $t|b|$ osztható b-vel, így van olyan q szám (konkrétan t vagy $-t$), amelyre $qb = t|b|$. Ezután $a = t|b| + r$ miatt $a = qb + r$ teljesül, és éppen ilyen r és q számok létezését akartuk bizonyítani.

Ugyan a fenti t egyértelműen meghatározott, és ebből egyértelműen kijött az r és a q is, nem lehetünk benne biztosak, hogy valami más módon nem kaphatunk-e más q és r értékeket.

Ezért hátravan még az egyértelműség bizonyítása.

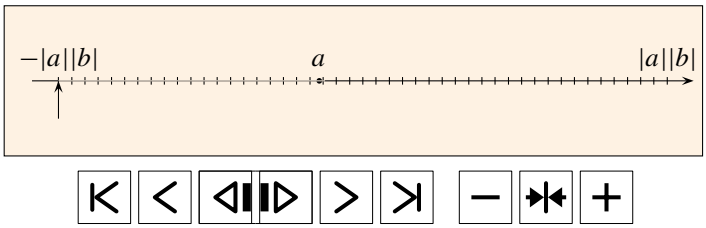
Tegyük fel, hogy egy a, b számpárhoz találtunk olyan q_1, q_2, r_1, r_2 számokat, amelyekre $a = bq_1 + r_1 = bq_2 + r_2$, ahol $0 \leq r_1 < |b|$ és $0 \leq r_2 < |b|$.



2.3. ábra.

Ekkor $b(q_1 - q_2) = r_2 - r_1$, amiből $b \mid r_2 - r_1$ következik. Mivel azonban $0 \le r_1 < |b|$ vagyis $-|b| < -r_1 \le 0$ és $0 \le r_2 < |b|$, így ezek összegére $-|b| < r_2 - r_1 < |b|$ (2.3). b-nek azonban csak egyetlen többszöröse esik ebbe az intervallumba, nevezetesen a 0, így $r_2 - r_1 = 0$, $r_1 = r_2$. Emiatt $bq_1 = bq_2$, tehát $q_1 = q_2$. □

A maradékos osztás elvét szemlélteti a 2.4. ábra animációja.



2.4. ábra. (animáció).

Itt elindíthat egy http://www.cs.elte.hu/~kfried/algebra1/Remainder.jar maradékos osztást végző programot.

Megjegyzés. Kicsit konkrétabban is meggondolható a létezés bizonyítása nemnegatív a és pozitív b számok esetén. Esetszétválasztással végezzük el a bizonyítást.

Ha $a = 0$, akkor tetszőleges pozitív b-re $a = 0 \cdot b + 0$, ahol 0 kielégíti a maradékra kirótt feltételt.

Ha $a > 0$ és $b > 0$, de $a < b$, akkor $q = 0$ és $r = a$ megfelelő, hiszen $a = b \cdot 0 + a$, ahol teljesül, hogy a maradék (a) nemnegatív, és kisebb, mint b (abszolút értéke).

Ha $a, b > 0$ és $a > b$, akkor vonjunk ki a-ból b-t, és vizsgáljuk meg az $a - b$ különbséget.

Ha $a - b < b$, akkor $q = 1$ és $r = a - b$ megfelelő, hiszen $a = b - 1 + (a - b)$, ahol az $a - b$ maradék nemnegatív (hiszen $a > b$ volt), és kisebb, mint $b (= |b|)$.

Ha $a - b > b$, akkor $a - b$-ből ismét vonjunk ki b-t, és vizsgáljuk meg az $a - 2b$ különbséget. Ha $a - 2b$ már kisebb, mint $b(= |b|)$, akkor $q = 2$ és $r = a - 2b$ megfelelő lesz, hiszen $a = b \cdot 2 + (1 - 2b)$, ahol az $a - 2b$ maradék nemnegatív, és kisebb, mint $b(= |b|)$.

Ha $a - 2b > b$, akkor $a - 2b$-ből ismét vonjunk ki b-t, és vizsgáljuk az $a - 3b$ különbséget.

Világos, hogy a fenti eljárást folytatva előbb-utóbb – de véges sok lépésben – eljutunk egy olyan $a - qb$ különbségig, amely már kisebb, mint b. Az első ilyen q és a vele képzett $r = a - bq$ maradék megfelelő lesz, hiszen $a = bq + (a - bq)$, ahol a maradék nemnegatív, hiszen $a - (q - 1)b$ még nem volt kisebb b-nél, viszont $a - bq$ már kisebb b-nél, és így b abszolút értékénél is.

Egyébként az eljárás azért ér véget előbb-utóbb, mert (például) a valós számokra érvényes az Archimédeszi axióma (alkalmas átfogalmazása: tetszőleges b természetes számhoz létezik az a természetes számnak olyan többszöröse, amely nagyobb, mint b).

Hasonlóan végezhetjük el a bizonyítást akkor is, ha a vagy b negatív, a következő módosításokkal: Ha $a < 0$ és $b > 0$, akkor adjuk hozzá az a-hoz a b-t egészen addig, amíg $a + (q - 1)b$ még kisebb, mint 0, de már $a + qb \geq 0$. Ekkor az $a = b \cdot (-q) + (a + qb)$ előállítást kapjuk.

Ha a is és b is negatív, akkor megint vonjuk ki az a-ból a b-t egészen addig, amíg az $a - (q - 1)b$ különbség még kisebb 0-nál, de $a - qb$ már nagyobb vagy egyenlő, mint 0. Ekkor az $a = bq + (a - qb)$ előállítást kapjuk.

Ha $a > 0$ és $b < 0$, akkor adjuk hozzá az a-hoz a b-t addig, amíg $a + qb$ kisebb nem lesz b abszolút értékénél, de még nemnegatív. Ekkor $a = b \cdot (-q) + (a + qb)$ lesz a kívánt előállítás.

Például:

Osszuk el maradékosan az $a = (-648)$-at $b = (-17)$-tel.

$-| - 17| \cdot | - 648| = -11\,016$, ez olyan többszöröse (-17)-nek, amely nyilvánvalóan kisebb, mint -648.

Adogassunk hozzá $|-17|$-et, amíg egy (-648)-at tartalmazó intervallumhoz nem jutunk: $-11\,016$, $-10\,099$, …, -663, -646, -429, ….

Mivel $-663 < -648 < -646$, ez lesz a keresett intervallum. $r = a - t|b|$, vagyis $r = -648 - (-663) = 15$. Ekkor viszont $q = 39$, tehát $-648 = 39 \cdot (-17) + 15$.

Természetesen a gyakorlatban nem így végezzük el a maradékos osztást, hanem megbecsüljük, hogy körülbelül mennyi lehet a hányados, és a visszaszorzással kapott maradékot – amennyiben túl nagy – ismét megpróbáljuk maradékosan osztani az osztandóval.

Az a helyzet, hogy nem tudunk osztani – nincs megfelelő osztó algoritmus –, olyan, mint amilyen az összeadásra, a kivonásra vagy a szorzásra van. Csak nagyságrendi becslés alapján számolnuk. Ráadásul valóban soha nem osztunk negatív számot, és soha nem osztunk negatív számmal. A fenti szorzásban ha például tudjuk, hogy 6-szor 17 az 102, akkor a $(-17)\cdot 30 = -510$ becslés után tudjuk, hogy már csak a $-648-(-510) = -138$ számot kell -17-tel osztani. Stb.

Megjegyzés. Más számkörökben nem feltétlenül teljesül a maradékos osztás tétele. Nem mintha nem lehetne maradékosan osztani, de a hányados és a maradék nem feltétlenül egyértelmű.

Ha pédául a páros számok halmaza az alaphalmazunk, akkor nem minden (a,b) páros számpárhoz létezik kívánt tulajdonságú páros q és r. Legyen mondjuk $a=10$ és $b=6$, ekkor nincs olyan páros q és r, amelyekre $10 = 6q+r$ és $0 \le r < 6$ teljesülne. (Ugyanakkor a racionális számok körében végtelen sok, a feltételeknek eleget tevő (q,r) számpárt találhatunk.)

Megjegyzés. A maradékos osztás vizsgálatakor hasznosak lehetnek a következő, könnyen igazolható (a bizonyítás konstrukciójából levezethető) összefüggések:

Legyen a és b két tetszőlegesen adott pozitív egész szám, és $a = bq+r$, ahol $0 \le r < |b|$. Ekkor:

$$\begin{aligned} -a &= b(-q-1)+(b-r), && \text{ahol} && (b-r) < b, \\ -a &= (-b)(q+1)+(b-r), && \text{ahol} && -(b-r) < |-b|, \\ a &= (-b)(-q)+r, && \text{ahol} && 0 \le r < |-b|. \end{aligned}$$

Egy fontos következménye a maradékos osztás tételének a következő:

2.3. Következmény. *Ha $d \mid a$ és $d \mid b$ és a-t maradékosan osztjuk b-vel, akkor a keletkező maradék osztható lesz d-vel.*

Bizonyítás. Az $a = qb+r$ felírásból $r = a-qb$, ahol a és b is osztható d-vel, vagyis a 2.6. Tétel értelmében r is osztható lesz vele. □

A maradékokra vonatkozó sokszor használt és fontos tételt az alábbi:

2.9. Tétel. *Ha a-nak c-vel való osztási maradéka r_1, b-nek c-vel való osztási maradéka r_2, akkor $(a \pm b)$-nek c-vel való osztási maradéka ugyanannyi, mint $(r_1 \pm r_2)$-nek c-vel való osztási maradéka, $a \cdot b$-nek a c-vel való osztási maradéka pedig megegyezik $r_1 \cdot r_2$-nek c-vel való osztási maradékával.*

Bizonyítás. Legyen

$$\begin{aligned} a &= cq_1 + r_1, && \text{ahol} && 0 \le r_1 < |c| \\ b &= cq_2 + r_2, && \text{ahol} && 0 \le r_2 < |c| \\ r_1 + r_2 &= cq_3 + r_3, && \text{ahol} && 0 \le r_3 < |c| \\ r_1 - r_2 &= cq_4 + r_4, && \text{ahol} && 0 \le r_3 < |c| \qquad \text{és} \\ r_1 \cdot r_2 &= cq_5 + r_5, && \text{ahol} && 0 \le r_4 < |c| \end{aligned}$$

Ekkor

$$\begin{aligned} a + b &= cq_1 + r_1 + cq_2 + r_2 = c(q_1 + q_2) + r_1 + r_2 = \\ &= c(q_1 + q_2) + cq_3 + r_3 = c(q_1 + q_2 + q_3) + r_3, \end{aligned}$$

továbbá

$$\begin{aligned} a - b &= cq_1 + r_1 - (cq_2 + r_2) = c(q_1 - q_2) + r_1 - r_2 = \\ &= c(q_1 - q_2) + cq_4 + r_4 = c(q_1 - q_2 + q_4) + r_4, \end{aligned}$$

végül

$$\begin{aligned} a \cdot b &= (cq_1 + r_1)(cq_2 + r_2) = c(cq_1q_2 + r_1q_2 + r_2q_1) + r_1 \cdot r_2 = \\ &= c(cq_1q_2 + r_1q_2 + r_2q_1 + q_5) + r_5, \end{aligned}$$

ahol $0 \le r_3 < |c|$, $0 \le r_4 < |c|$, $0 \le r_5 < |c|$. □

Megjegyzés. Vegyük észre, hogy nem arról van szó, hogy például $(a+b)$-nek c-vel való osztási maradáka megegyezne a-nak és b-nek c-vel való osztási maradékának összegével (hiszen az $|c|$-nél nagyobb is lehet), hanem annak csak c-vel való osztási maradékával egyenlő.

A tétel állítását a másik irányban alkalmazva fontos összefüggést kapunk:

2.4. Következmény. *Ha a_1 és a_2, illetve b_1 és b_2 ugyanazt a maradékot adják m-mel osztva, akkor $a_1 \pm b_1$ ugyanazt a maradékot adja m-mel osztva, mint $a_2 \pm b_2$.*

Bizonyítás. Legyen az a_1 és a_2, illetve b_1 és b_2 számok m-mel való osztási maradéka rendre r és s. A fenti tétel értelmében $a_1 \pm b_1$ és $a_2 \pm b_2$ is ugyanazt a maradékot adja, mint amit $r \pm s$ ad, tehát $a_1 \pm b_1$ és $a_2 \pm b_2$ ugyanazt a maradékot adja m-mel osztva. □

2.1. Megjegyzés. Maradékos osztásnál olykor szokás a legkisebb nemnegatív maradék helyett a legkisebb abszolút értékű maradékot venni. Így például a 7-tel való maradékos osztás maradékait 0, 1, 2, 3, 4, 5, 6 helyett -3, -2, -1, 0, 1, 2, 3-nak tekinteni. Nyilván a -3 a 4, a -2 az 5, a -1 pedig a 6 helyett jön szóba (ezek például a 2.9. Tétel alapján ugyanazt a maradékot adják 7-tel osztva, mert $-3+7=4$, $-2+7=5$, $-1+7=6$).

Feladatok

1. Minden természetes számhoz hozzárendelünk egy számot a következőképpen: összeadjuk a számjegyeit, és ha az nem egyjegyű, akkor az összeggel megismételjük az eljárást. Tesszük ezt mindaddig, amíg egyjegyű számot nem kapunk.

   Álljon két természetes szám relációban egymással, ha ugyanazt az egyjegyű számot rendeltük hozzá.

   Igazolja, hogy ez ekvivalenciareláció.

   Mik lesznek az ekvivalenciaosztályok?

2. Milyen egész n-re osztható (tetszőleges a, b egész számok esetén) $(a+b)$-vel az a^n+b^n?

   Milyen egész n-re osztható (tetszőleges a, b egész számok esetén) $(a-b)$-vel az a^n+b^n?

   Milyen egész n-re osztható (tetszőleges a, b egész számok esetén) $(a+b)$-vel az a^n-b^n?

   Milyen egész n-re osztható (tetszőleges a, b egész számok esetén) $(a-b)$-vel az a^n-b^n?

3. Milyen, n-re vonatkozó feltétel mellett osztható (tetszőleges a, b egész számok esetén) az a^n+b^n összeg egyszerre $(a+b)$-vel és $(a-b)$-vel is?

4. Milyen, n-re vonatkozó feltétel mellett osztható (tetszőleges a, b egész számok esetén) az a^n-b^n különbség egyszerre $(a+b)$-vel és $(a-b)$-vel is?

5. Keressen (a, b, n-re vonatkozó) többféle konkrét feltételt, amelyek mellett a^n+b^n szorzattá alakítható!

6. Keressen (a, b, n-re vonatkozó) többféle konkrét feltételt, amelyek mellett a^n-b^n szorzattá alakítható!

7. 1 és 100 között melyik természetes számnak van a legtöbb (pozitív) osztója?

8. Végezze el a következő maradékos osztásokat:
   -246-ot ossza el 17-tel, 246-ot -17-tel, -246-ot -17-tel, 246-ot 17-tel.
   Mit vesz észre a hányadosokkal és a maradékokkal kapcsolatban?

9. Ossza el maradékosan a 17-et 246-tal és -246-tal.

3. fejezet

Számrendszerek, oszthatósági szabályok

A számok nálunk használatos mai – tízes számrendszerbeli, helyiértékes – írásmódja hosszú idő alatt alakult ki. Ma már mindenki számára természetes, hogy ha a 324-es számot látjuk, mindannyian ugyanarra a – 3 százasból, 2 tízesből és 4 egyesből álló – számra gondolunk, de ez korántsem volt mindig így. Az idők során különböző népek különféle módszereket alkalmaztak a számok lejegyzésére, a római számok például (CCCXXIV) a mai napig tükrözik egy nem helyiértékes írásmód emlékét. A helyiértékes írásmód az időszámítás előtt 1900 körül alakult ki Mezopotámiában (http://hu.wikipedia.org/wiki/A_matematika_története). Bizonyos mértékegységeink váltószáma – például 60 másodperc = 1 perc, 60 perc = 1 óra – az ott használt hatvanas számrendszerre utalnak. A tízes számrendszert több ókori nép is használta, de általában helyiérték nélkül. A tízes számrendszer és a helyiérték összekapcsolása – csakúgy, mint a 0 önálló számjegyként való alkalmazása – hindu örökség. A legrégebbi tízes számrendszerben felírt helyiértékes számot tartalmazó régészeti emlék i. sz. 590 környékéről, Indiából származik (http://hu.wikipedia.org/wiki/Számjelölő_rendszerek aloldalán). A hindu számírás később arab közvetítéssel jutott el Európába, ahol igen lassan terjedt el, használata csak a XVI. századra vált általánossá.

A 324-es szám eredetileg 324 darab valamit – birkát, fát, kavicsot, lépést stb. – jelentett. Ha feljegyzést kívánunk készíteni erről a 324 valamiről, akkor kézenfekvő valamilyen egyszerű jelet, például egy strigulát 324-szer leírni. Ez a fajta írásmód létezett is, használatának megvan az az előnye, hogy nem kell hozzá ismerni valamiféle jeleket (számokat), elég mindössze azt ellenőrizni, hogy ugyanannyi birka jött-e haza a legelőről, mint ahány rovás van a pálcikán. Hátránya viszont, hogy már viszonylag kis számok esetén is

áttekinthetetlen, hosszadalmas, és használóját már a legegyszerűbb szorzási művelet is gyakorlatilag megoldhatatlan feladat elé állítja.

Válasszunk a 324 helyett egy kisebb számot, mondjuk a 24-et! A 24 ily módon lejegyezve: ||||||||||||||||||||||||. Látható, hogy első ránézésre még egy ilyen kis szám esetén is csak hozzávetőleges elképzelésünk lehet a leírt szám nagyságáról. Sokat segít, ha striguláinkat csoportosítjuk, mondjuk tízes csoportokba: |||||||||| |||||||||| ||||. Most elég csak azt ellenőriznünk, hogy hány teljes csoportunk és még hány strigulánk van. Nagyobb számok esetén tíz tízes csoportból képezhetünk egy nagyobb csoportot – és így tovább, a számrendszeren alapuló írásmód mélyén ez a csoportosítási ötlet húzódik meg. A 324 leírásakor 3 nagy (tízszer tízes), 2 kicsi (tízes), és egy csonka, 4 strigulából álló csoport lesz. A helyiértékes írásmód egyik előnye, hogy ezt röviden képes lejegyezni. A 324 megfelelően csoportosított strigula helyett csak azt soroljuk fel, hogy melyik fajta csoportból hány van – a csoportok nagyságrendjének csökkenő sorrendjében.

A számírásunknak tehát nem a számrendszer alapszáma a legnagyobb érdeme, hanem a helyiértékes írásmód. Ennek nagy előnye, hogy egy véges jelkészlet segítségével (tízes számrendszerben például a $0, 1, 2, \ldots, 8, 9$ számjegyek felhasználásával) tetszőleges nemnegatív egész szám egyszerűen leírható, könnyen visszaolvasható, és az így leírt számokkal viszonylag egyszerű algoritmusok alapján végezhetők el az alapműveletek.

Nem terjedhetett volna el azonban ez a felírás, ha nem lenne egyértelmű egy szám felírása. Azt, hogy ez a fajta írásmód alkalmas a számok egyértelmű lejegyzésére, a következő tétel alapján tudjuk.

3.1. Tétel. *Minden pozitív egész szám egyértelműen felírható*

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$$

alakban, ahol $\forall i$*-re* $0 \leq a_i < 10$*,* $a_i \in \mathbb{N}$ *és* $a_n \neq 0$*.*

Bizonyítás. A maradékos osztás tétele (2.8. Tétel) szerint léteznek az egyértelműen meghatározott q_0 és a_0 egész (sőt, nemnegatív) számok, amelyekre

$$A = 10q_0 + a_0, \qquad \text{ahol} \qquad 0 \leq a_0 < 10.$$

Hasonlóan

$$q_0 = 10q_1 + a_1, \qquad \text{ahol} \qquad 0 \leq a_1 < 10.$$

Így folytatva

$$q_1 = 10q_2 + a_2, \qquad \text{ahol} \qquad 0 \leq a_2 < 10.$$

$$\vdots$$

$$q_{k-1} = 10q_k + a_k, \qquad \text{ahol} \qquad 0 \le a_k < 10.$$
$$\vdots$$

Mivel $A > q_0 > q_1 > q_2 > \ldots > q_{k-1} > q_k > \ldots$ és mindegyik nemnegatív egész szám, előbb-utóbb eljutunk egy $q_n = 0$-ig. Ekkor:

$$q_{n-1} = 10q_n + a_n\text{-ből} \qquad\qquad q_{n-1} = a_n.$$

Ezt visszahelyettesítve:

$$q_{n-2} = 10a_n + a_{n-1}.$$

Folytatva a visszahelyettesítést:

$$q_{n-3} = 10^2 a_n + 10a_{n-1} + a_{n-2}.$$

És így tovább. Végül az

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$$

előállításhoz jutunk, ahol az a_n, a_{n-1}, …, a_0 egész számok mindegyike egyértelműen meghatározott, továbbá minden i-re $0 \le a_i < 10$ és $a_n \neq 0$ (ez utóbbi abból következik, hogy ellenkező esetben már q_{n-1} is nulla lett volna).

Bár az előállítás egyértelmű, mégis elképzelhető, hogy valami más úton egy másik felíráshoz jutunk. Ezért még be kell látnunk, hogy ha van kétféle felírás, akkor azok ugyanazok. Ha

$$A = a_n{\cdot}10^n{+}a_{n-1}{\cdot}10^{n-1}{+}\ldots{+}a_1{\cdot}10{+}a_0 = b_k{\cdot}10^k{+}b_{k-1}{\cdot}10^{k-1}{+}\ldots{+}b_1{\cdot}10{+}b_0,$$

(feltehető, hogy $n \ge k$, valamint $n \ge i > k$ esetén válasszuk b_i-t 0-nak), akkor ezek különbsége

$$0 = (a_n - b_n) \cdot 10^n + (a_{n-1} - b_{n-1}) \cdot 10^{n-1} + \ldots + (a_1 - b_1) \cdot 10 + (a_0 - b_0).$$

A bal oldalon álló 0-nak minden természetes szám osztója, ezért a jobb oldalon álló, vele egyenlő számnak is.

Mivel $(a_n - b_n) \cdot 10^n + (a_{n-1} - b_{n-1}) \cdot 10^{n-1} + \ldots + (a_1 - b_1) \cdot 10$ osztható 10-zel, így $(a_0 - b_0)$ is. Ez – mivel $0 \le a_0, b_0 < 10$ – csak úgy lehet, hogyha $a_0 = b_0$. Ezért

$$0 = (a_n - b_n) \cdot 10^n + (a_{n-1} - b_{n-1}) \cdot 10^{n-1} + \ldots + (a_1 - b_1) \cdot 10.$$

Most a 10^2-nal folytatható ugyanez a gondolatmenet, emiatt $a_1 = b_1$.

Folytatva a gondolatmenetet 10 következő hatványaira, n lépésben eljutunk a 10 n-edik hatványáig, az $a_n = b_n$ következtetésre jutunk, amiből azt kapjuk, hogy a két felírás ugyanaz. □

Itt talál egy programot, amely átír egy valamilyen (2–10) alapú számrendszerben felírt számot egy másik alapúra.

Itt elindíthat egy http://www.cs.elte.hu/~kfried/algebra1/Numeral.jar számrendszerek között konvertáló programot.

Megjegyzés. Az a_n, a_{n-1}, …, a_0 számokat szokás az

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$$

szám tízes számrendszerbeli *számjegyeinek* nevezni, a 10 hatványait pedig *helyiértékeknek*. Tételünk értelmében a tízes számrendszerbeli számjegyek fenti sorozata egyértelműen jellemzi a számot, ezen alapul a számok szokásos tízes számrendszerbeli írásmódja.

Megjegyzés. Az $a_n \neq 0$ kikötésre az egyértelműséghez volt szükség. Semmi elvi akadálya sincs annak, hogy megengedjük, hogy egy szám „0-val kezdődjön”, csak éppen ha megengedjük, akkor a felírás nem lesz egyértelmű, a 12-t például 012-nek, vagy 0012-nek stb. is írhatnánk. Tételünk tehát nem azt mondja, hogy 0-val nem kezdődhet szám, hanem azt, hogy a szám elejére írható nulláktól eltekintve egyértelmű a felírás.

Hasonló tétel teljesül más alapszámú számrendszerekre is:

3.2. Tétel. *Legyen $t \geq 2$ természetes szám. Ekkor minden pozitív egész szám egyértelműen írható fel*

$$A = a_n t^n a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

alakban, ahol minden i-re $0 \leq a_i < t$, $a_i \in \mathbb{N}$ és $a_n \neq 0$.

Bizonyítás. A 3.1. Tétel bizonyítása során sehol nem használtuk ki, hogy a számrendszer alapszáma éppen 10, így annak bizonyítása tetszőleges $t \geq 2$ természetes számra levezethető. A tétel állítása így tetszőleges t számrendszer alapszámra megfogalmazható, a bizonyításban pedig minden pontosan úgy felírható, mint a 3.1. Tételében, csak a 10 helyére mindenhova t-t kell írnunk. □

Például: $324 = 2 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 4 = 2244_5$.

Megjegyzés. Mivel a számírás során a 10-es számrendszert használjuk, ha nem tízes számrendszerben írunk fel egy számot, jelölnünk kell a felírásban a számrendszer alapszámát.

Megjegyzés. Amennyiben 10-nél nagyobb számot választunk a számrendszer alapszámául, a szokásos 10 számjegy nem elegendő. Ilyenkor új jeleket kell bevezetnünk a 10, 11, …, $t-1$ számok mint számjegyek jelölésére.

Informatikában például elterjedt a 16-os számrendszer, ahol a 10-re az A, 11-re a B, 12-re a C, 13-ra a D, 14-re az E, 15-re az F jeleket használják.

Például: $3A5B_{12} = 3 \cdot 12^3 + 10 \cdot 12^2 + 5 \cdot 12 + 11 = 6695_{10}$

Oszthatósági szabályok

A matematika egyik legrégibb ága a számelmélet. Azt hihetnénk, hogy nincs megoldatlan számelméleti probléma, azonban ez egyáltalán nincs így. Sőt!

A mai modern tudományok közül például a számítógéptudomány támaszkodik a számelmélet egyes eredményeire. Köztük arra, hogy egy számról ránézésre nem lehet eldönteni, hogy mik az osztói. Ezt használja fel a számítógépes titkosítás során: olyan nagy számokat használ titkosítási kód gyanánt, amelyek osztóiról csak az arra illetékesek tudnak, a szám pedig olyan nagy, hogy gyakorlatilag képtelenség megtalálni az osztóit. Erről később kicsit bővebben fogunk szólni.

Kisebb léptékben is gyakran van rá szükség, hogy megállapítsuk, mely számok osztói egy számnak, vagy – egy még egyszerűbb kérdés – hogy osztható-e egy szám valamelyik másikkal.

Ehhez bizonyos esetekben nincs szükség a maradékos osztás tényleges elvégzésére. Korábbi tanulmányaikból ismerhetünk már kritériumokat egyes számokkal való oszthatóságról.

Bontsuk kétfelé ezeket a kritériumokat. Az egyik fajta a szám felírásától független (például: egy szám akkor és csak akkor osztható 6-tal, ha 2-vel is és 3-mal is osztható). A másik fajta viszont a számnak a 10-es számrendszerbeli helyiértékes felírásából formálisan következtet.

Mi most az utóbbival fogunk részletesen foglalkozni.

Mindenekelőtt szögezzük le, hogy a 2.4. Tétel értelmében oszthatósági kérdések vizsgálatakor elegendő pozitív számok pozitív osztóit keresnünk.

Ezek az úgynevezett oszthatósági szabályok, amelyek alapján a szám alakjából szinte ránézésre, gyorsan eldönthető, hogy a szám bizonyos számokkal osztható-e. A legismertebb oszthatósági szabályok (amelyekkel már a korábbi tanulmányaink során is találkoztunk) a következők:

Az $A = a_n \cdot 10^n + a_{n-1}10^{n-1} + \ldots + a_1 \cdot 10 + a_0$ (tízes számrendszerben felírt) szám akkor és csak akkor osztható

(1) 10-zel, ha utolsó számjegye 0 (10-zel osztható).

(2) 2-vel, ha utolsó számjegye páros (2-vel osztható).

(3) 5-tel, ha utolsó számjegye 0 vagy 5 (5-tel osztható).

(4) 4-gyel, ha az utolsó két számjegyéből álló szám osztható 4-gyel.

(5) 25-tel, ha az utolsó két számjegyéből álló szám osztható 25-tel.

(6) 8-cal, ha az utolsó három számjegyéből álló szám osztható 8-cal.

(7) 9-cel, ha a szám számjegyeinek összege osztható 9-cel.

(8) 3-mal, ha a szám számjegyeinek összege osztható 3-mal.

(9) 11-gyel, ha a számjegyek váltott előjelű összege osztható 11-gyel.

Például: A 3 564 672 180 szám osztható 2-vel (mert az utolsó számjegye, a 0 páros), 3-mal (mert számjegyeinek összege, 42, osztható 3-mal), 4-gyel (mert az utolsó két számjegyéből álló szám, a 80 osztható 4-gyel), 5-tel (mert az utolsó számjegye, a 0 osztható 5-tel) és 10-zel (mert az utolsó számjegye 0). Nem osztható viszont sem 25-tel, sem 8-cal, sem 9-cel, sem 11-gyel. Más számokkal való oszthatóságáról közvetlenül a fenti szabályok alapján egyelőre nem mondhatunk semmit.

Megjegyzés. A fenti példában szereplő számról joggal állapíthatják meg néhányan, hogy például 6-tal is osztható, hiszen ha egy szám páros és 3-mal osztható, akkor 6-tal is osztható; vagy hogy 20-szal is osztható, hiszen ha 4-gyel is és 5-tel is osztható, akkor 20-szal is oszthatónak kell lennie. Olyan szabályokkal azonban, amelyek bizonyos osztók létezéséből következtetnek újabb osztók létezésére, most nem foglalkozunk. Azt viszont megjegyezzük, hogy általában **nem** igaz az, hogy ha egy szám osztható a-val is és b-vel is, akkor osztható ab-vel is. A fenti szám például osztható 4-gyel is és 6-tal is, de 24-gyel már nem.

Gyűjtsük táblázatba 10 egyes hatványainak a vizsgált osztók szerinti maradékát. (Az egyszerűség kedvéért a 0-kat hagyjuk ki.)

...	10^6	10^5	10^4	10^3	10^2	10^1	10^0	
...	0	0	0	0	0	0	1	2
...	1	1	1	1	1	1	1	3
...	0	0	0	0	0	2	1	4
...	0	0	0	0	0	0	1	5
...	0	0	0	0	4	2	1	8
...	1	1	1	1	1	1	1	9
...	0	0	0	0	0	0	1	10
...	1	10	1	10	1	10	1	11

Vegyük észre, hogy egyes számokkal való osztáskor csak az utolsó néhány 10-hatványt kell tekintetbe vennünk. Ezek (2, 4, 5, 8, 10) egy bizonyos hatvány után már osztói valamely 10-hatványnak. Mások osztási maradékát azért tudjuk könnyen meghatározni, mert azok a 10-nél 1-gyel kisebb vagy nagyobb szám osztói.

A megfigyeléseink alapján a fenti szabályokhoz hasonló szabályokat más alapszámú számrendszerekben is fel tudunk írni:

Az $A = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$ szám akkor és csak akkor osztható

(1) t-vel, ha utolsó számjegye 0.

(2), (3) t-nek egy tetszőleges d_1, osztójával, ha utolsó számjegye osztható d_1-gyel.

(4), (5) t^2-nek egy tetszőleges d_2 osztójával ha az utolsó két számjegyéből álló szám osztható d_2-vel.

(6) t^3-nek egy tetszőleges d_3 osztójával, ha az utolsó három számjegyből álló szám osztható d_3-mal.

(7) $(t-1)$-gyel, ha a számjegyek összege osztható $(t-1)$-gyel.

(8) $t-1$ egy tetszőleges d_4 osztójával, ha a számjegyek összege osztható d_4-gyel.

(9) $(t+1)$-gyel, ha a számjegyek váltott előjelű összege osztható $(t+1)$-gyel.

Továbbá:

(10) $t+1$ egy tetszőleges d_5 osztójával, ha a számjegyek váltott előjelű összege osztható d_5-tel.

Összefoglalva:

3.3. Tétel. *Az* $A = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ *szám akkor és csak akkor osztható*

(i) *d-vel, ahol* $d \mid t^k$, *ha* $d \mid a_{n-1}t^{k-1} + \ldots + a_1 t + a_0$ *(vagyis ha d osztója az utolsó k számjegyből álló számnak).*

(ii) *e-vel, ahol* $e \mid t-1$, *ha* $e \mid \sum_{i=0}^{n} a_i$ *(vagyis ha e osztója a számjegyek összegének).*

(iii) *f-fel, ahol* $f \mid t+1$, *ha* $f \mid \sum_{i=0}^{n} (-1)^i a_i$ *(vagyis ha f osztója a számjegyek váltott előjelű összegének).*

Megjegyzés. A tétel magába foglalja az összes korábban felsorolt szabályt: (i) vonatkozik az alapszámnak és az alapszám hatványainak osztóival való oszthatóságra, (ii) az alapszámnál eggyel kisebb számmal és annak egyéb osztóival való oszthatóságra, (iii) pedig az alapszámnál eggyel nagyobb számmal, illetve annak egyéb osztóival való oszthatóságra.

A tízes számrendszerbeli szabályokat a $t = 10$ speciális esetben kapjuk; (i) tartalmazza az (1), (2), (3), (4), (5) és (6) szabályokat, (ii) a (7) és (8) szabályokat, (iii) pedig a (9), továbbá (a tízes számrendszerben semmitmondó) (10) szabályokat.

Bizonyítás. (i) $A = (t^n a_n + \ldots + t^k a_k) + (t^{k-1}a_{k-1} + \ldots + a_0) = B + C$. (Az első tagot jelöltük B-vel, a másodikat C-vel.) A B szám egy olyan összeg, amelynek minden tagja osztható t^k-nal, ezért t^k minden osztójával, így d-vel is: $d \mid B$.

A 2.6. Tétel alapján ekkor ha $d \mid A(= B + C)$, akkor $d \mid C = A - B$, valamint ha $d \mid C$, akkor $d \mid A = B + C$.

(ii)
$$\begin{aligned} A = \Big(&(t^{n-1}-1)a_n + (t^{n-1}-1)a_{n-1} + \ldots + (t-1)a_1 \quad \Big) + \\ + \big(&\quad a_n + \quad a_{n-1} + \ldots + \quad a_1 + a_0 \big) = B + C \end{aligned}$$

Az első tagot jelöltük B-vel, a másodikat C-vel, itt tehát $C = \sum_{i=0}^{n} a_i$ a számjegyek összege.

Felhasználva, hogy tetszőleges $k \geq 0$ egész esetén $t - 1 \mid t^k - 1$ (2.7. Tétel) azt kapjuk, hogy B-nek minden tagja osztható $(t-1)$-gyel. Vagyis B osztható $t-1$ minden osztójával, így e-vel is.

A 2.6. Tétel alapján ekkor ha $e \mid A$, akkor $e \mid A - B = C$; ha pedig $e \mid C$, akkor $e \mid B + C = A$.

(iii)

$$A = \Big((t^n - (-1)^n)a_n + (t^{n-1} - (-1)^{n-1})a_{n-1} + \ldots + (t^3 + 1)a_3 + (t^2 - 1)a_2 + (t+1)a_1\Big) + \Big((-1)^n a_n + (-1)^{n-1}a_{n-1} + \ldots - a_3 + a_2 - a_1 + a_0\Big) = B + C$$

Az első tagot jelöltük B-vel, a másodikat C-vel, ahol $C = \sum_{i=0}^{n}(-1)^i a_i$, azaz A számjegyeinek váltott előjelű összege, és az egyesek helyén álló számjegy előjele pozitív.

Ahogy a (ii) esetben, most is felhasználjuk, hogy $t - (-1) \mid t^k - (-1)^k$ minden k nemnegatív egész számra, azaz $t + 1 \mid t^k - (-1)^k$.

Így – ismét a 2.7. Tételt alkalmazva – azt kapjuk, hogy a B összeg minden egyes tagja osztható $(t+1)$-gyel. Vagyis B osztható $(t+1)$-gyel, így $t+1$ minden osztójával, ezért f-fel is.

Innentől a bizonyítás a 2.6. Tétel felhasználásával ugyanúgy történik, mint az (i) és a (ii) esetben: A akkor és csak akkor osztható f-fel, ha C is. □

Például: A $24\,312\,561_7$ szám osztható 2-vel, mert a számjegyek összege páros ($2 \mid (7-1) = 6$), 3-mal, mert a számjegyek összege 3-mal osztható ($3 \mid (7-1) = 6$) és 6-tal, mert a számjegyek összege osztható 6-tal.

Viszont nem osztható 7-tel, mert nem 0-ra végződik és 4-gyel (és így 8-cal sem), mert a számjegyek váltott előjelű összege nem osztható 4-gyel.

3.1. Megjegyzés. Mindhárom bizonyítás azon alapult, hogy az A számot sikerült egy olyan $A = B + C$ összeg alakjában felírni, ahol az összeg egyik tagjáról (B-ről) megmutattuk, hogy mindenképp osztható a szabályban szereplő osztóval. Ebből azonban nemcsak az következik, hogy A akkor és csak akkor osztható a szabályban szereplő számmal, ha C osztható azzal, hanem az is, hogy A *ugyanazt a maradékot adja* a szóbanforgó számmal osztva, mint C. (Ha $A = B + C$, akkor A maradéka nyilván megegyezik $B + C$ maradékával, ami viszont – mivel B maradéka 0 – megegyezik C maradékával, lásd 2.9. Tétel.)

Ennélfogva a fenti tételnél erősebb állítás is megfogalmazható:

3.4. Tétel. *Az* $A = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ *szám ugyanazt a maradékot adja*

(i) t^k *tetszőleges osztójával osztva, mint* t *alapú számrendszerben felírva az utolsó* k *darab számjegyéből álló szám.*

(ii) $t-1$ *tetszőleges osztójával osztva, mint* t *alapú számrendszerben felírva a számjegyeinek összege.*

(iii) $t+1$ *tetszőleges osztójával osztva, mint* t *alapú számrendszerben felírva a számjegyeinek váltott előjelű összege.*

Bizonyítás. Lásd a 3.1. Megjegyzést. □

Következmény. Ezzel bebizonyítottuk ($t = 10$ mellett) a 10-es számrendszerben korábban felírt oszthatósági szabályokat is.

3.2. Megjegyzés. A későbbiekben külön jelölést fogunk bevezetni arra, hogy két szám ugyanazt a maradékot adja egy harmadikkal osztva (lásd kongruenciák, 8.1. Definíció), ami lényegesen egyszerűbbé teszi majd az ilyesfajta állítások lejegyzését.

3.3. Megjegyzés. Az eddigiek során szereplő oszthatósági szabályok a legismertebbek és legkönnyebben alkalmazhatók, de számos további szabály is kimondható.

Ezek egy része – mint például a 6-tal való oszthatóság szabálya (egy szám akkor és csak akkor osztható 6-tal, ha 2-vel is és 3-mal is osztható) – más számokkal való oszthatóságból következtet az illető számmal való oszthatóságra, és általában a maradékról – ha az nem 0 – nem mond semmit. Azt, hogy pontosan milyen körülmények között következtethetünk az a-val és b-vel való oszthatóságból az ab-vel való oszthatóságra, később fogjuk tisztázni.

Általában könnyű oszthatósági szabályt mondani olyan számokra, amelyek 1-gyel kisebbek vagy 1-gyel nagyobbak egy tízhatványnál (nem tízes alapú számrendszerekben pedig az alapszám valamelyik hatványánál). Ezt szemléltetik a következő példák:

3.1. Példa. Egy (tízes számrendszerben felírt) szám akkor és csak akkor osztható 37-tel, ha az a szám, amelyet úgy kapunk, hogy az eredeti szám számjegyeit hátulról kezdve hármas csoportokba osztjuk, majd az így kapott háromjegyű számokat összeadjuk, az összeg szintén osztható 37-tel.

A szabály igazolása történhet például úgy, hogy az eredeti számot átírjuk 1000-es számrendszerbe, majd alkalmazzuk rá az alapszámnál eggyel kisebb számra vonatkozó szabályt ($37 \mid 999$).

Mivel egyébként $999 = 37 \cdot 27$, a 27-tel való oszthatóságra pontosan ugyanez a szabály érvényes: Egy (tízes számrendszerben felírt) szám akkor és csak

akkor osztható 27-tel, ha az a szám, amelyet úgy kapunk, hogy az eredeti szám számjegyeit hátulról kezdve hármas csoportokba osztjuk, majd az így kapott háromjegyű számokat összeadjuk, az összeg is osztható 27-tel.

3.2. Példa. Egy (tízes számrendszerben felírt) szám akkor és csak akkor osztható 13-mal, ha az a szám, amelyet úgy kapunk, hogy az eredeti szám számjegyeit hátulról kezdve hármas csoportokba osztjuk, majd az így kapott háromjegyű számokat váltott előjellel összeadjuk is osztható 13-mal.

A szabályt ismét igazolhatjuk például úgy, hogy az eredeti számot átírjuk 1000-es számrendszerbe, majd alkalmazzuk rá az alapszámnál eggyel nagyobb szám osztóira vonatkozó szabályt ($13 \mid 1001$).

Hasonló igaz 1001 többi osztójára is, így 7-re, 11-re is.

Valójában tetszőleges számra gyárthatunk oszthatósági szabályt (bár a szabály alkalmazása gyakran nehézkesebb lehet, mint egyszerűen elvégezni az osztást). Ezt szemlélteti a következő példa:

3.3. Példa. Egy (tízes számrendszerben felírt) szám akkor és csak akkor osztható 7-tel, ha az a szám is osztható 7-tel, amelyet a következőképpen kapunk: szorozzuk meg az eredeti szám számjegyeit hátulról kezdve rendre a következő számokkal: 1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, ..., majd adjuk össze az így kapott szorzatokat.

Ennek igazolásához írjuk fel ismét azt a táblázatot (a 7-re), amelyben 10 hatványainak maradékait írtuk fel az adott számmal osztva, ezúttal a legkisebb abszolút értékű maradékokat beírva (lásd 2.1. Megjegyzés):

...	10^6	10^5	10^4	10^3	10^2	10^1	10^0	
	1	-2	-3	-1	2	3	1	7

A szabály itt láthatóan azon múlik, hogy az $A = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_1 10 + a_0$ számban szereplő tízhatványok (hátulról kezdve a 0-dik hatvánnyal) rendre ugyanazokat a maradékokat adják 7-tel osztva, mint a megadott számok: az 1 egyet, a 10 hármat, a 100 kettőt, az 1000 ugyanannyit, mint a -1 (vagyis 6-ot) stb.

Feladatok

1. Milyen alapú számrendszerben olvasható le a jegyek (esetleg váltott előjelű) összegéből a 7-tel való oszthatóság? Minden lehetséges számrendszeralapszámot adjon meg!

2. Milyen alapú számrendszerben olvasható le az utolsó néhány számjegyből a 7-tel való oszthatóság? Minden lehetséges számrendszeralapszámot adjon meg!

3. Egy t alapú számrendszerben a számjegyek összegéből következtethetünk a 4-gyel való oszthatóságra. Mivel való oszthatóságra következtethetünk a számok váltott előjelű összegéből?

4. Milyen számrendszer(ek)ben következtethetünk a számjegyek (esetleg váltott előjelű) összegéből és az utolsó néhány számjegyből a 11-gyel, valamint a 4-gyel való oszthatóságra?

5. Írja fel a 3.4. Tétel szerinti oszthatósági szabályokat a 8-as, 9-es, 17-es alapú számrendszerekben!

6. Igazolja, hogy 9-esből 3-as számrendszerre úgy lehet áttérni, hogy az egyes számjegyeket helyettesítjük a 3-as számrendszerbeli alakjukkal!

   Mondjon ki hasonló (helyes) állításokat!

7. A $t+1$ alapú számrendszerben felírt $\overline{tttt}$ szám négyzete $\overline{tttxyyyx}$. Határozza meg a számrendszer alapszámát!

8. Készítsen oszthatósági szabályt a 7-re a 11-es számrendszerben!

9. Igazolja, hogy bármely k egymást követő egész szám szorzata osztható $k!$-sal ($k! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (k-1) \cdot k$)

4. fejezet

Legnagyobb közös osztó, legkisebb közös többszörös

Két – nem feltétlenül különböző (egész) – szám legnagyobb közös osztójának értelemszerűen azt a számot nevezzük, amely mindkettőnek osztója, és az ilyen tulajdonságúak – vagyis a közös osztók – közül a legnagyobb:

4.1. Definíció. Az a és b számok *legnagyobb közös osztója* d, ha

1. $d \mid a$ és $d \mid b$, továbbá
2. ha valamely c számra $c \mid a$ és $c \mid b$, akkor $d \geq c$.

4.1. Jelölés. $d = (a, b)$ vagy $d = \text{lnko}(a, b)$.

Például: $(8, 12) = 4$, mert a 8 osztói: 1, -1, 2, -2, 4, -4, 8, -8; a 12 osztói: 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12; közös osztók: 1, -1, 2, -2, 4, -4. Ezek közül a legnagyobb a 4.

$(-8, 12) = 4$, mert a -8 osztói ugyanazok, mint a 8 osztói.

$(0, 6) = 6$, mert a 0-nak minden szám osztója, a 6 osztói közül a 6 a legnagyobb.

Megjegyzés. Általában $(a, a) = |a|$ és $(0, a) = |a|$, kivéve, ha $a = 0$.

Ha a és b is 0-val egyenlő, akkor nem létezik legnagyobb közös osztója a-nak és b-nek, ugyanis a 0-nak minden szám osztója, és az egész számok között nincsen legnagyobb.

Ha létezik (a, b) (azaz nem mind a kettő 0), akkor létezik közös osztójuk (például az 1), véges sok osztója van legalább az egyiknek, és ezek között

létezik legnagyobb – ráadásul egyetlen legnagyobb van köztük. Ezért a-nak és b-nek mindig létezik egy *egyértelműen meghatározott* legnagyobb közös osztója

Azt is megállapíthatjuk, hogy két szám legnagyobb közös osztója (ha egyáltalán létezik, vagyis ha nem mindkettő 0) mindig pozitív, ugyanis a közös osztók mindegyikének – így a legnagyobbnak is – az ellentettje is közös osztó. Ez a közös osztó nem lehet a 0, és egy nem 0 szám és az ellentettje közül mindig a pozitív a nagyobb.

Hasonlóképpen definiálható kettőnél több szám legnagyobb közös osztója is:

4.2. Definíció. Az a_1, a_2, …, a_k számok *legnagyobb közös osztója* d, ha

1. d osztója az a_1, a_2, …, a_n számok mindegyikének, valamint
2. ha egy c szám osztója az a_1, a_2, …, a_n számok mindegyikének, akkor $d \geq c$.

Például: $(18, 30, 45) = 3$, $(6, 15, 70) = 1$.

Számpárok közös osztóit vizsgálva felfedezhetjük, hogy két szám (hacsak nem 0 mindkettő) közös osztói között mindig van olyan – nevezetesen éppen a legnagyobb és annak ellentettje –, amely az összes közös osztónak többszöröse. (Például a 36 és a 60 közös pozitív osztói az 1, 2, 3, 4, 6, 12. Közülük a 12 a legnagyobb, és ez többszöröse mindegyik osztónak.)

4.3. Definíció. Az a és b egész számok *kitüntetett közös osztója* δ, ha

1. $\delta \mid a$ és $\delta \mid b$ (közös osztó), valamint
2. ha $c \mid a$ és $c \mid b$, akkor $c \mid \delta$ (kitüntetett), továbbá
3. $\delta \geq 0$ (a fenti tulajdonságúak közül a nemnegatív).

Ideiglenes házi jelölés: $\delta = \langle a, b \rangle$. (Ezt a jelölést csak addig használjuk, amíg feltétlenül meg akarjuk különböztetni a legnagyobb, illetve a kitüntetett közös osztót. Ilyen jelölés a matematikai szakirodalomban nincs.)

Megjegyzés. Hasonlóan definiálható kettőnél több (nem feltétlenül különböző) szám kitüntetett közös osztója is.

4.1. Megjegyzés. Vegyük észre, hogy a definíció $a = b = 0$ esetben is meghatároz egy számot: a 0-t. Az 1. tulajdonság szerint ugyanis δ mindkettőjüknek osztója (ez bármi lehet). A 2. tulajdonság szerint minden közös

osztónak többszöröse – ez $a = b = 0$ esetben csakis a 0-ra teljesül. Végül a 3. tulajdonság szerint nemnegatív, ez nyilván teljesül.

Azt is fontos észrevenni, hogy a kitüntetett közös osztó – ha létezik –, akkor *egyértelműen meghatározott*. Ha ugyanis két kitüntetett közös osztót találunk (δ_1 és δ_2), akkor az egyik osztója a másiknak, a másik az egyiknek, mindkettő nemnegatív, így csak egyenlők lehetnek.

4.1. Következmény. *Amennyiben két számnak létezik kitüntetett közös osztója is és legnagyobb közös osztója is, akkor azok megegyeznek.*

Bizonyítás. A legnagyobb közös osztó és a kitüntetett közös osztó tulajdonságai szerint $\delta \leq d$ és $d \mid \delta$, amiből a 2.1. Tétel alapján $d \leq \delta$, vagyis $\delta = d$ következik. □

Azt már láttuk, hogy csak a $(0, 0)$ párnak nem létezik legnagyobb közös osztója, viszont létezik kitüntetett közös osztója. Kérdés persze, hogy tetszőleges két egész számnak létezik-e kitüntetett közös osztója.

4.1. Tétel. *Tetszőleges két egész számnak létezik egyértelműen meghatározott kitüntetett közös osztója.*

Bizonyítás. Azt a fontos tényt használjuk, hogy ha egy szám osztója a-nak és b-nek is, akkor a különbségüknek is osztója, sőt, tetszőleges k, l egész számokra az $ak + bl$ számnak is (2.9. Tétel).

Egy eljárás során (amelynek *euklideszi algoritmus* a neve) a-ból és b-ből kiindulva lépésről lépésre olyan egyre kisebb és kisebb abszolút értékű számokat képezünk, amelyek mindegyike osztható a és b minden közös osztójával (2.3. Következmény).

Ehhez pedig a maradékos osztást fogjuk használni.

Először a-t osztjuk el maradékosan b-vel. A maradékot jelölje r_1. A 2.3. Következmény alapján $\langle a, b\rangle = \langle b, r_1\rangle$.

Ezután b-t osztjuk maradékosan a maradékkal, az újabb maradék legyen r_2: $\langle b, r_1\rangle = \langle r_1, r_2\rangle$. Most az első maradékot osszuk maradékosan a másodikkal és így tovább, mindig az utolsó előtti osztás során kapott maradékot az utolsó maradékkal:

$$\begin{aligned} a &= bq_1 + r_1, && \text{ahol} && 0 \leq r_1 < |b| \\ b &= r_1q_2 + r_2, && \text{ahol} && 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, && \text{ahol} && 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Mivel a maradékok nemnegatív egész számok szigorúan monoton csökkenő sorozatát alkotják: $r_1 > r_2 > r_3 > \ldots > r_k > r_{k+1} > \ldots \geq 0$, előbb-utóbb 0 maradékot kapunk. Legyen az első 0 maradék az $(n+1)$-edik:

$$r_{n-2} = r_{n-1}q_n + r_n, \qquad \text{ahol} \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + \underbrace{r_{n+1}}_{0}.$$

Megmutatjuk, hogy az utolsó nem 0 maradék, vagyis $\delta = r_n$ lesz a és b kitüntetett közös osztója.

1. Az algoritmus utolsó sorából következik, hogy $r_n \mid r_{n-1}$. Ekkor azonban az utolsó előtti egyenlőség jobb oldalának is osztója, így osztója a bal oldalnak, vagyis r_{n-2}-nek is. Sorról-sora „felfelé” haladva az algoritmuson egy hason gondolatmenetet követve azt kapjuk, hogy az összes korábbi maradéknak, így a második lépésben felírt $b = r_1q_1 + r_2$ miatt b-nek, majd az első osztásban szereplő $a = bq_1 + r_1$ miatt a-nak is osztója. Tehát közös osztó.

2. Tegyük most fel, hogy c osztója a-nak és b-nek is: $c \mid a$ és $c \mid b$. Ekkor az algoritmus első sorából $c \mid r_1$, majd ennek felhasználásával a második sorból $c \mid r_2$ és így tovább, ezúttal „lefelé” haladva az algoritmuson azt kapjuk, hogy c az összes maradéknak, így r_n-nek is osztója: $c \mid r_n$. Vagyis $\delta = r_n$ többszöröse az összes közös osztónak.

3. $\delta = r_n$ az algoritmus utolsó előtti sorában szereplő maradék, így nem lehet negatív. Mivel r_{n+1} volt az első 0 maradék, 0 sem lehet, vagyis pozitív.

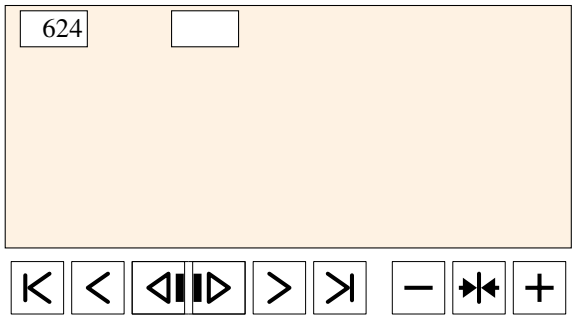
Azt pedig már láttuk, hogy a kitüntetett közös osztó egyértelmű (4.1. Megjegyzés második állítása):

Ha δ_1 és δ_2 egyaránt kitüntetett közös osztó, akkor kölcsönösen többszörösei egymásnak: $\delta_1 \mid \delta_2$, $\delta_2 \mid \delta_1$. Emiatt $|\delta_1| \leq |\delta_2|$ és $|\delta_2| \leq |\delta_1|$. Mivel pedig nemnegatívak, ez csak úgy lehet, ha $\delta_1 = \delta_2$. □

Az euklideszi algoritmust szemlélteti a 4.1. ábrán látható animáció.

http://www.cs.elte.hu/~kfried/algebra1/GCD.jar Ez a program az euklideszi algoritmus segítségével kiszámolja két szám legnagyobb közös osztóját.

Megjegyzés. Miután láttuk, hogy tetszőleges két szám (nem mindkettő 0) legnagyobb, illetve kitüntetett közös osztója megegyezik, a továbbiakban ha egész számokról van szó, a – szokásosabb – legnagyobb közös osztó elnevezést használhatjuk mindkettőre, és a kitüntetett közös osztót is (a, b)-vel fogjuk jelölni. (Ráadásul elfogadjuk, hogy $(0, 0)$ – ami egyébként nem létezik – is 0.) A kitüntetett közös osztó egyébként általában nem jelenti ugyanazt, mint a legnagyobb közös osztó. Különleges jelentősége van: a definíciója



4.1. ábra. (animáció).

csak az oszthatóság fogalmát használja fel, így olyankor is értelmes lehet (a 3. kikötés nélkül) – például (a többváltozós) polinomok körében –, amikor a legnagyobb közös osztó definíciójában szereplő kisebb, illetve nagyobb reláció nincs értelmezve.

4.2. Megjegyzés. Az euklideszi algoritmus – mint láttuk – arra is alkalmas, hogy segítségével megtaláljuk két szám kitüntetett közös osztóját. (A bizonyítás során nemcsak belátjuk, hogy létezik az adott szám, hanem megkonstruáljuk azt. Az ilyen típusú bizonyítást *konstruktív bizonyításnak* nevezzük.)

Például: $(150, 66) =?$

$$\begin{aligned} 150 &= 66 \cdot 2 + 18 \\ 66 &= 18 \cdot 3 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Az utolsó nem 0 maradék a 6, tehát $(150, 66) = 6$. Ennél több is igaz. A maradékok rendre kifejezhetők a kiinduló két számból:

$150-66\cdot 2 = 18$, ebből $66-(150-66\cdot 2)\cdot 3 = 12$, azaz $(-3)\cdot 150+7\cdot 66 = 12$. $18-12\cdot 1 = 6$, ebből $150-66\cdot 2-[(-3)\cdot 150+7\cdot 66]\cdot 1 = 4\cdot 150-9\cdot 66 = 6$.

Ennek a későbbiekben is hasznát vesszük.

4.2. Következmény. *Tetszőleges a, b egész számokhoz léteznek olyan x és y egész számok, amelyekre $(a, b) = ax+by$. (Két szám legnagyobb közös osztója felírható a két szám* lineáris kombinációjaként*.)*

http://www.cs.elte.hu/~kfried/algebra1/Equation.jar Ez a program megadja az $ax + by = (a, b)$ egyenlet egy megoldását.

Bizonyítás. A bizonyításhoz az euklideszi algoritmus lépéseit használjuk. Valójában azt fogjuk megmutatni (induktív módon, vagyis lépésről lépésre), hogy az (a, b) meghatározásának algoritmusában az *összes maradék* (így r_n is) előállítható a és b lineáris kombinációjaként.

Az algoritmus első egyenletének átrendezéséből: $r_1 = a - bq_1 = a \cdot 1 + b \cdot (-q_1)$. Vagyis $x_1 = 1$, $y_2 = -q_1$ választással r_1 előáll a kívánt alakban.

A második egyenletből: $r_2 = b - r_1 q_2$. Írjuk be r_1, helyébe az első egyenletből kifejezett alakját: $r_2 = b - (a - bq_1)q_2 = a \cdot (-q_2) + b \cdot (1 + q_1 q_2)$. Vagyis $x_2 = -q_2$, $y_2 = 1 + q_1 q_2$ választással r_2 is előáll a kívánt alakban.

Megmutatjuk, hogy ha a $(k-2)$-edik és a $(k-1)$-edik maradék előáll a és b lineáris kombinációjaként, akkor a k-adik is.

Legyen $r_{k-2} = ax_{k-2} + by_{k-2}$ és $r_{k-1} = ax_{k-1} + by_{k-1}$. Az algoritmus k-adik egyenletéből: $r_k = r_{k-2} - r_{k-1}q_k = (ax_{k-2} + by_{k-2}) - (ax_{k-1} + by_{k-1})q_k = a(x_{k-2} - x_{k-1}q_k) + b(y_{k-2} - y_{k-1}q_k)$. Az $x_k = (x_{k-2} - x_{k-1}q_k)$ és $y_k = (y_{k-2} - y_{k-1}q_k)$ választással $r_k = ax_k + by_k$.

Vagyis az első két maradék előállítható a kívánt alakban, és ha két egymást követő maradék előállítható, akkor a következő is, tehát az összes maradék (így $r_n = (a, b)$ is) felírható a és b lineáris kombinációjaként. □

Megjegyzés. Az alkalmazott indukció során csak véges sok lépést hajtottunk végre, így csak véges sok elemre örökítjük a tulajdonságot. Ezért nem beszélhetünk teljes indukcióról.

Az algoritmus alapján bizonyíthatjuk a következő egyszerű, a legnagyobb (kitüntetett) közös osztóra vonatkozó tételt is:

4.2. Tétel. *Tetszőleges c pozitív egész szám esetén* $(ac, bc) = (a, b)c$.

Bizonyítás. Azt már tudjuk, hogy $(a, b) = r_n$, ahol r_n az a és b euklideszi algoritmusában az utolsó nem 0 maradék. Írjuk fel ac és bc euklideszi algoritmusát:

$$\begin{aligned}
ac &= bcq_1 + r_1 c, && \text{ahol} \quad 0 \le r_1 c < |b| \\
bc &= r_1 q_2 c + r_2 c, && \text{ahol} \quad 0 \le r_2 c < r_1 c \\
&\vdots \\
r_{n-2}c &= r_{n-1}q_n c + r_n c, && \text{ahol} \quad 0 \le r_n c < r_{n-1} c \\
r_{n-1}c &= r_n q_{n+1} c + \underbrace{\overbrace{r_{n+1}}^{0} c}_{0}.
\end{aligned}$$

Látható, hogy ugyanazt kaptuk, mint ha a és b euklideszi algoritusának minden egyenlőségét megszoroztuk volna c-vel, így az utolsó nem 0 maradék most $r_n c = (a,b)c$. □

4.3. Megjegyzés. A tételt $c \neq 0$ esetére másképp is igazolhatjuk, többféleképpen is.

1. Bebizonyítjuk, hogy $c\langle a,b\rangle \mid \langle ca,cb\rangle$ és $\langle ca,cb\rangle \mid c\langle a,b\rangle$. (Ebből már következik, hogy ez a két pozitív szám egyenlő.)

Vezessük be a következő jelöléseket: $\langle a,b\rangle = d$, illetve $\langle ac,bc\rangle = t$. Azt akarjuk bebizonyítani, hogy $cd \mid t$ és $t \mid cd$.

Egyrészt $d \mid a$ és $d \mid b$, tehát $cd \mid ca$ és $cd \mid cb$, amiből $cd \mid t$.

Az is világos, hogy $c \mid t$, hiszen $c \mid ac$ és $c \mid bc$ miatt t többszöröse a c-nek. Legyen ekkor $t = c \cdot t_1$. Mivel $(t =)ct_1 \mid ca$ és $ct_1 \mid cb$, így a 2.1. Következmény alapján $t_1 \mid a$, $t_1 \mid b$, tehát $t_1 \mid d$. Emiatt pedig $(t =)ct_1 \mid cd$.

Arra jutottunk, hogy $cd \mid t$ és $t \mid cd$, de ez csak úgy lehet, ha $cd = t$. (Ne felejtsük el, hogy c pozitív, d és t nemnegatív.)

2. Egyrészt $(a;b)c$ többszöröse ac-nek és bc-nek is, így $(ac;bc)$-nek is. Másrészt viszont tudjuk, hogy létezik olyan α, β egész szám, amelyre $(ac;bc) = \alpha ac + \beta bc = (\alpha a + \beta b)c$. Mivel itt $\alpha a + \beta b$ osztható $(a;b)$-vel, így $(ac;bc)$ osztható $(a;b)c$-vel. Eszerint $(ac;bc)$ és $(a;b)c$ egymás asszociáltjai, illetve $c > 0$ esetén egyenlők.

4.3. Következmény. *Az eredeti állításnál többet is mondhatunk.*

1. Ha c tetszőleges egész szám, akkor $(ac,bc) = |c|(a,b)$.

2. Ha c tetszőleges olyan racionális szám, amelyre ca és cb is egész szám, teljesül, hogy $(ac,bc) = |c|(a,b)$.

Bizonyítás. 1. Az állítás $c = 0$-ra világos, negatív c-re a megjegyzésben látott gondolatmenetet követve $t = d|c|$ bizonyítható.

2. Ez az 1. állításból a következőképpen vezethető le. Legyen $c = \frac{r}{s}$. Ekkor $\frac{ra}{s}$, $\frac{rb}{s}$ egész számok, és

$$|s| \cdot \left(\frac{ra}{s}, \frac{rb}{s}\right) = (ra,rb) = |r|(a,b),$$

amiből $\frac{|r|}{|s|}(a,b) = \left(\frac{ra}{s}, \frac{rb}{s}\right)$. Ez viszont éppen azt jelenti, hogy $|c|(a,b) = (ca,cb)$ is fennáll. □

Ezen összefüggések felhasználásával az euklideszi algoritmus további érdekes következményei vezethetők le.

4.4. Következmény.

1. Ha $(a, b) = 1$ *és* $a \mid bc$*, akkor* $a \mid c$*.*

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

Bizonyítás. $(a, b) = 1$-ből következik, hogy $(ac, bc) = |c|$. Ezt használjuk mindkét állítás bizonyításához.

1. Ha most $a \mid bc$, akkor az a osztója ac-nek és bc-nek is, így osztója a kitüntetett közös osztójuknak, $|c|$-nek is: $a \mid |c|$, vagy (ami ezzel ekvivalens) $a \mid c$.

2. Tudjuk, hogy $|c| = (ac, bc)$, viszont $a \mid c$ miatt $c = ac_a$, és $b \mid c$ miatt $c = bc_b$. Ezekkel a kifejezésekkel is írjuk fel (ac, bc)-t: $(abc_b, abc_a) = |ab|(c_b, c_a)$. Ebből következik, hogy $|ab| \mid |c|$, vagy (ami ezzel ekvivalens) $ab \mid c$. □

4.4. Definíció. Az a és b számok *legkisebb közös többszöröse* a t pozitív egész szám, ha

1. $a \mid t$ és $b \mid t$ (vagyis t közös többszörösük), és

2. ha $a \mid k$ és $b \mid k$, akkor $t \leq k$ (vagyis t a legkisebb).

4.2. Jelölés. $t = [a, b]$ vagy $t = \mathrm{lkkt}(a, b)$.

Megjegyzés. A 0-nak semmilyen számmal sincs legkisebb közös többszöröse, hiszen egyetlen pozitív egész szám sem többszöröse a 0-nak. Ha azonban a és b egyike sem 0, akkor biztosan vannak pozitív egész közös többszöröseik – például $|ab|$, $2|ab|$ stb. –, és mivel pozitív egész számok tetszőleges halmazának van legkisebb eleme, a közös többszörösök között van legkisebb, és ez egyértelmű.

4.5. Definíció. Az a és b számok *kitüntetett közös többszöröse* a τ pozitív egész szám, ha

1. $a \mid \tau$ és $b \mid \tau$ (vagyis közös többszörös), és

2. ha $a \mid k$ és $b \mid k$, akkor $\tau \mid k$ (minden közös többszörösnek osztója).

Megjegyzés. Most is igaz, hogy a 0-nak egyetlen többszöröse van, a 0, ezért a 0-nak semmilyen más számmal sincsen kitüntetett közös többszöröse.

Megjegyzés. Könnyen meggondolható, hogy ha két számnak létezik legkisebb közös többszöröse, akkor az megegyezik a kitüntetett közös többszörösükkel. ($t \leq \tau$, $\tau \mid t$ miatt.)

Megjegyzés. Az is egyszerűen bizonyítható, hogy ha létezik a-nak és b-nek legkisebb közös többszöröse, akkor az egyértelmű. ($t_1 \leq t_2$, $t_2 \leq t_1$ miatt.)

Sőt, ha létezik a-nak és b-nek kitüntetett közös többszöröse, akkor az is egyértelmű. ($\tau_1 \mid \tau_2$, $\tau_2 \mid \tau_1$, valamint $\tau_1, \tau_2 > 0$ miatt.)

4.3. Tétel. *Tetszőleges a és b nem 0 egész számoknak létezik egyértelműen meghatározott kitüntetett közös többszöröse.*

Bizonyítás. A bizonyítás során azt fogjuk megmutatni, hogy a $\tau = \dfrac{|ab|}{(a,b)}$ (nyilvánvalóan pozitív) szám kielégíti a kitüntetett közös többszörössel szemben támasztott követelményeket.

1. A fenti τ többszöröse az a-nak és a b-nek, mert $\tau = |a|\dfrac{|b|}{(a,b)} = |b|\dfrac{|a|}{(a,b)}$, ahol $\dfrac{|b|}{(a,b)}$, illetve $\dfrac{|a|}{(a,b)}$ nyilván egész számok, hiszen (a,b) osztója a-nak is és b-nek is.

2. a és b minden többszörösének osztója a τ: tegyük fel, hogy $a \mid k$ és $b \mid k$ ($k \neq 0$). Ekkor $\dfrac{k}{a}$ és $\dfrac{k}{b}$ egész számok, így létezik legnagyobb közös osztójuk, és nyilván az is egész szám: $\left(\dfrac{k}{a}, \dfrac{k}{b}\right) = \left(\dfrac{kb}{ab}, \dfrac{ka}{ab}\right) = \dfrac{|k|}{|ab|}(a,b) = \dfrac{|k|}{\tau}$.

Mivel $\dfrac{|k|}{\tau}$ megegyezik két egész szám legnagyobb közös osztójával, nyilván maga is egész szám. Ez csak úgy lehet, ha $\tau \mid k$. (Az átalakítások során felhasználtuk a 4.2. Tételt, illetve annak 4.3. Következményét.)

Hátravan még az egyértelműség bizonyítása (ahogyan ezt korábban láttuk):

Tegyük fel, hogy τ_1, is és τ_2 is kitüntetett közös többszörös. Ekkor kölcsönösen osztói egymásnak, ami – mivel pozitívak – csak úgy lehet, ha egyenlőek (a 2.1. Tétel miatt). □

Megjegyzés. Más módon is bizonyíthatjuk az állítást. Legyen $(a,b) = d$. Ekkor $a = a_1 d$ valamilyen a_1-re, illetve $b = b_1 d$ valamilyen b_1-re, továbbá $(a_1, b_1) = 1$. Az előző bizonyításban használt τ a jelölésünkkel $|a_1 b_1|d$, mert $(a,b) \cdot |a_1 b_1|d = d^2|a_1||b_1| = |a_1|d \cdot |b_1|d = |a||b| = |ab|$.

Legyen most k valamely többszöröse a-nak és b-nek. Ekkor – mivel d osztója például a-nak – d osztója k-nak is: $k = k_1 d$. Így $a_1 d \mid k_1 d$, $b_1 d \mid k_1 d$. A 2.1. Következmény miatt ekkor $a_1 \mid k_1$ és $b_1 \mid k_1$. Mivel azonban $(a_1, b_1) = 1$, a 4.4. Következmény 2. állításából következik, hogy $a_1 b_1 \mid k_1$, így $a_1 d_1 b \mid k_1 d$, azaz $\tau \mid k$.

Megjegyzés. Az egyértelműség bizonyításakor nem elég arra hivatkozni, hogy a $\tau = \dfrac{|ab|}{(a,b)}$ szám egyértelműen meghatározott, hiszen csak azt mutattuk meg, hogy ez a szám megfelel kitüntetett közös többszörösnek, azt nem, hogy más szám nem felel meg.

Megjegyzés. A legnagyobb közös osztónál látottakhoz hasonlóan megállapíthatjuk, hogy két egész szám legkisebb közös többszöröse mindig megegyezik a két szám kitüntetett közös többszörösével, így a továbbiakban mindkettőt jelölhetjük $[a, b]$-vel.

Gyakran szükségünk lesz a következő elnevezésekre:

4.6. Definíció. Az a, b számokat *relatív prímeknek* nevezzük, ha $(a, b) = 1$.

Az a_1, a_2, …, a_k számokat *relatív prímeknek* nevezzük, ha $(a_1, a_2, \ldots, a_k) = 1$.

4.7. Definíció. Az a_1, a_2, …, a_k számokat *páronként relatív prímeknek* nevezzük, ha $\forall i, j$-re, ahol $i \neq j$ esetén $(a_i, a_j) = 1$.

Megjegyzés. Abból, hogy a_1, a_2, …, a_n páronként relatív prímek, következik, hogy együtt is relatív prímek (hiszen semelyik kettőnek sincs 1-nél nagyobb közös osztója), de fordítva nem. Lehet, hogy három szám közül bármely kettőnek van 1-nél nagyobb közös osztója, de ez a harmadiknak nem osztója. A 6, 10, 15 számok például együtt relatív prímek, hiszen $(6, 10, 15) = 1$, de közülük semelyik kettő sem relatív prím egymáshoz: $(6, 10) = 2$, $(6, 15) = 3$, $(10, 15) = 5$.

Idézzük fel a 4.4. Következmény relatív prímekkel kapcsolatos állításait!

1. Ha $(a, b) = 1$ mellett $a \mid bc$, akkor $a \mid c$;

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

A 2.6. Tételt követően megjegyeztük, hogy abból, hogy a oszt egy szorzatot, általában nem következik, hogy akár egyik tényezőjét is osztja. Most már tudjuk, hogy ha viszont a szorzat egyik tényezőjéhez relatív prím, akkor biztos, hogy osztója a másiknak.

Megjegyzés. Az oszthatósági szabályok kapcsán többször megemlítettük, hogy általában abból, hogy a is és b is oszt egy számot, nem következik, hogy ab is osztja az illető számot. Most már azonban tudjuk, hogy ha a és b relatív prímek egymáshoz, akkor igen, így oszthatósági szabályainkat kiegészíthetjük például a következőkkel:

Ha egy szám osztható 2-vel is és 3-mal is, akkor 6-tal is.

Ha egy szám osztható 4-gyel is és 3-mal is, akkor 12-vel is.

Általában: Ha egy szám osztható a-val is és b-vel is, akkor osztható a és b legkisebb közös többszörösével is, így ha $(a, b) = 1$, akkor ab-vel is.

Ha viszont a és b nem relatív prímek, akkor tudunk olyan számot mondani – nevezetesen például a legkisebb közös többszörösüket –, amely osztható a-val és b-vel, de nem osztható ab-vel. $[6, 10] = 30$ osztható 6-tal és 10-zel is, de nem osztható 60-nal.

Alkalmazások

Az eddigiekben látottakat rendszeresen alkalmazzuk már az általános iskolában is.

Ötödik-hatodik osztályban megismerkedünk a törtekkel és a rajtuk elvégezhető műveletekkel.

Végső soron a racionális számok összeadásra és szorzásra vett *testét* tanuljuk. (A test olyan algebrai strukúra, amelyen értelmezve van egy összeadás, amely asszociatív és invertálható, sőt, kommutatív, valamint egy szorzás, amely asszociatív – esetünkben még kommutatív is – és a 0-tól eltekintve invertálható, továbbá a szorzás disztributív az összeadásra nézve. Minderről később bővebben lesz szó.)

Törtek összeadásához közös nevezőre hoztuk a törteket, amihez rendszerint a nevezők *legkisebb közös többszörösét* kerestük. Törtek egyszerűsítésekor pedig szokás a számláló és a nevező *legnagyobb közös osztóját* meghatározni.

A vegyes törtek felírásához pedig „leválasztjuk” egy (pozitív) törtről az egészrészt. Mindeközben megállapítjuk, hogy a nevező hányszor van meg a számlálóban (ez lesz az egészrész), míg a maradék a keletkező vegyes tört számlálója.

Vegyük észre, hogy mindeközben *maradékos osztást* végzünk.

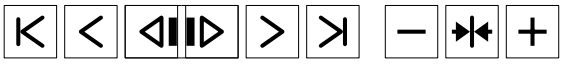
A $\frac{126}{24}$ tört esetén $126 = 5 \cdot 24 + 6$, vagyis $\frac{126}{24} = 5\frac{6}{24} = 5\frac{1}{4}$.

A $\frac{124}{28}$ esetében pedig $124 = 4 \cdot 28 + 12$, vagyis $\frac{126}{28} = 4\frac{3}{7}$. A $\frac{3}{7}$ nem írható vegyes tört alakba (csak triviális módon, ha 0 az egész rész), de a reciproka felírható. Ismét maradékos osztást végzünk: $\frac{7}{3} = 2\frac{1}{3}$, így felírhatjuk, hogy $\frac{124}{28} = 4 + \frac{1}{2\frac{1}{3}}$.

Ha a kapott tört számlálója (egyszerűsítés után) nem lett volna 1, folytathatnánk a maradékos osztások sorozatát. A maradékos osztások sorozatát folytatva egy adott tört lánctört alakját kapjuk.

A racionális számok lánctört-előállítása egyértelmű. Egy konkrét lánctörtelőállítást mutat a 4.2. ábrán látható animáció.

$\frac{17}{40}$



4.2. ábra. (animáció).

A valós számokat racionális számokkal szoktuk közelíteni. Ilyenkor az s valós számot – például – alkalmas tizedestörtekkel közelítjük több lépésben. Például a $\sqrt{2}$-t:

$$\begin{gathered} 1 < \sqrt{2} < 2 \\ 1{,}4 < \sqrt{2} < 1{,}4 \\ 1{,}41 < \sqrt{2} < 1{,}42 \\ 1{,}414 < \sqrt{2} < 1{,}415 \\ \vdots \end{gathered}$$

Meglepő módon a valós számokat az imént felírt tizedestörtekkel történő közelítésnél (bizonyos értelemben) pontosabban lehet lánctörtekkel közelíteni. Ennek részleteibe most nem megyünk bele (lásd [5]). Például a π két (lánc)tört közelítése: $\frac{22}{7} = 3 + \frac{1}{7}$ és $\frac{355}{113} = 3 + \frac{16}{113} = 3 + \frac{1}{7 + \frac{1}{16}}$. (Ez utóbbi közelítés tizedestört alakja például 6 tizedesjegye pontos eredményt ad π értékére.)

Egy olyan lánctörtet, amelyben minden számláló 1 (úgynevezett reguláris lánctört), meghatározzák a nevezőkben álló egész rész számok

(valamint az első egész rész). Ezért szokás egyszerűen ezekkel megadni egy lánctörtet. Ezzel a felírással a π-t például így adhatjuk meg: $[3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, \ldots]$

http://www.cs.elte.hu/~kfried/algebra1/Simplify.jar Ez a program törtegyszerűsítést végez.

http://www.cs.elte.hu/~kfried/algebra1/Continued.jar Ez a program felírja egy racionális szám lánctört fentiekben tárgyalt alakját.

Feladatok

1. Határozza meg a következő számpárok legnagyobb közös osztóját euklideszi algoritmussal!

   $(112, 42)$, $(150, 54)$, $(2000, 168)$

2. Igazolja, hogy a legnagyobb közös osztó – mint kétváltozós művelet – asszociatív, vagyis $(a, (b, c)) = ((a, b), c)$!

3. Igazolja, hogy ha $(a, b) = 1$, akkor $(a, b^2) = 1$!

4. Igazolja, hogy $(a, b)^2 = (a^2, b^2)$!

5. Mivel lehet egyenlő $(11a + 5b, 29a + 13b)$?

6. Láttuk, hogy hogy tetszőleges $a, b \in \mathbb{Z} \setminus \{0\}$ esetén $[a, b] = \dfrac{ab}{(a, b)}$. (4.3. Tétel) Igazolja, hogy tetszőleges $a, b, c \in \mathbb{Z} \setminus \{0\}$ esetén

   $$[a, b, c] = \frac{abc \cdot (a, b, c)}{(a, b) \cdot (a, c) \cdot (b, c)}!$$

7. Igazolja, hogy tetszőleges $a, b \in \mathbb{Z}$ esetén $(a + b, [a, b]) = (a, b)$!

8. Keressen olyan x, y egész számokat, amelyekre $(x, y) = 5$, $[x, y] = 20$! Keresse meg az összes lehetséges megoldást!

9. Mivel lehet egyenlő $(a + b, a^2 + ab + b^2)$, ha $(a, b) = 1$?

   Ennek felhasználásával határozza meg $(a^2 - b^2, a^3 - b^3)$ értékét (továbbra is $(a, b) = 1$)!

10. Egyszerűsítse a $\dfrac{112}{42}$, $\dfrac{150}{54}$, $\dfrac{2000}{168}$ törteket! Használja fel az első feladatban felírt euklideszi algoritmust!

11. Írja fel a $\frac{112}{42}$, $\frac{150}{54}$, $\frac{2000}{168}$ törtek lánctört alakját! Használja fel az első feladatban felírt euklideszi algoritmust!

    Írja fel, hogy általában az a és b számokon elvégzett euklideszi algoritmusból hogyan kapja meg az $\frac{a}{b}$ tört lánctört alakját!

12. Határozza meg a 45 és a 120 legkisebb közös többszörösét!

    Keressen olyan u és v számokat, amelyekre $45u + 120v = (45, 120)$!

    Keressen olyan x és y számokat, amelyekre $45x + 120y = [45, 120]$!

    Igazolja, hogy $a, b > 1$ $((a, b) = 1)$ esetén van olyan pozitív szám, amely nem áll elő pozitív x, y szorzókkal $ax + by$ alakban!

5. fejezet

Felbonthatatlan szám, prímszám

Azt már tudjuk, hogy tetszőleges egész számnak osztója az 1, a -1, továbbá maga a szám, valamint az ellentettje. Azt is tudjuk azonban, hogy a 0-nak végtelen sok, az egységeknek (1 és -1) pedig pontosan két osztójuk van. Vannak azonban olyan számok, amelyeknek az egységeken és saját asszociáltjain kívül nincs is más osztójuk:

5.1. Definíció. A q (0-tól és egységektől különböző) egész szám *felbonthatatlan,* ha valahányszor $q = ab$ valamely a, b halmazbeli elemekre, akkor ebből következik, hogy $a = \varepsilon$ vagy $b = \varepsilon$ (ε egység).

Egyszerűbben megfogalmazva: ha egy számnak csak olyan szorzatalakja van, amelyben valamelyik tényező egység, akkor az a szám felbonthatatlan. Teljesül ez a tulajdonság tehát akkor is, ha egy számnak nincsen szorzatalakja.

A felbonthatatlan számokat szokás *irreducíbilisnek* is nevezni. Azokat a 0-tól és egységektől különböző számokat, amelyek nem felbonthatatlanok, *összetett* vagy *reducíbilis* számoknak nevezzük.

Felbonthatatlan szám például a 2, a -2, a 3, a -3, az 5, a -5, a 7, a -7 stb. Összetett szám a $4 = 2 \cdot 2$, a $6 = 2 \cdot 3$, a $8 = 2 \cdot 4$ stb. A 0-t és az egységeket nem soroljuk sem a felbonthatatlan, sem az összetett számok közé.

Megjegyzés. A definíció szerint egy 0-tól és egységektől különböző szám akkor felbonthatatlan, ha minden szorzat alakjában van egység tényező.

Az egész számok körében ez azt jelenti, hogy akkor felbonthatatlan egy 0-tól és egységektől különböző szám, ha nincsen valódi osztója. Ahhoz tehát, hogy eldöntsük, hogy egy egész szám felbonthatatlan-e, elegendő azt megnézni, hogy a nála kisebb abszolút értékű számok közül melyek osztói a számnak. Ha van valódi osztója, akkor összetett; ha nincs, akkor felbonthatatlan a szám.

Megjegyzés. A felbonthatatlan szám vagy elem fogalma nemcsak az egész számok körében értelmezhető. Olyan halmazon, amelyen értelmes az oszthatóságot definiálni, van értelme felbonthatatlan elemről is beszélni. Persze nem mindenütt jutunk el ugyanolyan messzemenő következtetésekre, mint amilyeneket az egész számok körében már korábban is megismertünk, illetve rövidesen látni fogunk.

A páros számok halmazán belül például felbonthatatlan szám a 2, a 6 a 10 stb. (minden szorzat alakjukban van egység tényező, ugyanis *nincsen szorzat alakjuk*), viszont összetett szám a $4 = 2 \cdot 2$, a $8 = 2 \cdot 4$, a $12 = 2 \cdot 6$ stb. A páros egész számok körében a $4k+2$ alakú számok felbonthatatlanok.

5.2. Definíció. A p (0-tól és egységektől különböző) szám *prímszám,* ha abból, hogy $p \mid ab$ következik, hogy $p \mid a$ vagy $p \mid b$.

Például: A 4 nem prímszám, mert osztója például a $6 \cdot 10 = 60$-nak, de sem a 6-nak, sem a 10-nek nem osztója.

A 6 sem prímszám, mert osztója a $3 \cdot 8 = 24$-nek, de sem a 3-nak, sem a 8-nak nem osztója.

Megjegyzés. A fentiek kicsit ismerősen csenghetnek, de mégsem teljesen! Korábbi tanulmányaink során ugyanis – tévesen – a prímszám fogalmához a felbonthatatlanság tulajdonsága kapcsolódott. Bár az egész számok körében ugyanazok a prímek, mint a felbonthatatlanok (5.1. és 5.2. Tételek), ez azonban nincs így minden számkörben.

5.1. Következmény. *A prímszám definíciójából következik, hogy ha egy prímszám oszt egy (akárhány, de véges sok tényezős) szorzatot, akkor osztja legalább az egyik tényezőjét.*

Bizonyítás. A tényezők számára vonatkozó indukcióval bizonyítjuk az állítást. (Vigyázzunk, nem teljes indukció, mert csak véges sok tényező van. Ráadásul az egytényezős szorzatot nem definiáltuk, vagyis az indukció 2-től indul.)

A kéttényezős szorzatra a definíció szerint teljesül az állítás.

Legyen most a tényezők száma $k(\geq 3)$, és tegyük fel azt, hogy amennyiben egy p prímszám osztója egy $(k-1)$ tényezős szorzatnak, akkor valamelyik tényezőnek osztója.

Legyen p osztója egy k tényezős szorzatnak: $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_k$. Ekkor $p \mid a_1 \cdot (a_2 \cdot \ldots \cdot a_k)$, amiből a prímszám definíciója alapján következik, hogy $p \mid a_1$ vagy $p \mid a_2 \cdot \ldots \cdot a_k$.

Azaz p osztója vagy az a_1-nek, vagy egy $(k-1)$ tényezős szorzatnak. Az utóbbi esetben viszont az indukciós feltevés szerint ekkor osztója a $(k-1)$ tényezős szorzat valamelyik tényezőjének.

Végső soron azt kapjuk, hogy $p \mid a_1$, vagy $p \mid a_2$, vagy $p \mid a_3$, ..., vagy $p \mid a_k$. Vagyis p osztója legalább az egyik tényezőnek. □

Megjegyzés. Prímszámra a definíció alapján nem könnyű példát mondani, ugyanis azt, hogy egy szám prím vagy sem, már nem tudjuk véges sok számpár oszthatósági viszonyainak ellenőrzésével eldönteni. Ahhoz, hogy a definíció alapján például az 5-ről bebizonyítsuk, hogy prím, arra volna szükség, hogy az összes olyan szorzatról, amelynek osztója az 5 megmutassuk, hogy legalább az egyik tényezőjüknek is osztója. (Vagyis 5 minden többszörösének minden szorzattá bontásáról be kellene látnunk, hogy valamelyik tényezője is osztható 5-tel.)

Ehelyett be fogjuk bizonyítani, hogy minden prímszám felbonthatatlan is, amiből már következik, hogy a 2, 3, 5 stb. nemcsak felbonthatatlanok, hanem prímszámok is. Sőt, azt is bebizonyítjuk, hogy az egész számok körében pontosan a felbonthatatlan számok a prímszámok.

5.1. Tétel. *Minden prímszám felbonthatatlan is.*

Bizonyítás. Legyen p prímszám, amely felírható $p = ab$ alakban. Azt fogjuk belátni, hogy ekkor a szorzat valamelyik tényezője egység.

Ha $p = ab$, akkor $p \mid ab$, és mivel p prímszám, osztója a szorzat valamelyik tényezőjének, például a-nak. $ab \mid a$-ból, azaz $a \cdot b \mid a \cdot 1$-ből, viszont ($p \neq 0$, így $a \neq 0$ miatt) a 2.1. Következmény szerint $b \mid 1$, azaz b egység.

Ha p a b-t osztaná, akkor hasonlóan kapnánk, hogy a egység. □

Megjegyzés. A bizonyítás során a definíciókon kívül csupán azt használtuk fel, hogy egy szorzat csak úgy lehet 0 (és akkor valóban 0 is), ha valamelyik tényezője 0.

Megjegyzés. Az egész számok körében az osztók nagyságrendi relációját felhasználva is bebizonyítható az előző tétel: ha $p = ab$, akkor $p \mid ab$, így

ha például $ab \mid a$, akkor (mivel a osztói $-|a|$ és $|a|$ közé esnek) ebből az következik, hogy $|b| \leq 1$. Persze 0 nem lehet, ezért b egység.

Az egész számok körében azonban nemcsak az igaz, hogy a prím számok felbonthatatlanok, hanem az is, hogy a felbonthatatlan számok prímek:

5.2. Tétel. *Ha a q egész szám felbonthatatlan, akkor prímszám is.*

Bizonyítás. Tegyük fel, hogy q felbonthatatlan szám, és osztója egy ab szorzatnak. Belátjuk, hogy ekkor $q \mid a$ vagy $q \mid b$.

Mivel q felbonthatatlan, így (q, a) vagy egység, vagy q asszociáltja. Mégpedig pontosan akkor asszociáltja q-nak, ha $q \mid a$; ekkor pedig készen vagyunk.

Ha viszont (q, a) egység, tehát $q \nmid a$, akkor a 4.4. Következmény 1. állítása miatt $q \mid b$. □

A bizonyítás lényege a 4.4. Következmény 1. állítása, amelyhez (így a tétel bizonyításához) felhasználtuk az euklideszi algoritmust. Ezért egyrészt tetszőleges olyan struktúrában, ahol definiálható az oszthatóság és van maradékos osztás, teljesülni fog, hogy a felbonthatatlanság egybeesik a prímtulajdonsággal, másrészt ahol nincs maradékos osztás, ott így nem tudjuk bebizonyítani, hogy minden felbonthatatlan elem egyben prím is.

Megjegyzés. E két utóbbi tétel (5.2. és 5.1.) azt mondja ki, hogy az egész számok körében pontosan ugyanazok a prímszámok, mint a felbonthatatlanok.

A páros egész számok körében azonban például a 2, 6, 10 stb. felbonthatatlanok, de nem prímek, hiszen a 2 is, a 6 is és a 10 is osztja a $2 \cdot 30$ szorzatot, de sem a 2-nek, sem a 30-nak nem osztója egyik sem. Több is mondható: a páros egész számok körében nincsen prímszám. Minden n-re igaz ugyanis, hogy osztja a $2n$ szorzatot, de sem a 2-nek, sem saját magának nem osztója egyik sem. A felbonthatatlanok tehát nem mindenhol rendelkeznek a prímtulajdonsággal. (Az viszont igaz, hogy ahol egyáltalán vannak prímek, ott azok felbonthatatlanok is.)

A páros egész számok halmazán egységek sincsenek (mert nincs köztük az 1, így annak egyetlen osztója sem), így nincsenek asszociáltak sem.

Összegezve: a páros egész számok körében nincsenek egységek, nincsenek asszociáltak, nincsenek prímek, de vannak felbonthatatlanok, és ezek éppen a 4-gyel nem osztható páros számok.

5.1. Megjegyzés. Az 5.2. Tétel bizonyításában a definíciókon kívül az euklideszi algoritmust (maradékos osztást) is felhasználtuk, ez azonban nem mindenütt végezhető el.

Lássunk egy fontos, de nem túl egyszerű példát arra, hogy van olyan halmaz, ahol vannak egységek, asszociáltak, de nincs euklideszi algoritmus, és nem minden felbonthatatlan szám prímszám.

Tekintsük az $a+bX$ legfeljebb elsőfokú polinomokat az összes a, b egész számra. (Megengedjük, hogy $b=0$ is előfordulhasson.) Ilyen polinomokat össze tudunk adni, ki tudunk vonni egymásból. Az eredmény is ugyanilyen alakú, legfeljebb elsőfokú polinom lesz.

Össze is tudunk szorozni ilyen polinomokat, de a szorzat nem lesz elsőfokú. $(a+bX)\cdot(c+dX)=ac+(ad+bc)X+bdX^2$. Ha azonban az X^2 helyére egy egész számot írunk (persze mindig ugyanazt), akkor már elsőfokú polinomot fogunk kapni. Írjunk mondjuk mindig -5-öt az X^2 helyére. (Ezt úgy is elképzelhetjük, mintha lenne olyan szám, amelynek a négyzete -5.)

Eszerint ezeken a számokon elvégezhető az összeadás, a kivonás, a szorzás – és belátható, hogy ezek tulajdonságai a szokásosak.

Belátható, hogy az $a+bX$ $(a,b\in\mathbb{Z})$ alakú elemekből álló halmazban nem igaz, hogy minden felbonthatatlan szám egyben prímszám is. (Mellesleg itt a prímtulajdonságból a nagyságrendekkel manipuláló bizonyítás szerint nem tudnánk következtetni a felbonthatatlanságra, mert ezek között a számok között nincs nagyságrendi összehasonlítás. Mivel nincsen nagyságrendi összehasonlítás, az euklideszi algoritmus sem végezhető el.)

Pontosan azok az egységek, amelyek osztói az 1-nek. Ha $a+bX$ osztója az 1-nek, akkor a „reciproka” valamilyen c, d egész számokra $c+dX$ alakú. Írjuk fel a reciprokát:

$$\frac{1}{a+bX}=\frac{a-bX}{(a+bX)(a-bX)}=\frac{a-bX}{a^2-X^2b^2}$$

felhasználjuk, hogy $X^2=-5$, vagyis

$$\frac{1}{a+bX}=\frac{a}{a^2+5b^2}+\frac{a-bX}{a^2+5b^2},$$

ahol $\dfrac{a}{a^2+5b^2}$ és $\dfrac{b}{a^2+5b^2}$ is egész számok.

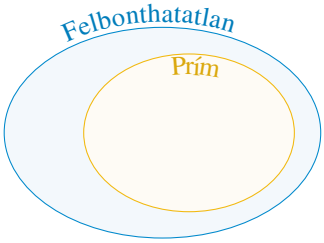
Ez viszont (nagyságrendi okok miatt) csak úgy lehet, ha a $a=\pm1$ és $b=0$. Vagyis a ±1-ről van szó, az egységek tehát ±1.

Ez egyszersmind azt is jelenti, hogy az $a+bX$ asszociáltjai $\pm(a+bX)$.

Belátható, hogy a 2 és a 3 felbonthatatlan, de nem prímszám. Ha például $(a+bX)(c+dX) = 2$, akkor az előzőekhez hasonló gondolatmenettel azt kapjuk, hogy az egyik tényező ± 1, a másik ± 2, ami a 2 asszociáltja.

Másrészt azonban $2 \cdot 3 = 6 = (1+X)(1-X)$ is fennáll, de az eddigiekhez hasonló módon belátható, hogy sem az $1+X$, sem az $1-X$ tényező nem osztható 2-vel.

Vagyis van olyan szorzattá bontása a 6-nak, amelynek tényezőit nem osztja a 2.



5.1. ábra. Minden prím felbonthatatlan, de nem minden felbonthatatlan szám pírm.

Megjegyzés.

Az egészből annyit érdemes megjegyzeni, hogy van olyan számkör, ahol nem esik egybe a felbonthatatlanok és a prímek halmaza. Van olyan felbonthatatlan szám, amely nem prímszám. (5.1. ábra)

Feladatok

1. Lehet-e három egymást követő szám mindegyike prímszám?
2. Lehet-e három egymást követő páratlan szám mindegyike prímszám?
3. Lehet-e két prímszám különbsége 5? Hogyan? Keresse meg az összes lehetőséget!
4. Tekintsük az $H_5 = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ számok halmazát!

   Igazolja, hogy az ilyen alakú elemeknek az összege, a különbsége és a szorzata is ilyen alakú.

   (Mivel ez a számhalmaz a valós számok részhalmaza, érvényesek rájuk a szokásos műveleti azonosságok.)

   Keressen felbonthatatlan számokat H_5-ben!

5. Lehet-e két négyzetszám különbsége 1? Hogyan? Hányféleképpen?
   Lehet-e két négyzetszám különbsége 2; 3; 4?
   Hány lehetőség van az egyes esetekben?

6. Lehet-e prímszám az $\frac{a^3+b^3}{2}$, ha a és b pozitív egész számok?

6. fejezet

A számelmélet alaptétele

A prímszámok, illetve a felbonthatatlan számok igen fontos szerepet játszanak a számelméletben. Egyfajta építőkövei az egész számoknak. Végső soron azt fogjuk bebizonyítani, hogy az 1-nél nagyobb abszolút értékű egész számok felírhatóak felbonthatatlan számok szorzataként. Az első lépésben ehhez bebizonyítjuk, hogy minden nem 0 és nem egység egész számnak van felbonthatatlan osztója. A felbonthatatlan számoknak önmaguk. Az összetett számoknak pedig a következő tétel szerint biztosan van felbonthatatlan osztója.

6.1. Tétel. *Az n összetett szám legkisebb abszolút értékű valódi osztója felbonthatatlan.*

Bizonyítás. Ha n összetett szám, akkor van valódi osztója. Legyen n valódi osztói közül a legkisebb abszolút értékű pozitív az $a(>0)$. (Hiszen ha a, akkor $-a$ is legkisebb abszolút értékű osztó.) Ekkor n előáll $n = aq$ alakban, ahol sem a, sem q nem egység hiszen a valódi osztó.

Belátjuk, hogy a nem lehet összetett szám. Ha a-nak nála kisebb abszolút értékű osztója a $c(>0)$, akkor egyrészt $c < a$, másrészt $c \mid a$, tehát $c \mid n$ (az oszthatóság tranzitivitása miatt). Mivel azonban n-nek a volt a legkisebb abszolút értékű (pozitív) valódi osztója, ez csak úgy lehetséges, hogy c nem valódi osztó, hanem egység. □

Vagyis (a bizonyítás lényege más szavakkal) ha az n legkisebb abszolút értékű valódi osztója nem lenne felbonthatatlan szám, akkor volna a legkisebbnél is kisebb abszolút értékű valódi osztója n-nek, ami lehetetlen. Tehát a felbonthatatlan.

Ha az n összetett számot felírjuk $n = ab$ alakban, ahol sem a, sem b nem egység, akkor vagy azt tapasztaljuk, hogy a is és b is felbonthatatlan,

vagy azt, hogy legalább az egyikük összetett szám. Azt, amelyik összetett szám, szintén valódi osztók szorzatára bonthatjuk. Ha az így kapott szorzat tényezői között van összetett szám, akkor azt tovább bonthatjuk. Például: $60 = 5 \cdot 12 = 5 \cdot \underbrace{3 \cdot 4}_{12} = 5 \cdot 3 \cdot \underbrace{2 \cdot 2}_{4}$.

Ezt az eljárást folytatva végül azt tapasztaljuk, hogy sikerült az n számot csupa felbonthatatlan szám szorzataként felírni, ráadásul a szorzatban szereplő felbonthatatlan számok ugyanazok lesznek akkor is, ha eredetileg az n egy más szorzatalakjából indulunk ki: Például: $60 = 3 \cdot 20 = 3 \cdot \underbrace{5 \cdot 4}_{20} = 3 \cdot 5 \cdot \underbrace{2 \cdot 2}_{4}$.

Ezt az észrevételt fogalmazza meg a következő tétel, amely a számelmélet egyik legfontosabb tétele:

6.2. Tétel. (A számelmélet alaptétele) *Minden* 0*-tól és egységektől különböző* n *egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és asszociáltaktól eltekintve egyértelmű.*

Bizonyítás. Először a felbonthatóságot igazoljuk.

Ha n felbonthatatlan szám, akkor tekintsük egytényezős szorzatnak.

Ha n összetett szám, akkor az előző tétel értelmében van felbonthatatlan osztója. Legyen ez p_1. Ekkor n előáll $n = p_1 n_1$ alakban, ahol (mivel valódi felbontásról van szó) $|n_1| < |n|$. Ha n_1 felbonthatatlan, akkor készen vagyunk. Ha összetett szám, akkor megint csak az előző tétel értelmében van felbonthatatlan osztója, legyen ez p_2. Ekkor n_1 előáll $n_1 = p_2 n_2$ alakban (vagyis $n = p_1 p_2 n_2$), ahol $|n_2| < |n_1|$. Ha n_2 felbonthatatlan szám, akkor készen vagyunk, ha nem, akkor folytathatjuk a felbontást. Mivel $|n| > |n_1| > |n_2| > \ldots (> 1)$ előbb vagy utóbb felbonthatatlan számot kell kapnunk, így ez az eljárás véges sok lépésen belül véget fog érni.

Végül az n szám előáll $n = p_1 p_2 \cdot \ldots \cdot p_k$ szorzat alakban, ahol p_1, p_2, …, p_k felbonthatatlan számok.

Igazolnunk kell még a felbontás egyértelműséget.

Tegyük fel, hogy az n szám kétféleképpen is előáll felbonthatatlanok szorzataként:

$$n = p_1 p_2 \cdot \ldots \cdot p_r \qquad \text{és} \qquad n = q_1 q_2 \cdot \ldots \cdot q_s.$$

Ekkor

$$p_1 p_2 \cdot \ldots \cdot p_r = q_1 q_2 \cdot \ldots \cdot q_s.$$

Ha a bal oldali szorzat tényezői közül valamelyik megegyezik a jobb oldali szorzat valamelyik tényezőjével (vagy annak asszociáltjával), akkor egysze-

rűsítünk vele (a megmaradó egység szorzókat összeszorozva továbbra is egységet, ε-t kapjuk). Az egyszerűsítések és az újraindexelés után azt kapjuk, hogy

$$p_{1'}p_{2'}\cdot\ldots\cdot p_{r'} = \varepsilon q_{1'}q_{2'}\cdot\ldots\cdot q_{s'},$$

ahol $p_{i'}$, $q_{j'}$ felbonthatatlanok, és páronként, semmilyen indexpárra sem asszociáltjai egymásnak.

Ekkor $p_{1'}$ nyilván osztója a $q_{1'}q_{2'}\cdot\ldots\cdot q_{s'}$ szorzatnak. Mivel azonban $p_{1'}$ prímszám (mert felbonthatatlan), abból, hogy oszt egy szorzatot, következik, hogy valamelyik tényezőjét is osztja (lásd a 5.1. Következményt), vagyis van olyan $q_{j'}$, amelyre $p_{1'} \mid q_{j'}$. Ez azonban ellentmondás, hiszen $p_{1'}$ és $q_{j'}$ is felbonthatatlan, és $p_{1'} \neq \varepsilon q_{j'}$ (hiszen akkor egyszerűsítettünk volna vele). □

6.1. Megjegyzés. Ezt az összefüggést évezredek óta ismerték és használták a matematikusok, és teljesen természetesnek tekintették. (Egyébként a 1-et sem zárták ki a vizsgálatból; tulajdonképpen prímszámnak tekintették.)

A tétel eredetileg azt mondta ki, hogy a (pozitív) természetes számok felírhatók (pozitív) prímszámok szorzataként, és ha két ilyen felírást is találunk, akkor azok csak sorrendben térhetnek el egymástól. Az általánosítás (nemcsak egész számokra, hanem más halmazokra történő) kimondása és korrekt bizonyításának szándéka csak párszáz éves múltra tekint vissza.

A számelmélet alaptétele nem minden számkörben (összeadással és szorzással ellátott halmazon) igaz. Összetett algebrai vizsgálatok szükségesek ahhoz, hogy általánosan meg tudjuk mondani, hogy mely struktúrákban érvényes.

Az 5.1. Megjegyzésben említett $a + bX$, $a, b \in \mathbb{Z}$ struktúrában például nemcsak hogy nem működik a számelmélet alaptételére adott bizonyítás (mert a felbonthatatlanok nem feltétlenül prímek), hanem valóban nem is érvényes a számelmélet alaptétele. Például a $6 = 2 \cdot 3 = (1 + X)(1 - X)$ felbontás is prímszámok szorzatából áll, vagyis nem egyértelmű a felírás. (Nem bizonyítottuk, de $1 \pm X$ is prímszám.)

Végiggondolva a tételre adott bizonyítást, az egyértelműséghez felhasználtuk annak a bizonyítását, hogy minden felbonthatatlan szám egyszersmind prímszám is – ehhez pedig a maradékos osztást (az euklideszi algoritmust).

Igaz ugyan, hogy mi támaszkodtunk a prímszám és felbonthatatlan azonosságára, aminek bizonyítása az euklideszi algoritmuson alapul, de léteznek az alaptételnek más, az euklideszi algoritmust nem használó bizonyításai is.

Sőt, vannak olyan számkörök, amelyekben nincsen euklideszi algoritmus (mert például nincsen maradékos osztás, mert nincsen nagyságrendi rendezés az elemek között), viszont a számelmélet alaptétele mégis teljesül.

Az azonban elmondható, hogy ha valamely halmazon (integritási tartományban) elvégezhető a maradékos osztás (ott elvégezhető az euklideszi algoritmus és a felbonthatatlan számok egyszersmind prímek is), akkor ott érvényes a számelmélet alaptétele is.

Megjegyzés. Mint láttuk, a páros egész számok halmazán nincsenek egységek (mert nincs köztük az 1, így annak egyetlen osztója sem), nincsenek asszociáltak, nincsenek prímszámok, de vannak felbonthatlan számok. Ezen a halmazon a számelmélet alaptétele (annak is az egyértelműség része) nem teljesül, hiszen például $36 = 2 \cdot 18 = 6 \cdot 6$, ahol a 2, a 6 és a 18 egyaránt tovább nem bontható számok.

Megjegyzés. A számelmélet alaptételének kimondásához az $n \neq 0$ és $n \neq \varepsilon$ kikötésre nyilván szükség van, hiszen sem a 0, sem az egységek nem állnak elő felbonthatatlanok szorzataként.

Az egyértelműségre vonatkozó állítás pedig azt jelenti, hogy az előállítás akkor egyértelmű, ha egyrészt a tényezők különböző sorrendjével felírt szorzatokat nem tekintjük különbözőknek, másrészt ha valahány (az egészek körében páros sok) tényező helyett az asszociáltját (vagyis az ellentettjét) írjuk (például: $10 = 2 \cdot 5 = (-2)(-5)$), akkor az így kapott előállítást nem tekintjük az eredetitől különbözőnek.

Megjegyzés. A tétel arra is magyarázatot ad, hogy miért nem tekintjük az 1-et (és a -1-et, általában az egységeket) felbonthatatlannak, illetve prímnek annak ellenére, hogy nekik sincs valódi osztójuk, illetve igaz rájuk, hogy ha osztanak egy szorzatot, akkor annak valamelyik (történetesen az összes) tényezőjét is osztják. Ha ugyanis például az 1-et felbonthatatlannak tekintenénk, akkor semelyik szám előállítása nem lenne egyértelmű; akárhány 1-es szerepelhetne benne (Például: $10 = 2 \cdot 5 = 2 \cdot 5 \cdot 1 = 2 \cdot 5 \cdot 1 \cdot 1$ stb.).

Megjegyzés. Ha az n szám prímtényezős előállításában az azonos prímeket egy csoportba gyűjtjük, és szorzatukat az illető prím hatványaként írjuk fel, akkor a következő alakhoz jutunk:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

vagy rövidebben

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

ahol $p_i \neq p_j$ ha $i \neq j$, és $\forall i$-re $\alpha_i > 0$ egész szám. Ezt az alakot szokás az n szám *kanonikus alak*jának nevezni.

http://www.cs.elte.hu/~kfried/algebra1/Decompose.jar Ez a program megadja egy szám prímtényezős alakját.

Kényelmi okokból – mint azt később látni fogjuk – a kanonikus alakot időnként kiegészítjük olyan prímek 0-dik hatványával is, amelyek eredetileg nem szerepelnek az n prímtényezős felbontásában. Ezért célszerű az $\alpha_i > 0$ kikötést $\alpha_i \geq 0$-ra módosítani. (Ezzel persze már nem lesz egyértelmű a felírás, de akkor már nem ez lesz a lényeg.)

Azt már a 2. fejezetben megállapítottuk, hogy minden számnak osztói az egységek és saját asszociáltjaik, továbbá hogy az $n \neq 0$ szám osztói a $[-|n|, |n|]$ intervallumba esnek. Ezek között nyilván minden pozitívnak van egy negatív asszociáltja, azaz szám szerint az osztók fele pozitív, a fele negatív.

A következőkben – a kanonikus alak felhasználásával – arra keressük a választ, hogy egy n természetes számnak hány pozitív osztója van.

6.2. Megjegyzés. A továbbiakban *kizárólag* pozitív egész számok pozitív osztóira fogunk szorítkozni, a prímtényezős felbontásában, illetve a kanonikus alakban szereplő prímszámokról is feltesszük, hogy pozitívak. Minden esetben egyszerűen meggondolható, hogy milyen módosításokra lenne szükség, ha negatív számokról is szeretnénk nyilatkozni.

6.1. Jelölés. Azt a függvényt, amely egy pozitív számhoz a pozitív osztói számát rendeli, d-vel jelöljük: $d(n)$ az n pozitív szám pozitív osztóinak számát jelöli. Például $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$ stb.

Figyeljük meg az alábbiakat.

- Egy p prímszámnak két (pozitív) osztója van: 1 és p; $d(p) = 2$.
- Egy p^α alakú prímhatvány pozitív osztói $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$; a számuk pedig $\alpha + 1$; $d(p^\alpha) = p + 1$.
- Ha p és q két különböző prímszám, akkor a pq szám pozitív osztói az 1, a p, a q és a pq; összesen 4 darab; $d(pq) = 4$.
- Ha n egy $p^\alpha q^\beta$ alakú szám (ahol p és q két különböző prím), akkor az osztói a következők:

$$\begin{array}{rrrcr} 1, & q, & q^2, & \ldots & q^\beta, \\ p, & pq, & pq^2, & \ldots & pq^\beta, \\ p^2, & p^2q, & p^2q^2, & \ldots & p^2q^\beta, \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^\alpha, & p^\alpha q, & p^\alpha q^2, & \ldots & p^\alpha q^\beta \end{array}$$

Ez összesen $(\alpha+1)(\beta+1)$ darab; $d(p^\alpha q^\beta)=(\alpha+1)(\beta+1)$.

Általánosítsuk ezirányú megfigyeléseinket tetszőleges természetes számra.

6.3. Tétel. *Az $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ számnak a t szám akkor és csak akkor osztója, ha a t kanonikus alakja $t=p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$, ahol minden i-re $0\le\beta_i\le\alpha_i$.*

Bizonyítás. 1. Belátjuk, hogy n minden osztója $p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$, ahol minden i-re $0\le\beta_i\le\alpha_i$ alakú.

Ha t osztója az n-nek, akkor van olyan q, amelyre $tq=n$. Ekkor n prímtényezői éppen t és q prímtényezőiből tevődnek össze (a számelmélet alaptétele miatt), vagyis t minden prímtényezője az n-nek is prímtényezője. Így t kanonikus alakjában csak olyan prímszámok szerepelhetnek, mint n kanonikus alakjában, ráadásul legfeljebb akkora hatványon, mint n-ben.

2. Most tegyük fel, hogy t kanonikus alakja $p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$, ahol $0\le\beta_i\le\alpha_i$. Belátjuk, hogy ekkor $t\mid n$.

A $q=p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}\dots p_k^{\alpha_k-\beta_k}$ számmal megszorozva t-t éppen n-et kapunk. Mivel $\beta_i\le\alpha_i$ minden i indexre, így q egész szám, ami azt jelenti, hogy $t\mid n$. □

6.4. Tétel. *Az $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ kanonikus alakban felírt szám (pozitív) osztóinak száma: $d(n)=(\alpha_1+1)(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1)$.*

Bizonyítás. A 6.3. Tétel szerint egy n szám összes osztója $t=p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$ alakú, ahol $\forall i$-re $\beta_i\le\alpha_i$.

Annyi különböző osztó van, ahányféleképpen a $\beta_1,\beta_2,\dots,\beta_k$ kitevőket meg tudjuk választani az adott határokon belül. A β_1 kitevő összesen (α_1+1)-féle értéket vehet fel (lehet $0,1,\dots,\alpha_1$). A β_2 kitevő ettől függetlenül (α_2+1)-féle értéket vehet fel; általában bármelyik i-re az i-edik kitevő az összes többitől függetlenül (α_i+1)-féle lehet.

Vagyis a kitevőket összesen $\big((\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)\big)$-féleképpen választhatjuk meg, azaz ennyi az n szám osztóinak a száma. □

Például: a $4536=2^3\cdot3^4\cdot7$ szám osztóinak száma $d(4536)=(3+1)(4+1)(1+1)=40$.

Megjegyzés. A számok osztóival kapcsolatban rengeteg kérdést feltehetünk, sok érdekes megfigyelést végezhetünk. Megkérdezhetjük például, hogy

mennyi az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ kanonikus alakú szám osztóinak összege (erre később visszatérünk), illetve szorzata.

1. Észrevehetjük, hogy minden $t \geq 2$ számhoz végtelen sok olyan szám létezik, amelynek osztói száma éppen t. Éppen 12 osztója van például minden prímszám tizenegyedik hatványának, továbbá minden $p^2 \cdot q^3$ vagy $p^5 \cdot q$ vagy $p^2 \cdot q \cdot r$ alakú számnak, ahol p, q és r különböző prímek, hiszen $12 = (11+1) = (1+1) \cdot (1+5) = (1+2) \cdot (1+3)$. (Egyébként azt is meg tudjuk állapítani, hogy más típusú számnak nem lehet éppen 12 osztója.)

2. Egyszerűen belátható az a közismert tény is, hogy azok a számok, amelyek osztóinak száma páratlan szám, éppen a négyzetszámok. Ha ugyanis $t \mid n$, akkor létezik olyan q, amelyre $t \cdot q = n$. Ekkor viszont q is osztója az n számnak. Vagyis valahányszor találtunk egy osztót, mindjárt kettőt találtunk, azaz minden osztónak van egy párja. Így páratlan sok osztót csak úgy kaphatunk, ha valamelyik osztónak a párja saját maga, azaz ha van olyan osztó, amelyet éppen saját magával szorozva kapjuk meg az n számot, tehát ha n négyzetszám. (t-t és q-t $t \neq q$ esetén osztópároknak nevezzük.)

A kanonikus alak, illetve az osztók számára vonatkozó tétel felhasználásával a következőképpen bizonyíthatjuk az állítást:

6.1. Állítás. *Egy természetes számnak pontosan akkor van páratlan sok pozitív osztója, ha négyzetszám.*

Bizonyítás. 1. Ha n négyzetszám, akkor létezik olyan t szám, amelyre $t^2 = n$.

Ha $t = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}$, akkor $n = t^2 = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \dots p_k^{2\beta_k}$.

Ekkor $d(n) = (2\beta_1+1)(2\beta_2+1)\dots(2\beta_k+1)$, ami nyilván páratlan szám, hiszen ez olyan szorzat, amelynek minden tényezője páratlan.

2. Megfordítva: Tegyük fel, hogy az $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ számnak páratlan sok osztója van, vagyis $d(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$ szorzat páratlan. Ez csak úgy lehet, ha a szorzat minden tényezője páratlan, vagyis ha minden i-re $\alpha_i + 1$ páratlan szám, ami pontosan akkor teljesül, ha az n kanonikus alakjában minden kitevő páros.

Legyen ekkor $\alpha_1 = 2\beta_1, \alpha_2 = 2\beta_2, \dots \alpha_k = 2\beta_k$. Ezt felhasználva az n szám $n = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \dots p_k^{2\beta_k}$ alakba írható, vagyis $n = t^2$, ahol $t = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}$. Tehát n négyzetszám. □

A számok kanonikus alakját felhasználhatjuk két szám legnagyobb közös osztójának, illetve legkisebb közös többszörösének meghatározására is. Ehhez célszerű a két számot ugyanazon prímek hatványaiként felírni. Ha például a

szóbanforgó két szám a 126 és a 400, akkor a következő alakban írjuk fel őket: $126 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1$, illetve $400 = 2^4 \cdot 3^0 \cdot 5^2 \cdot 7^0$.

6.5. Tétel. *Az* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *és* a $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}$ *számok legnagyobb közös osztója* $(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}$. *(*$\forall i$, $1 \le i \le k$ *esetén* $0 \le \alpha_i, \beta_i$*)*

(Itt most – annak érdekében, hogy a két számban ugyanazok a prímtényezők szerepeljenek – megengedtük, hogy egyes kitevők 0-val egyenlők legyenek.)

Bizonyítás. Az a és b számok összes közös osztója a 6.3. Tétel értelmében

$$t = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \dots p_k^{\gamma_k}$$

alakú, ahol minden i-re $0 \le \gamma_i \le \alpha_i$ és $(0 \le)\gamma_i \le \beta_i$, vagyis $0 \le \gamma_i \le \min(\alpha_i, \beta_i)$. A fenti szám ilyen alakú, tehát közös osztó, és az ilyen alakúak közül nyilván akkor kapjuk a legnagyobbat, ha az összes kitevőt a lehető legnagyobbra választjuk, vagyis ha minden i-re $\gamma_i = \min(\alpha_i, \beta_i)$, ami a fenti számra teljesül. □

Például: $(126, 400) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 2$.

http://www.cs.elte.hu/~kfried/algebra1/GCDPrime.jar Ez a program megadja két szám prímtényezős alakjából azok legnagyobb közös osztójának prímtényezős alakját.

6.6. Tétel. *Az* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *és* a $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_k^{\beta_k}$ *számok legkisebb közös többszöröse* $[a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \dots p_k^{\max(\alpha_k,\beta_k)}$.

Bizonyítás. A 6.3. Tétel értelmében a és b minden közös többszöröse $t = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \dots p_k^{\gamma_k} \cdot q_1^{\delta_1} \cdot q_2^{\delta_2} \dots q_k^{\delta_k}$ alakú, ahol minden i-re $\gamma_i \ge \alpha_i$ és $\gamma_i \ge \beta_i$, vagyis $\gamma_i \ge max(\alpha_i, \beta_i)$, $q_1^{\delta_1} \cdot q_2^{\delta_2} \dots q_k^{\delta_k}$ pedig egy tetszőleges egész szám kanonikus alakja. A fenti szám ilyen alakú (minden j-re $\delta_j = 0$), tehát közös többszörös. Az ilyen alakúak közül nyilván akkor kapjuk a legkisebbet, ha az összes kitevőt a lehető legkisebbre válsztjuk, vagyis ha minden i-re $\gamma_i = \max(\alpha_i, \beta_i)$ és minden j-re $\delta_j = 0$. Ez a fenti számra teljesül. □

Például: $[126, 400] = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 25\,200$.

Megjegyzés. Általános iskolában a számelmélet alaptételét bizonyítás nélkül elfogadjuk, és a legnagyobb közös osztót (valamint annak segítségével a legkisebb közös többszöröst) rendszerint a most leírt módon határozzuk meg (és nem az euklideszi algoritmussal).

Megjegyzés. Két szám legnagyobb közös osztójának és legkisebb közös többszörösének meghatározására már korábban is volt eljárásunk: a legnagyobb közös osztót megkaphattuk az euklideszi algoritmus segítségével, a legnagyobb közös osztó és a két szám szorzatának birtokában pedig már ki tudtuk számítani a legkisebb közös többszöröst (4.3. Tétel).

Láttuk azonban, hogy vannak olyan számkörök, amelyekben nincs euklideszi algoritmus (például mert nincsen nagyságrendi rendezés az elemek között, így nincsen maradékos osztás), viszont a számelmélet alaptétele mégis teljesül. Bár mi az alaptétel bizonyítása során támaszkodtunk a prímszám és felbonthatatlan azonosságára, aminek bizonyítása az euklideszi algoritmuson alapul, de – mint említettük – léteznek az alaptételnek más, az euklideszi algoritmust nem használó bizonyításai is. Ezekben a számkörökben a 6.5. és 6.6. Tételek segítségével határozható meg a legnagyobb közös osztó és a legkisebb közös többszörös, sőt létezésüket is ezek a tételek, illetve a számelmélet alaptétele garantálja.

A továbbiakban relatív prímekkel kapcsolatos kérdésekre keresünk választ – még mindig a számelmélet alaptétele segítségével.

6.7. Tétel. *Tetszőleges a, b és c egész számokra $(a, bc) = 1$ akkor és csak akkor teljesül, ha $(a, b) = 1$ és $(a, c) = 1$.*

Bizonyítás. 1. Tegyük fel először, hogy $(a, bc) = 1$. Eszerint bc kanonikus alakjában egyetlen olyan prímszám sem szerepelhet, amely a felírásában szerepel (különben lenne 1-nél nagyobb közös osztójuk). Ez azt jelenti, hogy sem b-nek, sem c-nek nincs olyan prímosztója, amely a-nak is osztója lenne. Így a és b, valamint a és c is relatív prímek. (Hiszen egyiknek sincs közös prímosztója.)

2. Most tegyük fel, hogy $(a, b) = 1$ és $(a, c) = 1$. Ekkor sem b-nek, sem c-nek nincs a kanonikus felírásában olyan prímszám, amely osztója lenne a-nak, vagyis bc felírásában sem szerepel ilyen. Így tehát $(a, bc) = 1$. □

6.8. Tétel. *Ha $(a, b) = 1$, akkor az ab szorzat tetszőleges d osztója egyértelműen előállítható $a'b'$ alakban, ahol $a' \mid a$ és $b' \mid b$. (És ekkor $(a', b') = (a', b) = (a, b') = 1$.)*

Bizonyítás. Legyen $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$ és $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \dots q_l^{\beta_l}$. Ekkor

$$ab = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} \cdot q_2^{\beta_2} \dots q_l^{\beta_l},$$

ahol (mivel $(a, b) = 1$) $p_i \neq q_j$.

Ha most $d \mid ab$, akkor a 6.3. Tétel miatt

$$d = p_1^{\alpha_1'} \cdot p_2^{\alpha_2'} \dots p_k^{\alpha_k'} q_1^{\beta_1'} \cdot q_2^{\beta_2'} \dots q_l^{\beta_l'},$$

ahol $0 \le \alpha_i' \le \alpha_i$ és $0 \le \beta_i' \le \beta_i$.

Bármelyik d osztóról is van szó, az $a' = p_1^{\alpha_1'} \cdot p_2^{\alpha_2'} \dots p_k^{\alpha_k'}$ és $b' = q_1^{\beta_1'} \cdot q_2^{\beta_2'} \dots q_l^{\beta_l'}$ számok egyértelműen meghatározottak, továbbá $a' \mid a$ és $b' \mid b$.

A relatív prím tulajdonságok az oszthatóság tranzitivitása miatt visszavezethetők $(a, b) = 1$-re. □

Megjegyzés. Az, hogy egy ab szorzat tetszőleges d osztója előállítható $a'b'$ alakban, ahol $a' \mid a$ és $b' \mid b$, mindig igaz, az $(a, b) = 1$ feltételre az egyértelműséghez van szükség, amit az garantál, hogy a-nak és b-nek nincs közös prímtényezője.

Megjegyzés. A tétel megfordítása is igaz, sőt triviális: Ha $a'' \mid a$ és $b'' \mid b$, akkor (függetlenül attól, hogy a és b relatív prímek vagy nem), $a''b'' \mid ab$. Ha ugyanis $a'' \mid a$, akkor van olyan q_1 egész szám, amelyre $a''q_1 = a$, és ha $b'' \mid b$, akkor van olyan q_2 egész szám, amelyre $b''q_2 = b$. Ekkor viszont $a''b''q_1q_2 = ab$. Vagyis $a''b'' \mid ab$.

6.3. Megjegyzés. A 6.7. és 6.8. Tételek a számelmélet alaptétele nélkül, csak a legnagyobb közös osztó tulajdonságait felhasználva is bizonyíthatók.

Feladatok

1. Igazolja a 4. fejezet 1–9. feladatait a számelmélet alaptételének felhasználásával is!
2. Határozza meg az n szám osztóinak szorzatát!
3. Melyik az a legkisebb n természetes szám, amelyre $d(n) = 1$; 2; 3; 10; 12; 45?
4. Igazolja, hogy tetszőleges a, b természetes számokra $d(ab) \le d(a) \cdot d(b)$!
5. Igazolja, hogy végtelen sok n természetes számra teljesül, hogy $d(n + 1) \ge 2d(n)$!
6. Igazolja, hogy a $2d(n^2) = 3d(n)$ összefüggés csak prímszám n esetén teljesülhet!
7. Igazolja, hogy $d(n) \le n$ tetszőleges n természetes szám esetén!
8. Igazolja, hogy $d(n) \le 2\sqrt{n}$ tetszőleges n természetes szám esetén!

7. fejezet

A prímszámokról

A korábbiakban már megismerkedtünk a prímszám fogalmával és néhány fontos, prímszámokkal kapcsolatos tétellel. Mivel az egész számok körében egy szám akkor és csak akkor prím, ha az ellentettje az, és egy számot akkor és csak akkor oszt egy prím, ha annak ellentettje osztja, ebben a fejezetben vizsgálódásaink elsősorban a pozitív egészekre szorítkoznak. Könnyen meggondolható, hogy eredményeink hogyan általánosíthatóak az egész számok halmazára. Most először azt fogjuk megnézni, hogyan lehet egy számról eldönteni, hogy prím-e, illetve hogyan lehet egy adott korlátig megtalálni az összes (pozitív) prímszámot.

(Sem most, sem a későbbiekben nem teszünk különbséget prím és felbonthatatlan között, mindvégig a rövidebb prím elnevezést fogjuk használni. Meggondolható, hogy mely esetekben támaszkodunk a prímek felbonthatatlanságára, amely esetekben a prímségére.)

A prímszámok megkeresésére szolgál a következő, *eratosztenészi szita* nevű eljárás:

Írjuk fel először a számokat 2-től n-ig, ahol n az a szám, ameddig kíváncsiak vagyunk a prímekre:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, ..., n

7.1. ábra.

Az első szám, a 2, prímszám, ezt karikázzuk be, az összes többi többszörösét pedig (azok biztos nem prímek, hiszen a 2 valódi osztójuk) húzzuk át:

(2), 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, …, n

7.2. ábra.

Ezután karikázzuk be az első még meg nem jelölt (a bekarikázatlanok közül az első át nem húzott) számot (a 3-at), és húzzuk át a nála nagyobb többszöröseit (ezek közül persze bizonyosakat – amelyek 2-vel is oszthatók – már az előbb áthúztunk):

(2), (3), ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, …, n

7.3. ábra.

Ezután ismét karikázzuk be az első még meg nem jelölt számot, majd húzzuk át saját maga kivételével az összes többszörösét, és így tovább, addig folytassuk az eljárást (a szitálást), amíg az összes összetett szám (az adott korlátig) ki nem hullik a rostán (át nem lesz húzva).

91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

7.4. ábra. Az eratosztenészi szita első lépése $n = 100$-ra

Kérdés, hogy van-e rá garancia, hogy ez az állapot előbb-utóbb bekövetkezik, és ha igen, akkor mikor, illetve hogy a prímszámok biztosan mind fentmaradnak-e.

Ahhoz, hogy válaszolni tudjunk ezekre a kérdésekre, tegyünk először néhány megfigyelést az eljárásról:

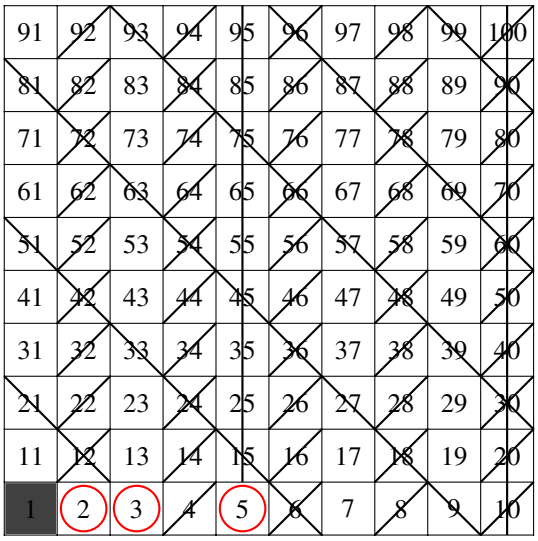
91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

7.5. ábra. Az eratosztenészi szita második lépése $n = 100$-ra

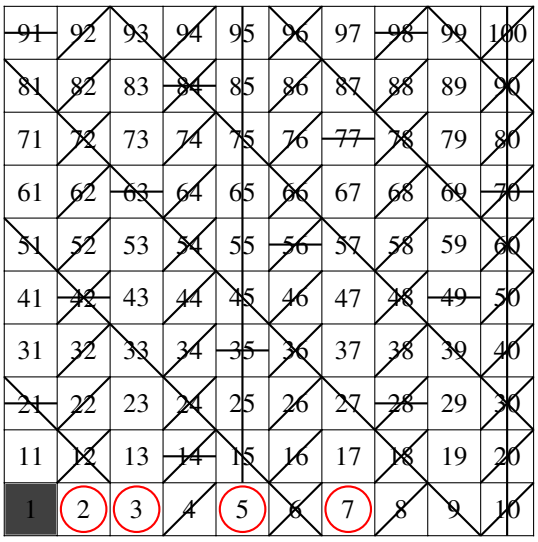
91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

7.6. ábra. Az eratosztenészi szita harmadik lépése $n = 100$-ra

- A bekarikázott számok mindig prímek, hiszen az első bekarikázott szám (a 2) prím, és mindig az első még meg nem jelölt számot karikázzuk be, vagyis egy olyan számot, amelyre igaz az, hogy a nála kisebb számok között nincsen prímosztója (hiszen ha lenne, akkor az illető prím többszörösei között őt is áthúztuk volna), vagyis prím.



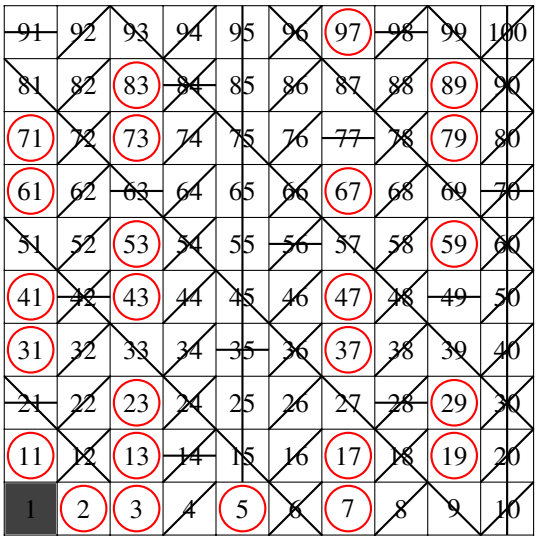
7.7. ábra. Az eratosztenészi szita negyedik lépése $n = 100$-ra



7.8. ábra. Az eratosztenészi szita ötödik lépése $n = 100$-ra

- Az áthúzott számok mind összetettek, hiszen akkor húzunk át egy számot, ha ő egy nála kisebb (prím)szám többszöröse.

- Azt is megállapíthatjuk, hogy akkor húzunk át egy összetett számot, amikor éppen a legkisebb prímosztója szerint szitálunk.



7.9. ábra. A megmaradt számok $n = 100$-ig prímek

Ezzel az eljárással elérhető, hogy előbb utóbb minden szám (az adott határig) vagy be legyen karikázva, vagy át legyen húzva, hiszen bármilyen n korlát esetén n-ig véges sok (pozitív egész) szám van, ezek között véges sok a prím, és minden prímnek véges sok többszöröse van.

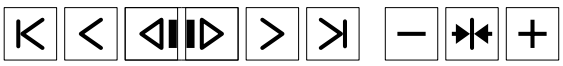
Valójában azonban nincs szükség arra, hogy addig folytassuk az eljárást, amíg n-ig minden számot meg nem jelölünk így vagy úgy (karikázással vagy áthúzással). Ha például 100-ig szeretnénk megtalálni az összes prímet, akkor azt fogjuk tapasztalni, hogy miután kihúztuk a 2, a 3, az 5 és a 7 összes többszörösét, az első még meg nem jelölt számnak – a 11-nek – már nincs olyan többszöröse (100-ig), amit át ne húztunk volna már korábban. Ugyanez a helyzet a 13-mal, a 17-tel és az összes többi 7-nél nagyobb prímmel is, ami azt jelenti, hogy további szitálálásra nincs szükség, most már az összes megjelöletlen szám prím.

Az http://www.cs.elte.hu/~kfried/algebra1/ERATOS-.EXE itt elindítható (DOS, grafikus) PROGRAMBAN az eratosztenészi szitát modelleztük. Minden számnak egy-egy képernyőpont felel meg: 480 sorban és 480 oszlopban. Eszerint $480 \cdot 480 = 230\,400$-ig (pontosabban $230\,399$-ig) *szitálunk*.

Az 7.10. ábrán látható animáció 2-től 224-ig szitál.

Az, hogy egy p prímnek már nincs áthúzatlan többszöröse n-ig azt jelenti, hogy nincs olyan szám (n-ig), amelynek a legkisebb prímosztója p lenne

	2	3	4	5	6	7	8	9	10	11	12	13	14	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134
135	136	137	138	139	140	141	142	143	144	145	146	147	148	149
150	151	152	153	154	155	156	157	158	159	160	161	162	163	164
165	166	167	168	169	170	171	172	173	174	175	176	177	178	179
180	181	182	183	184	185	186	187	188	189	190	191	192	193	194
195	196	197	198	199	200	201	202	203	204	205	206	207	208	209
210	211	212	213	214	215	216	217	218	219	220	221	222	223	224



7.10. ábra. (animáció).

(vagyis már a p-nél kisebb prímek valamelyikének a többszörösei között kihúztuk).

A 2, 3, . . . , 100 számok között nyilván nincs olyan összetett szám, amelynek a legkisebb prímosztója 11 vagy annál nagyobb prím lenne, hiszen ha egy a szám legkisebb prímosztója a 11, akkor a felírható $a = 11a_1$, alakban, ahol $a_1 \geq 11$. Ha viszont $a_1 \geq 11$, akkor $a = 11a_1 \geq 11 \cdot 11 = 121$. Vagyis a 121-nél kisebb számok közül semelyiknek nem lehet a 11 a legkisebb prímosztója.

Általában is igaz:

7.1. Állítás. *Ha n összetett szám legkisebb prímosztója p, akkor $p^2 \leq n$.*

Bizonyítás. Az n felírható $n = pn_1$, alakban, ahol $n_1 \geq p$, így $pn_1 \geq p^2$, vagyis a $n \geq p^2$. □

(Persze ha n nem összetett szám, akkor a legkisebb prímosztója maga n.)

Ez azt jelenti, hogy ha n-ig szeretnénk megtalálni a prímeket, akkor a szitálást elegendő azokra a prímszámokra elvégezni, amelyeknek négyzete nem nagyobb n-nél. (Ha tehát n prímszám, akkor is elég az $\lfloor\sqrt{n}\rfloor$ számig található prímszámokig vizsgálni a lehetséges prímosztókat.)

Megjegyzés. Ha nem feltétlenül a prímszámokat akarjuk megtalálni, akkor az eratosztenészi szitához hasonlóan más szitálási szabályokat is kitalálhatunk. Megvizsgálva, hogy különféle szabályok esetén mikor milyen számok maradnak fent a rostán, sok érdekességre bukkanhatunk.

Ha például az

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, ...,

7.11. ábra.

sorozatban bekarikázzuk az 1-et, és áthúzunk minden másodikat:

(1), ~~2~~, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, ...,

7.12. ábra.

majd a fennmaradó számok közül bekarikázzuk az első még meg nem jelöltet – a 3-at – és áthúzunk minden harmadikat:

(1), (3), ~~5~~, 7, 9, ~~11~~, 13, 15, ~~17~~, ...,

7.13. ábra.

majd az így megmaradt számok közül bekarikázzuk az első még meg nem jelöltet (a 7-et), és áthúzzuk az összes annyiadikat, amennyi az utoljára bekarikázott szám (a fennmaradt számok közül minden hetediket), és így tovább, akkor a bekarikázott számokat (1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, ...) nevezik *szerencsés számoknak.* A szerencsés számok sok szempontból a prímszámokhoz hasonlóan viselkednek, például éppen oly szeszélyesen helyezkednek el a természetes számok között, mint a prímszámok.

Azt az észrevételünket, miszerint ha egy n összetett szám legkisebb prímosztója p, akkor $n \geq p^2$, érdemes a következő formában is megfogalmazni:

7.1. Tétel. *Az n összetett szám legkisebb prímosztója nem lehet nagyobb $\sqrt{n}$-nél.*

91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

7.14. ábra. Szerencsés számok keresése $n = 100$-ig – 1. lépés

91		93		95		97		99	
81		83		85		87		89	
71		73		75		77		79	
61		63		65		67		69	
51		53		55		57		59	
41		43		45		47		49	
31		33		35		37		39	
21		23		25		27		29	
11		13		15		17		19	
1		3		5		7		9	

7.15. ábra. Szerencsés számok keresése $n = 100$-ig – 2. lépés

91		93				97		99
~~81~~				85		87		
		73		75				79
~~61~~		63				67		69
51				55		57		
		43		45				49
31		33				37		~~39~~
21				25		27		
		13		15				~~19~~
(1)		(3)				(7)		9

7.16. ábra. Szerencsés számok keresése $n = 100$-ig – 3. lépés

~~91~~		93				97		99
				85		87		
		73		75				79
		63				67		69
51				55		~~57~~		
		43		45				49
31		33				37		
21				25		~~27~~		
		13		15				
(1)		(3)				(7)		(9)

7.17. ábra. Szerencsés számok keresése $n = 100$-ig – 4. lépés

		93				~~97~~		99	
				85		87			
		73		75				79	
		63				67		69	
51				55					
		43		~~45~~				49	
31		33				37			
21				25					
		(13)		15					
(1)		(3)				(7)		(9)	

7.18. ábra. Szerencsés számok keresése $n = 100$-ig – 5. lépés

		93						99	
				85		87			
		73		75				79	
		63				67		69	
51				~~55~~					
		43						49	
31		33				37			
21				25					
		(13)		(15)					
(1)		(3)				(7)		(9)	

7.19. ábra. Szerencsés számok keresése $n = 100$-ig – 6. lépés

		93						99	
				85		87			
		73		75				79	
		63				67		69	
51									
		43						49	
31		33				37			
21				25					
		13		15					
1		3				7		9	

7.20. ábra. Szerencsés számok keresése $n = 100$-ig – 7. lépés

		93						99	
						87			
		73		75				79	
		63				67		69	
51									
		43						49	
31		33				37			
21				25					
		13		15					
1		3				7		9	

7.21. ábra. A szerencsés számok $n = 100$-ig

Bizonyítás. Azt már tudjuk (7.1. Állítás), hogy ha n legkisebb prímosztója p, akkor $p^2 \leq n$, amiből már következik, hogy $p \leq \sqrt{n}$. □

Megjegyzés. Ha egy számról szeretnénk eldönteni, hogy prím-e vagy sem, akkor az előző tétel szerint ehhez elegendő megvizsgálni, hogy a szám négyzetgyökénél nem nagyobb prímek között van-e olyan, amivel osztható. Ha van, akkor a szám összetett, ha nincs, akkor prím.

Ha például arra vagyunk kíváncsiak, hogy a 751 prímszám-e, akkor elegendő azt megvizsgálni, hogy a 2, 3, 5, 7, 11, 13, 17, 19, 23 prímek valamelyikével osztható-e (a következő prím – a 29 – négyzete már nagyobb, mint 751). Mivel egyikkel sem osztható, így prímszám. (Az oszthatóságok vizsgálata során segítenek az oszthatósági szabályok.)

Azt már tudjuk, miként lehet egy számról eldönteni, hogy prím-e, és mi módon lehet megkeresni egy adott korlátig az összes prímet. Felmerül a kérdés, hogy egyáltalán hány prímszám van, valamint hogyan helyezkednek el a prímszámok a pozitív egészek 1, 2, 3, 4, ... sorozatában.

7.2. Tétel. *Végtelen sok prímszám van.*

Bizonyítás. A tétel sokféleképpen bizonyítható, a most következő bizonyítás Eukleidésztől származik.

Tegyük fel, hogy az állítással ellentétben véges sok prímszám van (indirekt bizonyítás), amelyek pontosan a következők:

$$p_1,\ p_2,\ p_3,\ \dots\ p_n.$$

Tekintsük az $A = p_1p_2p_3 \dots p_n + 1$ számot.

Ez a szám láthatóan a $p_1p_2p_3 \dots p_n$ prímek egyikével sem osztható (bármelyikkel osztva 1 maradékot ad), vagyis – mivel indirekt feltevésünk szerint a sorozatban az összes prímszám szerepel – nincs prímosztója. Ez azonban ellentmond a 6.1. Tételnek, miszerint minden (1-nél nagyobb) számnak van prímosztója. □

Megjegyzés. A bizonyítás lényege az, hogy abból a feltevésből, hogy véges sok prímszám van, ellentmondásra jutunk, tehát végtelen sok prímnek kell lennie.

Az *nem* következik a bizonyításból, hogy ha az első néhány ismert prímet összeszorozzuk, és a szorzatukhoz hozzáadunk 1-et, akkor az így kapott szám prím lesz, és általában nem is igaz. Igaz ugyan, hogy

$$2 + 1 = 3 \text{ prím},$$

$2 \cdot 3 + 1 = 7$ prím,
$2 \cdot 3 \cdot 5 + 1 = 31$ prím,
$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ prím, és
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ is prím.

De már $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$ nem prím,
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510\,511 = 19 \cdot 26\,869$ sem prím

és így tovább, elkészítve a $p_1p_2p_3 \dots p_n + 1$ számot, ahol p_i, az i-edik prímszámot jelenti, a kapott szám – n értékétől függően – hol prím lesz, hol nem. (A továbbiakban például ha $p_n = 19$, 23, 29, 37, 41, 43 vagy 47, akkor nem kapunk prímet, ha $p_n = 31$, akkor prímet kapunk.)

Nyilvánvaló, hogy a végtelen sok prímszám közül az egyetlen páros a 2, az összes többi páratlan. A páratlan számok azonban – a 4-gyel való osztási maradékuk szerint – két csoportba sorolhatók, bizonyosak $4k-1$, mások $4k+1$ alakúak. Tudjuk, hogy legalább az egyik halmazban végtelen sok prímnek kell lennie (hiszen végtelen sok páratlan prím van, és mindegyik benne van a két halmaz valamelyikében), de kérdés, hogy vajon mindkettőben végtelen sok prím van-e, vagy csak az egyikben (és akkor melyikben). Erről szól a következő tétel:

7.3. Tétel.

(a) Végtelen sok $4k - 1$ alakú prímszám van.

(b) Végtelen sok $4k + 1$ alakú prímszám van.

Bizonyítás. Először az (a) állítást bizonyítjuk, a (b) állítás bizonyítása egy későbbi összefüggésből fog következni (11.1. Következmény).

(a) Tegyük fel (indirekt módon), hogy véges sok $4k - 1$ alakú prímszám van, és ezek a következők: $p_1, p_2, p_3, \dots p_n$. Tekintsük a következő számot:

$$A = 4p_1p_2p_3 \dots p_n - 1$$

Ennek a számnak nyilvánvalóan a sem a 2, sem a $p_1, p_2, p_3, \dots, p_n$ prímek nem osztói. Az sem lehet, hogy minden prímosztója $4k+1$ alakú, hiszen maga a szám nem $4k+1$ alakú, márpedig $4k+1$ alakú számok szorzata $4k+1$ alakú: $((4a + 1)(4b + 1) = 4(4ab + a + b) + 1)$. Vagyis kell, hogy legyen $4k-1$ alakú prímosztója, ami ellentmond annak, hogy $p_1, p_2, p_3, \dots, p_n$ az összes $4k - 1$ alakú prím. □

Más számokkal való osztási maradékuk szerint is csoportosíthatjuk a prímszámokat. Azt például, hogy végtelen sok $6k - 1$ alakú prím van, ugyanúgy láthatjuk be, mint a $4k - 1$ alakúakra vonatkozó állítást (felhasználva,

hogy $6k$ alakú prím nincs; $6k+2$ alakú csak egy van, a 2; $6k+3$ alakú is csak egy van, a 3; $6k+4$ alakú nincs, a $6k+1$ alakúaknak pedig a szorzata is $6k+1$ alakú). Az is igaz, hogy végtelen sok $6k+1$ alakú prímszám van, de ezt már nehezebb bizonyítani.

Ebből következik:

7.2. Állítás. *Minden* 3*-nál nagyobb prímszám* $6k+1$ *vagy* $6k-1$ *alakú.*

Az eddigiek szerint a következő számtani sorozatok

(1) 1, 3, 5, 7, 9, 11, ...

(2) 3, 7, 11, 15, 19, ...

(3) 1, 5, 9, 13, 17, ...

(4) 5, 11, 17, 23, 29, ...

(5) 1, 7, 13, 19, 25, 31 , ...

mindegyikében végtelen sok prímszám van. Ha most azt vizsgáljuk, hogy általában hány (különböző) prímszám lehet egy (csak pozitív tagokból álló) számtani sorozatban, érdekes eredményre juthatunk. Azt már a fentiekből tudjuk, hogy lehet végtelen sok.

Olyan számtani sorozatra is könnyű példát mondani, amelyben egyetlen prímszám sincs, például:

(6) 4, 8, 12, 16, 20, 24, ...

(7) 10, 30, 50, 70, 90, ...

Általában is elmondhatjuk, hogy soha nincs prímszám az $a+nd$ számtani sorozatban, ha a sorozat a kezdőeleme összetett szám, továbbá a kezdőelem és a d differencia nem relatív prímek (hiszen a és d legnagyobb közös osztójával a sorozat minden tagja osztható lesz).

Ha az $a+nd$ számtani sorozat kezdőeleméről nem kötjük ki, hogy legyen összetett szám, de a és d most sem relatív prímek, akkor lehet, hogy éppen egyetlen egy prímszám van a sorozatban:

(8) 5, 10, 15, 20, 25, ...

(9) 3, 9, 15, 21, 27, 33, ...

Az az érdekes, hogy más eset nem fordulhat elő: egy pozitív tagú számtani sorozatban vagy 0 vagy 1 vagy végtelen sok prímszám van. 0 vagy 1 is csak úgy lehetett, hogy $(a, d) > 1$.

Vagyis az nem lehetséges, hogy egy csupa pozitív tagból álló számtani sorozatban pontosan 2, 3, 4, ... stb. prímszám legyen. (Ha negatív tagokat is megengedünk, akkor két prím is lehet a sorozatban, ilyen például a következő: $-6, -2, 2, 6, 10, 14, \ldots$) Ez lényegében a következő tételen múlik, amelyet bizonyítás nélkül közlünk:

7.4. Tétel. (Dirichlet) *Ha $d > 0$ és $(a, d) = 1$, akkor az $a + nd$ ($n = 0, 1, 2, \ldots$) számtani sorozatban végtelen sok prímszám van.*

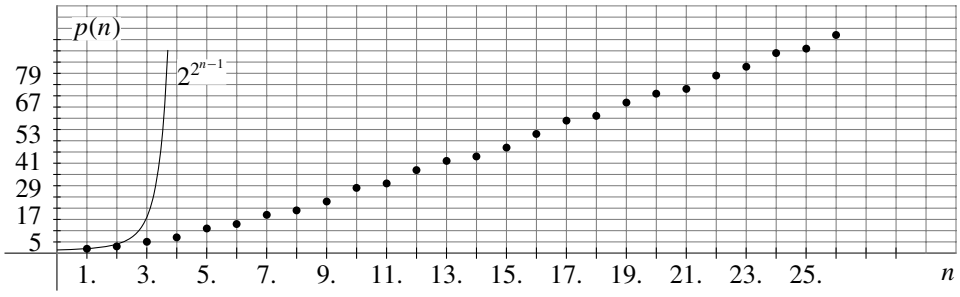
A tétel bizonyítása meglehetősen nehéz, de Dr. Szalay Mihály könyvében (Számelmélet, Speciális matematika-tankönyvek sorozat, Typotex kiadó, http://www.typotex.hu/konyv/szalay_mihaly_szamelmelet)

Megjegyzés. Érdekes kérdés, hogy más nevezetes sorozatokban hány prím lehet. A mai napig megoldatlan probléma például az, hogy a Fibonacci-sorozatban (vagyis az 1, 1, 2, 3, 5, 8, 13, 21, ... sorozatban, ahol $a_1 = a_2 = 1$ és $a_n = a_{n-1} + a_{n-2}$, ha $n > 2$) végtelen sok prímszám van-e.

Az is izgalmas kérdés, hogy milyen nagyságrendű lehet az n-edik prímszám. Azt már láttuk, hogy az n-edik prímszám legfeljebb akkora, mint az őt megelőző prímek szorzatánál 1-gyel nagyobb szám.

Az n-edik pozitív prímszámra ennek segítségével adhatunk egy felső korlátot:

7.5. Tétel. *A prímszámok $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... sorozatában az n-edik prímszámra igaz, hogy $p_n \leq 2^{2^{n-1}}$.*



7.22. ábra.

Bizonyítás. A tételt teljes indukcióval bizonyítjuk. n=1-re igaz az állítás, hiszen $p_1 = 2 \leq 2^{2^0} = 2$. Meg fogjuk mutatni, hogy ha az $n = 1, 2, 3, \ldots k$

értékek mindegyikére igaz az állítás, akkor $n = k + 1$-re is igaz. Tegyük fel tehát, hogy $p_i \leq 2^{2^{i-1}}$ minden i-re, ahol $1 \leq i \leq k$. Ekkor az is igaz az $A = p_1 p_2 p_3 \dots p_k + 1$ számra (a benne szereplő szorzatot tényezőnként becsülve az indukciós feltevés alapján), hogy

$$A \leq 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 = 2^{1+2+4+\dots+2^{k-1}} + 1 = 2^{2^k-1} + 1.$$

Újabb felső becslést alkalmazva (felhasználva, hogy $1 \leq 2^{2^k-1}$):

$$2^{2^k-1} + 1 \leq 2^{2^k-1} + 2^{2^k-1} = 2 \cdot 2^{2^k-1} = 2^{2^k}.$$

Vagyis azt kaptuk, hogy $A \leq \dots \leq 2^{2^k}$. Mi viszont azt szeretnénk belátni, hogy $p_{k+1} \leq 2^{2^k}$. Ehhez nyilvánvalóan elég azt megmutati, hogy $p_{k+1} \leq A$.

A 7.2. Tétel bizonyításában láttuk, hogy A-nak az első k prímszámon kívül van prím osztója. Eszerint a $(k+1)$-edik prímszám nem lehet A-nál nagyobb, így $p_{k+1} \leq 2^{2^k}$. □

Megjegyzés. Az imént kapott felső korlátot kipróbálva az első néhány prímre azt kapjuk, hogy:

$$\begin{aligned} p_1 &= 2 \leq 2^{2^0} = 2, \\ p_2 &= 3 \leq 2^{2^1} = 4, \\ p_3 &= 5 \leq 2^{2^2} = 16, \\ p_4 &= 7 \leq 2^{2^3} = 256, \\ &\dots, \end{aligned}$$

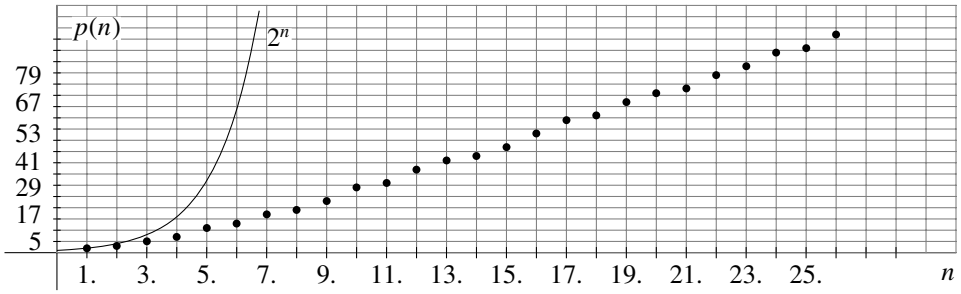
vagyis tételünk meglehetősen durva felső becslést ad az n-edik prímre. Léteznek finomabb becslések is, de az ezekre vonatkozó bizonyítások meghaladják kereteinket.

Bertrand (1822–1900) francia matematikus sejtette meg, és Csebisev (1821–1894) orosz matematikus bizonyította először a következő tételt, amely azt modja ki, hogy tetszőleges szám és a kétszerese között mindig van prímszám:

7.6. Tétel. (Csebisev-tétel) *Tetszőleges $n > 1$ egészhez létezik olyan p prímszám, amelyre $n < p < 2n$.*

A tételt nem bizonyítjuk.

7.3. Állítás. *Csebisev tételéből következik, hogy az n-edik prímszám legfeljebb 2^n, azaz $p_n \leq 2^n$.*



7.23. ábra.

Bizonyítás. A bizonyítást ismét teljes indukcióval végezhetjük el.

$p_1 \leq 2$, és a tétel szerint van prímszám p_1 és $2p_1$ között, vagyis $p_2 \leq 2p_1 \leq 2 \cdot 2 = 2^2$. (Konkrétan $p_2 = 3$.)

Ugyancsak a tétel szerint van prímszám p_2 és $2p_2$ között is, vagyis $p_3 \leq 2p_2 \leq 2 \cdot 2^2 = 2^3$.

Tegyük fel, hogy k-ig teljesül a tétel állítása. Ebből belátjuk, hogy $p_{k+1} \leq 2^{k+1}$.

Mivel $p_k \leq 2^k$ és Csebisev tétele szerint van prímszám p_k és $2p_k$ között, így biztos, hogy $p_{k+1} \leq 2 \cdot p_k \leq 2^{k+1}$, vagyis minden n-re teljesül az állítás. □

Érdekes megvizsgálni, hogy milyen gyakran fordulnak elő a prímszámok a természetes számok között. A prímek *sűrűségéről,* a pozitív egészek közti elhelyezkedéséről szól a következő néhány tétel. Először azt vizsgáljuk meg, hogy mekkora hézagok fordulhatnak elő a prímszámpárok között, vagyis milyen hosszú lehet egymást követő összetett számok sorozata.

Nem nehéz 2, 3, 4, sőt 5 egymást követő összetett számot találni, például: 24, 25, 26, 27, 28 vagy 32, 33, 34, 35, 36 stb. Még 100 alatt hetet is találhatunk: 90, 91, 92, 93, 94, 95, 96. A következő három elemnél hosszabb blokk, a 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126 – már tizenhárom egymást követő összetett számot tartalmaz. Az a kérdés, hogy található-e még ennél is hosszabb, sőt sokkal hosszabb, vagy akár egy tetszőlegesen megadott korlátnál is hosszabb egymást követő összetett számokból álló sorozat.

Erről szól a következő tétel:

7.7. Tétel. *Tetszőleges n pozitív egész számhoz létezik n darab egymást követő összetett szám.*

Bizonyítás.

Tekintsük a következő n darab számot (ahol $(n+1)!$ az $1, 2, 3, 4, \ldots, n, (n+1)$ számok szorzatát jelöli):

$$\begin{aligned}
&(n+1)!+2\\
&(n+1)!+3\\
&(n+1)!+4\\
&(n+1)!+5\\
&\ldots\\
&(n+1)!+n\\
&(n+1)!+n+1
\end{aligned}$$

E számok nyilvánvalóan egymást követő számok, és mindegyik összetett szám, hiszen az első osztható 2-vel, a második 3-mal, a harmadik 4-gyel, és így tovább, mindegyik összeg első tagja szorzótényezőként tartalmazza a második tagot, így mindegyik szám osztható a második taggal. □

Megjegyzés. A tétel *nem* azt állítja, hogy tetszőlegesen megadott n-hez létezik két olyan szomszédos prímszám, amelyek távolsága *éppen* n, hanem azt, hogy tetszőlegesen megadott n-hez létezik két olyan szomszédos prímszám, amelyek távolsága *legalább* n. Az, hogy melyik ez a két prím, nem derül ki a bizonyításból. (A bizonyításban megadott n darab egymást követő szám biztosan összetett, de sem az előző számról – az $(n+1)!+1$-ről –, sem a következőről – az $(n+1)!+(n+2)$-ről – nem tudjuk, hogy prím-e vagy összetett.)

Nyilvánvalóan nincs például két olyan szomszédos prímszám, amelyek távolsága éppen 11. (Ha ugyanis p prím, akkor vagy $p=2$, vagy p páratlan. Ha $p=2$, akkor a következő prím a 3, különbségük nem 11. Ha p páratlan, akkor $p+11$ egy nyilvánvalóan kettőnél nagyobb páros szám, így nem lehet prím.) Hasonlóan gondolható meg, hogy semmilyen 1-nél nagyobb páratlan n-re nincs két olyan prím, amelyek távolsága éppen n. (Az egyetlen olyan pozitív prímpár, ahol a két prím távolsága 1, a 2 és a 3.)

Megjegyzés. A bizonyítás egyben módszert is ad arra, hogy kívánt számú, egymást követő összetett számot konstruáljunk. Ez a módszer azonban nem valami takarékos, közel sem a lehető legkisebb összetett számokat adja meg. Ha ezzel a módszerrel szeretnénk például 5 egymást követő összetett számot találni, akkor mivel $6! = 720$, a következő 5 számot kapnánk: 722, 723, 724, 725, 726; vagyis sokkal nagyobb számokat, mint korábbi példánkban. (Mellesleg ez a sorozat „felfelé” már nem folytatható, mert a 727 prím, de „lefelé” igen: sem a 721, sem a 720 nem prím.)

Lényegesen takarékosabb a következő eljárás:

Keressünk egy n-nél nagyobb p prímszámot (ha takarékosak akarunk lenni, akkor a lehető legkisebb ilyet), és szorozzuk össze p-ig (őt is beleértve) az összes prímet. Ha most ehhez a szorzathoz adunk hozzá rendre 2-t, 3-at, 4-et, ..., $(n+1)$-et, akkor is n egymást követő összetett számot kapunk.

Ha például 5 egymást követő összetett számot szeretnénk, akkor a lehető legkisebb 5-nél nagyobb prím a 7, így a szóbanforgó összetett számok a következők lesznek:

$$2 \cdot 3 \cdot 5 \cdot 7 + 2 = 212$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 3 = 213$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 4 = 214$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 5 = 215$$
$$2 \cdot 3 \cdot 5 \cdot 7 + 6 = 216$$

(Most is folytatható a sorozat, ezúttal „felfelé": a 217, 218, 219, 220, 221 és 222 számok is összetettek)

Könnyen belátható, hogy ez az eljárás is mindig n egymást követő összetett számot ad meg, ugyanis a 2, 3, 4, ..., $(n+1)$ számok mindegyikének minden prímosztója szerepel a $2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$ szorzatban, hiszen $p \geq n+1$.

Megjegyzés. Tételünk nem jelenti azt, hogy a nagyobb számok felé haladva egyre nőnének a prímek közötti hézagok. A „nagyobb" számok között is előfordulnak ún. *ikerprímek*, azaz olyan szomszédos prímek (mint például a 3 és az 5; vagy az 5 és a 7), amelyek különbsége 2. Ilyen „nagy" ikerprímekre példa a következő két szám: 1 000 000 000 061 és 1 000 000 000 063, bár nem ez az ismert legnagyobb ikerprímpár. Az, hogy az ikerprímek száma végtelen-e, megoldatlan probléma.

Ismert, hogy a pozitív egész számok reciprokaiból képzett $a_n = \sum_{i=1}^{n} \frac{1}{i}$ sorozat divergens (tetszőleges valós számnál van nagyobb tagja a sorozatnak), míg a négyzetszámok reciprokaiból képzett $b_n = \sum_{i=1}^{n} \frac{1}{i^2}$ sorozat konvergens ($\frac{\pi^2}{6}$-hoz tart). Ez azt jelenti, hogy a négyzetszámok viszonylag ritkán fordulnak elő a pozitív egészek között. Vajon mi a helyzet a prímekkel? Erről szól a következő tétel, amelyet bizonyítás nélkül közlünk:

7.8. Tétel. *A pozitív prímszámok reciprokaiból képzett* $c_n = \sum_{i=1}^{n} \frac{1}{p_i}$ *sorozat divergens.*

E tétel szerint a prímszámok sűrűbben fordulnak elő a természetes számok között, mint a négyzetszámok. (Átlagosan valamely n-ig több a prím-

szám, mint a négyzetszám. Nagy vonalakban a k-adik prímszám „gyakran” kisebb, mint a k-adik négyzetszám, $p_k \leq k^2$.)

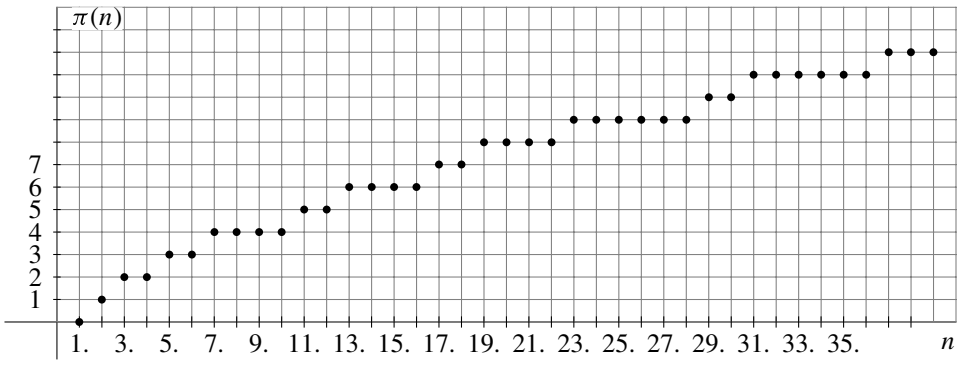
A prímszámok sűrűségének jellemzésére alkalmas annak vizsgálata, hogy egy adott korlátig hány prímszám fordul elő, illetve hogy egy adott korlátig a pozitív egészeknek hányad része prímszám.

Jelöljük $\pi(x)$-szel az x egész számnál nem nagyobb pozitív prímek darabszámát, és vizsgáljuk a $\dfrac{\pi(x)}{x}$ hányadost:

x	2	3	4	5	6	7	8	9	10	11	...
$\pi(x)$	1	2	2	3	3	4	4	4	4	5	...
$\dfrac{\pi(x)}{x}$	$\dfrac{1}{2}$	$\dfrac{2}{3}$	$\dfrac{1}{2}$	$\dfrac{3}{5}$	$\dfrac{1}{2}$	$\dfrac{4}{7}$	$\dfrac{1}{2}$	$\dfrac{4}{9}$	$\dfrac{2}{5}$	$\dfrac{5}{11}$	...

Azt tapasztaljuk, hogy kezdetben kb. a számok fele prím. Folytatva a vizsgálódást azt tapasztaljuk, hogy – kisebb-nagyobb ingadozásokkal ugyan, de – csökken ez az arány, például $\pi(100) = 25$, vagyis 100-ig a számok negyedrésze prím. Vajon mi a helyzet a későbbiekben? Nagy vonalakban csökken a prímek aránya, vagy sűrűsödések és ritkulások váltogatják egymást? Van-e határértéke a végtelenben a $\dfrac{\pi(x)}{x}$ sorozatnak? Erről szól a következő tétel:

7.9. Tétel. *Legyen $\pi(x)$ az x-nél nem nagyobb pozitív prímek száma. Ekkor $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x} = 0$ (azaz a prímszámok sorozata 0 sűrűségű).*

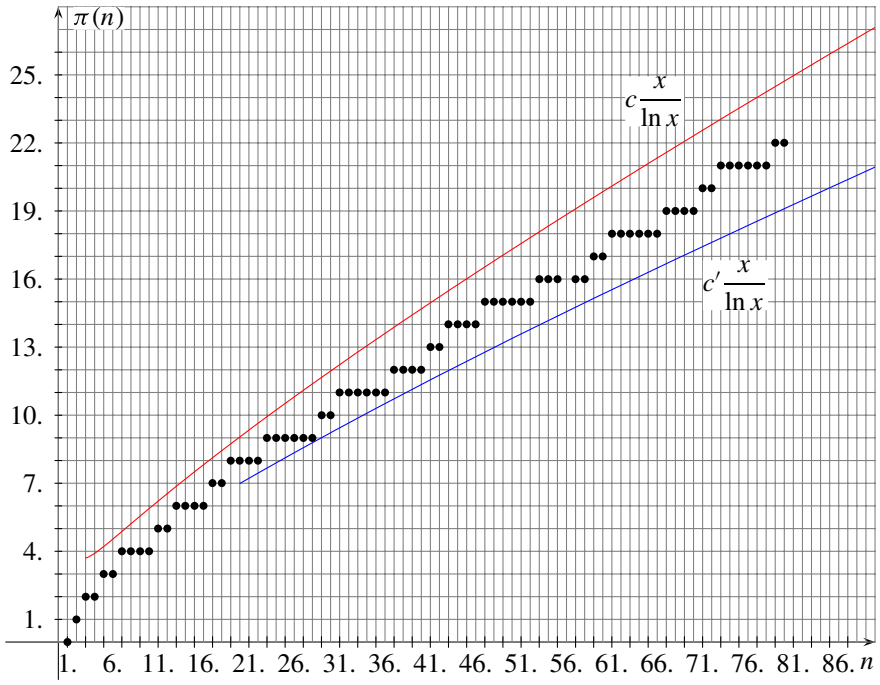


7.24. ábra.

A tételt nem bizonyítjuk, viszont kimondunk – szintén bizonyítás nélkül – egy erősebb tételt, amelyből következik:

7.10. Tétel. *Léteznek olyan $c > 1$ és $0 < c' < 1$ konstansok, hogy elég nagy x-re*

$$c'\frac{x}{\ln x} < \pi(x) < c\frac{x}{\ln x}.$$



7.25. ábra.

Megjegyzés. A tétel szerint

$$\frac{c'}{\ln x} < \frac{\pi(x)}{x} < \frac{c}{\ln x}.$$

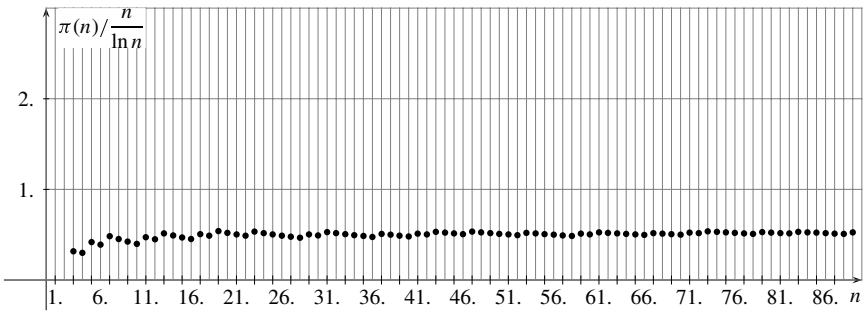
Ebből pedig valóban következik, hogy ha $x \to \infty$, akkor $\dfrac{\pi(x)}{x} \to 0$, hiszen ekkor $\ln x \to \infty$, azaz $\dfrac{1}{\ln x} \to 0$.

$\pi(x)$-ről egy még ennél erősebb eredmény is ismert, amelyet szintén bizonyítás nélkül közlünk:

7.11. Tétel. (Nagy prímszámtétel) *Legyen $\pi(x)$ az x-nél nem nagyobb prímek száma. Ekkor:*

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\dfrac{x}{\ln x}\right)} = 1$$

(azaz $\pi(x)$ és $\dfrac{x}{\ln x}$ „aszimptotikusan” egyenlők).



7.26. ábra.

Megjegyzés. Az aszimptotikus egyenlőséget szemléletesen úgy mondjuk, hogy „összesimulnak". Azt láttuk, hogy a természetes számok körében a prímszámok sűrűbben helyezkednek el, mint a négyzetszámok (például n-ig nagyságrendben több, mint $\sqrt{n}$ van), és most azt látjuk, hogy körülbelül olyan sűrűn helyezkednek el, mint az $\dfrac{x}{\ln x}$ függvény pontjai, azaz n-ig körülbelül $\dfrac{n}{\ln n}$.

A prímek szabálytalan elhelyezkedése, számos érdekessége sokakat késztetett arra, hogy megpróbáljanak olyan függvényt keresni, amelynek az n helyen felvett helyettesítési értéke az n-edik prím, vagy olyat, amely minden természetes számhoz prímszámot rendel, vagy legalább olyat, amely minden prímet felvesz valahol. Eddig azonban olyan egyszerű képletet, amely – legalábbis burkolt formában – ne magukra a prímszámokra támaszkodna, nem sikerült megadni. (Lásd Laczkovich Miklósnak ebben a témában a Középiskolai Matematikai Lapokban 1999-ben megjelent érdekfeszítő cikkét [4].)

Vizsgáljuk meg az $f(n) = n^2 - n + 41$ polinom helyettesítési értékeit:

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$f(n)$	41	43	47	53	61	71	83	97	113	131	151	163	...

Azt tapasztaljuk, hogy az $n = 1, 2, 3, \ldots, 40$ értékek mindegyikére prímszám a helyettesítési érték. Az $n = 41$ helyen azonban már nyilván nem kaphatunk prímet, mert a helyettesítési érték osztható 41-gyel (és persze nagyobb is, mint 41).

Hasonló a helyzet más polinomokkal is.

Ahhoz, hogy ezt bebizonyítsuk, meg kell értenünk valamit, aminek a bizonyítását most nem részletezzük (ezzel a második kötetben fogunk foglalkozni).

7.4. Állítás. *Egy nem konstans polinom nem veheti fel a* 0 *értéket végtelen sokszor.*

Megjegyzés. Szemléletesen a következőről van szó: Középiskolai tapasztalataink alapján tudjuk, hogy ha egy másodfokú polinom valahol 0-t vesz fel, vagyis van gyöke, akkor a polinomot gyöktényezős alakban írhatjuk fel. Azonban egy másodfokú polinom sem mindig írható fel gyöktényezős alakban. Az viszont a magasabb fokú polinomokra is teljesül, hogy ha valamely x_0 helyen gyöke van, akkor kiemelhető belőle egy $(x - x_0)$ szorzótényező. Ezért egy n-edfokú polinom legfeljebb n darab elsőfokú tényező szorzatára bomlik, vagyis legfeljebb n darab gyöke lehet, tehát legfeljebb n helyen veheti fel a 0 függvényértéket.

7.1. Következmény. *Egy nem konstans polinom egyetlen függvényértéket sem vehet fel végtelen sokszor.*

Bizonyítás. Az $f(x)$ nem konstans polinom pontosan akkor veszi fel az a értéket, amikor az $f(x) - a$ a 0-t. Ezért a 7.4. Állítás szerint az $f(x)$ nem konstans polinom nem vehet fel végtelen sokszor semmilyen a értéket sem. □

7.12. Tétel. *Nincs olyan egész együtthatós, nem konstans polinom, amely minden természetes szám helyen prím értéket vesz fel.*

Bizonyítás. Tekintsük az $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ polinomot, ahol az $a_0, a_1, \ldots, a_{n-1}, a_n$ együtthatók egész számok.

Ha $a_0 = 0$, akkor tetszőleges n-re az $x = n$ helyen felvett helyettesítési érték osztható n-nel, így ha például n összetett szám, akkor a helyettesítési érték sem lehet prím.

Ha $a_0 \neq 0$, akkor vizsgáljuk meg, hogy milyen értékeket vehet fel a polinom az $x = 0, |a_0|, |2a_0|, |3a_0|, \ldots$ helyeken. Nyilván az összes ilyen helyen osztható lesz a helyettesítési érték a_0-lal. Egy a_0-lal osztható szám csak úgy lehet prímszám, ha vagy $|a_0| = 1$, vagy a_0 maga ennek a prímnek asszociáltja. Az, hogy a fenti helyek mindegyikén ugyanannak a prímnek az asszociáltja legyen a helyettesítési érték, nem lehetséges, hiszen egy polinom nem veheti fel végtelen sokszor ugyanazt az értéket (a_0-t vagy $|a_0|$-t). Ha pedig $a_0 = 1$, akkor például az $x = 0$ helyen nem lesz prím a helyettesítési érték (hiszen $f(0) = a_0$, ami most 1, és az 1 nem prím).

Vagyis a fenti polinom semmilyen esetben sem vehet fel csak prím értékeket. □

Pierre Fermat híres francia matematikus (1601–1665) azt sejtette, hogy a $2^{2^k}+1$ alakú számok (az úgynevezett *Fermat-számok*) tetszőleges k természetes szám esetén prímek. Valójában ha $k = 0$, 1, 2, 3, vagy 4, akkor tényleg prímeket kapunk:

k	0	1	2	3	4
$2^{2^k}+1$	3	5	17	257	65 537

prímek, de – mint azt Leonhard Euler (1707–1783) megmutatta, hogy $k = 5$-re $2^{32}+1 = 4\,294\,967\,297 (= 641 \cdot 6\,700\,417)$ már nem prím. Azóta több, mint 40 további Fermat-számot vizsgáltak meg (többnyire számítógépek segítségével), és egyetlen további prímet sem találtak közöttük. Nem csak az megoldatlan probléma, hogy létezik-e végtelen sok *Fermat-prím* (vagyis olyan $2^{2^k}+1$ alakú szám, ami prím), hanem az is, hogy létezik-e legalább még egy a felsoroltakon kívül.

Arra nézve viszont, hogy egyáltalán mikor lehet prím egy $2^n + 1$ alakú szám, a következő tétel mond ki szükséges feltételt (olyan feltétel, amely elégséges is – mint ez az imént kiderült – nem ismeretes):

7.13. Tétel. *Egy $2^n + 1$ alakú szám csak úgy lehet prím, ha $n = 2^k$ ($n \in \mathbb{N}$, $n \geq 1$).*

Bizonyítás. Tekintsünk egy $N = 2^n + 1$ alakú számot, és írjuk fel az n-et egy páratlan szám és egy 2-hatvány szorzataként. n páratlan prímtényezői (ha vannak ilyenek) szorzata legyen m, a 2-eseké pedig 2^k.

Azt kell bebizonyítanunk, hogy ha $N = 2^n + 1$ prímszám, akkor m csak 1 lehet.

$$N = 2^{2^k \cdot m} + 1 = (2^{2^k})^m + 1.$$

Ekkor – mivel m páratlan – a 2.7. Tétel miatt $(2^{2^k})^m + 1^m$ osztható $2^{2^k} + 1$-gyel, ami 1-nél nagyobb, így N nem prímszám. Ezek szerint n-nek nem lehetnek páratlan prímtényezői. □

A következő tétel arra ad szükséges (de ezúttal sem elégséges) feltételt, hogy egy $2^n - 1$ alakú szám prím lehessen:

7.14. Tétel. *Egy $2^n - 1$ alakú szám csak úgy lehet prím, ha az n kitevő prímszám.*

Bizonyítás. Indirekt bizonyítjuk: belátjuk, hogy ha n összetett szám, akkor $2^n - 1$ is összetett.

Ha n összetett, akkor például $n = ab$, ahol $a, b \geq 1$, tehát $2^a \geq 2$, $2^b \geq 2$.

Ezt felhasználva $2^n-1 = 2^{ab}-1 = (2^a)^b-1^b$. Tudjuk azonban (2.7. Tétel), hogy így $2^a - 1 \mid (2^a)^b - 1^b = 2^n - 1$.

Ekkor viszont 2^n-1 nem lehet prím, hiszen $2^a-1 \geq 2$, vagyis (2^n-1)-nek valódi osztója. □

Megjegyzés. A $2^p - 1$ alakú számokat (ahol p prím) Mersenne francia matematikus (1588–1648) után *Mersenne-féle számoknak,* az ilyen alakú prímeket *Mersenne-prímeknek* nevezik. Az első néhány Mersenne-szám:

p	2	3	5	7	11	13
2^p-1	3	7	31	127	2047	8191
	prím	prím	prím	prím	nem prím	prím
					$23 \cdot 89$	

’

Pillanatnyilag összesen 44 Mersenne-prím ismert, a legnagyobbnak 9 808 358 számjegye van. Megoldatlan kérdés, hogy van-e végtelen sok Mersenne-prím.

Végül a számelmélet egyik leghíresebb megoldatlan problémáját említjük meg, az úgynevezett Goldbach-sejtést (amely Goldbach (1690–1764) német matematikusnak egy Eulerhez írt leveléből származik):

Sejtés (Goldbach). *Minden 2-nél nagyobb páros szám előáll két prím összegeként, és minden 5-nél nagyobb páratlan szám előáll három prím összegeként.*

Megjegyzés. Nyilván elég az állítás első felét bizonyítani, abból már következik a második. Ha ugyanis a 2-nél nagyobb páros számok mindegyikéhez hozzáadunk 3-at, akkor megkapjuk az összes 5-nél nagyobb páratlan számot, és ha egy páros számot már előállítottunk két prímszám összegeként, akkor a nála 3-mal nagyobb páratlan számot megkaphatjuk e két prím és a 3 (ami szintén prím), vagyis három prím összegeként.

Napjainkig igen sok jelentős részeredmény született a Goldbach-sejtéssel kapcsolatban.

Részletesebben lásd például Klopfer Ervin: Goldbach sejt ... és?, Informatika, Scientific review of the Dennis Gabor college, ISSN: 1419-2527, 2010, 35.szám, http://www.gdf.hu/node/635, http://www.gdf.hu/sites/default/files/informatika_35_3.pdf

További érdekességek olvashatók a prímszámokról az interneten, például: http://hu.wikipedia.org/wiki/Prímszámok_listája

Titkosítás

Manapság a prímszámok legfontosabb alkalmazási területe a számítógépes titkosítás elmélete.

http://hu.wikipedia.org/wiki/RSA-eljárás

http://vassanyi.ginf.hu/info/rsa/primek.html

A titkosításhoz használt algoritmusok „nagy” prímeket használnak, ugyanakkor újabb és újabb algoritmusokat keresünk egy szám prímtényezős felbontásának meghatározására.

Erre szolgálnak a prímtesztek.

http://hu.wikipedia.org/wiki/Prímteszt

Feladatok

1. Igazolja, hogy végtelen sok $6k - 1$ alakú prímszám van!
2. Igazolja, hogy tetszőleges prímszám 30-cal osztva 1-et vagy prímszámot ad maradékul!
3. A 7.11. Tétel milyen nagyságrendi becslést ad a prímszámok számára 10^2-ig; 10^3-ig; 10^4-ig; 10^5-ig; 10^6-ig; 10^9-ig; 10^{12}-ig?
4. Keresse meg az első 50 szerencsés számot! (Definíció a 83. oldalon.)

8. fejezet

Kongruencia

A korábbiakban – a maradékos osztás, illetve az oszthatósági szabályok tárgyalása során (ld. a 3.2. Megjegyzést) – már felmerült, hogy célszerű lenne külön jelölést bevezetni arra, hogy két szám ugyanazt a maradékot adja valamivel osztva.

8.1. Definíció. Legyen a és b tetszőleges egész szám, $m \geq 2$ egész szám. Azt mondjuk, hogy a *kongruens* b*-vel modulo* m, ha a és b ugyanazt a maradékot adja m-mel osztva.

8.1. Jelölés. $a \equiv b \pmod{m}$ vagy rövidebben: $a \equiv b\ (m)$

Azt, hogy a és b nem kongruensek (inkongruensek) modulo m, így jelöljük: $a \not\equiv b \pmod{m}$.

Például:	$3 \equiv 23 \pmod{10}$,	de	$3 \not\equiv 4 \pmod{10}$
	$3 \equiv -7 \pmod{10}$		$3 \not\equiv -3 \pmod{10}$
	$3 \equiv 23 \pmod{5}$		$3 \not\equiv 7 \pmod{5}$
	$3 \equiv 8 \pmod{5}$		$3 \not\equiv 8 \pmod{10}$

Megjegyzés. Az $m \geq 2$ kikötésnek valójában nincs különösebb jelentősége, de ha tetszőleges egész szám lehetne a modulus, akkor

1. $a \equiv b \pmod{m}$ ugyanakkor teljesül, mint $a \equiv b \pmod{-m}$;
2. tetszőleges a-ra $a \equiv 0 \pmod{1}$ (ami meglehetősen semmitmondó); valamint
3. az $a \equiv b \pmod{0}$ eset csak akkor lenne lehetséges, ha $a = b$. (Ez tehát maga az egynlőség, és – mint majd látni fogjuk –, a kongruencia bizonyos értelemben ugyanolyan típusú reláció, mint az egyenlőség.)

Emiatt elegendő az $m > 1$ modulusokkal foglalkoznunk.

Gyakran kényelmesebb a kongruencia egy másik definíciójával dolgoznunk:

8.2. Definíció. Legyen $m \geq 2$. Azt mondjuk, hogy a és b kongruens modulo m ($a \equiv b \pmod{m}$), ha $m \mid a - b$.

Csak akkor van jogunk két definíciót is használni egy fogalomra, hogyha mindkettő ugyanazt jelenti.

8.1. Tétel. *A kongruenciára adott 8.1. és 8.2. Definíciók ekvivalensek egymással.*

Bizonyítás. Osszuk a-t és b-t maradékosan m-mel.

$$\begin{aligned} a &= mq_1 + r_1, \quad \text{ahol} \quad 0 \leq r_1 < m, \quad \text{illetve} \\ b &= mq_2 + r_2, \quad \text{ahol} \quad 0 \leq r_2 < m. \end{aligned}$$

Ekkor $a - b = m(q_1 - q_2) + r_1 - r_2$.

1. 8.1. $\Rightarrow$ 8.2.

Az első definíció szerint $a \equiv b \pmod{m}$ azt jelenti, hogy $r_1 = r_2$. Ekkor $r_1 - r_2 = 0$, vagyis $a - b = m(q_1 - q_2)$, így $m \mid a - b$ teljesül.

2. 8.2. $\Rightarrow$ 8.1.

Tegyük most fel, hogy a második definíció szerint $m \mid a-b$. Ekkor $a-b = m(q_1 - q_2) + r_1 - r_2$ miatt $m \mid r_1 - r_2$, ami $0 \leq r_1 < m$ és $0 \leq r_2 < m$ miatt csak úgy teljesülhet, ha $r_1 - r_2 = 0$, vagyis ha $r_1 = r_2$, azaz a-nak és b-nek az m szerinti maradéka ugyanannyi. Ez pedig az első definíciónak felel meg. □

Megjegyzés. A kongruencia fogalmának felhasználásával a 3.4. Tétel (a t alapú számrendszerben megfogalmazott oszthatósági szabályok) a következő formában írható:

Az $A = \sum_{i=0}^{n} a_i t^i$ számra a következők teljesülnek:

(i) Ha $d \mid t^k$, akkor $A \equiv \sum_{i=0}^{k-1} a_i t^i \pmod{d}$

(ii) Ha $d \mid t - 1$, akkor $A \equiv \sum_{i=0}^{n} a_i \pmod{d}$

(iii) Ha $d \mid t+1$, akkor $A \equiv \sum_{i=0}^{n}(-1)^n a_i \pmod{d}$.

Rögzített modulus mellett a kongruencia kétváltozós (binér) reláció. Vizsgáljuk meg, hogy milyen tulajdonságai vannak a kongruenciarelációnak.

8.2. Tétel. *Tetszőleges a, b, c -re és rögzített $m(>1)$-re*

1. $a \equiv a \pmod{m}$ *(reflexív)*
2. *ha* $a \equiv b \pmod{m}$, *akkor* $b \equiv a \pmod{m}$ *(szimmetrikus)*
3. *ha* $a \equiv b \pmod{m}$ *és* $b \equiv c \pmod{m}$, *akkor* $a \equiv c \pmod{m}$. *(tranzitív)*

Megjegyzés. Ezek a tulajdonságok az *egyenlőség* relációra is teljesülnek, az ilyen tulajdonságokkal rendelkező relációt neveztük ekvivalenciarelációnak.

Bizonyítás. 1. a ugyanazt a maradékot adja bármivel osztva, mint a.

2. Ha a ugyanazt a maradékot adja m-mel osztva, mint b, akkor b nyilván ugyanazt a maradéklot adja m-mel osztva, mint a.

3. Ha a ugyanazt a maradékot adja m-mel osztva, mint b, és b ugyanazt a maradékot adja m-mel osztva, mint c, akkor nyilván c ugyanazt a maradékot adja m-mel osztva, mint a. □

Megjegyzés. Az, hogy a kongruencia ekvivalenciareláció azt jelenti, hogy ha egy-egy halmazba gyűjtjük azokat a számokat, amelyek egy adott modulusra nézve kongruensek egymással (ugyanazt a maradékot adják m-mel osztva), akkor megkapjuk az egész számok egy osztályozását (vagyis ezzel az egész számok halmazát szétbontjuk közös elemet nem tartalmazó, nem üres részhalmazokra).

Például: (mod 2) egy osztályba kerülnek azok a számok, amelyek 0-t adnak maradékul 2-vel osztva (párosak), egy másik osztályba pedig azok, amelyek 1-et adnak maradékul 2-vel osztva (páratlanok).

(mod 3) három osztályt kapunk: az egyikben a $3k$, egy másikban a $3k+1$, a harmadikban pedig a $3k+2$ alakú számok lesznek.

Általában (mod m) éppen m osztályt kapunk, mert a számok m-mel osztva m-féle maradékot adnak: 0-t, 1-et, 2-t, ..., $m-1$-et.

Ha például (mod 8) végezzük el a számok osztályozását, a következő táblázatban az egy oszlopban szereplő számok kerülnek egy osztályba:

$\dots$	$\dots$	-14	-13	-12	-11	-10	-9
-8	-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	$\dots$

Általában (mod m):

	$\dots$	$-2m+2$	$\dots$	$-m-2$	$-m-1$
$-m$	$-m+1$	$-m+2$	$\dots$	-2	-1
0	1	2	$\dots$	$m-2$	$m-1$
m	$m+1$	$m+2$	$\dots$	$2m-2$	$2m-1$
$2m$	$2m+1$	$2m+2$	$\dots$	$3m-2$	$3m-1$
$3m$	$3m+1$	$3m+2$	$\dots$	$\dots$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
(km)	$(km+1)$	$(km+2)$	$\dots$	$(km+m-2)$	$(km+m-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Itt az osztályok az egy oszlopba sorolt elemek.

Az, hogy az egy oszlopba (osztályba) tartozó számok ugyanazt a maradékot adják m-mel osztva azt is jelenti, hogy ha mi az egész osztályról szeretnénk nyilatkozni, akkor mindegy, hogy melyik elemét említjük, melyik eleméről nevezzük el az osztályt. Például (mod 8) az, hogy a „3 osztálya”, ugyanazt jelenti, mint a „19 osztálya” vagy a „-5 osztálya”. (Hasonló a helyzet ahhoz, mint amikor iskolai osztályokról – vagy bármilyen más ekvivalenciaosztályokról – beszélünk; ha Kiss Pista és Nagy Jóska egy osztályba járnak, akkor „az az osztály, ahova Kiss Pista jár”, ugyanazt az osztályt jelenti, mint az „az az osztály, ahova Nagy Jóska jár”.)

A kongruenciareláció által létrehozott ekvivalenciaosztályokat *maradékosztályoknak* nevezzük, azt az elemet pedig, amelyikkel az osztályt jellemezzük, az illető osztály *reprezentáns elemének.* Mint láttuk, bármelyik osztály, bármelyik elemével reprezentálható.

8.3. Definíció. Azoknak az elemeknek a halmazát, amelyek (mod m) kongruensek a-val, az *a elem által reprezentált m* szerinti (vagy (mod m)) *maradékosztálynak* nevezzük.

Megjegyzés. A kongruenciareláció fogalma – mint ezt később látni fogjuk – általánosabban is definiálható.

Általában egy halmazon értelmezett ekvivalenciarelációt akkor szokás kongruenciarelációnak hívni (az általa létrehozott ekvivalenciaosztályokat pedig maradékosztályoknak), ha a halmazon értelmezett műveletekre teljesül, hogy akárhogy választunk ki az a-val, valamint a b-vel reprezentált osztályokból egy-egy elemet, a rajtuk elvégzett művelet eredménye mindig ugyanabban az osztályban lesz, vagyis a művelet eredménye – abból a szempontból, hogy melyik osztályban lesz az eredmény – független a reprezentáns elemek megválasztásától.

Jelöljük például $\circ$-rel a műveletet, $\sim$-mal az kongruenciarelációt. A fenti tulajdonságot így fogalmazhatjuk meg: Ha $a_1 \sim b_1$ és $a_2 \sim b_2$, akkor $a_1 \circ a_2 \sim b_1 \circ b_2$.

Láttunk már ilyesmit a 2.9. Tételben, amikor azt fogalmaztuk meg, hogy $a + b$ (valamint $a - b$, illetve $a \cdot b$) ugyanazt a maradékot adja m-mel osztva, mint a maradékaik összege (különbsége, szorzata), akkor valójában azt állapítottuk meg, hogy $a \sim r_a$ és $b \sim r_b$ esetén $a + b \sim r_a + r_b$, illetve $a - b \sim r_a - r_b$ és $a \cdot b \sim r_a \cdot r_b$.

Azt, hogy az egész számokon értelmezett kongruenciareláció ebben az általánosabb értelemben is kongruenciareláció, a következő tétel biztosítja:

8.3. Tétel. *Ha* $a \equiv b \pmod{m}$ *és* $c \equiv d \pmod{m}$, *akkor*

(i) $a \pm c \equiv b \pm d \pmod{m}$ *és*

(ii) $ac \equiv bd \pmod{m}$.

Bizonyítás. Ha $a \equiv b \pmod{m}$, akkor $m \mid a - b$, és ha $c \equiv d \pmod{m}$, akkor $m \mid c - d$.

Ekkor viszont:

(i) $m \mid (a-b) \pm (c-d) = (a+c) \mp (b+d)$, vagyis $a \pm c \equiv b \pm d \pmod{m}$.

(ii) $m \mid (a-b)c + (c-d)b = ac - bd$, vagyis $ac \equiv bd \pmod{m}$. □

Megjegyzés. Ebből a tételből már következik a 2.9. Tétel is. Ez azonban általánosabb annál.

8.1. Megjegyzés. Az, hogy a művelet eredménye tetszőlegesen megadott két (nem feltétlenül különböző) osztály esetén a reprezentáns elemek megválasztásától függetlenül mindig ugyanabban az osztályban lesz, lehetőséget ad arra, hogy magukon a maradékosztályokon értelmezzünk műveleteket, a következő módon:

Jelöljük $\bar{a}$-val az a elem, $\bar{b}$-vel a b elem által reprezentált maradékosztályt. Ekkor a két maradékosztály összegén az $a+b$, szorzatán pedig az $a \cdot b$ maradékosztályát értjük. Vagyis:

$$\bar{a} \oplus \bar{b} := \overline{a+b} \qquad \text{(összeadás) és}$$
$$\bar{a} \otimes \bar{b} := \overline{a \cdot b} \qquad \text{(szorzás)}$$

Könnyen belátható, pontosabban visszavezethető a reprezentánsokra érvényes műveleti tulajdonságokra, hogy tetszőleges modulus esetén a (mod m) maradékosztályok így definiált összeadása kommutatív, asszociatív és invertálható, a szorzása kommutatív és asszociatív, továbbá a szorzás disztributív az összeadásra nézve – vagyis a maradékosztályok kommutatív, egységelemes gyűrűt alkotnak (az egységelem mindig az 1 által reprezentált maradékosztály).

Nézzünk meg néhány példát egy-egy ilyen maradékosztály-gyűrűre!

Az alaphalmaz tehát mindig a maradékosztályok $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$ halmaza az éppen aktuális (mod m) modulusra nézve, a két művelet pedig a fent definiált összeadás és szorzás:

(mod 2)

$\oplus$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\otimes$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

(mod 3)

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

(mod 4)

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(mod 5)

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(mod 6)

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(mod 7)

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

A táblázatokról önmagukban is sok érdekesség leolvasható. Észrevehetjük, hogy a (mod 4) vagy (mod 6) maradékosztály-gyűrű nem integritástartomány, hiszen nem zérusosztómentes: modulo 4 szerint $\bar{2} \otimes \bar{2} = \bar{0}$, modulo 6 szerint pedig például $\bar{2} \otimes \bar{3} = \bar{0}$. (Hasonló a helyzet minden olyan modulus esetén, amely összetett szám, hiszen olyankor m felírható $m = ab$ alakban, ahol a és b valódi osztók ($1 < a, b < m$), tehát egyikük sem a $\bar{0} = \bar{m}$ maradékosztályt képviseli, és ilyenkor $\bar{a} \otimes \bar{b} = \bar{0}$.)

A szorzás táblázatokról leolvasható, hogy mely elemek (maradékosztályok) osztói melyeknek. (Most akkor mondjuk, hogy $\bar{a} \mid \bar{b}$, ha $\exists \bar{q}$, amelyre $\bar{a} \otimes \bar{q} = \bar{b}$.) Ha kíváncsiak vagyunk, hogy egy elem mely elemeknek az osztója, csak a sorát (vagy az oszlopát) kell végignéznünk, abban fel van sorolva az összes többszöröse. Például modulo 6 szerint a $\bar{4}$ osztója a $\bar{2}$-nek, hiszen $\bar{4} \otimes \bar{2} = (\bar{4} \otimes \bar{5} =)\bar{2}$.

Különösen érdekesek azok az elemek, amelyeknek a sorában (illetve oszlopában) az összes elem előfordul. Ezek ugyanis az összes elemnek osztói, tehát egységek. Ilyen például modulo 6 az $\bar{1}$ és az $\bar{5}(= -\bar{1})$, ami még nem olyan meglepő, de például modulo 5 vagy modulo 7 a $\bar{0}$ kivételével az összes maradékosztály. (A fenti táblázatokból nem derül ki, de modulo 10 az 1, a 3, a 7 és a 9 által reprezentált maradékosztályok lesznek az egységek, ami azt is jelenti, hogy éppen az ezekben a maradékosztályokban szereplő számok azok, amelyeknek a többszörösei között tízes számrendszerben minden lehetséges jegyvégződés előfordul.) Sejthető, hogy általában modulo m azok a maradékosztályok lesznek az egységek, amelyeket a modulushoz relatív prím elemek képviselnek. Ezek részletesebb tanulmányozására később visszatérünk. (8.3. Megjegyzés.)

Megjegyzés. Érdemes a 8.3. Tétel néhány speciális esetével, illetve következményével külön is foglalkoznunk:

(1) Ha $a \equiv b \pmod{m}$, akkor tetszőleges c-re

(i) $a + c \equiv b + c \pmod{m}$ és

(ii) $ac \equiv bc \pmod{m}$. (Ez éppen a tétel állítása a $d = c$ esetben.)

(2) Ha $a \equiv b \pmod{m}$, akkor tetszőleges k-ra $a \equiv b + km \pmod{m}$, (hiszen minden k egész számra $0 \equiv km \pmod{m}$.)

(3) Ha $a \equiv b \pmod{m}$, akkor tetszőleges $n \in \mathbb{N}$-re $a^n \equiv b^n \pmod{m}$. (A tétel második állításának ismételt alkalmazásával adódik a $c = a$ és $d = b$ esetben.)

(4) A 2.7. Tétel első állítását, miszerint $\forall\ a, b$-re $a - b \mid a^n - b^n$ szintén beláthatjuk ugyanennek a tételnek a segítségével.

Nyilván $a - b \equiv 0 \pmod{a - b}$. Ekkor $a \equiv b \pmod{a - b}$, így (3) miatt $a^n \equiv b^n \pmod{a - b}$. Ez viszont a kongruencia 8.2. Definíciója szerint éppen azt jelenti, hogy $a - b \mid a^n - b^n$. (Korábban, a 2.7. Tételben persze ennél többet is beláttunk, nevezetesen azt, hogy az $a^n - b^n$ algebrai kifejezés osztható az $a - b$ algebrai kifejezéssel.)

Megjegyzés. A 8.3. Tétel megfordítása nyilván nem igaz (azaz $a \pm c \equiv b \pm d$-ből vagy $ac \equiv bd$-ből nem következtethetünk arra, hogy $a \equiv b$ és $c \equiv d$). Vegyük észre azonban, hogy az (1)(i) következmény állítása megfordítható:

(i) Ha $a + c \equiv b + c \pmod{m}$, akkor $a \equiv b \pmod{m}$, hiszen $c \equiv c \pmod{m}$, ezért $a + c - c \equiv b + c - c \pmod{m}$.

(Az (ii) állítás megfordítása nem igaz. Abból, hogy $ac \equiv bc \pmod{m}$, *nem* következik $a \equiv b \pmod{m}$. Például $9 \cdot 2 \equiv 5 \cdot 2 \pmod{8}$, de $9 \not\equiv 5 \pmod{8}$.)

Igaz viszont a következő:

8.4. Tétel. *Ha* $ac \equiv bc \pmod{m}$, *akkor* $a \equiv b \left(\mod \dfrac{m}{(c, m)}\right)$.

Bizonyítás. Legyen $(c, m) = d$. Ekkor c, illetve m a következő alakba írható: $c = c'd$, illetve $m = m'd$, ahol $(c, m') = 1$. Ha $ac \equiv bc \pmod{m}$, akkor $m \mid ac - bc$, vagyis $m'd \mid (a - b)c'd$. d nem 0, ezért a 2.1. Következmény alapján $m' \mid (a - b)c'$. Mivel $(m', c') = 1$, ez csak úgy lehetséges, (lásd 4.4 1. állítása), ha $m' \mid (a - b)$, vagyis $a \equiv b \pmod{m'}$ ahol $m' = \dfrac{m}{(c, m)}$. $\square$

Például $9 \cdot 2 \equiv 5 \cdot 2 \pmod{8}$, ebből következik, hogy $9 \equiv 5 \pmod{4}$.

Megjegyzés. Speciálisan, ha c és m relatív prímek, akkor a tétel így szól:

Ha $ac \equiv bc \pmod{m}$ és $(c, m) = 1$, akkor $a \equiv b \pmod{m}$.

Megjegyzés. A (2) következmény megfordítása nyilvánvalóan igaz.

A (3) következmény megfordítása nem igaz. (Például $2^2 \equiv (-2)^2 \pmod{10}$, de $2 \not\equiv -2 \pmod{10}$.)

Az eddigiekben többször képviseltettünk a maradékosztályokat egy-egy elemükkel. Ez a későbbiekben is hasznos lesz, ezért bevezetünk egy fogalmat erre.

8.4. Definíció. Az $a_1, a_2, a_3, \ldots$ számok halmazát *modulo m teljes maradékrendszer*nek nevezzük, ha közöttük minden m szerinti maradékosztályból *pontosan* egy elem szerepel.

Például: modulo 10 teljes maradékrendszert alkotnak a következő számhalmazok:

$\{33, 12, -3, 1, 100, 28, -11, 6, -55, 1004\}$ vagy

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ (legkisebb pozitív maradékrendszer)

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (legkisebb nem negatív maradékrendszer)

$\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$, illetve

$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4\}$ (legkisebb abszolút értékű maradékrendszerek).

Nem alkotnak (mod 10) teljes maradékrendszert: $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (a $\bar{0}$ osztály nincs képviselve) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ (a $\bar{0}$ osztályból két elem is szerepel).

8.5. Tétel. *Az $a_1, a_2, a_3, \ldots$ számok akkor és csak akkor alkotnak teljes maradékrendszert az m modulus szerint, ha*

(a) számuk pontosan m, és

(b) közülük bármelyik kettő inkongruens modulo m.

Bizonyítás. A bizonyítás két lépésből áll. Először bebizonyítjuk, hogy az adott feltétel szükséges, majd azt, hogy elégséges is.

1. lépés: a feltétel szükséges.

Ha az adott számok teljes maradékrendszert alkotnak m szerint, akkor minden maradékosztályból pontosan egy elem szerepel köztük. A maradékosztályok száma m, így éppen m elem kell ahhoz, hogy minden osztály pontosan egyszer legyen képviselve. Mivel pedig semelyik osztályból nem szerepel két elem, közülük bármelyik kettő inkongruens.

2. lépés: a feltétel elégséges.

Ha m szám közül bármelyik kettő inkongruens modulo m, akkor semelyik kettő nincs egy maradékosztályban. Mivel a számuk megegyezik az m szerinti maradékosztályok számával, és semelyik osztályból sincs két elem, ez csak úgy lehetséges, ha minden osztályból pontosan egy szerepel közöttük, vagyis ha teljes maradékrendszert alkotnak. □

8.2. Megjegyzés. A tétel ismeretében figyeljük meg, hogy ha bizonyos változtatásokat végzünk egy m szerinti teljes maradékrendszeren, milyen feltételek mellett kaphatunk újra teljes maradékrendszert!

Mivel egy m szerinti teljes maradékrendszer elemszáma m, ezen nem változtathatunk. Nyilván nem hagyhatunk el és nem vehetünk hozzá elemeket. Az nem nagy trükk – bár nyilván megengedhető –, hogy kicserélünk egy elemet egy vele kongruensre, hiszen ekkor változatlanul ugyanazok az osztályok lesznek képviselve, csak az illető osztályt egy másik eleme fogja képviselni.

Ennél merészebb lépés, hogy a teljes maradékrendszer minden eleméhez hozzáadjuk ugyanazt az egész számot.

Például 10 szerint teljes maradékrendszert alkotnak a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 számok. Hozzájuk adva b-t, a következőket kapjuk: $0+b$, $1+b$, $2+b$, $3+b$, $4+b$, $5+b$, $6+b$, $7+b$, $8+b$, $9+b$.

Ezek az elemek szám szerint megvannak, és semelyik kettő sem lehet kongruens, mert $a_1+b \equiv a_2+b \pmod{10}$ azt jelentené, hogy $a_1 \equiv a_2 \pmod{10}$, vagyis ez is teljes maradékrendszer lesz.

Ez b értékétől függően a következő maradékosztályokat jelenti (b-t nyilván csak a 10 szerinti maradéka alapján kell vizsgálnunk):

$b=0:$	0,	1,	2,	3,	4,	5,	6,	7,	8,	9
$b=1:$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$b=2:$	2,	3,	4,	5,	6,	7,	8,	9,	10,	11
$b=3:$	3,	4,	5,	6,	7,	8,	9,	10,	11,	12
$b=4:$	4,	5,	6,	7,	8,	9,	10,	11,	12,	13
$b=5:$	5,	6,	7,	8,	9,	10,	11,	12,	13,	14
$b=6:$	6,	7,	8,	9,	10,	11,	12,	13,	14,	15
$b=7:$	7,	8,	9,	10,	11,	12,	13,	14,	15,	16
$b=8:$	8,	9,	10,	11,	12,	13,	14,	15,	16,	17
$b=9:$	9,	10,	11,	12,	13,	14,	15,	16,	17,	18

Könnyen ellenőrízhető, hogy minden esetben teljes maradékrendszert kaptunk, csak a képviselt maradékosztályok felsorolási sorrendje változott meg. Az is könnyen meggondolható, hogy $k = 10$-re megint az eredeti sorrendet kapnánk, csak éppen minden maradékosztályt egy 10-zel nagyobb szám képviselne.

Fogalmazzuk meg általánosan ezt a megfigyelésünket.

8.6. Tétel. *Ha az $a_1, a_2, a_3, \ldots, a_m$ számok teljes maradékrendszert alkotnak modulo m, akkor tetszőleges $b \in \mathbb{Z}$ esetén az $a_1+b, a_2+b, a_3+b, \ldots, a_m+b$ számok is teljes maradékrendszert alkotnak m szerint.*

Bizonyítás. Mivel az $a_1 + b, a_2 + b, a_3 + b, \ldots, a_m + b$ számok darabszáma m, elegendő azt bizonyítani, hogy közülük bármelyik kettő inkongruens m szerint. Ez pedig igaz, hiszen ha volna köztük kettő, amelyre $a_i + b \equiv a_j + b \pmod{m}$ (ahol $i \neq j$) teljesülne, akkor b-t levonva mindkét oldalból, azt kapnánk, hogy: $a_i \equiv a_j \pmod{m}$, ami ellentmondana annak, hogy eredetileg egymással inkongruensek voltak az elemek, vagyis hogy teljes maradékrendszerből indultunk ki. □

Tehát egy teljes maradékrendszer minden eleméhez hozzáadhatjuk ugyanazt a számot.

Azt tapasztaltuk tehát, hogy a teljes maradékrendszer minden elemét ugyanazzal a számmal növelve ismét teljes maradékrendszert kapunk. Felmerül a kérdés, hogy vajon mi a helyzet akkor, ha egy m szerinti teljes maradékrendszer minden elemét megszorozzuk egy (egész) számmal? Például a 10 szerinti 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 teljes maradékrendszer minden elemét c-vel szorozva a következőket kapjuk (c-t csak kongruencia erejéig tekintjük különbözőnek):

$c=0:$	0,	0,	0,	0,	0,	0,	0,	0,	0,	0
$c=1:$	0,	1,	2,	3,	4,	5,	6,	7,	8,	9
$c=2:$	0,	2,	4,	6,	8,	10,	12,	14,	16,	18
$c=3:$	0,	3,	6,	9,	12,	15,	18,	21,	24,	27
$c=4:$	0,	4,	8,	12,	16,	20,	24,	28,	32,	36
$c=5:$	0,	5,	10,	15,	20,	25,	30,	35,	40,	45
$c=6:$	0,	6,	12,	18,	24,	30,	36,	42,	48,	54
$c=7:$	0,	7,	14,	21,	28,	35,	42,	49,	56,	63
$c=8:$	0,	8,	16,	24,	32,	40,	48,	56,	64,	72
$c=9:$	0,	9,	18,	27,	36,	45,	54,	63,	72,	81

Megállapíthatjuk, hogy $c = 0, 2, 4, 5, 6, 8$ esetben nem kaptunk teljes maradékrendszert, míg $c = 1, 3, 7, 9$ esetén igen. Ez utóbbiak éppen azok a szorzók, amelyek relatív prímek a 10-hez (vagyis a modulushoz).

Nem nehéz meggondolni (a 8.4. Tétel alapján), hogy modulo 10 olyan c szorzók esetén kapunk teljes maradékrendszert, amelyek többszörösei között mindenféle jegyvégződés előfordul. Hiszen ha $(c, 10) = 1$, akkor $ac \equiv bc$ (mod m)-ből következik, hogy $a \equiv b \pmod m$ (és visszafelé is teljesül, hogy $a \equiv b \pmod m$-bők következik, hogy $ac \equiv bc \pmod m$). (Vagyis a modulushoz relatív prímmel szorozva a maradkérendszer tagjait, pontosan akkor esik egy osztályba két szorzás után kapott maradék, ha eredetileg is egybeestek.)

Általában egy m modulus esetén akkor kapunk egy teljes maradékrendszerből szorzással ismét teljes maradékrendszert, ha a c szorzó többszörösei között az összes lehetséges m-mel való osztási maradék előfordul. Ez pedig azokra a c számokra teljesül, amelyek relatív prímek a modulushoz.

8.7. Tétel. *Ha az $a_1, a_2, a_3, \ldots, a_m$ számok teljes maradékrendszert alkotnak az m modulus szerint, és $c \in \mathbb{Z}$-re $(c, m) = 1$, akkor az $a_1c, a_2c, a_3c, \ldots, a_mc$ számok is teljes maradékrendszert alkotnak m szerint.*

Bizonyítás. Mivel az $a_1c, a_2c, a_3c, \ldots, a_mc$ elemek darabszáma nyilván m, most is elég azt megmutatnunk, hogy közülük bármelyik kettő inkongruens (mod m). Ez pedig teljesül, hiszen ha $a_ic \equiv a_jc \pmod m$ lenne, akkor mivel $(c, m) = 1$, ebből a 8.4. Tétel értelmében $a_i \equiv a_j \pmod m$ következne, ami ellentmondana annak, hogy teljes maradékrendszerből indultunk ki. □

A tételt kiegészíthetjük azzal, hogy másfajta c szorzó esetén nem kaptunk teljes maradékrszendszert.

8.8. Tétel. *Ha az $a_1, a_2, a_3, \ldots, a_m$ számok teljes maradékrendszert alkotnak (*mod m*), és $c \in \mathbb{Z}$-re $(c, m) \neq 1$, akkor az $a_1c, a_2c, a_3c, \ldots, a_mc$ számok nem alkotnak teljes maradékrendszert m szerint. (Egyébként semmilyen modulus szerint sem.)*

Bizonyítás. Először is szögezzük le, hogy a $\bar{0} \cdot c \equiv 0 \pmod{m}$.

Legyen $(m, c) = d \neq 1$. Ekkor $\frac{m}{d} = m_1$ és $\frac{c}{d} = c_1$ egész számok. $m_1 \cdot c = m_1 \cdot d \cdot c_1 = m \cdot c_1$, így $m_1 c \equiv 0 \pmod{m}$, holott $m_1 \not\equiv 0$, mert $m_1 < m$, de nem 0.

Azt kaptuk tehát, hogy két különböző osztályba tartozó reprezentás c-vel való szorzata is a 0 osztályába esik. Így a teljes maradékrendszer c-szerese nem alkot teljes maradékrendszert m szerint. Mivel pedig m eleme van, más modulus szerint sem teljes maradékrendszer. □

Tudjuk, hogy egy maradékosztály elemei m-mel osztva ugyanazt a maradékot adják. Ennél azonban több is mondható. Nevezetesen az, hogy az ugyanahhoz a maradékosztályhoz tartozó elemek m-mel vett legnagyobb közös osztója ugyanannyi:

8.9. Tétel. *Ha* $a \equiv b \pmod{m}$, *akkor* $(a, m) = (b, m)$.

Bizonyítás. Azt fogjuk bebizonyítani, hogy a-nak m-mel vett legnagyobb közös osztója egyenlő a-nak m szerinti maradékának és m-nek legnagyobb közös osztójával. Ebből már következik, hogy a osztályában minden elemre teljesül ez a tulajdonság, ezért mindegyik elem m-mel vett legnagyobb közös osztója ugyanannyi.

Legyen $a = q_1 m + r_1$. Nyilvánvaló, hogy a és r_1 ugyanabba a maradékosztályba esnek. Ha $r_1 = 0$, akkor ez a $\bar{0}$ maradékosztály, és minden eleme m-mel vett legnagyobb közös osztója m.

Ha $r_1 \neq 0$, akkor használjuk az euklideszi algoritmust a legnagyobb közös osztó kiszámításához. Ennek az első osztása: $a = q_1 m + r_1$ ($r_1 \neq 0$ miatt folytatódik), a második osztása $m = q_2 r_1 + r_2$. Ez viszont éppen az (m, r_1) kiszámításához vezető euklideszi algoritmus első osztása. Ezek szerint ugyanahhoz a legnagyobb közös osztóhoz vezet mindkét algoritmus: $(a, m) = (r_1, m)$. □

Megjegyzés. Más gondolatmenettel is bebizonyítható a tétel állítása. Legyen $a \equiv b \pmod{m}$. Ekkor $a = a_1 m + q$, $b = b_1 m + q$ (m-mel osztva ugyanazt a maradékot adják). Ebből $a - a_1 m = q$. a és m legnagyobb közös osztója nyilván osztója a bal oldalon minden tagnak, így a jobb oldalon álló q-nak is osztója. Másrészt viszont a $b = b_1 m + q$ összefüggésben a jobb oldalon álló tagoknak osztója, hiszen osztója m-nek is és q-nak is, tehát osztója a bal oldalon álló b-nek is.

Azt kaptuk, hogy (a, m) osztója b-nek, így (b, m)-nek is. Fordított szereposztással viszont az adódik, hogy $(b, m) \mid (a, m)$, amiből $(a, m) = (b, m)$.

Megjegyzés. A tétel megfordítása (vagyis hogy ha két elemnek m-mel vett legnagyobb közös osztója egyenlő, akkor egy osztályba esnének) nyilván nem igaz. Ha a modulus 10, akkor például $(2, 10) = (6, 10) = 2$, de 2 és 6 nem esnek egy maradékosztályba 10 szerint.

Tételünk értelmében az egy maradékosztályban levő elemek mindegyikének ugyanaz a modulussal vett legnagyobb közös osztója.

8.1. Következmény. *Speciálisan: ha egy szám relatív prím a modulushoz, akkor ez az általa képviselt maradékosztály minden elemére jellemző tulajdonság. (Nem függ attól, hogy mely elemével reprezentáljuk az osztályt.)*

Ezért jogunk van egy teljes maradékosztályról azt mondani, hogy relatív prím a modulushoz (amennyiben egy tetszőleges reprezentánsa relatív prím hozzá).

8.5. Definíció. Az r elem által reprezentált maradékosztályt *redukált maradékosztály*nak nevezzük az m modulus szerint, ha $(r, m) = 1$.

8.3. Megjegyzés. Most már válaszolhatunk arra a korábbi kérdésünkre is, hogy a modulo m maradékosztály-gyűrűben miért éppen a redukált maradékosztályok lesznek az egységek. Ez azon múlik, hogy ha r relatív prím a modulushoz, akkor a 8.7. Tétel értelmében a 0, 1, 2, …, $m-1$ teljes maradékrendszer minden elemét megszorozva r-rel, ismét teljes maradékrendszert kapunk: 0, r, $2r$, $3r$, …, $(m-1)r$. Ez éppen azt jelenti, hogy a szorzás művelettáblázatában az $\bar{r}$ sorában (illetve oszlopában) – vagyis a többszörösei között – minden maradékosztály (pontosan egyszer) szerepel.

Ez egyszersmind azt is jelenti, hogy a redukált maradékosztályok sorában (oszlopában) pontosan egyszer szerepel az 1-es (is). Ebből az összefüggésből vezetjük le a következő tételt.

8.10. Tétel. (Wilson-tétel) *Minden p prímszám esetén*

$$(p-1)! \equiv -1 \pmod{p}$$

Bizonyítás. Ha $p = 2$, akkor $(p-1)! = 1$, ami valóban kongruens (-1)-gyel (mod 2).

Legyen $p > 2$. A $(p-1)$!-ban szereplő tényezők a 0 maradékosztályon kívül az összes többi. A prímszámok esetében ezek éppen a redukált maradékosztályok. Mint az imént láttuk, minden nem 0 maradékosztálynak van *inverz* maradékosztálya, tehát amellyel megszorozva 1-et ad. Mikor lesz egy maradékosztály inverze önmaga? $a^2 \equiv 1 \pmod{p}$-ből $a^2 - 1 = (a-1)(a+1) \equiv 0 \pmod{p}$, végső soron pedig $a \equiv 1$ vagy $-1 \pmod{p}$ következik.

Az 1 párja az 1, a (-1) párja a (-1) (ezek szorzata (-1)), a többi maradékosztálynak ezektől és önmaguktól különböző az inverze, az ilyen párok szorzata 1. Tehát ha mindet összeszorozzuk, akkor éppen (-1)-et kapunk. □

8.6. Definíció. Az $r_1, r_2, r_3, \ldots$ elemek halmazát $(\mathrm{mod}\ m)$ *redukált maradékrendszernek* nevezzük, ha minden redukált maradékosztályból pontosan egy szerepel közöttük.

Például: (mod 10) redukált maradékrendszerek a következők:
1, 3, 7, 9 $\qquad -1, 1, -3, 3 \qquad 1, -11, 27, -107$

nem redukált maradékrendszerek:
1, 2, 3, 4 (sem a 2, sem a 4 nem relatív prím a 10-hez)
1, 3, 7, -9 (az 1 ugyanabból az osztályból való, mint a -9)
1, -1, 3 (a 7 osztálya nincsen képviselve)

http://www.cs.elte.hu/~kfried/algebra1/RemainderSystem.jarEz a program megadja egy m számhoz egy redukált maradékrendszerét.

A redukált maradékrendszer minden eleme redukált maradékosztályból való. Így ha egyszer 4 relatív prímet találtunk a 10-hez, akkor minden redukált maradékrendszerében 4 elem lesz.

Ezért világos, hogy elemek egy halmaza akkor és csak akkor alkot redukált maradékrendszert a 10 modulus szerint, ha

- az elemek száma 4,
- minden elem relatív prím a 10-hez, és
- bármelyik két elem inkongruens egymással (mod 10).

Általában az m modulus szerinti redukált maradékrendszernek annyi eleme van, ahány redukált maradékosztály van (mod m); redukált maradékosztályból pedig annyi van, ahány elem például az $1, 2, \ldots, m-1, m$ teljes maradékrendszer elemei közül relatív prím a modulushoz.

8.2. Jelölés. $\varphi(m)$-mel jelöljük a $(\mathrm{mod}\ m)$ redukált maradékosztályok számát. (Ami nyilván megegyezik az $1, 2, \ldots, m-1, m$ számok közül az m-hez relatív prímek darabszámával.)

Például: $\varphi(10) = 4$, $\varphi(2) = 1$, $\varphi(9) = 6$, $\varphi(11) = 10$, $\varphi(30) = 8$, $\varphi(31) = 30$.

Megjegyzés. Azt, hogy egy adott m-hez hogyan lehet kiszámolni $\varphi(m)$ értékét, egy konkrét példán szemléltetjük:

Például $\varphi(120) =?$ Arra vagyunk kíváncsiak, hogy az 1, 2, ..., 118, 119, 120 számok közül hány relatív prím a 120-hoz. Nevezzük „rossz"-nak azokat a számokat, amelyek *nem* relatív prímek a 120-hoz, és számoljuk össze, hogy a fenti 120 darab szám közül hány „rossz". Egy szám akkor lesz „rossz", ha van közös prímosztója a 120-szal, vagyis

– ha páros – ilyenből 120-ig nyilván 60 van,
vagy – ha 3-mal osztható – ilyenből 120-ig (minden harmadik) 40 van,
vagy – ha 5-tel osztható – ilyenből 120-ig (minden ötödik) 24 van.

Ha most összeadjuk a „rosszak" imént kapott darabszámait, akkor a $60 + 40 + 24$ összegben kétszeresen számoltuk azokat, amelyek a 2, 3, 5 prímtényezők közül két prímmel is oszthatók, vagyis azokat, amelyek

– 2-vel is és 3-mal is (6-tal) oszthatók – ilyenből 20 van,
– 2-vel is és 5-tel is (10-zel) oszthatók – ilyenből 12 van;
– 3-mal is és 5-tel is (15-tel) oszthatók – ilyenből 8 van.

Ha most a fenti összegből levonjuk azoknak a darabszámát, amelyeket kétszeresen számoltunk, akkor a $60+40+24-(20+12+8)$ összegbe nincsenek beleszámolva azok a számok, amelyek 2-vel is, 3-mal is és 5-tel is oszthatók (az első lépésben háromszorosan számoltuk ezeket a számokat, majd a kétféle prímosztóval rendelkezők között is háromszor számoltuk meg ezeket, tehát a végső összeghez eddig háromszor adtuk hozzá, és háromszor vontuk ki a darabszámukat). Ilyen szám (30-cal osztható) 4 van 120-ig, ezek darabszámát még hozzá kell adnunk összegünkhöz.

Így azt kapjuk, hogy összesen $60+40+24-(20+12+8)+4 = 88$ „rossz" számunk van 120-ig. A 120 szám közül 88 nem relatív prím a 120-hoz, vagyis a maradék $120 - 88 = 32$ a relatív prímek száma. Vagyis $\varphi(120) = 32$.

8.4. Megjegyzés. Végső soron a 120 prímosztóihoz (2, 3, 5) a következőket csináltuk: 120 számból elhagyutnk $\frac{120}{2}$, $\frac{120}{3}$, $\frac{120}{5}$ számot, majd hozzávettünk $\frac{120}{2\cdot 3}$, $\frac{120}{2\cdot 5}$, $\frac{120}{3\cdot 5}$ számot, végül elhagytunk $\frac{120}{2\cdot 3\cdot 5}$ számot.

A kapott érték: $120 - 60 - 40 - 24 + 20 + 12 + 8 - 4 = 32$.

Ha tetszőleges n számot tekintettünk volna, amelynek az összes prímosztója $(p_1, p_2, \ldots, p_k)$, akkor a következő számolást kellett volna elvégeznünk:

$$n - \frac{n}{p_1} - \ldots - \frac{n}{p_k} + \frac{n}{p_1 \cdot p_2} + \ldots + \frac{n}{p_{k-1} \cdot p_k} - \ldots + / - \frac{n}{p_1 p_2 \ldots p_k}.$$

(A $+/-$ attól függően összeadás vagy kivonás, hogy páros vagy páratlan sok prímosztója van n-nek.)

Ezt a gondolatmenetet érdemes megjegyezni, másutt is elő fog fordulni ehhez hasonló.

8.11. Tétel. *Az r_1, r_2, r_3, ... számok akkor és csak akkor alkotnak redukált maradékrendszert* (mod m)*, ha*

(a) az elemek száma $\varphi(m)$,

(b) $\forall$ i-re $(r_i, m) = 1$, és

(c) $\forall$ $i \neq j$-re $r_i \not\equiv r_j \pmod{m}$.

Bizonyítás. A bizonyítást két lépésben végezzük el.

1. A feltétel szükséges (vagyis egy redukált maradékrendszernek teljesítenie kell (a), (b), (c)-t).

(a) Ha az adott számok redukált maradékrendszert alkotnak (mod m), akkor minden redukált maradékosztályból pontosan egy szerepel közöttük. Mivel (mod m) pontosan $\varphi(m)$ redukált maradékosztály van, pontosan ennyi elemre van szükség ahhoz, hogy minden redukált maradékosztály képviselve legyen.

(b) Mivel a redukált maradékosztályok minden eleme relatív prím a modulushoz, így az őket képviselő elemek is.

(c) Mivel semelyik maradékosztályból nem szerepelhet két elem, közülük bármelyik kettő inkongruens.

2. A feltétel elégséges (vagyis ha egy elemrendszer teljesíti az (a), (b), (c) feltételeket, akkor az redukált maradékrendszer).

A (b) feltétel miatt csak redukált maradékosztályokból való elemek szerepelnek. A (c) feltétel miatt semelyik redukált maradékosztályból nem szerepel két elem, vagyis minden elem más maradékosztályból való. Az (a) feltétel szerint pontosan annyi elem van, mint ahány redukált maradékosztály. A három feltétel egyszerre csak úgy teljesülhet, ha minden redukált maradékosztályt pontosan egy elem képvisel, vagyis ha a megadott elemek redukált maradékrendszert alkotnak. □

Megjegyzés. Redukált maradékrendszerekre már nem igaz, hogy ha minden elemükhöz hozzáadjuk ugyanazt a számot, akkor is redukált maradékrendszert kapunk. Például (mod 10) redukált maradékrendszert alkotnak az 1, 3, 7, 9 számok. Könnyen meggondolható, hogy az $1+b$, $3+b$, $7+1$, $9+b$ számok akkor és csak akkor alkotnak redukált maradékrendszert, ha $b \equiv 0 \pmod{10}$.

Általában is igaz:

8.1. Állítás. *Legyen r_1, r_2, …, $r_{\varphi(m)}$ redukált maradékrendszer m szerint. Ekkor az $r_1 + b$, $r_2 + b$, …, $r_{\varphi(m)} + b$ akkor és csak akkor redukált maradékrendszer m szerint, ha b osztható az m összes prímosztójával.*

Az viszont a redukált maradékrendszerre is teljesül, hogy ha minden elemét megszorozzuk ugyanazzal a számmal, akkor pontosan akkor kapunk ismét redukált maradékrendszert, ha a szám relatív prím a modulushoz.

8.12. Tétel. *Ha az r_1, r_2, …, $r_{\varphi(m)}$ számok redukált maradékrendszert alkotnak* (mod m) *és $c \in \mathbb{Z}$-re $(c, m) = 1$, akkor az r_1c, r_2c, …, $r_{\varphi(m)}c$ számok is redukált maradékrendszert alkotnak* (mod m).

Bizonyítás. Az r_1c, r_2c, …, $r_{\varphi(m)}c$ elemek darabszáma $\varphi(m)$.

Az, hogy közülük bármelyik kettő inkongruens (mod m), ugyanúgy látható be, mint a teljes maradékrendszerekre vonatkozó 8.7. Tétel esetén történt. ($(c, m) = 1$ esetén $a \equiv b \iff ac \equiv bc$.)

Az, hogy $\forall i$-re $(r_ic, m) = 1$ a 6.7. Tétel alapján teljesül, hiszen $(r_i, m) = 1$ és $(c, m) = 1$. □

8.2. Állítás. *Vegyük egy m modulus két tetszőleges redukált maradékrendszerét: $r_1, r_2, \ldots, r_{\varphi(m)}$ és $s_1, s_2, \ldots, s_{\varphi(m)}$! Ekkor $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv s_1 \cdot s_2 \cdot \ldots \cdot s_{\varphi(m)}$.*

Bizonyítás. A két redukált maradékrendszer elemei összepárosíthatók aszerint, hogy ugyanabból a maradékosztályból kerülnek ki – ezek egymással kongruensek. A 8.3. Tétel (ii) állításából következik, hogy $a \equiv b$ és $c \equiv d$ esetén $ac \equiv bd$. Ez nemcsak kettő, hanem akárhány tényezőre is teljesül. Itt most $\varphi(m)$ elem szerepel, vagyis teljesül, hogy a két szorzat kongruens m szerint. □

Megjegyzés. A korábbiakban már láttuk, hogy a kongruenciareláció tulajdonságainak következtében lehetőségünk van arra, hogy a maradékosztályok között értelmezzünk összeadást és szorzást. Ha most a redukált maradékosztályokra szorítkozunk, akkor ezek összege általában nem lesz redukált maradékosztály (tehát ha az alaphalmazunk a redukált maradékosztályok halmaza, akkor ebből az alaphalmazból az összeadás kivezet), szorzatuk azonban igen (a 6.7. Tétel következtében). Vizsgáljuk meg, hogy különböző modulusok esetén hogyan alakul a redukált maradékosztályok „szorzótáblája”!

(mod 4)

$\otimes$	$\bar{1}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$

(mod 5)

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(mod 6)

$\otimes$	$\bar{1}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$

(mod 7)

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

(mod 8)

$\otimes$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

(mod 9)

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{7}$	$\bar{2}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{7}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{1}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

(mod 10)

$\otimes$	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{1}$	$\bar{9}$	$\bar{3}$
$\bar{9}$	$\bar{9}$	$\bar{7}$	$\bar{3}$	$\bar{1}$

(mod 11)

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\overline{10}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\overline{10}$	$\bar{2}$	$\bar{5}$	$\bar{8}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{9}$	$\bar{2}$	$\bar{6}$	$\overline{10}$	$\bar{3}$	$\bar{7}$
$\bar{5}$	$\bar{5}$	$\overline{10}$	$\bar{4}$	$\bar{9}$	$\bar{3}$	$\bar{8}$	$\bar{2}$	$\bar{7}$	$\bar{1}$	$\bar{6}$
$\bar{6}$	$\bar{6}$	$\bar{1}$	$\bar{7}$	$\bar{2}$	$\bar{8}$	$\bar{3}$	$\bar{9}$	$\bar{4}$	$\overline{10}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{3}$	$\overline{10}$	$\bar{6}$	$\bar{2}$	$\bar{9}$	$\bar{5}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\bar{8}$	$\bar{8}$	$\bar{5}$	$\bar{2}$	$\overline{10}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{9}$	$\bar{9}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\overline{10}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\overline{10}$	$\overline{10}$	$\bar{9}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

A fenti műveleti táblázatokat megfigyelve sok érdekességet vehetünk észre, például hogy mindegyik táblázat szimmetrikus a főátlójára, ezzel is mutatva, hogy a maradékosztályok szorzása kommutatív; vagy hogy minden táblázatban minden sorban és minden oszlopban minden elem pontosan egyszer fordul elő stb.

Ha megvizsgáljuk, hogy most mely elemek osztói melyeknek, akkor azt tapasztaljuk, hogy mindegyik mindegyiknek, vagyis a redukált maradékosztályok halmazán a szorzás invertálható művelet. Ez egyben azt is jelenti – összevetve korábbi tapasztalatainkkal –, hogy ha egy prím modulusra vizsgáljuk az összes (mod p) maradékosztályt, akkor azok az összeadásra és a szorzásra nézve *testet* alkotnak (hiszen prím modulus esetén a $\bar{0}$ maradékosztály kivételével minden maradékosztály redukált).

Megjegyzés. Érdekes kérdés annak a vizsgálata, hogy egy szám hatványai mikor milyen maradékot adnak m-mel osztva. Ennek során derül ki, például hogy a négyzetszámok nem végződhetnek akármilyen számjegyre; hogy nincs $3k-1$ vagy $4k-1$ alakú négyzetszám stb.

Az, hogy egy szám hatványai milyen maradékokat adnak m-mel osztva, pusztán attól függ, hogy maga a szám milyen maradékot ad m-mel osztva. Ha például (mod 10) vizsgáljuk egy teljes maradékrendszer elemeinek hatványait (mindenhol a legkisebb nem negatív számmal képviselve az eredmény maradékosztályát), akkor a következőket tapasztaljuk:

ha	$a \equiv 0$	1	2	3	4	5	6	7	8	9	(mod 10),
akkor	$a^2 \equiv 0$	1	4	9	6	5	6	9	4	1	(mod 10),
	$a^3 \equiv 0$	1	8	7	4	5	6	3	2	9	(mod 10),
	$a^4 \equiv 0$	1	6	1	6	5	6	1	6	1	(mod 10),
	$a^5 \equiv 0$	1	2	3	4	5	6	7	8	9	(mod 10),
	$\vdots$										

(miután megkaptuk az első sort, innentől kezdve nyilván ismétlődik). Ha (mod 7) végzünk hasonló vizsgálatot:

$$\begin{array}{lrcccccccc} \text{ha} & a & \equiv 0 & 1 & 2 & 3 & 4 & 5 & 6 & (\text{mod } 7), \\ \text{akkor} & a^2 & \equiv 0 & 1 & 4 & 2 & 2 & 4 & 1 & (\text{mod } 7) \\ & a^3 & \equiv 0 & 1 & 1 & 6 & 1 & 6 & 6 & (\text{mod } 7) \\ & a^4 & \equiv 0 & 1 & 2 & 4 & 4 & 2 & 1 & (\text{mod } 7) \\ & a^5 & \equiv 0 & 1 & 4 & 5 & 2 & 3 & 6 & (\text{mod } 7) \\ & a^6 & \equiv 0 & 1 & 1 & 1 & 1 & 1 & 1 & (\text{mod } 7) \\ & a^7 & \equiv 0 & 1 & 2 & 3 & 4 & 5 & 6 & (\text{mod } 7) \\ & \vdots & & & & & & & & \end{array}$$

(innentől ismétlődik).

Számos egyéb – általánosítható – észrevétel mellett kiolvasható a táblázatból például az, hogy bármelyik a elem hatványait is vizsgálva, az $a, a^2, a^3, a^4, \ldots$ sorozat minden elemét kicserélve az m-mel való osztási maradékára, periodikus sorozatot kapunk. Ez persze nem túl meglepő, hiszen m-mel osztva csak véges sok (legfeljebb m féle) maradék fordulhat elő, így előbb-utóbb valamelyik maradék meg fog ismétlődni, és ha például a^x ugyanazt a maradékot adja, mint a^y, akkor (ld. például 2.9. Tétel) a^{x+1} maradéka nyilván megegyezik a^{y+1} maradékával, a^{x+2} maradéka a^{y+2} maradékával és így tovább, az első ismétlődéstől kezdve a maradékok periodikusan ismétlődnek.

Érdekes kérdés, hogy mit mondhatunk a periódusok hosszáról. Mint láttuk, (mod 10) bizonyos elemek esetén (0, 1, 5, 6) 1 a periódushossz, másoknál (4, 9) 2, megint másoknál (2, 3, 7, 8) 4; (mod 7) pedig a periódushossz – az illető elemektől függően – 1 vagy 2 vagy 3 vagy 6.

A 8.1. táblázat tartalmazza, hogy különböző modulusokkal kísérletezve milyen periódushosszokat tapasztalhatunk:

Észrevehető, hogy az előforduló periódushosszok minden sorban osztói az ott szereplő legnagyobb periódushossznak, és hogy a legnagyobb periódushossz minden m-re osztója $\varphi(m)$-nek. Vizsgálódásunkból az is kiderül, hogy prím modulusok esetén minden elemnél „tiszta” periódikus sorozatot kapunk, azaz előbb-utóbb minden elemnek (a 0 kivételével, annak nyilván minden hatványa 0-t ad maradékul) lesz egy olyan hatványa, ami 1-et ad maradékul a (prím) modulussal osztva, és ilyenkor a következő hatvánnyal előről ismétlődik a sorozat. Nem prím modulusok esetén pontosan azoknak az elemeknek lesz olyan hatványa, ami 1-et ad maradékul a modulussal osztva, amelyek relatív prímek a modulushoz. (Ez persze a prím modulusokra is igaz, hiszen épp arról van szó, hogy prím modulus esetén a $\bar{0}$ maradékosztály kivételével minden maradékosztály redukált.)

modulus:	előforduló periódushosszok
(2)	1
(3)	1, 2
(4)	1, 2
(5)	1, 2, 4
(6)	1, 2
(7)	1, 2, 3, 6
(8)	1, 2
(9)	1, 2, 3, 6
(10)	1, 2, 4
(11)	1, 2, 5, 10
(12)	1, 2
(13)	1, 2, 3, 4, 6, 12
⋮	

8.1. táblázat.

Észrevételeink közül először azt fogjuk igazolni, hogy ha egy elem relatív prím a modulushoz, akkor van olyan hatványa (nevezetesen a $\varphi(m)$-edik hatványa például ilyen), amely 1-et ad maradékul m-mel osztva.

8.13. Tétel. (Euler kongruenciatétele) *Ha* $(a, m) = 1$, *akkor* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás. Legyen r_1, r_2, …, $r_{\varphi(m)}$ egy redukált maradékrendszer (mod m). Ekkor (mivel $(a, m) = 1$) a 8.12. Tétel következtében az ar_1, ar_2, …, $ar_{\varphi(m)}$ is redukált maradékrendszer lesz (mod m). A redukált maradékrendszerekben szereplő elemek szorzata a 8.2. Állítás értelmében mindig ugyanabba az osztályba esik.

$$r_1 r_2 \dots r_{\varphi(m)} \equiv a r_1 a r_2 \dots a r_{\varphi(m)} \pmod{m},$$

azaz

$$r_1 r_2 \dots r_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \pmod{m}.$$

Mivel az r_1, r_2, …, $r_{\varphi(m)}$ elemek mindegyike redukált maradékosztályból való, mindegyik relatív prím a modulushoz, így a 8.4. Tétel értelmében oszthatunk velük, tehát $1 \equiv a^{\varphi(m)} \pmod{m}$. □

Megjegyzés. Könnyen meggondolható, hogy azoknak az elemeknek, amelyek nem relatív prímek a modulushoz, semelyik hatványa nem lehet 1-gyel kongruens (mod m). Ha például egy páros szám hatványait vizsgáljuk (mod 10), akkor nyilván minden hatványuk is páros lesz, és egy páros szám nem adhat 1-et maradékul 10-zel osztva. (Általában ha $(a, m) = d$,

akkor a minden hatványa osztható d-vel, így minden hatványának az m-mel való osztási maradéka is osztható lesz d-vel (hiszen m is osztható d-vel).)

Megjegyzés. A tétel nem állítja, hogy $(a, m) = 1$ esetén a-nak a $\varphi(m)$-edik lenne a legkisebb, m-mel osztva 1 maradékot adó hatványa, csupán azt, hogy a $\varphi(m)$-edik biztosan ilyen. (Tetszőleges m-re például az $a = m - 1$ relatív prím az m-hez, de már a négyzete 1-et ad maradékul m-mel osztva.)

Megjegyzés. Az viszont következik a tételből, hogy ha $(a, m) = 1$, akkor az a legkisebb pozitív egész k kitevő, amelyre $a^k \equiv 1 \pmod{m}$, osztója kell, hogy legyen $\varphi(m)$-nek. Legyen ugyanis $\varphi(m) = kq+r$, ahol $0 \leq r < k$. Ekkor $a^{\varphi(m)} = a^{kq+r}$, így $a^{\varphi(m)} \equiv a^{kq+r} \pmod{m}$.

Felhasználva, hogy $a^{kq+r} = (a^k)^q \cdot a^r$, továbbá (a tételből) hogy $a^{\varphi(m)} \equiv 1 \pmod{m}$, azt kapjuk, hogy $1 \equiv (a^k)^q \cdot a^r \pmod{m}$.

Ha $a^k \equiv 1 \pmod{m}$, akkor ebből az következik, hogy $1 \equiv a^r \pmod{m}$. Mivel r nemnegatív, viszont kisebb k-nál, az, hogy k volt a legkisebb pozitív egész kitevő, amelyre $a^k \equiv 1 \pmod{m}$, csak úgy lehet, hogy $r = 0$, ami viszont azt jelenti, hogy $k \mid \varphi(m)$.

Ez egyben arra is magyarázatot ad, hogy miért voltak a modulushoz relatív prím elemek esetén a tapasztalt periódushosszok a $\varphi(m)$-nek osztói.

A modulushoz nem relatív prím elemek esetén ugyanez a tapasztalatunk az $m \mapsto \varphi(m)$ függvénynek azon a – későbbiekben tárgyalásra kerülő – tulajdonságán múlik, hogy ha $d \mid m$, akkor $\varphi(d) \mid \varphi(m)$. A bizonyítást most nem részletezzük.

Megjegyzés. Foglalkozzunk most a tételnek azokkal a speciális eseteivel, amikor a modulus prím. Tetszőleges p prím esetén $\varphi(p) = p - 1$, hiszen egy prímszámhoz minden nála kisebb pozitív egész relatív prím. Ezt felhasználva, a 8.13. Tétel a következőt jelenti:

Legyen p prím, és $(a, p) = 1$ (vagyis $p \nmid a$). Ekkor $a^{p-1} = 1 \pmod{p}$.

Ebből az is következik, hogy $a^p \equiv a \pmod{p}$.

Ez viszont akkor is teljesül, ha $p \mid a$.

Érdemes az Euler-tételnek ezt a következményét külön is megfogalmaznunk:

8.14. Tétel. („kis" Fermat-tétel) *Tetszőleges a egészre és p prímre teljesül, hogy $a^p \equiv a \pmod{p}$, vagy másképp $p \mid a^p - a$.*

Bizonyítás. Ha $(a,p)=1$, akkor a 8.13. Tétel alapján $a^{p-1}\equiv 1 \pmod{p}$, amiből $a^p \equiv a \pmod{p}$.

Ha $(a,p)\neq 1$, akkor $p \mid a$, vagyis a minden hatványa p-vel kongruens modulo p, ezért $a^p \equiv a \pmod{p}$. □

Megjegyzés. Érdemes hangsúlyozni, hogy bár a „kis" Fermat-tétel minden a-ra igaz; akkor, amikor az előző (Euler) tételre hivatkozunk, akkor ezzel csak azokra az a-kra bizonyítjuk, amelyek relatív prímek a p-hez. Az, ugyanis, hogy $a^{p-1}\equiv 1 \pmod{p}$ (vagy másképp megfogalmazva az, hogy $p \mid a^{p-1}-1$), akkor és csak akkor igaz, ha $(a,p)=1$. (Egyéb a-kra viszont triviális az állítás.)

Megjegyzés. Szintén következménye az Euler-tételnek, hogy a (mod m) redukált maradékosztályok mindegyikének van a szorzásra nézve inverze. Ha ugyanis $(a,m)=1$, akkor a tétel miatt van olyan szám – nevezetesen az $a^{\varphi(m)-1}$–, amellyel megszorozva a szorzat az 1 által reprezentált maradékosztályban lesz. Ez egyben azt is jelenti, hogy ha az $\bar{a}$ osztályt szorozzuk meg az $\overline{a^{\varphi(m)-1}}$ osztállyal (ami nyilván szintén redukált maradékosztály, hiszen ha a relatív prím az m-hez, akkor minden hatványa is relatív prím az m-hez), akkor az 1 osztályt kapjuk.

Feladatok

1. Igazolja, hogy tetszőleges n esetén egy n-hez relatív prím differenciájú számtani sorozat n egymást követő eleme n szerint teljes maradékrendszer. (Vagyis ha $(n,d)=1$, akkor a_k+d, a_k+2d, …, a_k+nd teljes maradékrendszer n szerint.)

2. Igaz-e, hogy tetszőleges p prímszámhoz és egy p-hez relatív prím differenciájú számtani sorozatban mindig van olyan $p-1$ egymást követő tag, hogy azok p szerint redukált maradékrendszert alkotnak!

3. Egy számtani sorozat valamely $p-1$ egymást követő eleme redukált maradékrendszer p-hez. Mi mondható el a számtani sorozat differenciájáról?

4. Mi lehet az m szám, ha egy redukált maradékrendszere: $1, 41, -5, -13$.

5. Igazolja, hogy ha a és b pozitív egész számok, $(a,b)=1$, valamint $c=(a-1)(b-1)$, akkor minden $d\geq c$ számhoz van olyan pozitív x és y, amelyre $ax+by=d$!

   Keressen olyan a, b számokat, amelyekre nem találhatók olyan x, y pozitív egész számok, hogy $ax+by=c-1$!

6. Igazolja, hogy $24 \mid 5^{20} - 1$!
7. Igazolja, hogy minden n-re $6 \mid 1^n + 2^n + 3^n$!
8. Igazolja a 8.1. Állítást!

9. fejezet

Lineáris kongruenciák

Az eddigiekben a kongruenciareláció és az általa létrehozott maradékosztályok legfontosabb tulajdonságaival foglalkoztunk. Gyakran van szükségünk arra, hogy ismeretlent – vagy ismeretleneket – is tartalmazó konguenciákkal dolgozzunk. Ilyenkor az ismeretlen lehetséges értékeit keressük. A legegyszerűbb eset az, amikor egy ismeretlen szerepel, az is az első hatványon.

Erre vezet például a következő feladat: „Édesanyám három tortát sütött a születésnapomra, mindegyiket ugyanannyi szeletre vágta fel. Heten ugyanannyi szelet tortát ettünk, végül megmaradt két szelet. Hány szeletes lehetett egy torta?" (Vagy: „Hány szeletet ettünk külön-külön?") – Olyan x számot keresünk (egy tortán belül a szeletek száma), amelyeknek a háromszorosa (összesen a szeletek száma) kettőt ad maradékul héttel osztva, vagyis olyanokat, amelyeket a $3x \equiv 2 \pmod 7$ nyitott mondatban az x helyébe írva igaz állítást kapunk. Az ilyen számokat a $3x \equiv 2 \pmod 7$ *kongruencia megoldása*inak nevezzük. (A másik feladat megoldása, amikor az elfogyasztott tortaszeletek számára vagyunk kíváncsiak: $7y+2$ osztható 3-mal, vagyis $7y \equiv -2 \pmod 3$.)

A következőkben az ilyen legegyszerűbb típusú, $ax \equiv b \pmod m$ alakú, úgynevezett *lineáris kongruenciák*kal foglalkozunk. Azt szeretnénk tisztázni, hogy a-tól, b-től és m-től függően mikor van megoldása a kongruenciának; ha van, akkor hány megoldás van, és hogyan lehet a megoldásokat megtalálni.

9.1. Definíció. Az $ax \equiv b \pmod m$ *lineáris kongruencia megoldása* az x_i szám, ha teljesül, hogy $ax_i \equiv b \pmod m$.

Például:

A $3x \equiv 2 \pmod 7$ kongruenciának – mint az könnyen ellenőrizhető – megoldásai a 3, 10, 17, -11 stb. számok. (A kongruenciának minden $7k+3$

alakú szám megoldása, de persze az eredeti szöveges feladat szempontjából – ami tortaszeletekről szól – sem a negatívak, sem a „túl nagy” számok nem jönnek szóba.)

Kongruenciák megoldásainak keresése közben szükség lehet arra, hogy a kongruencián különféle átalakításokat végezzünk. Vigyáznunk kell azonban arra, hogy az új kongruenciának ugyanazok legyenek a megoldásai, mint az eredetinek.

9.2. Definíció. Azokat az átalakításokat, amelyek során egy kongruenciából az eredetivel ekvivalens kongruenciát kapunk, *ekvivalens átalakításoknak* nevezzük.

Két kongruenciát *ekvivalensnek* nevezünk, ha ugyanazok a megoldásaik.

Például:

A $324x \equiv 658 \pmod{10}$ kongruencia ekvivalens a $4x \equiv 8 \pmod{10}$ kongruenciával (mert $324 \equiv 4$ és $658 \equiv 8 \pmod{10}$). Általában is igaz, hogy ha az $ax \equiv b \pmod{m}$ kongruenciában az a, illetve b helyére vele kongruens számot írok, az ekvivalens átalakítás, részben a kongruenciareláció tranzitivitása, részben a 8.3. Tétel, illetve annak következményei miatt.

A $4x \equiv 8 \pmod{10}$ kongruencia *nem* ekvivalens a $20x \equiv 40 \pmod{10}$ kongruenciával (hiszen az utóbbinak minden szám megoldása, az előbbinek például az 1 nyilván nem).

A $3x \equiv 2 \pmod{7}$ viszont ekvivalens azza, hogy $3x \equiv 9 \pmod{7}$, ami pedig ekvivalens az $x \equiv 3 \pmod{7}$ kongruenciával.

Megjegyzés. A 8.3. Tétel alapján nyilvánvaló, hogy ha egy x_0 szám megoldása az $ax \equiv b \pmod{m}$ kongruenciának, akkor az összes $x_0 + km$ alakú szám is megoldása (ahol k tetszőleges egész szám), vagyis az összes m szerint x_0-lal kongruens szám is megoldás. Emiatt célszerű nem külön megoldásként kezelni ezeket, amennyiben a megoldások számára vagyunk kíváncsiak. (Hiszen ha különbözőnek tekintenénk minden megoldást, akkor minden olyan esetben, amikor egyáltalán van megoldás, mindig végtelen sok lenne.)

9.3. Definíció. Az $ax \equiv b \pmod{m}$ *kongruencia megoldásainak számán* az egymással m szerint inkongruens megoldások számát értjük.

Mivel ha egy szám megoldás, akkor az általa reprezentált maradékosztály minden eleme megoldás (ha pedig nem, akkor az általa reprezentált maradékosztály egy eleme sem), azt a kérdést, hogy hány különböző megoldása van egy kongruenciának, úgy is feltehetjük, hogy hány maradékosztály megoldása van a kongruenciának.

Például:

A $2x \equiv 3 \pmod{10}$ kongruenciának nincs megoldása (hiszen $2x$ mindig páros szám, és páros szám nem adhat páratlan maradékot (3-at) egy páros számmal (10-zel) osztva).

A $3x \equiv 2 \pmod{10}$ kongruenciának pontosan egy megoldása van (hiszen a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 teljes maradékrendszer elemei között pontosan egy olyan van (nevezetesen a 4), amelynek a háromszorosa kettőt ad maradékul 10-zel osztva).

A $2x \equiv 4 \pmod{10}$ kongruenciának két megoldása van (mert a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 teljes maradékrendszer elemei között két olyan van (nevezetesen a 2 és a 7), amelynek a kétszerese négyet ad maradékul 10-zel osztva).

Mint az a fenti példákból is látszik, az $ax \equiv b \pmod{m}$ összes megoldását megtalálhatjuk például úgy, hogy egy $\pmod{m}$ teljes maradékrendszer elemeit rendre beírjuk az x helyébe, és ellenőrizzük, hogy kielégítik-e a kongruenciát. Ez azonban nagy modulus vagy nagy együtthatók esetén hosszadalmas és kényelmetlen számolás lehet, de még ha ezzel a módszerrel szeretnénk dolgozni, akkor is sok munkát megtakaríthatnánk azzal, ha előre tudnánk, hogy hány megoldásra számítsunk. Ha például előre tudjuk, hogy két megoldás van, akkor amint találtunk két megoldást, abbahagyhatjuk a további elemek ellenőrzését, ha pedig előre tudjuk, hogy nincs megoldás, akkor bele sem kell fognunk a keresésbe. Szerencsére nem nehéz szükséges és elégséges feltételt adni a lineáris kongruencia megoldásának létézésre.

9.1. Tétel. *Az* $ax \equiv b \pmod{m}$ *kongruenciának akkor és csak akkor van megoldása, ha* $(a, m) \mid b$.

Bizonyítás. 1. A feltétel szükséges (vagyis ha van megoldás, akkor $(a, m) \mid b$):

Ha van olyan x_0 szám, amely megoldása a kongruenciának, akkor erre az x_0-ra teljesül, hogy $ax_0 \equiv b \pmod{m}$, tehát $m \mid ax_0 - b$. Ekkor m minden osztója, így (a, m) is osztója az $ax_0 - b$ különbségnek.

Azt is tudjuk, hogy $(a, m) \mid a$, és így $(a, m) \mid ax_0$. Emiatt $(a, m) \mid ax_0 - b$ csak úgy teljesülhet, ha $(a, m) \mid b$.

2. A feltétel elégséges (vagyis ha $(a, m) \mid b$, akkor létezik megoldás):

A 4.2. Következményből tudjuk, hogy léteznek olyan x és y számok, amelyekre $(a, m) = ax + my$. Ha $(a, m) \mid b$, akkor van olyan q szám, amelyre $(a, m)q = b$. Ezt felhasználva: $(a, m)q = axq + myq = b$, vagyis $myq = b - axq$. Ezek szerint $m \mid b - axq$, tehát $axq \equiv b \pmod{m}$. Ez viszont azt jelenti, hogy az xq szám megoldása a kongruenciának. □

Megjegyzés. A tétel bizonyítása (a 2. rész) arra nézve is ad útmutatást, hogy ha van megoldása egy kongruenciának, akkor hogyan található meg egy megoldás: először állítsuk elő a és m legnagyobb közös osztóját (az euklideszi algoritmus segítségével) a és m lineáris kombinációjaként, vagyis $(a, m) = ax + my$ alakban. Ezután nézzük meg, hogy (a, m) hányszor van meg b-ben. Ha a hányados q, akkor xq egy megoldás.

Keressük meg például a $48x \equiv 10 \pmod{14}$ kongruencia egy megoldását (tudjuk, hogy van, hiszen $(48, 14) = 2$, és $2 \mid 10$).

Végezzük el a 48 és a 14 euklideszi algoritmusát: $48 = 14 \cdot 3 + 6$, $14 = 6 \cdot 2 + 2$, $6 = 2 \cdot 3 + 0$.

Az első sorból: $6 = 48 - 14 \cdot 3$. A másodikból:

$$2 = 14 - 6 \cdot 2 = 14 - (48 - 14 \cdot 3) \cdot 2 = 48 \cdot (-2) + 14 \cdot 7.$$

Vagyis $x = -2$. Mivel a 10-ben 5-ször van meg a 2, a keresett megoldás a -10 (vagy másképp a 4) maradékosztálya.

Azt persze még nem tudjuk, hogy más megoldás nincs-e (a konkrét példában van; a 11 maradékosztályában szereplő elemek is megoldások, és mivel a 11 maradékosztálya különbözik a -10 maradékosztályától, ez a fentitől különböző megoldást jelent). Mielőtt megvizsgálnánk, hogy mikor hány megoldása van egy lineáris kongruenciának, foglalkozzunk először azzal a speciális esettel, amikor $(a, m) = 1$. Ilyen esetekben mindig van megoldás, hiszen tetszőleges b esetén $1 \mid b$.

9.2. Tétel. *Ha $(a, m) = 1$, akkor az $ax \equiv b \pmod{m}$ kongruenciának pontosan egy megoldása van, mégpedig az $x \equiv a^{\varphi(m)-1}b \pmod{m}$.*

Bizonyítás. Arról, hogy az $a^{\varphi(m)-1}b$ valóban megoldás, behelyettesítéssel meggyőződhetünk: A 8.13. Tétel értelmében $a^{\varphi(m)} \equiv 1 \pmod{m}$. Ebből következik (8.3. Tétel), hogy $a^{\varphi(m)}b \equiv b \pmod{m}$. Felhasználva, hogy $a^{\varphi(m)} = aa^{\varphi(m)-1}$ azt kapjuk, hogy

$$a\underbrace{a^{\varphi(m)-1}b}_{x} \equiv b \pmod{m},$$

vagyis az $x = a^{\varphi(m)-1}b$ és így az $x \equiv a^{\varphi(m)-1}b \pmod{m}$ valóban megoldás.

Be kell még látnunk, hogy több megoldás nincs. Ehhez nyilván elég azt megmutatni, hogy a 0, 1, 2, 3, …, $m - 1$ teljes maradékrendszer elemei között nem lehet olyan x_1, és x_2 ($x_1 \not\equiv x_2$), amelyekre $ax_1 \equiv b \pmod{m}$ és $ax_2 \equiv b \pmod{m}$ is teljesül.

Ha lenne ilyen x_1 és x_2, akkor $ax_1 - ax_2 = \underbrace{b-b}_{0} \pmod m$ is teljesülne, ami azt jelentené, hogy $m \mid ax_1 - ax_2 = a(x_1 - x_2)$. Mivel $(a, m) = 1$, ez csak úgy lehetséges, ha $m \mid x_1 - x_2$. Viszont tudjuk, hogy $0 \leq x_1 < m$ és $0 \leq x_2 < m$, amiből következik, hogy $|x_1 - x_2| < m$. Emiatt m csak úgy oszthatja az $x_1 - x_2$ különbséget, ha az 0, vagyis ha $x_1 = x_2$.

Tehát nem lehet egynél több maradékosztályból való megoldás. □

Például:

A bevezető példaként említett $3x \equiv 2 \pmod 7$ kongruenciának az egyetlen megoldása az $x = 3^{\varphi(7)-1} \cdot 2 \pmod 7$. Mivel $\varphi(7) = 6$, ez a $3^5 \cdot 2$ szám maradékosztályát jelenti, ami – mint arról némi számolással meggyőződhetünk – a 3 maradékosztálya. A $3 \cdot 3 = 9$ valóban kongruens 2-vel modulo 7.

Mielőtt általában foglalkoznánk azzal a kérdéssel, hogy hány megoldása van – ha van – egy olyan kongruenciának, ahol a és m nem relatív prímek, és hogyan lehet ezeket megtalálni, érdemes egy konkrét példát megvizsgálnunk:

Például $6x \equiv 69 \pmod{15}$

A kongruenciának nyilván van megoldása, mert $(6, 15) = 3$, és $3 \mid 69$. A kongruenciareláció tranzitivitása miatt a 69 helyett írhatunk 9-et (vele kongruenset), így a fenti kongruenciának pontosan azok lesznek a megoldásai, mint a $6x \equiv 9 \pmod{15}$ kongruenciának.

A 8.4. Tétel értelmében ez a kongruencia ekvivalens a $2x \equiv 3 \pmod 5$ kongruenciával. Itt $(2, 5) = 1$, ezért a 9.2. Tétel értelmében egyetlen megoldása az $x \equiv 2^{\varphi(5)-1} \cdot 3 \pmod 5$. Mivel $\varphi(5) = 4$, $2^{\varphi(5)-1} \cdot 3 = 2^3 \cdot 3 = 24$, és $24 \equiv 4 \pmod 5$, a $2x \equiv 3 \pmod 5$ kongruenciának az $x \equiv 4 \pmod 5$ a megoldása, így a vele ekvivalens $6x \equiv 9 \pmod{15}$ kongruenciának is pontosan azok a számok lesznek a megoldásai, amelyek 4-gyel kongruensek modulo 5 (5-tel osztva 4-et adnak maradékul).

Minket azonban az érdekel, hogy hány különböző maradékosztály elégíti ki a $6x \equiv 9 \pmod{15}$ kongruenciát, vagyis hogy a kapott (mod 5 szerinti) egyetlen maradékosztályba (azaz a 4 maradékosztályába) tartozó számok mely és hány különböző maradékosztályt jelentenek (mod 15). Ehhez azt kell meggondolnunk, hogy az $5k + 4$ alakú ($\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots$) számok hányféle maradékot adhatnak 15-tel osztva.

Ha $x \equiv 4 \pmod 5$, akkor mivel lehet kongruens az x modulo 15? Milyen maradékot adhat 15-tel osztva egy szám, amely 5-tel osztva 4 maradékot ad?

Ha egy szám 5-tel osztva 4 maradékot ad, akkor $15k + r$ alakban írva 5-tel osztva úgy adhat 4 maradékot, ha r 4-et ad maradékul 5-tel osztva, és 0 és 14 között 3 ilyen szám van: a 4, a 9 és a 15. (Más lehetőség nincs.)

Vagyis a (mod 5) egyetlen maradékosztályt jelentő megoldások (mod 15) három maradékosztályt alkotnak, így az eredeti kongruenciának három különböző megoldása van: $x_1 \equiv 4 \pmod{15}$, $x_2 \equiv 9 \pmod{15}$ és $x_3 \equiv 14 \pmod{15}$.

9.3. Tétel. *Ha az* $ax \equiv b \pmod{m}$ *kongruenciának van megoldása (vagyis ha* $(a, m) \mid b$*), akkor a megoldások száma* (a, m).

Bizonyítás. Legyen $a = (a, m)a'$ és $m = (a, m)m'$, ahol $(a', m') = 1$. Ha $(a, m) \mid b$, akkor b is felírható $b = (a, m)b'$ alakban. Ekkor minden olyan szám, amely kielégíti az $ax \equiv b \pmod{m}$ kongruenciát (a 8.4. Tétel miatt) megoldása az $a'x \equiv b' \pmod{m'}$ kongruenciának is, és viszont.

Mivel $(a', m') = 1$, az $a'x \equiv b' \pmod{m'}$ kongruenciának a 9.2. Tétel értelmében egyetlen megoldása van. Nevezzük ezt x_0-nak.

Az x megoldásra ezek szerint $x \equiv x_0 \pmod{m'}$, és azt szeretnénk tudni, hogy x milyen maradékot adhat m-mel osztva. Ezért x-et $my + r$ alakban keressük. Ez m'-vel osztva csak akkor adhat x_0 maradékot, ha r ad x_0 maradékot m'-vel osztva, hiszen $m' \mid m$. A $0, 1, 2, \ldots, m-1$ maradékosztályok közül ennek eleget tesz az x_0, az $x_0 + m'$, az $x_0 + 2m'$ stb., összességében az $x_0 + km'$, ahol $k = 0, 1, \ldots, (m, a) - 1$. (Hiszen $(m, a)m'$ már m-mel lenne egyenlő, ez azonban nincs a keresésben felsorolt maradékosztályok között.) Ha belátjuk, hogy pontosan ezek a megoldások, akkor ebből az is látszik, hogy megoldásként m' darab maradékosztályt kaptunk.

Megmutatjuk, hogy ha $(a, m) = d$, akkor az $x_0, x_0 + m', x_0 + 2m', x_0 + 3m', \ldots, x_0 + (d-1)m'$ számok közül bármelyik kettő inkongruens (mod m), viszont mind megoldása az $a'x \equiv b' \pmod{m'}$ és az $ax \equiv b \pmod{m}$ kongruenciának.

Az $x_0, x_0 + m', x_0 + 2m', x_0 + 3m', \ldots, x_0 + (d-1)m'$ számok pontosan akkor inkongruensek egymással páronként, amikor a $0, m', 2m', 3m', \ldots, (d-1)m'$ számok inkongruensek, amelyek 0 és $m-1$ közé eső különböző számok ($m' \neq 0$), tehát különböző maradékosztályokba esnek, így valóban inkongruensek.

Másrészt $a'(x_0 + km') = a'x_0 + a'km' \equiv a'x_0 \pmod{m'}$, amiről viszont tudjuk, hogy b'-vel kongruens (modulo m'), tehát $x_0 + km'$ megoldása az $a'x \equiv b' \pmod{m'}$ kongruenciának, másrészt $m' \mid a'(x_0 + km') - b'$, amiből d-vel szorozva $m \mid a(x_0 + km') - b$ (2.1. Következmény), tehát $a(x_0 + km') \equiv b \pmod{m}$, azaz $x_0 + km'$ az eredeti kongruenciának is megoldása. □

9.1. Megjegyzés. A lineáris kongruencia egy másik lehetséges megoldási módszerét mutatjuk be néhány konkrét példán keresztül.

A $6x \equiv 9 \pmod{15}$ kongruenciát osztjuk 3-mal (és tudjuk, hogy ezzel a megoldások számát is harmadoltuk): $2x \equiv 3 \pmod{5}$. A jobb oldalhoz hozzáadunk 5-öt (ez 0-val kongruens): $2x \equiv 8 \pmod{5}$. A kapott kongruenciát elosztjuk 2-vel (és mivel a modulust nem osztjuk, a megoldások száma változatlan): $x \equiv 4 \pmod{5}$.

Nézzünk egy másik példát: $42x \equiv 72 \pmod{17}$. A 17 alkalmas többszöröseivel csökkenthetjük a jobb és a bal oldalon szereplő kifejezéseket is: $8x \equiv 4 \pmod{17}$. Osszuk 4-gyel a kongruenciát: $2x \equiv 1 \pmod{17}$, adjunk hozzá 17-et a jobb oldalhoz: $2x \equiv 18 \pmod{17}$, osszunk 2-vel: $x \equiv 9 \pmod{17}$. És ezúttal csupa ekvivalens átalakítást végeztünk.

Vagy – ha csak a bal oldalt csökkentjük $2x \cdot 17 \equiv 0 \pmod{17}$-tel, akkor – a $8x \equiv 72 \pmod{17}$ kongruenciát 8-cal osztva ugyanerre az eredményre jutunk.

A lineáris kongruenciák megoldására sok más lehetőség van, ezek küzöl egyet látni fogunk még a későbbiekben.

Megjegyzés. Most már tudjuk, hogy az $ax \equiv b \pmod{m}$ lineáris kongruenciának akkor és csak akkor van megoldása, ha $(a, m) \mid b$, és hogy ha egy szám megoldása, akkor az illető szám által reprezentált maradékosztály minden eleme megoldás. Azt is tudjuk, hogy ha vannak megoldások, akkor ezek (a, m) darab különböző maradékosztályt alkotnak. Arra nézve is láttunk különböző módszereket, hogy hogyan lehet megtalálni a megoldásokat.

A következő fejezetben további megoldási módszerekkel is megismerkedhetünk. Előtte azonban lássunk példát egy alkalmazásra.

Szimultán kongruenciarendszerek, a kínai maradéktétel

Egy tréfás feladatban egy pásztor a birkáit terelgetve a karámba azt tapasztalja, hogy ha egyszerre kettőt terel be a kapun, akkor a végén 1 kimarad. Ha hármat terel be egyszerre a kapun, akkor 2 marad ki a végén. Ha négyesével terelgeti, akkor 3 marad a végén. Ha ötösével, akkor pedig 4. Hány birkája lehet a pásztornak? Hány birkája lehet, ha tudjuk, hogy 300 és 350 között van a számuk?

A birkák száma (ezt keressük) olyan szám, amely 2-vel osztva 1-et, 3-mal osztva 2-t, 4-gyel osztva 3-at, 5-tel osztva 4-et ad maradékul:

$$x \equiv 1 \pmod 2,$$
$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 4,$$
$$x \equiv 4 \pmod 5.$$

9.4. Definíció. Az olyan kongruenciarendszert, amelynek közös megoldását keressük, *szimultán kongruenciarendszernek* nevezzük.

Egy lehetséges megoldási menet, hogy megoldjuk az első kongruenciát, majd a megoldásként kapott maradékosztály(ok)on megoldjuk a másodikat, majd a kapott maradékosztály(ok)on a harmadikat, végül a kapott maradékosztály(ok)on a negyediket is megoldjuk.

Az első kongruencia megoldása a $2k_1 + 1$ alakú számok, pl. 1, 3, 5, 7, 9, 11, ... (egy 2 differenciájú számtani sorozat).

A második kongruencia megoldásai a $3k_2 + 2$ alakú számok, az előzőek közül az 5, 11, 17, 23, 29, 35, ... (egy 6 differenciájú számtani sorozat).

A harmadik kongruencia megoldásai a $4k_3 + 3$ alakú számok, az iméntiek közül a 11, 23, 35, 47, 59, ... (egy 12 differenciájú számtani sorozat).

Végül a negyedik kongruencia megoldásai az $5k_4 + 4$ alakú számok, az előzőek közül az 59, 119, ... (egy 60 differenciájú számtani sorozat).

A legutolsó sorozat elemei lehetnek megoldások. (Ezek közül azonban egy sem esik 300 és 350 közé, 299 és 359 tagjai a sorozatnak.)

(A feladat trükkös megoldása az, hogy adunk a pásztornak még egy birkát, így a birkák száma osztható lesz 2-vel, 3-mal, 4-gyel és 5-tel is – végső soron 60-nal –, tehát a birkák száma eredetileg $60k - 1$ alakú.)

Az is lehet, hogy nem a fenti maradékokat adja a birkák száma, hanem:

$$x \equiv 1 \pmod 2, \tag{9.1}$$
$$x \equiv 1 \pmod 3, \tag{9.2}$$
$$x \equiv 2 \pmod 4, \tag{9.3}$$
$$x \equiv 2 \pmod 5. \tag{9.4}$$

Azt látjuk, hogy mindegyik kongruencia külön-külön megoldható, hiszen – csakúgy, mint az előbb – a megoldások vannak felírva. Hamar észrevehetjük azonban, hogy a (9.3) szerint x páros szám, (9.1) szerint viszont páratlan. Eszerint ez a kongruenciarendszer nem megoldható.

Mi itt a probléma? Próbáljunk meg elégséges feltételt adni arra, hogy egy kongruenciarendszer megoldható legyen!

Itt most az a gond, hogy egy szám nem adhat 2 szerint páratlan maradékot, ha 4 szerint páros maradékot ad. Általában ha két olyan modulus szerepel a kongruenciarendszerben, amelyek maradékai egymásnak ellentmondanak, akkor hasonló gondok léphetnek fel. Ez akkor történhet meg, amikor két modulus nem relatív prím egymáshoz.

Csak olyan kongruenciarendszereket vizsgáljunk tehát ezentúl, amelyekben a szereplő modulusok relatív prímek.

Az is nyilvánvaló, hogy egy kongruenciarendszerben nemcsak direkt megoldások szerepelhetnek. Például:

$$3x \equiv 7 \pmod 2$$
$$2x \equiv 3 \pmod 5$$

Hogyan oldhatjuk meg? Nyilván mindkét kongruenciát megoldhatjuk külön-külön (ha van megoldás). Ezért amellett, hogy a modulosokról azt feltételezzük, hogy egymással páronként relatív prímek, azt is megköveteljük, hogy az egyes kongruenciák külön-külön megoldhatók legyenek.

Az első kongruencia megoldása $x \equiv 1 \pmod 2$, a másodiké $x \equiv 4 \pmod 5$.

$$x \equiv 1 \pmod 2$$
$$x \equiv 4 \pmod 5$$

Az első megoldása a $2k_1 + 1$ alakú számok: 1, 3, 5, 7, 9, 11, 13, ...

A másodiké (ezekből) a 9, 19, 29, ..., vagyis a kongruenciarendszer megoldásai $10k + 9$ alakúak.

Ahhoz tehát, hogy egy szimultán kongruenciarendszer megoldható legyen, szükséges feltétel, hogy minden egyes kongruencia megoldható legyen. A kongruenciákat *redukáljuk,* vagyis mindegyiket osztjuk a modulus és az x együtthatójának legnagyobb közös osztójával. (Erre azért van szükség, mert a modulusokról szeretnénk feltételezni, hogy páronként relatív prímek, ami egyébként nem biztos, hogy teljesül – nekünk elég, ha csak a redukálás után teljesül.)

Ezek után mindgyik kongruenciát megoldjuk. Végül olyan szimultán kongruenciarendszert kapunk, amelyben minden kongruencia redukált, a modulusok páronként relatív prímek.

9.4. Tétel. (Kínai maradéktétel) *Ha egy szimultán lineáris kongruenciarendszerben a szereplő kongruenciák redukáltak (a modulusok relatív prímek x együtthatójához), a modulusok páronként relatív prímek, akkor a kongruenciarendszer megoldható. A megoldás a modulusok szorzata mint modulus szerint egyetlen maradékosztály.*

Bizonyítás. A kongruenciák mindegyike megoldható, mert mindegyik redukált. A kongruenciákat egyesével megoldjuk, és felírjuk a megoldásukat:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ x &\equiv b_3 \pmod{m_3} \\ &\vdots \\ x &\equiv b_{n-1} \pmod{m_{n-1}} \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

Ezek után megkeressük az első két kongruencia közös megoldását, felírjuk egy $(m_1 \cdot m_2)$ modulus szerinti kongruenciaként. (Kongruenciáról kongruenciára haladva induktívan lehet meghatározni a megoldást.)

Egyrész $x \equiv b_1 \pmod{m_1}$ megoldása b_1 maradékosztálya. Ebből kiválasztunk egy teljes maradékrendszert m_2 szerint, például $b_1, b_1 + m_1, b_1 + 2m_1, \ldots, b_1 + (m_2 - 1)m_1$. Ebben a maradékrendszerben *pontosan egy* megoldása van a második kongruenciának, legyen $b_1 + km_2$. Az első két kongruencia tehát helyettesíthető az $x \equiv b_1 + km_2 \pmod{m_2}$ kongruenciával, és ez a megoldás egyértelmű.

A kongruenciarendszer megoldása egyértelmű, mert minden egyes lépésben egyetlen megoldás van. □

Megjegyzés. Az első példaként elmondott feladatban minden kongruencia redukált volt, de nem volt minden moduluspár relatív prím, mégis meg tudtuk oldani a kongruenciarendszert. Az $x \equiv 1 \pmod 2$ és $x \equiv 3 \pmod 4$ kongruenciák annak ellenére megoldhatók szimultán, hogy nem relatív prímek a modulusok, mert az utóbbiból következik az előbbi. (Ha egy szám 4-gyel osztva 3 maradékot ad, akkor 2-vel osztva 1-et.) A tétel feltétele tehát nem szükséges, csak elégséges, de sokkal egyszerűbb így kimondani, mint külön feltételként vizsgálni azokat az eseteket, amelykben a modulusok nem relatív prímek egymáshoz.

A következő fejezetben a lineáris kongruencia egy teljesen más típusú megoldási módszerével ismerkedünk meg.

Feladatok

1. Állapítsa meg, hogy a következő kongruenciák közül melyek megoldhatók. Amelyek igen, azokat oldja is meg!

$$\begin{aligned} 3x &\equiv 14 && \pmod 4 \\ 4x &\equiv 14 && \pmod{11} \\ 2\,465\,746x &\equiv 14 && \pmod 3 \\ 2\,465\,746x &\equiv 3 && \pmod{14} \\ 4x &\equiv 2\,465\,746 && \pmod{45} \end{aligned}$$

2. Ismert „tréfás” feladat a következő (egyes források szerint P. A. M. Dirac Nobel-díjas angol fizikus feladata): *Hét ember elmegy kókuszdiót gyűjteni. Találnak is jó sokat, de rájuk esteledik, így az osztozkodást reggelre hagyva lefekszenek aludni. Éjszaka egyikük felébred, s nem bízván a társaiban egymaga kívánja 7 részre osztani a dió-kupacot. Ezt 1 maradékkal meg is tudja tenni. Az „egyheted” részt eldugja, a maradékot a fa tetején figyelő majomnak dobja, s visszafekszik aludni. Az éjszaka során mind a 6 társa egymás után ugyanígy jár el (mindig 1 dió marad), s reggel – mintha éjszaka mi sem történt volna – közösen is elosztják a kupacot (s az 1 maradékot a majomnak adják). Legalább hány diót gyűjtöttek összesen?* Oldja meg! (Forrás: Középiskolai Matematika Lapok)

3. Vizsgálja meg, hogy a következő szimultán kongruenciák közül melyek megoldhatók! Amelyek igen, azokat oldja is meg!

$$\begin{aligned} 7x &\equiv 3 && \pmod 8 \\ 3x &\equiv -11 && \pmod 3 \end{aligned}$$

$$\begin{aligned} 7x &\equiv 8 && \pmod 3 \\ -11x &\equiv 3 && \pmod 8 \end{aligned}$$

$$\begin{aligned} -15x &\equiv -3 && \pmod 5 \\ -15x &\equiv 5 && \pmod 3 \end{aligned}$$

4. Keresse meg mindazokat az egész számokat, amelyek 3-mal osztva 0, 7-tel osztva 2 maradékot adnak!

5. Keressen olyan a, b, c egész számokat, amelyekkel $2a + 3b$ osztható 5-tel, $3b + 5c$ osztható 2-vel és $2a + 5c$ osztható 3-mal! Keressen több megoldást!

10. fejezet

Lineáris diofantoszi egyenletek

Az előző fejezetben látott bevezető feladatban (Édesanyám három tortát sütött a születésnapomra, mindegyiket ugyanannyi szeletre vágta fel. Heten ugyanannyi szelet tortát ettünk, végül megmaradt két szelet.) két kérdést is feltettünk: Hány szeletes lehetett egy torta? Hány szeletet ettünk külön-külön? Egyrészt olyan x-et keresünk, amelyre $3x-2$ osztható 7-tel, másrészt olyan y-t, amelyre $7y+2$ osztható 3-mal. Azaz $3x-2=7y$ vagy $7y+2=3x$. A felírt kongruencia esetén nem látszott, de ebből a felírásból igen: a két kérdés ugyanarra az egyenletre vezet. A feladat alapján x és y csak egész szám lehet.

10.1. Definíció. Azokat az egyenleteket, amelyek együtthatói egész számok, és a megoldásaikat is az egész számok körében keressük, *diofantoszi egyenlet*eknek nevezzük.

(Az elnevezés az ókori görög tudós Diofantosz nevére utal, aki a III. században Alexandriában „Aritmetika" címen 13 kötetben tárgyalt számelméleti kérdéseket. Diofantoszról lásd például: Sain Márton: Nincs királyi út!, Gondolat, Budapest, 1986, http://mek.oszk.hu/05000/05052/; Oystein Ore: Number Theory and Its History, Dover Publications Ins., New York.)

A diofantoszi egyenleteket is csoportosíthatjuk aszerint, hogy hány ismeretlent tartalmaznak, illetve hogy az ismeretlenek milyen hatványokon szerepelnek bennük. Ennek megfelelően beszélhetünk egy-, két- stb ismeretlenes, illetve első-, másod- stb fokú diofantoszi egyenletekről. Ebben a fejezetben az elsőfokú (lineáris) diofantoszi egyenletekről lesz szó – elsőként ezen belül a legegyszerűbb fajtáról, az egyismeretlenesről.

10.1. Tétel. *Az $ax-b=0$ diofantoszi egyenlet esetén a következő eseteket különböztetjük meg:*

1. $a = 0$ *és* $b \neq 0$. *Ebben az esetben nincs megoldás.*
2. $a = 0$ *és* $b = 0$. *Ebben az esetben minden egész szám megoldás.*
3. $a \neq 0$. *Ebben az esetben akkor és csak akkor van megoldás, ha* $a \mid b$, *és ilyenkor az egyetlen megoldás:* $x = \frac{b}{a}$.

Bizonyítás. 1. Ha $a = 0$, akkor tetszőleges x esetén ax is 0. Így ha $b \neq 0$, akkor semmilyen szám nem elégíti ki az egyenletet.

2. Ha $a = b = 0$, akkor az egyenlet azonosság, minden szám megoldása.

3. Ha $a \neq 0$, és van olyan x_0 egész szám, amelyre $ax_0 - b = 0$, akkor ugyanerre az x_0-ra $ax_0 = b$. Ilyen x_0 létezése az oszthatóság definíciója alapján éppen azt jelenti, hogy $a \mid b$. Megfordítva, ha $a \mid b$, akkor létezik olyan q, amelyre $aq = b$. Ekkor az $x = q$ megoldása az egyenletnek. □

A következő legegyszerűbb típus a kétismeretlenes lineáris diofantoszi egyenlet, amely általánosan az $ax + by = c$ alakba írható. Ezt átrendezve viszont az $by = c - ax$ (vagy az $ax = c - by$) alakot kapjuk, amelyről leolvasható, hogy az egyenletnek akkor és csak akkor van megoldása, ha létezik olyan x, amelyre $b \mid c - ax$ (vagy $a \mid c - by$), vagyis ha létezik olyan x, amelyre $ax \equiv c \pmod{b}$ (vagy $by \equiv c \pmod{a}$). Ez azt jelenti, hogy az $ax + by = c$ kétismeretlenes lineáris diofantoszi egyenletnek akkor és csak akkor van megoldása, ha az $ax \equiv c \pmod{b}$ (vagy – ami ezzel ekvivalens – a $by \equiv c \pmod{a}$) kongruencia megoldható.

10.2. Tétel. *Az* $ax+by = c$ *diofantoszi egyenlet akkor és csak akkor oldható meg, ha* $(a, b) \mid c$.

Bizonyítás. Egyrészt ha $(a, b) \nmid c$, akkor az egyenlet nem oldható meg, mert a bal oldal osztható (a, b)-vel, a jobb oldal azonban nem.

Másrészt tudjuk (4.2. Következmény), hogy a és b legnagyobb közös osztója felírható $au + bv$ alakban. Ha $(a, b) \mid c$, akkor $c = q \cdot (a, b) = qau + qbv$, vagyis $x = qu$, $y = qv$ egy lehetséges megoldás. □

Megjegyzés. Másképp is beláthatjuk a tételt. Mint azt korábban láttuk, a fenti egyenlet akkor és csak akkor oldható meg, amikor az $ax \equiv c \pmod{b}$ kongruencia. Azt pedig már láttuk (9.1. Tétel), hogy a kongruencia megoldhatóságának szükséges és elégséges feltétele az, hogy $(a, b) \mid c$ teljesüljön.

Megjegyzés. A kétismeretlenes lineáris diofantoszi egyenlet átalakítható egyismeretlenes lineáris kongruenciává (kétféleképpen is), és minden line-

áris kongruencia átalakítható kétismeretlenes lineáris diofantoszi egyenletté. Keressük ugyanis az $ax \equiv b \pmod{m}$ kongruencia megoldásait. Ekkor fennáll, hogy $m \mid ax - b$, vagyis létezik olyan szám (jelölje $-y$), amelyre $m \cdot (-y) = ax - b$, tehát az $ax + my = b$ kétismeretlenes lineáris diofantoszi egyenlet megoldásait keressük. (Persze konkrétan ebben az esetben elsősorban x-et.) A jelölés egységessége érdekében a kétismeretlenes lineáris diofantoszi egyenletet a következőkben $ax + my = b$ alakban fogjuk felírni.

A kétismeretlenes lineáris diofantoszi egyenletek és a lineáris kongruenciák közötti szoros rokonság egyben módszereket is jelent számunkra az $ax + my = b$ egyenlet megoldásához:

1. módszer: Tekintsük az $ax \equiv b \pmod{m}$ lineáris kongruenciát. Ennek megkereshetjük az összes megoldását például úgy, hogy a $0, 1, 2, \ldots, m-1$ teljes maradékrendszer elemeit rendre behelyettesítjük, és kiválasztjuk azokat, amelyek kielégítik a kongruenciát. Ha valamelyik $x_i \in \{0, 1, 2, \ldots, m-1\}$ szám megoldása a kongruenciának, akkor az összes $x_i + km$ alakú szám is megoldása. Minden olyan x' szám esetén, ahol x' megoldása a kongruenciának, az $(x', \dfrac{b - ax'}{m})$ számpár megoldása a diofantoszi egyenletnek.

2. módszer: Az $ax + my = b$ diofantoszi egyenlet egy megoldását – a lineáris kongruenciáknál látottakhoz hasonlóan – az euklideszi algoritmus segítségével is megtalálhatjuk. Legyen $(a, m) = d$. Ha $d \mid b$ (csak ilyenkor van megoldás), akkor b felírható $b = b'd$ alakban. Tudjuk (4.2. Következmény), hogy d előállítható a és m lineáris kombinációjaként, keressük meg azt az x'-t és y'-t, amelyre $d = ax' + my'$. Erre az x'-re és y'-re teljesül, hogy $b = b'd = ax'b' + my'b'$, amiből látszik, hogy az $(x'b', y'b')$ számpár megoldása az egyenletnek.

3. módszer: Az $ax \equiv b \pmod{m}$ lineáris kongruenciát úgy is megoldhatjuk, hogy a és m legnagyobb közös osztójával osztva visszavezetjük az $a'x \equiv b' \pmod{m'}$ kongruenciára, ahol $a' = \dfrac{a}{(a, m)}$, $b' = \dfrac{b}{(a, m)}$, $m' = \dfrac{m}{(a, m)}$. Ebben a kongruenciában $(a', m') = 1$, így a 9.2. Tétel értelmében minden olyan x' szám megoldása, amelyre $x' \equiv a^{\varphi(m)-1}b \pmod{m}$. Bármelyik ilyen x' szám esetén az $(x', \dfrac{b - ax'}{m})$ számpár megoldása a diofantoszi egyenletnek.

A kétismeretlenes lineáris diofantoszi egyenletet nemcsak a kongruenciára visszavezetve tudjuk megoldani. Merőben heurisztikusan magunk is ki tudunk gondolni egy lehetséges megoldást. Lássunk egy konkrét példát erre.

$$80x + 120y = 1000$$

Az egyenlet nyilván ekvivalens a következővel (osztunk az együtthatók legnagyobb közös osztójával, 40-nel):

$$2x + 3y = 25$$

Fejezzük ki az egyenletből x-et (általában a kisebb abszolút értékű együtthatóval rendelkező ismeretlent):

$$x = \frac{-3y + 25}{2}$$

„Válasszuk le" az egészeket úgy, hogy a számlálóban szereplő együthatókat maradékosan osztjuk a nevezővel:

$$x = -2y + 12 + \frac{y + 1}{2}$$

Mi most az egyenlet egész megoldásait keressük, és látható, hogy x akkor és csak akkor lesz egész, ha $\frac{y+1}{2} = k$ egész szám, vagyis ha $y = 2k - 1$. Ha $y = 2k - 1$, akkor $x = -2(2k - 1) + 12 + k = 14 - 3k$. Vagyis az egyenletnek tetszőleges k egész szám esetén megoldása a $(14 - 3k, 2k - 1)$ számpár.

Módszerünk általában is alkalmazható:

4. módszer (együtthatók csökkentésének módszere): $ax + my = b$ (ahol $(a, m) \mid b$, vagyis az egyenlet megoldható)

Ha a két ismeretlen együtthatója, a és m egyenlő abszolút értékű, azaz $ax + ay = b$ vagy $ax - ay = b$, akkor $x + y = \frac{b}{a}$ vagy $x - y = \frac{b}{a}$. Két egész szám összege, illetve különbsége $\frac{b}{a}$. Ezek szerint tetszőleges k egész szám esetén az első esetben minden $\left(k, \frac{b}{a} - k\right)$, a második esetben pedig minden $\left(k, k - \frac{b}{a}\right)$ alakú számpár megoldás.

Ha $|a| \neq |m|$, akkor fejezzük ki azt az ismeretlent, amelynek kisebb az együtthatója abszolút értéke. Feltehetjük, hogy ez az a, vagyis $|a| < |m|$:

$$x = \frac{b - my}{a}.$$

Osszuk b-t, illetve m-et maradékosan a-val: $b = aq_1 + r_1$ és $m = aq_2 + r_2$, ahol $0 \leq r_1, r_2 < |a| (< |m|)$.

Ekkor

$$x = \frac{aq_1 + r_1 - (aq_2 + r_2)y}{a} = q_1 - q_2 y + \frac{r_1 - r_2 y}{a}.$$

Akkor és csak akkor kapunk egész megoldást x-re, ha $\dfrac{r_1 - r_2 y}{a} = k$ egész szám, vagyis ha léteznek olyan k és y egész számok, amelyek megoldásai az

$$ak + r_2 = r_1$$

kétismeretlenes lineáris diofantoszi egyenletnek.

Ezzel eredeti egyenletünket visszavezettük egy olyanra, amelyben a nagyobb abszolút értékű együttható abszolút értéke kisebb, mint az eredeti egyenlet nagyobb abszolút értékű együtthatójáé ($r_1 < |a| < |m|$ miatt). Ezt az eljárást folytatva előbb-utóbb eljutunk egy olyan egyenlethez, amelyben már valamelyik ismeretlen együtthatója 1 lesz, és innen kezdve egyenletről egyenletre visszahelyettesítve a megoldásokat kaphatjuk meg az eredeti egyenlet megoldásait.

10.1. Megjegyzés. A fenti levezetést másképp is végigvihetjük. Nem kell feltétlenül felírni a törteket. Nézzük meg a gondolatmenetet egy konkrét példán. $54x + 21y = 24$. A kiinduló egyenletben feltettük, hogy $(a, m) \mid b$. Ha $(a, m) > 1$, akkor oszthatunk vele. Ez a 3, osszunk vele: $18x + 7y = 8$.

A 18-at maradékosan osztjuk 7-tel: $(2 \cdot 7 + 4)x + 7y = 8$, átrendezve: $7 \cdot (2x + y) + 4x = 8$. Jelöljük y_1-gyel $(2x + y)$-t. Ekkor $4x + 7y_1 = 8$. (Máris kaptunk egy olyan egyenletet, amelynek az együtthatói abszolút értékben kisebbek, mint az eredeti egyenlet együtthatói.)

Most maradékosan osztjuk a 7-et 4-gyel. $(4 + 3)y_1 + 4x = 8$, átrendezve: $4(y_1 + x) + 3y_1 = 8$. Jelöljük x_1-gyel $(y_1 + x)$-et. Ekkor $4x_1 + 3y_1 = 8$. (Már látunk egy nyilvánvaló megoldást: $x_1 = 2$, $y_1 = 0$, de folytassuk tovább az eljárást, mert máskor nem biztos, hogy ilyen szerencsések leszünk.)

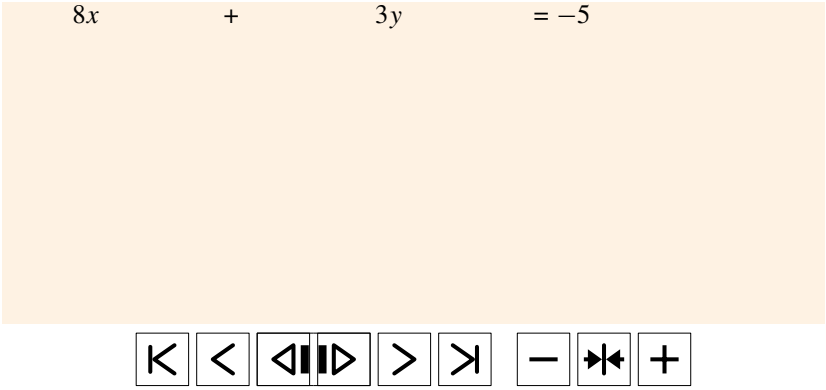
Maradékosan osztjuk a 4-et 3-mal. $(3 + 1)x_1 + 3y_1 = 8$, átrendezve: $3(x_1 + y_1) + x_1 = 8$. Jelöljük y_2-vel $(x_1 + y_1)$-et. Ekkor $x_1 + 3y_2 = 8$. Mivel az együtthatók relatív prímek voltak, előbb-utóbb az egyik együttható 1 lesz. Az ehhez az együtthatóhoz tartozó ismeretlent b-nek, a másikat 0-nak választva megoldást kapunk: $y_2 = 0$, $x_1 = 8$.

Ebből $y_2 = x_1 + y_1$ miatt $y_1 = -8$. Ezek után $x_1 = y_1 + x$ alapján $x = 16$. Mivel $y_1 = 2x + y$ volt, így $y = -40$. Vagyis kaptunk egy megoldást.

A módszert egy konkrét példán szemlélteti a 10.1. ábra animációja.

10.2. Megjegyzés. Írjuk fel a $\dfrac{18}{7}$ törtet lánctört alakban:

$$\frac{18}{7} = 2 + \frac{4}{7} = 2 + \frac{1}{\frac{7}{4}} = 2 + \frac{1}{1 + \frac{3}{4}} = 2 + \frac{1}{1 + \frac{1}{\frac{4}{3}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}$$



10.1. ábra. (animáció).

vagy rövidebben (a törtek reciprok átírásának lépését kihagyva)

$$\frac{18}{7} = 2 + \frac{4}{7} = 2 + \frac{1}{1 + \frac{3}{4}} = 2 + \frac{1}{1 + \frac{1}{1+\frac{1}{3}}}$$

Azt tapasztaljuk, hogy itt minden tört a 10.1. Megjegyzésben szereplő egyenlet együtthatóból tevődik össze. (18 és 7, 4 és 7, 4 és 3, 1 és 3. Azért ebben a sorrendben írjuk a párokat, mert az egyik együttható – a kisebbik – változatlan marad.)

Semmi meglepő nincs ebben, mert mindkét eljárás alapja az euklideszi algoritmus.

Megoldási módszereink egy része nem – vagy nem feltétlenül – szolgáltatja az összes megoldást, így hasznos lenne, hogy ha egy megtalált megoldásból többet, esetleg mindet meg tudnánk határozni.

Vegyük észre, hogy ha az eredeti egyenletben ($ax + my = b$) az ax-et ugyanannyival növeljük, mint amennyivel az my-t csökkentjük, akkor továbbra is fennáll az egyenlőség. Ha azt is tudjuk garantálni, hogy a hozzáadott és levont szám a-val és m-mel is osztható (például maga am), akkor az x_0, y_0 megoldáshoz egy újabb megoldást kapunk: $b = ax_0 + am + my_0 - am = a(x_0 + m) + m(y_0 - a)$, azaz $x_1 = x_0 + m$ és $y_1 = y_0 - a$ szintén megoldások. Ez a gondolat áll amögött, hogy mit mondhatunk általában:

10.3. Tétel. *Ha az (x_0, y_0) számpár megoldása az $ax + my = b$ diofantoszi egyenletnek, akkor tetszőleges k egész szám esetén az*

$$\left(x_0 + k\frac{m}{(a,m)}, y_0 - k\frac{a}{(a,m)}\right) \tag{10.1}$$

számpár is megoldás, és az összes megoldás felírható ilyen alakban.

Bizonyítás. Először belátjuk, hogy az összes megoldás felírható ilyen alakban.

Ha $ax_0 + my_0 = b$ és $ax' + my' = b$ is fennáll, akkor ax' pontosan annyival több ax_0-nál, mint amennyivel my' kevesebb my_0-nál, vagyis van olyan u, amelyre $ax_0 + u = ax'$, $my_0 - u = my'$. Ezekből az következik, hogy $a \mid u$, és $m \mid u$, tehát $[a, m] \mid u$. Eszerint van olyan k, amelyre $k[a, m] = u$. Tudván, hogy $[a, m] = \dfrac{am}{(a, m)}$, azt kapjuk, hogy $u = k\dfrac{am}{(a, m)}$, amiből $ax' = ax_0 + k\dfrac{am}{(a, m)}$ és $my' = my_0 - k\dfrac{am}{(a, m)}$. Az első összefüggésben minden tag osztható a-val, a másodikban pedig mindegyik osztható m-mel, azaz (a 2.1. Következmény alapján, illetve mivel $(a, m) \mid m$ és $(a, m) \mid a$) tetszőleges egész k számra

$$(x', y') = \left(x_0 + k\frac{m}{(a, m)}, y_0 - k\frac{a}{(a, m)}\right).$$

A fenti gondolatmenettel azt mutattuk meg, hogy minden megoldás (10.1) alakban írható, miközben a konstrukció (hogy ugyanis egy már megtalált megoldásban ugyanannyit adunk az egyik taghoz, mint amennyit levonunk a másikból) következményeként azt is megkaptuk, hogy minden ilyen alakú pár megoldása az egyenletnek. □

Másik bizonyítás. A tétel állítása másképpen is belátható.

Ha az (x_0, y_0) számpár megoldása az $ax + my = b$ egyenletnek, akkor

$$ax_0 + my_0 = b.$$

Ha az (x', y') számpár is megoldása az $ax + my = b$ egyenletnek, akkor

$$ax' + my' = b.$$

Ekkor:

$$a(x' - x_0) + m(y' - y_0) = 0,$$

vagyis

$$a(x' - x_0) = m(y_0 - y'),$$

és így

$$\frac{a}{(a, m)}(x' - x_0) = \frac{m}{(a, m)}(y_0 - y').$$

Felhasználva, hogy $\left(\dfrac{a}{(a, m)}, \dfrac{m}{(a, m)}\right) = 1$, az előbbi egyenlőség csak úgy lehetséges, ha

$$\frac{m}{(a, m)} \mid (x' - x_0) \qquad \text{és} \qquad \frac{a}{(a, m)} \mid (y_0 - y'),$$

vagyis ha van olyan k_1 és k_2, amelyre

$$\frac{m}{(a,m)}k_1 = (x' - x_0) \qquad \text{és} \qquad \frac{a}{(a,m)}k_2 = (y_0 - y'),$$

azaz

$$x' = x_0 + \frac{m}{(a,m)}k_1 \qquad \text{és} \qquad y' = y_0 - \frac{a}{(a,m)}k_2.$$

Behelyettesítve az $\frac{a}{(a,m)}(x' - x_0) = \frac{m}{(a,m)}(y_0 - y')$ egyenlőségbe x' és y' imént nyert alakját, ezt kapjuk:

$$\frac{a}{(a,m)}\left(x_0 + \frac{m}{(a,m)}k_1 - x_0\right) = \frac{m}{(a,m)}\left(y_0 - y_0 + \frac{a}{(a,m)}k_2\right).$$

Ebből:

$$\frac{m}{(a,m)}k_1 = \frac{a}{(a,m)}k_2,$$

vagyis az összetartozó x' és y' értékpárok esetén $k_1 = k_2$, tehát az egyenlet megoldásai valóban csak a kívánt

$$(x', y') = \left(x_0 + k\frac{m}{(a,m)}, y_0 - k\frac{a}{(a,m)}\right)$$

alakúak lehetnek (k tetszőleges egész szám).

Hátravan még annak az igazolása, hogy az ilyen alakú számpárok tetszőleges k egész szám esetén megoldások.

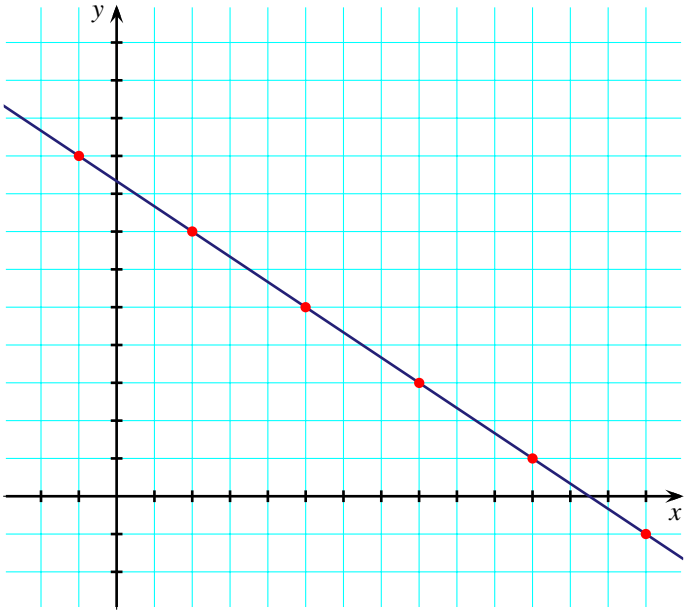
Ezt egyszerű behelyettesítéssel mutathatjuk meg.

$$ax' + my' = a\left(x_0 + k\frac{m}{(a,m)}\right) + m\left(y_0 - k\frac{a}{(a,m)}\right) = ax_0 + my_0.$$

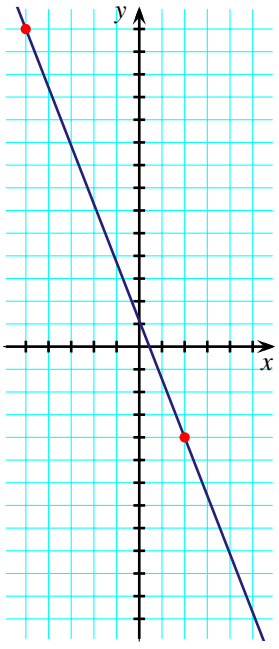
Tehát ha az (x_0, y_0) pár megoldása az egyenletnek, akkor – k értékétől függetlenül – az (x', y') pár is megoldása. □

Megjegyzés. Az $ax + my = b$ kétismeretlenes egyenlet egy egyenes egyenlete a síkban. Az egyenlet egész megoldásainak az egyenesnek azok a pontjai felelnek meg, amelyeknek mindkét koordinátája egész szám, vagyis azok a rácspontok, amelyekre az egyenes illeszkedik. Tételünkből kiderül, hogy ha egy kétismeretlenes diofantoszi egyenletnek van megoldása, akkor végtelen sok megoldása van, ami azt is jelenti, hogy ha egy racionális meredekségű egyenes áthalad egy rácsponton, akkor végtelen sok rácsponton halad át.

http://www.cs.elte.hu/~kfried/algebra1/Equation2.jarEz a program egy $ax + by = c$ alakú diofantoszi egyenlet egy megoldását adja meg.



10.2. ábra. A $2x + 3y = 25$ egyenese és néhány megoldása



10.3. ábra. A $18x + 7y = 8$ egyenese és néhány megoldása

A (kettőnél) több ismeretlent tartalmazó diofantoszi egyenletekkel most részletesen nem foglalkozunk, de bizonyítás nélkül megemlítjük a következő tételt:

10.4. Tétel. *Az* $a_1x_l+a_2x_2+\ldots+a_nx_n = b$ *lineáris diofantoszi egyenletnek akkor és csak akkor van megoldása, ha* $(a_1, a_2, \ldots, a_n) \mid b$.

Megjegyzés. Tételünk a 10.2. Tétel általánosítása, bizonyítása is hasonlóan végezhető el: a szükségesség nyilvánvaló, az elégségesség pedig azon múlik, hogy a 4.2. Tétel általánosítása is igaz, vagyis belátható, hogy akárhány szám legnagyobb közös osztója is előállítható az illető számok lineáris kombinációjaként.

Megjegyzés. Az együtthatók csökkentésének módszere ((4.) módszer) a többismeretlenes lineáris diofantoszi egyenletek megoldására is alkalmazható.

Megjegyzés. Nézzük meg egy konkrét kongruencia megoldását!

$$30a + 31b + 28c = 365$$

Osszuk az együtthatókat maradékosan a legkisebb együtthatóval, 28-cal, és alakítsuk át az egyenletet ennek megfelelően:

$$28(a + b + c) + 2a + 3b = 365.$$

Vezessük be a $c_1 = a + b + c$ jelölést.

$$2a + 3b + 28c_1 = 365.$$

Osszuk az együtthatókat maradékosan a legkisebb együtthatóval, 2-vel, majd rendezzük az egyenletet:

$$2(a + b + 14c_1) + b = 365.$$

Egy lehetséges megoldás, hogy $b = 1$ és $a+b+14c_1 = 182$, azaz $a+14c_1 = 181$. Mivel $182 = 12 \cdot 14 + 13$, lehet $a = 13$, $c_1 = 12$. Ebből $c = -2$. Eszerint $13 \cdot 30 + 1 \cdot 31 - 2 \cdot 28 = 365$.

Mivel $31+31+28 = 30+30+30$, az a-t 3-mal csökkentve (illetve növelve), a b-t 2-vel, a c-t pedig 1-gyel növelve (illetve csökkentve) új megoldásokat kapunk: $a = 10$, $b = 3$, $c = -1$ $(10 \cdot 30 + 3 \cdot 31 - 1 \cdot 28 = 365)$; $a = 7$, $b = 5$, $c = 0$ $(7{\cdot}30+5{\cdot}31-0{\cdot}28 = 365)$; $a = 4$, $b = 7$, $c = 1$ $(4{\cdot}30+7{\cdot}31+1{\cdot}28 = 365)$ stb.

Ebben az esetben nem vizsgáljuk, hogy minden megoldást megkaptunk-e.

Feladatok

1. Írja át a $2x \equiv 5 \pmod 9$ kongruenciát lineáris diofantoszi egyenlet alakba, majd írja fel azt a másik kongruenciát, amelyre ezen kívül még átírható! Oldja meg a kongruenciákat! Oldja meg a diofantoszi egyenletet!

2. Az egyik busz indítási idejéről a következő iformációkat olvashatjuk: Minden órában indul busz. A követési idő 7-8 perc, amit úgy kell érteni, hogy 7 **vagy** 8 perc elteltével indítják a következő buszt.

   Egy órán belül milyen busz indítási időpontok lehetnek? Keresse meg az összes lehetőséget!

3. Egy patakból egy 8 és egy 5 literes űrtartalmú edény segítségével ki szeretnénk mérni 2 l vizet.

   Írjon fel a feladatra kongruenciát, diofantoszi egyenletet, oldja meg ezeket, illetve keressen intuitív megoldást!

4. Oldja meg a $3x + 4y + 5z = 6$ diofantoszi egyenletet!

11. fejezet

Néhány nevezetes diofantoszi probléma

Pitagoraszi számhármasok

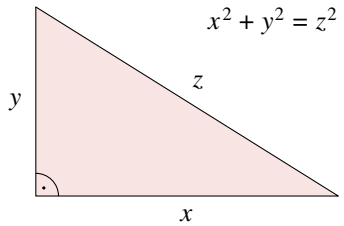
11.1. Definíció. Az

$$x^2 + y^2 = z^2 \tag{11.1}$$

(háromismeretlenes, másodfokú) diofantoszi egyenlet pozitív (egész) megoldásait *pitagoraszi számhármasoknak* nevezzük.

Például: 3, 4, 5; 6, 8, 10; 5, 12, 13

Megjegyzés. Mint ezt a név is tükrözi, ezek olyan számhármasok, amelyek tagjai egész számok, és amennyiben ezek egy háromszög oldalhosszai, akkor az így megadott oldalhosszúságokból szerkeszthető háromszög derékszögű:



11.1. ábra. $x, y, z \in \mathbb{N}$

Megjegyzés. Ha valamely x_0, y_0, z_0 számhármas megoldása a (11.1) egyenletnek, akkor tetszőleges c egész szám esetén a cx_0, cy_0, cz_0 számhár-

mas is megoldás (az egyenlet c^2-szeresét kapjuk). Emiatt elegendő azokkal a megoldásokkal foglalkoznunk, amelyekre $(x_0, y_0, z_0) = 1$.

11.2. Definíció. Az $x^2+y^2 = z^2$ egyenlet megoldásai közül *alapmegoldásoknak* nevezzük azokat x_0, y_0, z_0 számhármasokat, amelyekre $(x_0, y_0, z_0) = 1$.

Például: A fenti példák közül a 6, 8, 10 nem alapmegoldás, mert a $3, 4, 5$ megoldásból 2-vel való szorzással kapható, a benne szereplő számok legnagyobb közös osztója 2; a másik kettő viszont alapmegoldás.

11.1. Tétel. *Az $x^2 + y^2 = z^2$ egyenlet alapmegoldásai $x_0 = 2mn$, $y_0 = m^2 - n^2$, $z_0 = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, továbbá m és n közül pontosan az egyik páros. (x_0 és y_0 szerepe felcserélhető.)*

Bizonyítás. A bizonyítás során végig fel fogjuk használni azt a tényt, hogy egy számnak és négyzetének pontosan ugyanazok a prímtényezői. (Ez a kanonikus alakból következik.)

1. Először megmutatjuk, hogy ha x_0, y_0, z_0 alapmegoldás, vagyis $x_0^2+y_0^2 = z_0^2$, és $(x_0, y_0, z_0) = 1$, akkor az is teljesül, hogy (x_0, y_0), (y_0, z_0) és (x_0, z_0) is 1.

Ha x_0, y_0, z_0 megoldás, akkor $x_0^2 = z_0^2 - y_0^2$, $y_0^2 = z_0^2 - x_0^2$, $z_0^2 = x_0^2 + y_0^2$, így ha bármelyik jobb oldali kifejezésben is van 1-nél nagyobb közös osztója a két tagnak, akkor van közös prímosztója is, és ez a bal oldali tagnak is osztója. Márpedig egy számnak és négyzetének pontosan ugyanazok a prímosztói. Tehát akármelyik két tagnak is van közös prímosztója, az a harmadik tagnak is osztója.

Ebből már az is következik, hogy nem lehet mind a három szám páros.

2. Belátjuk, hogy a három számból pontosan egy lehet páros. (Ismét felhasználjuk: egy szám pontosan akkor osztható 2-vel – vagyis páros –, amikor a négyzete.)

Nyilván kizárt, hogy két páros van köztük, mert ezeknek akár összege, akár különbsége a harmadik, az is páros lenne. Az is kizárt, hogy mindegyik páratlan, mert két páratlan szám összege és különbsége is páros. Így csak az lehet, hogy egy páros és két páratlan van köztük.

3. Megmutatjuk, hogy nem lehet a z_0 a páros szám közülük.

Ekkor ugyanis x_0 is és y_0 is páratlan lenne, mondjuk $x_0 = 2a + 1$, $y_0 = 2b + 1$. A négyzetösszegük ekkor:

$$x_0^2 + y_0^2 = (2a+1)^2 + (2b+1)^2 = 4\underbrace{(a^2 + a + b^2 + b)}_{k} + 2$$

volna, vagyis z_0^2-nek $4k+2$ alakúnak kellene lennie. Ez viszont lehetetlen, mert egy páros szám négyzete mindig osztható 4-gyel.

4. Ezért vagy az x_0, vagy az y_0 a páros. Tegyük fel, hogy x_0 az. Ekkor:

$$x_0^2 = z_0^2 - y_0^2 = (z_0 - y_0)(z_0 + y_0).$$

Mivel y_0 és z_0 páratlan, $z_0 - y_0$ is és $z_0 + y_0$ is páros. Írhatjuk ezért, hogy

$$\frac{x_0^2}{4} = \frac{z_0^2 - y_0^2}{4} = \frac{z_0 - y_0}{2} \cdot \frac{z_0 + y_0}{2}.$$

Megmutatjuk, hogy $\frac{z_0 - y_0}{2}$ és $\frac{z_0 + y_0}{2}$ relatív prímek.

Két szám legnagyobb közös osztója tetszőleges lineáris kombinációjuknak is osztója (hiszen ha u és v osztható d-vel, akkor $ru + sv$ is osztható d-vel – persze újabb osztók bejöhetnek). A két szám egyik lineáris kombinációja lehet az összegük: z_0, a másik pedig a különbségük: y_0: $(z_0, y_0) = 1$ Mivel a lineáris kombinációk legnagyobb közös osztója 1, így az eredeti számoknak is csak 1 lehet a legnagyobb közös osztója.

Ha egy négyzetszámot két egymással relatív prím szorzatára bontjuk, akkor azok is négyzetszámok lesznek. (A négyzetszám prímtényezőit kétfelé osztjuk, ezek kitevője páros, így a tényezőkben is páros lesz a prímtényezők kitevője.) Ezért

$$\frac{x_0^2}{4} = \left(\frac{x_0}{2}\right)^2 = \left(\frac{z_0 - y_0}{2}\right)\left(\frac{z_0 + y_0}{2}\right)$$

miatt $\frac{z_0 - y_0}{2} = n^2$ és $\frac{z_0 + y_0}{2} = m^2$ valamilyen n, m egész számokra, ahol nyilván $m > n$, és $(m^2, n^2) = 1$ miatt $(m, n) = 1$.

Ezt felhasználva:

$$\begin{aligned} x_0 \text{ (vagy } y_0) &= 2mn \\ y_0 \text{ (vagy } x_0) &= m^2 - n^2 \\ z_0 &= m^2 + n^2 \end{aligned}$$

adódik ($m > n$, $(m, n) = 1$, és pontosan az egyik, nevezetesen a $2mn$ páros). Az alapmegoldások tehát csak ilyen alakúak lehetnek.

5. Legyen most x_0, y_0 és z_0 a fenti alakú. Bebizonyítjuk, hogy ez a számhármas alapmegoldás.

Behelyettesítéssel megmutatjuk, hogy *tetszőleges* m és n egész számok esetén az ilyen alakú számok megoldásai az egyenletnek:

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 =$$

$$= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2.$$

Meg kell még mutatnunk, hogy ha m és n közül pontosan az egyik páros, akkor a fentiek valóban alapmegoldások, vagyis relatív prímek.

Mint azt a 4. lépésben láttuk, $(m^2 - n^2, m^2 + n^2) \mid 2(m^2, n^2) = 2$ (mert $(m, n) = 1$), tehát legfeljebb 2 lehetne a három szám közös osztója. Ám n és m közül pontosan az egyik páros, tehát sem $m^2 - n^2$, sem $m^2 + n^2$ nem osztható 2-vel. Így ezek a számok relatív prímek.

Tehát pontosan a fenti alakú számok az alapmegoldások. □

Megjegyzés. A tételből nyilvánvalóan következik, hogy végtelen sok alapmegoldás van; tetszőleges n-hez végtelen sok olyan m-et találhatunk, amely nagyobb nála, ellenkező paritású, és relatív prím hozzá, és minden ilyen n, m számpárhoz tartozik egy alapmegoldás.

Például:

n	1	1	1	...	2	2	...	3	...
m	2	4	6	...	3	3	...	4	...
$x_0 = 2mn$	4	8	12	...	12	20	...	24	...
$y_0 = m^2 - n^2$	3	15	35	...	5	21	...	7	...
$z_0 = m^2 + n^2$	5	17	37	...	13	29	...	25	...

Megjegyzés. A pitagoraszi számhármasok első ismert „összeírása" a Plimpton 322-es babilóniai agyagtábla kb i.e. 1800-ból. Részletesebben lásd Oystein Ore: Number Theory and Its History, Dover Publications Ins., New York.; Otto Neugebauer, Egzakt tudományok az Ókorban, Gondolat, Budapest, 1984.

A „nagy" Fermat-tétel

Mint az előzőekben láttuk, az $x^2 + y^2 = z^2$ diofantoszi egyenletnek végtelen sok megoldása van. Felmerül a kérdés, hogy mi a helyzet más kitevők esetén, azaz n-től függően mit mondhatunk az $x^n + y^n = z^n$ egyenlet megoldhatóságáról.

Nyilvánvalóan léteznek úgynevezett *triviális megoldások*; minden n-re megoldás például a $(0, 0, 0)$ számhármas, illetve tetszőleges x_0 egész esetén az $x_0 = z_0$, $y_0 = 0$ számhármas, páratlan n-re az $(1, -1, 0)$ stb. *Fermat sejtése* (amelyet mintegy 400 év elteltével, óvatos becslések szerint legalább 7 éves kemény munkával, hatalmas matematikai eszköztár felvonultatásával Andrew Wiles eredetileg több mint 1000 oldalon bizonyított be) a következő volt:

11.2. Tétel. (Nagy Fermat-tétel) *Ha $n \geq 3$, akkor az $x^n + y^n = z^n$ egyenletnek nincs megoldása a pozitív egész számok halmazán.*

Elemi eszközökkel a tételt (Fermat állításával ellentétben) valószínűleg nem lehet bebizonyítani. Azt még elemi eszközökkel is átlátjuk, hogy a tételt elegendő 2-nél nagyobb *prímkitevőkre,* valamint az $n = 4$ kitevőre bizonyítani. Megmutatható ugyanis, hogy ha ezekre igaz lenne az állítás, akkor ebből már következne, hogy minden más kitevőre is igaz. (Magyarul ha n prím és $n = 4$ esetén nincs megoldása az egyenletnek, akkor másra sincs.)

Ha ugyanis az n kitevőnek van páratlan prímosztója, akkor felírható $n = pa$ alakban, ahol p páratlan prím. Ekkor az eredeti egyenlet

$$(x^a)^p + (y^a)^p = (z^a)^p$$

alakban írható, amiről látszik, hogy ha a p kitevő esetén nincs megoldása az egyenletnek, akkor az n kitevő esetén sem lehet megoldás.

Ha pedig az n kitevőnek nincs páratlan prímosztója, akkor kettő hatványa, azaz $n = 2^k$. Ekkor viszont az egyenlet a következő alakba írható:

$$\left(x^{2^{k-2}}\right)^4 + \left(y^{2^{k-2}}\right)^4 = \left(z^{2^{k-2}}\right)^4,$$

amiről leolvasható, hogy ha negyedik hatványokra nincs megoldás, akkor semmilyen nagyobb kettő hatvány kitevő esetén sincs megoldás.

400 év alatt a *Fermat-sejtés* a számelmélet egyik leghíresebb megoldatlan problémájává vált. Az $n = 4$ kitevőre és számos konkrét prímkitevőre – igen mély algebrai eszközök felhasználásával – bizonyították a sejtést, de tetszőleges 2-nél nagyobb n-re sem bizonyítani, sem cáfolni nem sikerült. Rendkívül nagy szenzáció volt, amikor Wiles előállt a nagy titokban végzett kutatásai eredményével –, ez azonban első változatában hibás volt. A tétel bizonyításának javítása alig pár évet váratott magára.

Waring-féle problémakör

Próbáljuk meg a pozitív egész számokat a lehető legkevesebb négyzetszám összegeként előállítani:

$$\begin{array}{lll} 1 = 1^2 & 2 = 1^2 + 1^2 & 3 = 1^2 + 1^2 + 1^2 \\ 4 = 2^2 & 5 = 2^2 + 1^2 & 6 = 2^2 + 1^2 + 1^2 \\ 7 = 2^2 + 1^2 + 1^2 + 1^2 & 8 = 2^2 + 2^2 & 9 = 3^2 \\ 10 = 3^2 + 1^2 & 11 = 3^2 + 1^2 + 1^2 & 12 = 2^2 + 2^2 + 2^2 \end{array}$$

$$13 = 3^2 + 2^2 \qquad 14 = 3^2 + 2^2 + 1^2 \qquad 15 = 3^2 + 2^2 + 1^2 + 1^2$$
$$16 = 4^2 \qquad 17 = 4^2 + 1^2 \qquad 18 = 3^2 + 3^2$$
$$19 = 3^2 + 3^2 + 1^2 \qquad 20 = 4^2 + 2^2 \qquad \vdots$$

Az nyilvánvaló, hogy tetszőleges n pozitív egész szám előállítható négyzetszámok összegeként, hiszen – ha másképp nem – n db 1-es összegeként mindenképp előáll. Érdekes kérdés (akár ragaszkodunk ahhoz, hogy a lehető legkevesebb négyzetszám összegeként írjuk fel a számokat, akár nem), hogy melyik számot hányféleképpen tudom előállítani négyzetszámok összegeként; hogy ehhez – függően a számtól – mikor hány négyzetszámra van szükség; van-e egy olyan n-től független g darabszám, amelyről elmondhatjuk, hogy g darab négyzetszám összegeként minden (pozitív egész) szám előállítható; hogy mi a helyzet akkor, ha nem négyzetszámok, hanem köbszámok, negyedik hatványok stb. összegeként szeretnénk előállítani a számokat.

Az alábbiakban bizonyítás nélkül ismertetünk néhány eredményt.

Először tisztázzuk, hogy milyen feltétel mellett írható fel egy természetes szám *két* négyzetszám összegeként.

11.3. Tétel. (Fermat két négyzetszám tétele) *Az $n = x^2 + y^2$ diofantoszi egyenlet akkor és csak akkor oldható meg a nemnegatív egész számok halmazán, ha az n kanonikus alakjában minden $4k - 1$ alakú prímtényező páros hatványon szerepel.*

Például: A 20 és 100 közötti számok közül a következők állnak elő legfeljebb két négyzetszám összegeként:

$$25 = 5^2, \quad 26 = 5^2 + 1^2, \quad 29 = 5^2 + 2^2, \quad 32 = 4^2 + 4^2,$$
$$34 = 5^2 + 3^2, \quad 36 = 6^2, \quad 37 = 6^2 + 1^2, \quad 40 = 6^2 + 2^2,$$
$$41 = 5^2 + 4^2, \quad 45 = 6^2 + 3^2, \quad 49 = 7^2, \quad 50 = 5^2 + 5^2,$$
$$52 = 6^2 + 4^2, \quad 53 = 7^2 + 2^2, \quad 58 = 7^2 + 3^2, \quad 61 = 6^2 + 5^2,$$
$$64 = 8^2, \quad 65 = 8^2 + 1^2, \quad 68 = 8^2 + 2^2, \quad 72 = 6^2 + 6^2,$$
$$73 = 8^2 + 3^2, \quad 74 = 7^2 + 5^2, \quad 80 = 8^2 + 4^2, \quad 81 = 9^2,$$
$$82 = 9^2 + 1^2, \quad 85 = 9^2 + 2^2, \quad 89 = 8^2 + 5^2, \quad 90 = 9^2 + 3^2,$$
$$97 = 9^2 + 4^2, \quad 98 = 7^2 + 7^2.$$

Bizonyítás. (Euler ötletével.) Az egyszerűség kedvéért a két négyzetszám összegeként előálló számokat nevezzük most négyzetösszegnek.

I. Először belátjuk, hogy minden olyan szám négyzetösszeg, amelynek prímtényezős felbontásában a $4k-1$ alakú prímek páros hatványon szerepelnek.

A bizonyítást több lépésben végezzük el.

1. Ha két szám négyzetösszeg, akkor a szorzatuk is az:

$$(a^2+b^2)(u^2+v^2) = a^2u^2+a^2v^2+b^2u^2+b^2v^2 = (au+bv)^2+(av-bu)^2.$$

Eszerint elegendő alkalmas tényezőnként vizsgálni a számot.

2. A 2 nyilván négyzetösszeg.

3. A $4k-1$ alakú prímszámok nyilvánvalóan nem négyzetösszegek (négyzetszámok 4 szerint a maradéka 0 vagy 1 lehet), de a négyzeteik nyilván igen.

4. Belátjuk, hogy a $4k+1$ alakú prímszámok felírhatók két négyzetszám összegeként. Ha a p prímszám $4k+1$ alakú, akkor megadható hozzá egy alkalmas x, amelyre x^2+1 többszöröse p-nek, azaz $x^2+1 = tp$ valamely t-re.

A Wilson-tétel (8.10. Tétel) szerint $1\cdot 2\cdot \ldots \cdot (4k) \equiv -1 \pmod{p}$. Ez kongruens $(-2k)\cdot(2k)\cdot(-2k+1)\cdot(2k-1)\cdot\ldots(-2)\cdot 2\cdot(-1)\cdot$ 1-gyel, illetve (az előjeleket alkalmasan összegyűjtve) $(-1)\cdot(2k)^2\cdot(2k-1)^2\cdot\ldots\cdot 1^2$-nel. Ez a -1 szorzótól eltekintve négyzetszám, ezért x-nek választhatjuk a $(2k)\cdot(2k-1)\cdot\ldots\cdot 1 = (2k)!$-t. Erre nyilván $x^2+1 \equiv 0 \pmod{p}$, azaz van olyan t, amelyre $pt = x^2+1$. Sőt, választhatjuk x-nek a $(2k)!$ p szerinti maradékát (hiszen azonos maradékot adó számok négyzete ugyanazzal kongruens), így p-nek még kisebb többszörösét írjuk fel x^2+1 alakban.

Mutatunk egy eljárást (*végtelen leszállás*), amely szerint az $x^2+y^2 = tp$ felíráshoz találunk olyan u, v és $t_1 < t$ számokat, amelyekkel $u^2+v^2 = t_1p$. Ennek az eljárásnak véges sokszori alkalmazásával eljutunk $1\cdot p$ felírásáig.

Legyen most x-nek és y-nak t szerinti *legkisebb abszolút értékű maradéka* x_1 és y_1, és tekintsük az xx_1+yy_1, xy_1-x_1y, valamint az $x_1^2+y_1^2$ számokat. Határozzuk meg, mivel kongruensek ezek t szerint.

$$x_1^2+y_1^2 \equiv xx_1+yy_1 \equiv x^2+y^2 \equiv 0, \qquad xy_1-x_1y \equiv xy-xy \equiv 0 \pmod{t}$$

Mindegyik 0-val kongruens, vagyis ezek a számok oszthatók t-vel. Legyen ekkor

$$u = \frac{xx_1+yy_1}{t}, \qquad v = \frac{xy_1-x_1y}{t}.$$

$$u^2+v^2 = \frac{x^2x_1^2+y^2y_1^2+2xx_1yy_1+x^2y_1^2+x_1^2y^2-2xx_1yy_1}{t^2} =$$
$$= \frac{x^2(x_1^2+y_1^2)+y^2(x_1^2+y_1^2)}{t^2} = \frac{x^2+y^2}{t}\cdot\frac{x_1^2+y_1^2}{t} = p\cdot\frac{x_1^2+y_1^2}{t}$$

nyilván egész szám, p-nek többszöröse. Legyen ekkor $t_1 = \dfrac{x_1^2+y_1^2}{t}$. Már csak azt kell belátnunk, hogy $t_1 < t$.

Mivel x_1 és y_1 az x-nek, illetve az y-nak t szerinti legkisebb abszolút értékű maradéka, $|x_1| \leq \frac{t}{2}$ és $|y_1| \leq \frac{t}{2}$. Ezért $x_1^2 + y_1^2 \leq 2\frac{t^2}{4} < t^2$. Azaz $t_1 = \frac{x_1^2 + y_1^2}{t} < t$.

Az eljárást addig folytatva, amíg lehet, a $tp > t_1p > t_2p > \ldots > p$ számok mindegyikét négyzetösszeg alakban írjuk fel. Ebből nekünk csak a p felírhatósága volt a célunk.

Összefoglalva: ha egy szám kanonikus alakjában a 2, $4k+1$ alakú prímek, illetve $4k-1$ alakú prímek páros hatványai szerepelnek, akkor az felírható két négyzetszám összegeként.

II. Most bebizonyítjuk, hogy ha egy szám felírható két négyzetszám összegeként, akkor semelyik $4k-1$ alakú prímtényezője sem szerepelhet páratlan hatványon.

1. Egy négyzetösszeget elosztva a 2 vagy egy $4k+1$ alakú prímtényezőjével, ismét négyzetösszeget kapunk. Legyen ugyanis p az a^2+b^2-nek $4k+1$ alakú prímosztója vagy a 2. Ekkor $p = u^2 + v^2$, mint azt a bizonyítás első részében láttuk. Mivel

$$(au+bv)(au-bv) = a^2u^2 - b^2v^2 = a^2u^2 + b^2u^2 - b^2u^2 - b^2v^2 = \\ = (a^2+b^2)u^2 - b^2(u^2+v^2)$$

osztható p-vel (mert $p \mid (a^2+b^2)$ és $p = (u^2+v^2)$), így vagy $au+bv$, vagy $au-bv$ biztosan osztható p-vel (mert p prímszám).

(a) Ha $p \mid au+bv$, akkor tekintsük az

$$\left(\frac{au+bv}{p}\right)^2 + \left(\frac{av-bu}{p}\right)^2$$

összeget. Elvégezve a műveleteket az

$$\left(\frac{au+bv}{p}\right)^2 + \left(\frac{av-bu}{p}\right)^2 = \frac{a^2u^2+b^2v^2+a^2v^2+b^2u^2}{p^2} = \\ = \frac{(a^2+b^2)(u^2+v^2)}{p^2} = \frac{a^2+b^2}{p}$$

egész számot kapjuk. A kiinduló összeg első tagja szintén egész szám, ezért a második tag is az. Vagyis előállítottuk $\frac{a^2+b^2}{p}$-t két egész szám négyzetösszegeként.

(b) Ha $p \mid au-bv$, akkor tekintsük az

$$\left(\frac{au-bv}{p}\right)^2 + \left(\frac{av+bu}{p}\right)^2$$

összeget, és az előbbihez hasonló gondolatmenettel igazolható, hogy ez is az $\dfrac{a^2+b^2}{p}$ két egész szám négyzetösszegeként való felírása.

Ezek szerint egy négyzetösszeget elosztva minden $4k+1$ alakú, illetve 2-es prímosztójával, továbbra is négyzetösszeget kapunk.

2. Ha $(a,b)=d$, akkor még d^2-tel is oszthatunk (hiszen $d^2 \mid a^2$, $d^2 \mid b^2$), és továbbra is négyzetösszeget kapunk:

$$\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2$$

3. Végül bebizonyítjuk, hogy ha az a^2+b^2 négyzetösszegnek van $4k-1$ alakú prímtényezője, akkor az a-t és b-t is osztja. (És $\left(\dfrac{a}{p}\right)^2+\left(\dfrac{b}{p}\right)^2$ négyzetösszeg.)

Ha p osztója a^2+b^2-nek és $p=4t-1$, akkor ha p nem osztója a-nak (így b-nek sem), akkor $a^2 \equiv -b^2 \pmod{p}$, vagyis minden páratlan hatványukra igaz, hogy az egyik a másik ellentettjével kongruens. A kis Fermat-tétel alapján azonban

$$1 \equiv a^{p-1} = a^{4t-2} = \left(a^2\right)^{2t-1} \pmod{p},$$
$$1 \equiv b^{p-1} = b^{4t-2} = \left(b^2\right)^{2t-1} \pmod{p},$$

ami ellentmondás ($1 \not\equiv -1$). Ezért a is és b is osztható p-vel.

Összefoglalva: egy a^2+b^2 négyzetösszeg kanonikus alakjában szereplő $4k-1$ alakú prímek a-t és b-t is osztják, a többi prímtényező viszont önmagában is négyzetösszeg. □

Az iménti bizonyításban szerepelt egy állítás, amelynek következményeként be tudjuk bizonyítani:

11.1. Következmény. *Végtelen sok $4k+1$ alakú prímszám van.*

Bizonyítás. Ha csak véges sok $4k+1$ alakú prímszám van, akkor ezek szorzatát jelöljük c-vel, és vizsgáljuk a $d=(2c)^2+1=(2c)^2+1^2$ számot. Mivel $(2c)$ és 1 relatív prím, így (az előző tétel II./3. pontja alapján) nincsen $4k-1$ alakú prímosztója. A 2 sem osztója, tehát csak $4k+1$ alakú osztója lehet. Mivel azonban d a felírásához használt összes $4k+1$ alakú prímhez relatív prím, így biztosan van más $4k+1$ alakú prím is. □

11.4. Tétel. (Gauss) *Az $n^2=x^2+y^2+z^2$ diofantoszi egyenlet akkor és csak akkor oldható meg, ha n nem $4^k(8l+7)$ alakú.*

Például: Azok a 20 és 100 közötti számok, amelyek legfeljebb két négyzetszám összegeként nem állnak elő, de három négyzetszám összegeként előállnak, a következők:

$$
\begin{array}{lll}
21 = 4^2 + 2^2 + 1^2, & 22 = 3^2 + 3^2 + 2^2, & 24 = 4^2 + 2^2 + 2^2, \\
27 = 5^2 + 1^2 + 1^2, & 30 = 5^2 + 2^2 + 1^2, & 33 = 5^2 + 2^2 + 2^2, \\
35 = 5^2 + 3^2 + 1^2, & 38 = 5^2 + 3^2 + 2^2, & 42 = 5^2 + 4^2 + 1^2, \\
43 = 5^2 + 3^2 + 3^2, & 44 = 6^2 + 2^2 + 2^2, & 46 = 6^2 + 3^2 + 1^2, \\
48 = 4^2 + 4^2 + 4^2, & 51 = 5^2 + 5^2 + 1^2, & 54 = 7^2 + 2^2 + 1^2, \\
56 = 6^2 + 4^2 + 2^2, & 57 = 7^2 + 2^2 + 2^2, & 59 = 5^2 + 5^2 + 3^2, \\
62 = 6^2 + 5^2 + 1^2, & 66 = 8^2 + 1^2 + 1^2, & 67 = 7^2 + 3^2 + 3^2, \\
69 = 8^2 + 2^2 + 1^2, & 70 = 6^2 + 5^2 + 3^2, & 75 = 5^2 + 5^2 + 5^2, \\
76 = 6^2 + 6^2 + 2^2, & 77 = 8^2 + 3^2 + 2^2, & 78 = 7^2 + 5^2 + 2^2, \\
83 = 9^2 + 1^2 + 1^2, & 84 = 8^2 + 4^2 + 2^2, & 86 = 9^2 + 2^2 + 1^2, \\
88 = 6^2 + 6^2 + 4^2, & 91 = 9^2 + 3^2 + 1^2, & 93 = 8^2 + 5^2 + 2^2, \\
94 = 9^2 + 3^2 + 2^2, & 96 = 8^2 + 4^2 + 4^2, & 99 = 9^2 + 3^2 + 3^2.
\end{array}
$$

11.5. Tétel. (Lagrange) *Minden n természetes szám előállítható legfeljebb négy négyzetszám összegeként.*

Például:

$$
\begin{array}{ll}
23 = 3^2 + 3^2 + 2^2 + 1^2, & 28 = 3^2 + 3^2 + 3^2 + 1^2, \\
31 = 3^2 + 3^2 + 3^2 + 2^2, & 39 = 6^2 + 1^2 + 1^2 + 1^2, \\
47 = 5^2 + 3^2 + 3^2 + 2^2, & 55 = 5^2 + 5^2 + 2^2 + 1^2, \\
60 = 7^2 + 3^2 + 1^2 + 1^2, & 63 = 7^2 + 3^2 + 2^2 + 1^2, \\
71 = 7^2 + 3^2 + 3^2 + 2^2, & 79 = 5^2 + 5^2 + 5^2 + 2^2, \\
87 = 7^2 + 5^2 + 3^2 + 2^2, & 92 = 7^2 + 5^2 + 3^2 + 3^2, \\
95 = 7^2 + 6^2 + 3^2 + 1^2. &
\end{array}
$$

Megjegyzés. A fenti példákban szereplő számok nagy része nemcsak egyféleképpen áll elő, például

$$99 = 9^2 + 3^2 + 3^2 = 7^2 + 7^2 + 1^2 \quad 95 = 7^2 + 6^2 + 3^2 + 1^2 = 9^2 + 3^2 + 2^2 + 1^2.$$

Általánosan megfogalmazva a Waring-féle probléma a következő: Van-e tetszőleges k (pozitív egész) kitevő esetén olyan $g(k)$ szám, amelyre igaz,

hogy minden pozitív egész előáll legfeljebb $g(k)$ darab k-adik hatvány összegeként?

A fentiekből tudjuk, hogy $k = 2$ esetén létezik ilyen szám, mégpedig $g(2) = 4$. Hilbert (német matematikus 1862–1943) 1909-ben bizonyította, hogy tetszőleges k esetén van ilyen $g(k)$ szám.

Pell-egyenletek

Számos számelméleti probléma visszavezethető egy $x^2 - dy^2 = 1$ típusú egyenlet (d egy adott konstans) megoldásainak keresésére. Az ilyen alakú diofantoszi egyenleteket nevezik *Pell-féle egyenleteknek.*

Ha d negatív vagy ha d pozitív négyzetszám, akkor csak néhány (és triviális) megoldása van az egyenletnek:

- Ha $d \leq -2$, akkor $-d \geq 2$, így $x^2 - dy^2 \geq x^2 + 2y^2$, ezért az egyenletnek ilyenkor csak az $(1, 0)$ és a $(-1, 0)$ számpár megoldása.
- Ha $d = -1$, akkor az $x^2 + y^2 = 1$ egyenletet kapjuk, amelynek összes megoldása: $(1, 0)$, $(-1, 0)$, $(0, 1)$, $(0, -1)$.
- Ha $d = k^2$, akkor az $x^2 - k^2y^2 = (x - ky)(x + ky) = 1$ egyenletet kapjuk. Mivel két egész szám szorzata csak úgy lehet 1, ha vagy mindkettő 1, vagy mindkettő -1, $(x - ky) = (x + ky) = 1$ vagy $(x - ky) = (x + ky) = -1$. Ha $d \neq 0$ (és így k sem), akkor az első esetben az $(1, 0)$, a második esetben a $(-1, 0)$ számpár a megoldás.

A $d = 0$ esetben nyilván végtelen sok megoldás van, ilyenkor $x = \pm 1$, y pedig tetszőleges szám lehet.

Azokban az esetekben, amikor $d > 1$ és d nem négyzetszám, igaz a következő tétel (amelyet bizonyítás nélkül közlünk):

11.6. Tétel. *Ha $d > 1$ és $d \neq k^2$, akkor az $x^2 - dy^2 = 1$ diofantoszi egyenletnek végtelen sok megoldása van.*

Megjegyzés. A tételben szereplő egyenlet egy hiperbola egyenlete. Az, hogy az egyenletnek végtelen sok megoldása van, azt jelenti, hogy minden ilyen egyenletű hiperbola végtelen sok rácsponton halad át.

Megjegyzés. Nem is nagyon meglepő módon a számelméleti kérdések egy részére analitikus válasszal tudunk szolgálni (prímszámok sűrűsége). Más

kérdések során – például az utóbbi tétel esetében – másodrendű görbékre illeszkedő rácspontokat keresünk. Hasonló volt az eset a Nagy Fermat-tétel esetében is. A matematikának azt az ágát, amelynek segítségével megválaszolták ezt a kérdést, algebrai geometriának nevezzük. Ez a matematikának egy fiatal, nagyon mély, sokféle matematika diszciplínához kapcsolódó ága.

Feladatok

1. Egy tepsi süteményt egybevágó téglalap alapú darabokra szeletelünk az edény szélével párhuzamos vágásokkal. A szélén lévő szeletek száma a belső szeletek számának fele. Hány szeletre vághattuk fel a süteményt?

2. Keressen olyan pitagoraszi számhármasokat, amelynek számai számtani sorozatot alkotnak!

   Van-e olyan pitagoraszi számhármas, amelynek számai mértani sorozatot alkotnak?

3. Igazolja, hogy minden pitagoraszi számhármas számai között van legalább egy 3-mal osztható szám! (Mondja meg, hogy milyen esetben lehet több is?)

   Igazolja, hogy a 3-mal osztható szám nem lehet a legnagyobb!

   Igazolja, hogy minden pitagoraszi számhármas számai között van legalább egy 5-tel osztható szám! (Mondja meg, hogy milyen esetben lehet több is?)

   Lehet-e az 5-tel osztható szám a legnagyobb?

   Igazolja, hogy a pitagoraszi számhármasok számaira a 2-n, 3-on, 5-ön kívül más számmal való az előzőekéhez hasonló oszthatóságot nem lehet megmutatni!

4. Írja fel $\frac{2}{7}$-et két 1 számlálójú tört összegeként! (Minden lehetséges módon!) Felírható-e $\frac{3}{7}$ két 1 számlálójú tört összegeként?

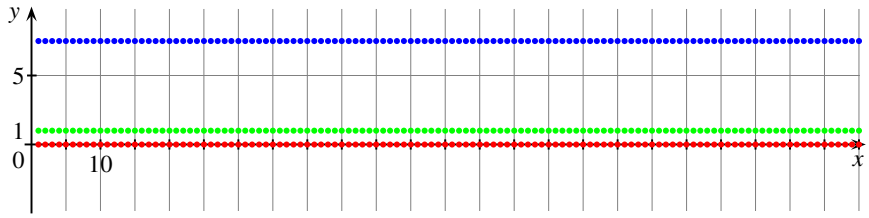
12. fejezet

Számelméleti függvények

12.1. Definíció. A pozitív egész számok halmazán értelmezett függvényeket *számelméleti függvények*nek nevezzük.

Például:

(1) $f_0 \colon n \mapsto 0$ (az azonosan 0 függvény) (12.1. ábra)



12.1. ábra. A konstans függvény is számelméleti függvény

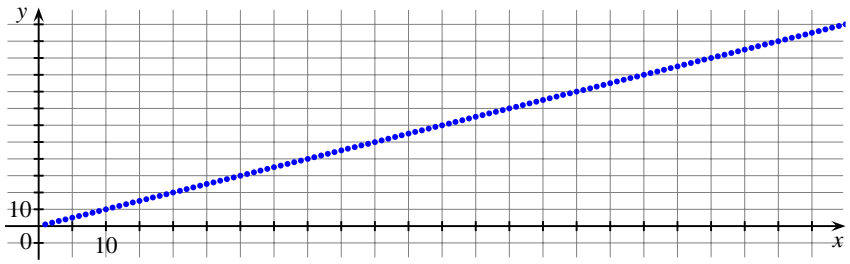
(2) $f_1 \colon n \mapsto 1$, illetve $f_c \colon n \mapsto c$ (konstans függvény) (12.1. ábra)

(3) $f_n \colon n \mapsto n$ (minden számhoz saját magát rendeljük) (12.2. ábra)

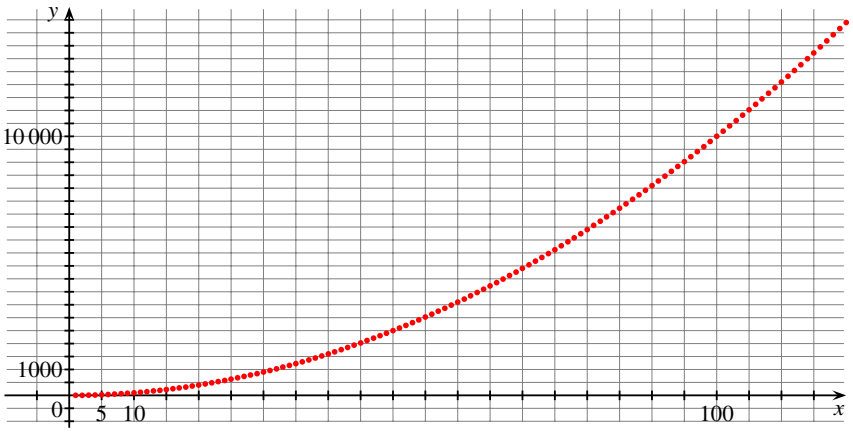
(4) $f_{n^2} \colon n \mapsto n^2$ (minden számhoz hozzárendeljük a négyzetét) (12.3. ábra)

(5) $n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$, $n \mapsto \sum_{i=0}^{k} a_i$ (minden számhoz hozzárendeljük számjegyeinek összegét) (12.4. ábra)

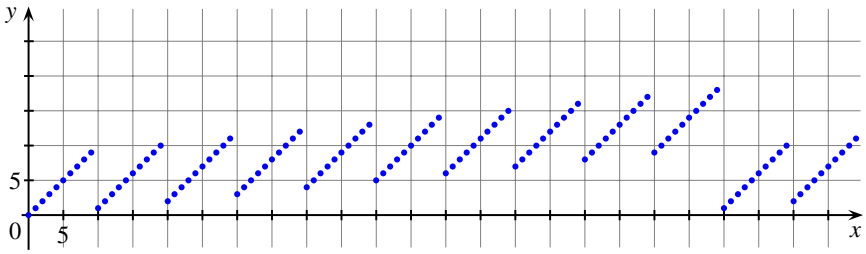
(6) $n = kq + r$ ahol $0 \leq r < |k|$ $(k \geq 2)$, $n \mapsto r$ (minden számhoz a k-val való osztási maradékát rendeljük) (12.5., 12.6. ábra)



12.2. ábra. Az indentitás függvény is számelméleti függvény



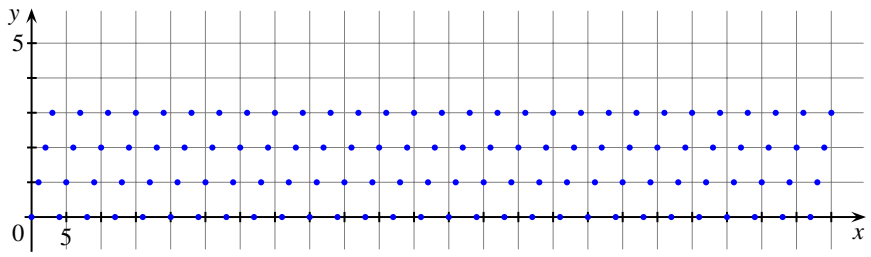
12.3. ábra. Az n^2 függvény



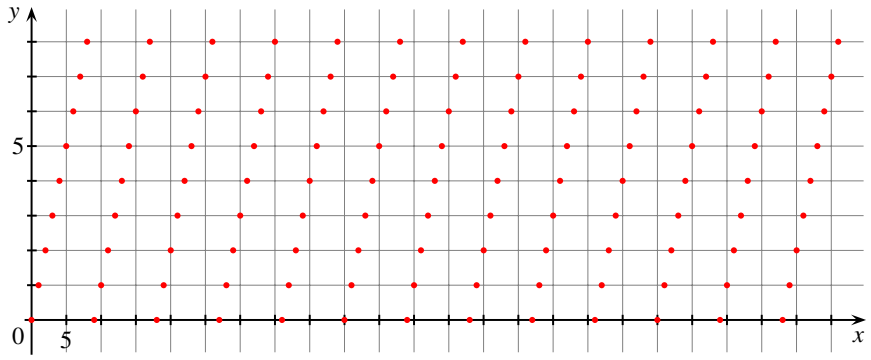
12.4. ábra. A számjegyek összege függvény

(7) $n \mapsto d(n)$ (minden számhoz hozzárendeljük pozitív osztóinak számát) (12.7. ábra)

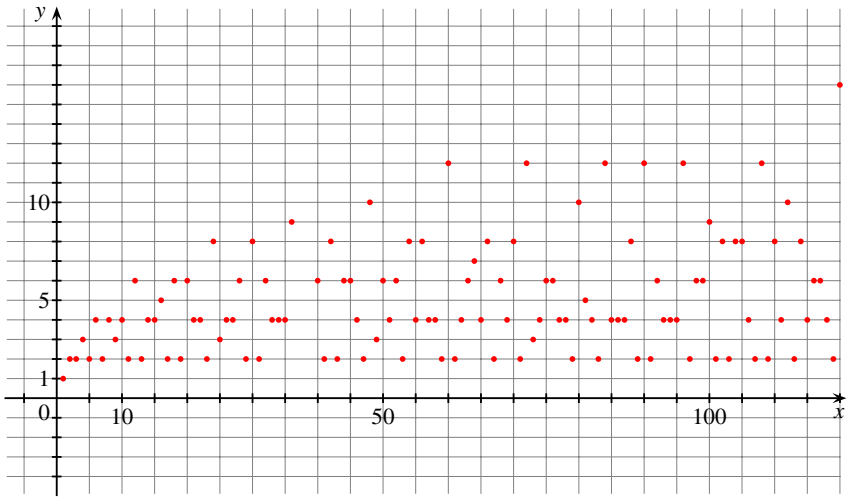
http://www.cs.elte.hu/~kfried/algebra1/DividorsNum.jarEz a program megadja egy szám pozitív osztóinak számát ($d(n)$).



12.5. ábra. A számok 5 szerinti maradéka



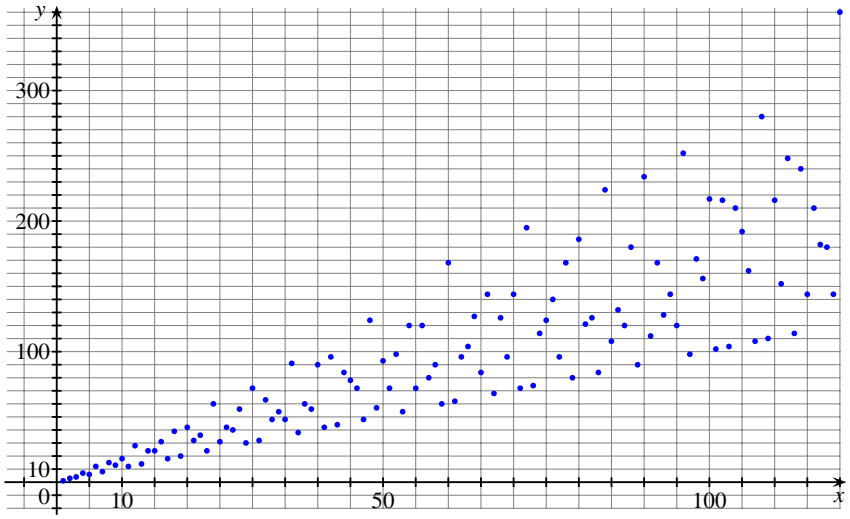
12.6. ábra. A számok 9 szerinti maradéka



12.7. ábra. A számok pozitív osztóinak száma

(8) $\sigma(n)\colon n \mapsto \sum_{d_i|n} d_i$ (minden számhoz hozzárendeljük pozitív osztóinak összegét) (12.8. ábra)

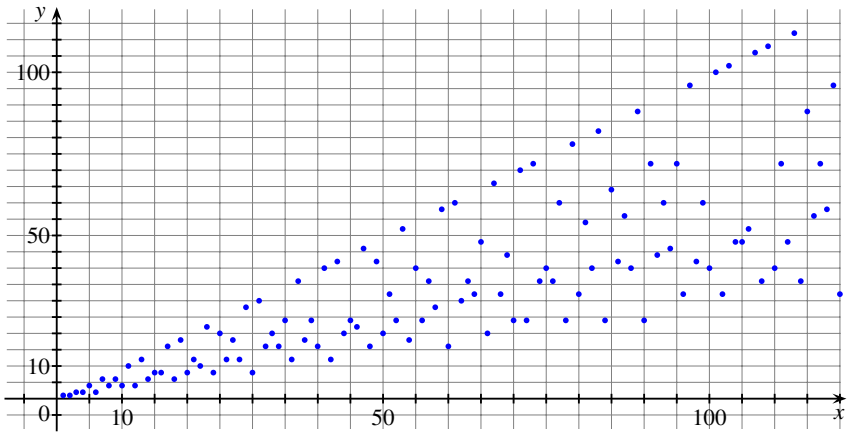
http://www.cs.elte.hu/~kfried/algebra1/DividorSum.jarEz a program megadja egy szám pozitív osztóinak összegét ($\sigma(n)$).



12.8. ábra. A számok pozitív osztóinak összege

(9) $n \mapsto \varphi(n)$ (minden számhoz hozzárendeljük a nála nem nagyobb számok között a hozzá relatív prímek darabszámát) (12.9. ábra)

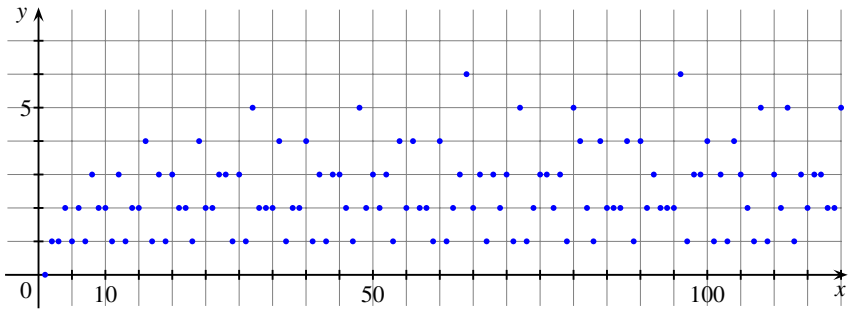
http://www.cs.elte.hu/~kfried/algebra1/Phi.jarEz a program megadja egy n számhoz a $\varphi(n)$ értéket.



12.9. ábra. A φ számelméleti függvény

(10) $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $\nu(n)\colon n \mapsto \alpha_1 + \alpha_2 + \dots + \alpha_k$ (minden számhoz hozzárendeljük prímtényezőinek számát) (12.10. ábra)

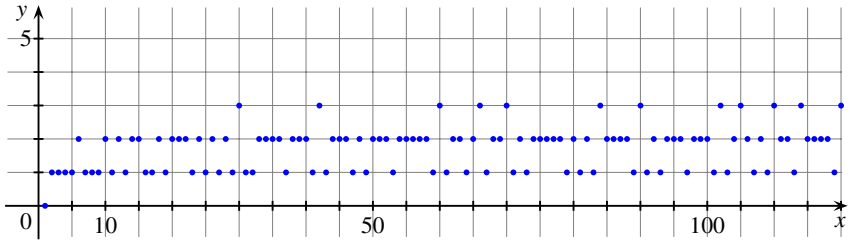
http://www.cs.elte.hu/~kfried/algebra1/PrimeDividors.jarEz a program megadja egy n szám kanonikus alakjában szereplő prímek számát.



12.10. ábra. A prímtényezők száma

(11) $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $\kappa(n)\colon n \mapsto k$ (minden számhoz hozzárendeljük különböző prímtényezőinek számát) (12.11. ábra)

http://www.cs.elte.hu/~kfried/algebra1/PrimeDividors2.jarEz a program megadja egy n szám kanonikus alakjában szereplő különböző prímtényezők számát.

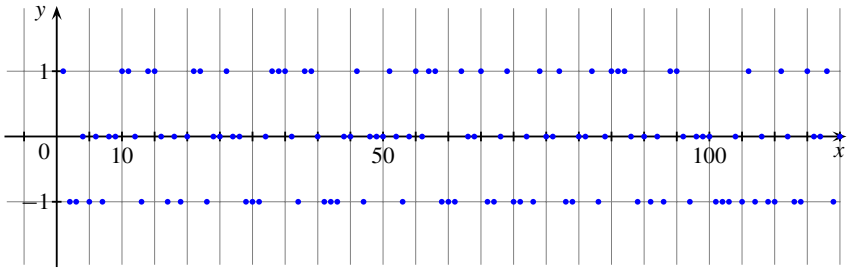


12.11. ábra. A különböző prímosztók száma

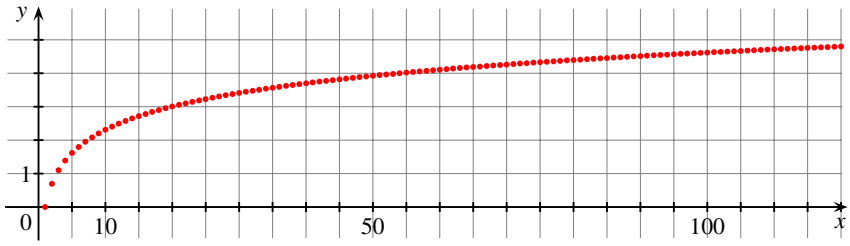
(12) $\mu(n) = \begin{cases} 1 & \text{ha } n = 1 \\ (-1)^r & \text{ha } n = p_1 p_2 \dots p_r, \text{ ahol } p_i \neq p_j \\ 0 & \text{egyébként} \end{cases}$ (Moebius-függvény) (12.12. ábra)

(13) $f\colon x \mapsto \ln x$ (minden számhoz a természetes alapú logaritmusát rendeljük) (12.13. ábra)

12.2. Definíció. Az $f(n)$ számelméleti függvény *multiplikatív,* ha minden $(a, b) = 1$ számpárra, $f(ab) = f(a)f(b)$.



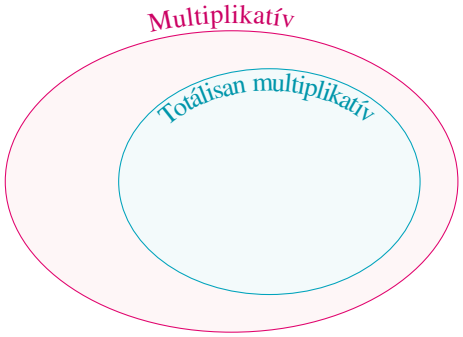
12.12. ábra. A Moebius számelméleti függvény



12.13. ábra. $n \mapsto \ln n$ – ez is számelméleti függvény!

Ha az $f(ab) = f(a)f(b)$ összefüggés nemcsak a relatív prím, hanem tetszőleges a, b számokra teljesül, akkor az $f(n)$ függvény *totálisan multiplikatív.*

12.1. Állítás. *Minden totálisan multiplikatív függvény multiplikatív is.*



12.14. ábra. Minden totálisan multiplikatív függvény multiplikatív is

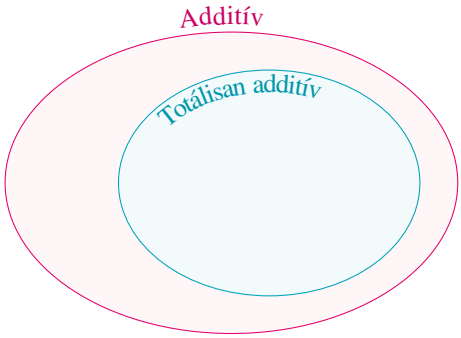
Bizonyítás. Ha minden a, b számpárra teljesül a multiplikativitás, akkor a relatív prím párokra is biztosan teljesül. □

Megjegyzés. A definíció szerint úgy tűnik, mintha a multiplikativitáshoz egy további feltételt kellene kielégítenük a számpároknak a totális multiplikativitáshoz képest, azonban éppen ellenkezőleg: egy megszorítást ($f(ab) = f(a)f(b)$) kell kevesebb elemnek teljesítenie a nem totálisan multiplikatív függvényeknek.

12.3. Definíció. Az $f(n)$ számelméleti függvény *additív*, ha minden $(a, b) = 1$ számpárra $f(ab) = f(a) + f(b)$.

Ha az $f(ab) = f(a) + f(b)$ összefüggés nemcsak a relatív prím, hanem minden a, b számpárra teljesül, akkor az $f(n)$ függvény totálisan additív.

12.2. Állítás. *Minden totálisan additív függvény additív is.*



12.15. ábra. Minden totálisan additív függvény additív is

Bizonyítás. Ha minden a, b számpárra teljesül az additivitás, akkor a relatív prím párokra is biztosan teljesül. □

A fenti példák közül:

(1) Az f_0 függvény totálisan multiplikatív is és totálisan additív is (hiszen minden a, b számpárra $f(ab) = f(a)f(b) = f(a) + f(b) = 0$).

(2) Az f_1 függvény totálisan multiplikatív, de nem additív (hiszen minden a, b számpárra $f(ab) = f(a)f(b) = 1$, míg $f(a)+f(b) = 2$). Ha $c \neq 0$ és $c \neq 1$, akkor az f_c függvény nem is multiplikatív és nem is additív (hiszen $f(ab) = c$, míg $f(a)f(b) = c^2$ és $f(a) + f(b) = 2c$).

(3) Az f_n függvény totálisan multiplikatív és nem additív (tetszőleges a, b számpár esetén $f(a) = a$, $f(b) = b$, $f(ab) = ab = f(a)f(b)$, de $f(a) + f(b) = a + b$, ami általában nem egyenlő ab-vel).

(4) Az f_{n^2} függvény totálisan multiplikatív és nem additív (minden a, b-re $f(ab) = (ab)^2 = a^2b^2 = f(a)f(b)$, de $f(a) + f(b) = a^2 + b^2$).

(5) A függvény nem is multiplikatív és nem is additív (ha például $a = 15$ és $b = 37$, akkor $f(15) = 6$ és $f(37) = 10$, így $f(15)f(37) = 60$ és $f(15) + f(37) = 16$ míg $f(15 \cdot 37) = f(555) = 15$).

(6) A függvény nem is multiplikatív és nem is additív (mert egy szorzat k-val való osztási maradéka általában nem egyezik meg a tényezők maradékainak szorzatával (csak a maradékok szorzatának maradékával), illetve összegével).

(7) A $d(n)$ függvény multiplikatív (de nem totálisan) és nem additív. A multiplikativitást a 12.1. Tételben tisztázzuk. Nem totálisan multiplikatív, mert például ha $a = 4$ és $b = 6$, akkor $d(4 \cdot 6) = d(24) = 8$, míg $d(4)d(6) = 3 \cdot 4 = 12$. Nem is additív, mert például $d(4) + d(7) = 3 + 2 = 5$, míg $d(4 \cdot 7) = 6$.

(8) A $\sigma(n)$ függvény multiplikatív (de nem totálisan) és nem additív. A multiplikativitást a 12.1. Tételben tisztázzuk. Nem totálisan multiplikatív, mert például $a = 4$ és $b = 6$ esetén $\sigma(4) = 1+2+4 = 7$ és $\sigma(6) = 1+2+3+6 = 12$, így $\sigma(4)\sigma(6) = 84$, míg $\sigma(4\cdot6) = \sigma(24) = 1+2+3+4+6+8+12+24 = 60$. Nem is additív, mert például $\sigma(4)+\sigma(7) = 7+8 = 15$, míg $\sigma(4\cdot7) = \sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

(9) A $\varphi(n)$ függvény multiplikatív (de nem totálisan) és nem additív. A multiplikativitást a 12.1. Tételben tisztázzuk. Nem totálisan multiplikatív, hiszen például $\varphi(4) = 2$ és $\varphi(6) = 2$, így $\varphi(4)\varphi(6) = 4$, míg $\varphi(4 \cdot 6) = \varphi(24) = 8$. Nem is additív, mert például $\varphi(4 \cdot 7) = 12$, $\varphi(4) + \varphi(7) = 8$.

(10) A $\nu(n)$ függvény nem multiplikatív, de totálisan additív. (Nem multiplikatív, mert például $\nu(6) = 2$ és $\nu(7) = 1$, így $\nu(6)\nu(7) = 2$, de $\nu(6\cdot7) = 3$. Totálisan additív, hiszen az ab szorzat prímtényezőit az a prímtényezőinek és a b prímtényezőinek egyesítése alkotja.)

(11) A $\kappa(n)$ függvény nem multiplikatív, de additív (nem totálisan). (Nem multiplikatív, mert például $\kappa(6) = 2$ és $\kappa(7) = 1$, így $\kappa(6)\kappa(7) = 2$, de $\kappa(6 \cdot 7) = 3$. Additív, mert ha $(a, b) = 1$, akkor a-nak és b-nek nincs közös prímtényezője, így az ab szorzatnak éppen annyi különböző prímtényezője lesz, amennyi a-nak és b-nek összesen volt. Nem totálisan additív, hiszen például $\kappa(4) + \kappa(6) = 1 + 2 = 3$, míg $\kappa(4 \cdot 6) = 2$.)

(12) A $\mu(n)$ függvény multiplikatív (nem totálisan) és nem additív. A multiplikativitást a 12.1. Tételben tisztázzuk. Nem totálisan multiplikatív, mert például $\mu(6) = (-1)^2 = 1$ és $\mu(10) = (-1)^2 = 1$ így $\mu(6)\mu(10) = 1$, míg $\mu(6 \cdot 10) = 0$. A függvény nem additív, mert például $\mu(1 \cdot 2) = -1$, de $\mu(1) + \mu(2) = 0$.

(13) Az $\ln x$ függvény totálisan additív, mert tetszőleges a, b számokra $\ln(ab) = \ln a + \ln b$. Természetesen nem multiplikatív, például $1 = \ln(1 \cdot e) \neq \ln 1 \cdot \ln e = 0 \cdot 1 = 0$. Ez – bár számelméleti függvény – nem tipikus számelméleti függvény.

A fentiek egy részét érdemes külön tételként is megfogalmaznunk:

12.1. Tétel. *A (7) $d(n)$, (8) $\sigma(n)$, (9) $\varphi(n)$, (12) $\mu(n)$ függvények multiplikatívak:*

Bizonyítás. Mindegyik függvény multiplikativitásának bizonyításához vegyük az

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \qquad \text{és} \qquad b = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

számokat. Ha a és b relatív prímek, akkor semmilyen i-re és j-re nem egyenlő p_i és q_j.

(7) $d(n)$: A 6.4. Tétel értelmében

$$d(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1), \quad d(b) = (\beta_1 + 1)(\beta_2 + 1) \dots (\beta_l + 1).$$

Ugyanakkor

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}.$$

Ha most $(a, b) = 1$, akkor $p_i \neq q_j$, így

$$\begin{aligned} d(ab) &= (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)(\beta_1 + 1)(\beta_2 + 1) \dots (\beta_l + 1) = \\ &= d(a)d(b), \end{aligned}$$

tehát φ valóban multiplikatív.

(8) $\sigma(n)$: Ha $(a, b) = 1$, akkor a 6.8. Tétel értelmében az ab szorzat tetszőleges d osztója előáll $a'b'$ alakban, ahol $a' \mid a$ és $b' \mid b$. Ekkor az ab szorzat osztóinak összege:

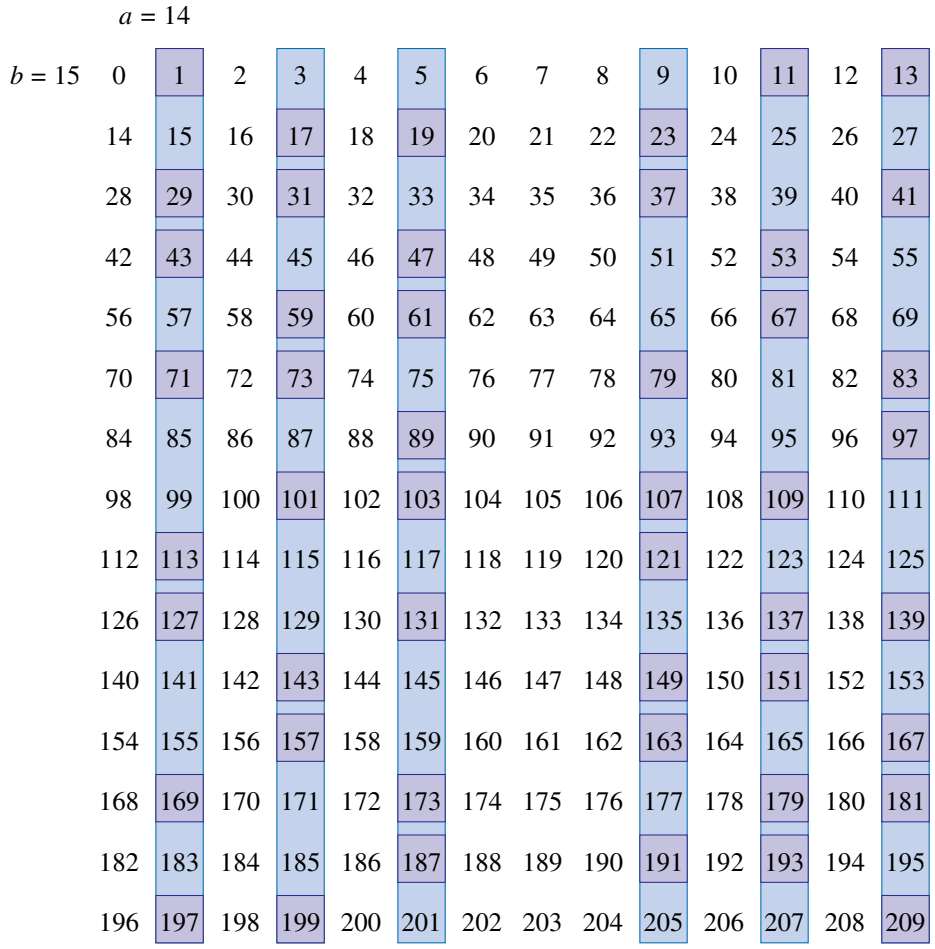
$$\sigma(ab) = \sum_{a_i \mid a} \sum_{b_j \mid b} a_i b_j = \sum_{a_i \mid a} a_i \sum_{b_j \mid b} b_j = \sigma(a)\sigma(b),$$

vagyis a függvény multiplikatív.

(9) $\varphi(n)$: Számoljuk össze, hogy hány olyan, ab-nél nem nagyobb (pozitív egész) szám van, amely relatív prím ab-hez! A 6.7. Tétel értelmében az ab szorzathoz pontosan azok a számok lesznek relatív prímek, amelyek a-hoz is és b-hez is relatív prímek. Azokat az ab-nél nem nagyobb számokat, amelyek a-hoz relatív prímek, a következő felsorolás tartalmazza (ezek közül kell majd kiválasztanunk azokat, amelyek b-hez is relatív prímek) ($a = 14$, $b = 15$ esetén a kiválasztás folyamatát a 12.16. ábra szemlélteti):

$$\begin{array}{rccccc}
0\text{–}a\text{:} & r_1 & r_2 & \dots & r_{\varphi(a)} \\
a\text{–}2a\text{:} & a+r_1 & a+r_2 & \dots & a+r_{\varphi(a)} \\
2a\text{–}3a\text{:} & 2a+r_1 & 2a+r_2 & \dots & 2a+r_{\varphi(a)} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(b-1)a\text{–}ba\text{:} & (b-1)a+r_1 & (b-1)a+r_2 & \dots & (b-1)a+r_{\varphi(a)}
\end{array}$$

Az első sor elemei redukált maradékrendszert alkotnak (mod a), így minden sorban $\varphi(a)$ darab elem van, vagyis a táblázatnak $\varphi(a)$ darab oszlopa van. Minden oszlopban b darab elemet soroltunk fel, és ezek az elemek teljes ma-



12.16. ábra. Konkrét értékekre a relatív prímek kiválasztása (animáció)

radékrendszert alkotnak (mod b), mert a 0, 1, 2, ..., $(b-1)$ teljes maradékrendszerből származtatható a b-hez relatív prím ka-val szorozva ($0 \leq k < b$) és r_i-vel növelve. Egy b szerinti teljes maradékrendszerben $\varphi(b)$ darab b-hez relatív prím van. Így minden oszlopból $\varphi(b)$ elem lesz relatív prím a-hoz és b-hez is, azaz ab-hez. Az oszlopok száma $\varphi(a)$, minden oszlopban $\varphi(b)$ relatív prím ab-hez, azaz összesen $\varphi(a) \cdot \varphi(b)$, így $\varphi(a) \cdot \varphi(b) = \varphi(ab)$. (Az ab-hez relatív prímek száma az a-hoz és b-hez relatív prímek számának szorzata.)

(12) $\mu(n)$: Ha akár a, akár b kanonikus alakjában van olyan prím, amelyik legalább második hatványon szerepel, akkor ez a prím az ab szorzatban is legalább második hatványon fog szerepelni, így minden olyan esetben, amikor $\mu(a) = 0$ vagy $\mu(b) = 0$, $\mu(ab)$ is 0 lesz, vagyis ilyenkor $\mu(a)\mu(b) = \mu(ab)$ teljesül. Ha a és b kanonikus alakjában minden prím első hatványon szerepel, és $(a, b) = 1$, vagyis a-nak és b-nek nincs közös prímtényezője, akkor az ab szorzatban is minden prím első hatványon szerepel. Ha ekkor a-nak $k \geq 1$, b-nek pedig $l \geq 1$ prímtényezője van, akkor $\mu(a) = (-1)^k$ és $\mu(b) = (-1)^l$, így

$$\mu(a)\mu(b) = (-1)^k(-1)^l = (-1)^{k+l} = \mu(ab).$$

Végül, ha a és b közül legalább az egyik 1 (például a), akkor $\mu(a) = 1$, $\mu(ab) = \mu(b)$ miatt $\mu(ab) = \mu(a)\mu(b)$. Tehát a függvény multiplikatív. □

Multiplikatív, illetve additív számelméleti függvényekről szólnak a következő tételek:

12.2. Tétel. *Ha $f(n)$ nem azonosan 0 multiplikatív számelméleti függvény, akkor $f(1) = 1$.*

Bizonyítás. Mivel tetszőleges a esetén $(1, a) = 1$, a multiplikatívitás miatt minden a-ra, $f(a) = f(1 \cdot a) = f(1)f(a)$. Mivel nem az azonosan 0 függvényről van szó, van olyan a szám, amelyre $f(a) \neq 0$. Erre az a számra a fenti egyenlőség csak úgy teljesülhet, ha $f(1) = 1$. □

12.3. Tétel. *Ha $g(n)$ additív számelméleti függvény, akkor $g(1) = 0$.*

Bizonyítás. Mivel tetszőleges a esetén $(1, a) = 1$, az additivitás miatt minden a-ra $g(a) = g(1 \cdot a) = g(1) + g(a)$, ami csak úgy teljesülhet, ha $g(1) = 0$. □

Megjegyzés. A fenti két tétel megfordítása nyilvánvalóan nem igaz, abból, hogy egy függvény az $n = 1$ helyen 1-et vagy 0-t vesz fel, semmi nem következik a függvény egészére nézve.

Megjegyzés. Azt már láttuk korábban, hogy az azonosan 0 függvény multiplikatív ((1) példa). A fenti két tételből következik, hogy az egyetlen

olyan függvény, amely egyszerre multiplikatív is és additív is, az azonosan 0 függvény.

12.4. Tétel. *Multiplikatív, illetve additív számelméleti függvény helyettesítési értékeinek kiszámításához elegendő a függvényértékeket a prímhatvány helyeken ismerni.*

Bizonyítás. Legyen $f(n)$ multiplikatív, $g(n)$ additív számelméleti függvény. Ekkor ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, akkor mivel $i \neq j$ esetén $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$, a multiplikativitás, illetve az additivitás miatt

$$f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \ldots \cdot f(p_k^{\alpha_k}),$$

$$g(n) = g(p_1^{\alpha_1}) + g(p_2^{\alpha_2}) + \ldots + g(p_k^{\alpha_k}). \square$$

Megjegyzés. Miután a multiplikatív és additív függvények tetszőleges függvényértékét meghatározhatjuk a prímhatvány helyeken felvett függvényértékből, megpróbálhatunk zárt képletet adni ezekre a függvényekre. Ezt a $d(n)$ függvény esetében a 6.4. Tételben már meg is tettük (és éppen fordítva, a multiplikativitásának bizonyításához használtuk fel). A 12.4. Tétel alapján próbáljuk meghatározni a $\sigma(n)$ és $\varphi(n)$ függvényeket is zárt alakban.

12.5. Tétel. *Legyen* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Ekkor

(a) $d(n) = (a_1 + 1) \cdot (a_2 + 1) \cdot \ldots \cdot (a_k + 1)$

(b) $\sigma(n) = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \dfrac{p_k^{\alpha_k+1} - 1}{p_k - 1}$

(c) $\varphi(n) = n \left(1 - \dfrac{1}{p_1}\right) \cdot \left(1 - \dfrac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \dfrac{1}{p_k}\right)$

Bizonyítás. (a) Lásd a 6.4. Tételt.

(b) A p^α prímhatvány nála nem nagyobb pozitív osztói, vagyis olyan hatványai a p-nek, amelyek kitevője 0 és α közé esik: 1, p, p^2, p^3, …, p^α. Ezek összege $1+p+p^2+p^2+\ldots+p^\alpha$, ami mértani sorozat összege: $\dfrac{p^{\alpha+1} - 1}{p - 1}$, így $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p - 1}$.

Ebből a 12.4. Tétel alapján már következik a tétel állítása.

(c) Egy prímhatványhoz, p^α-hoz 1 és p^α között a p többszörösei nem relatív prímek, a többi szám igen. Mivel minden p-edik szám osztható p-vel (többszöröse p-nek), a p^α szám közül $\frac{p^\alpha}{p} = p^{\alpha-1}$-et kell kihagynunk, így megmarad $p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$ – ez tehát $\varphi(p^\alpha)$.

Ebből a 12.4. Tétel alapján már következik a tétel állítása. □

Összegzési függvény, megfordítási függvény

12.4. Definíció. Az $F(n)$ függvényt az $f(n)$ számelméleti függvény *összegzési függvényének* nevezzük, ha $F(n) = \sum_{d|n} f(d)$. Ugyanekkor az $f(n)$ függvényt az $F(n)$ *megfordítási függvényének* nevezzük.

Megjegyzés. A megfordítási függvényt másképp Moebius-transzformáltnak is nevezzük, az elnevezést a 12.4. Állítás indokolja.

12.1. Megjegyzés. Az, hogy $F(n)$ az $f(n)$ függvény összegzési függvénye részletesebben leírva ezt jelenti:

$$\begin{aligned}
F(1) &= f(1)\\
F(2) &= f(1) + f(2)\\
F(3) &= f(1) + f(3)\\
F(4) &= f(1) + f(2) + f(4)\\
F(5) &= f(1) + f(5)\\
F(6) &= f(1) + f(2) + f(3) + f(6)\\
F(7) &= f(1) + f(7)\\
F(8) &= f(1) + f(2) + f(4) + f(8)\\
F(9) &= f(1) + f(3) + f(9)\\
&\vdots\\
F(n) &= f(d_1) + f(d_2) + \ldots + f(d_k)
\end{aligned}$$

(ahol $d_1 = 1$, d_2, …, $d_k = n$ az n szám összes osztója).

Például:

(1) Az $f_0\colon n \mapsto 0$ (azonosan 0) függvény összegzési függvénye önmaga. (Tetszőleges $d_i \mid n$ esetén $f(d_i) = 0$, így $F(n)$ értéke minden n-re nullák összege, vagyis 0.)

(2) Az $f_1 \colon n \mapsto 1$ (konstans 1) függvény összegzési függvénye $d(n)$. (Tetszőleges $d_i \mid n$ esetén $f(d_i) = 1$, így $F(n)$ értékének kiszámításához annyi 1-est kell összeadnunk, ahány osztója van n-nek, vagyis $d(n)$ darabot. Hasonlóan gondolható meg, hogy az $f_c \colon n \mapsto c$ függvény összegzési függvénye $c \cdot d(n)$.)

(3) Az $f_n \colon n \mapsto n$ függvény összegzési függvénye $\sigma(n)$. (Tetszőleges $d_i \mid n$ esetén $f(d_i) = d_i$, így $F(n)$ értékének kiszámításához éppen n osztóit kell összeadnunk.)

(4) A $\mu(n)$ függvény összegzési függvénye az 1 helyen 1-et vesz fel, minden más helyen 0.

Bizonyítás. Ennek igazolása kicsit hosszadalmasabb:

Legyen $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.

n osztói közül csak azokhoz rendel 0-tól különböző értéket a μ függvény, amelyekben minden prím első hatványon szerepel. Így:

- $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ (1 darab), a hozzá rendelt érték $(-1)^k$
- azok, amelyek közül egy prím kimarad (k-féle), a hozzá rendelt érték $(-1)^{k-1}$
- azok, amelyek közül kétféle prím marad ki ($\binom{k}{2}$-féle), a hozzá rendelt érték $(-1)^{k-2}$

  $\vdots$
- azok, amelyek közül t-féle prím marad ki ($\binom{k}{t}$-féle), a hozzá rendelt érték $(-1)^{k-t}$

  $\vdots$
- végül azok, amelyek egyetlen prímtényezőből állnak ($\binom{k}{k}$-féle), a hozzá rendelt érték $(-1)^{k-k}$

Vagyis összesen

$$\binom{k}{0} \cdot (-1)^k + \binom{k}{1} \cdot (-1)^{k-1} + \binom{k}{2} \cdot (-1)^{k-2} + \ldots$$
$$\ldots + \binom{k}{t} \cdot (-1)^{k-t} + \ldots + \binom{k}{k} \cdot (-1)^{k-k}.$$

Vegyük észre, hogy ez nem más, mint az $((-1)+1)^k$ összeg kiírása a binomiális tétel szerint. Ez viszont 0, tehát valóban $\mu(n) = 0$, ha $n > 1$. □

12.3. Állítás. *Minden pozitív értékű multiplikatív függvényből készíthető additív függvény. Minden additív függvényből készíthető multiplikatív függvény.*

Bizonyítás. Ha $f(n)$ pozitív értékű multiplikatív függvény, akkor például a $g(n) = \ln f(n)$ függvény additív. Legyen ugyanis $(n_1, n_2) = 1$. Ekkor $f(n_1 n_2) = f(n_1) f(n_2)$, így

$$\begin{aligned} g(n_1 n_2) &= \ln\big(f(n_1 n_2)\big) = \ln\big(f(n_1) f(n_2)\big) = \\ &= \ln\big(f(n_1)\big) + \ln\big(f(n_2)\big) = g(n_1) + g(n_2). \end{aligned}$$

(Mivel $f(n)$ semmilyen n-re sem negatív, így minden n-re létezik $f(n)$-nek logaritmusa.)

Ha $g(n)$ additív függvény, akkor például az $f(n) = 2^{g(n)}$ függvény multiplikatív. Legyen ugyanis $(n_1, n_2) = 1$. Ekkor $g(n_1 n_2) = g(n_1) + g(n_2)$, így

$$\begin{aligned} f(n_1 n_2) &= 2^{g(n_1 n_2)} = 2^{g(n_1)+g(n_2)} = \\ &= 2^{g(n_1)} \cdot 2^{g(n_2)} = f(n_1) \cdot f(n_2) \ \square \end{aligned}$$

Megjegyzés. Ennek a megállapításnak mindössze annyi a jelentősége, hogy az additív számelméleti függvények sok fontos tulajdonságát megkapjuk, ha megfeleltethetők alkalmas multiplikatív számelméleti függvénynek.

Megjegyzés. A multiplikativitás és az additivitás eddig látott tulajdonságai alapján az előbbi bizonyos fajta polinomialitást (mint a hatványfüggvények, pl. x, x^2 stb.), az utóbbi valamilyen logaritmikus tulajdonságot mutat. Tény, hogy minden – a teljes valóson értelmezett és egyébként folytonos, de a természetes számokra leszűkített – hatványfüggvény multiplikatív, és minden logaritmusfüggvény additív számelméleti függvény.

12.6. Tétel. *Legyen az $F(n)$ függvény az $f(n)$ összegzési függvénye. Ekkor $F(n)$ akkor és csak akkor multiplikatív, ha $f(n)$ multiplikatív.*

Bizonyítás. Ha $F(n)$ és $f(n)$ közül az egyik a konstans 0 függvény, akkor a másik is az, ebben az esetben triviális az állítás. A továbbiakban arra az esetre szorítkozunk, amikor sem $F(n)$, sem $f(n)$ nem azonosan 0.

Tegyük fel először, hogy $f(n)$ multiplikatív, vagyis ha $(a,b)=1$, akkor $f(ab)=f(a)f(b)$. Legyen a összes osztója: $1=a_1, a_2, \ldots, a=a_r$, a b összes osztója: $1=b_1, b_2, \ldots, b=b_s$.

Ekkor – mivel $(a,b)=1$ – az ab összes osztója (a 6.8. Tétel alapján):

$$\begin{array}{llll} a_1b_1, & a_2b_1, & \ldots, & a_rb_1, \\ a_1b_2, & a_2b_2, & \ldots, & a_rb_2, \\ \vdots & & & \\ a_1b_s, & a_2b_s, & \ldots, & a_rb_s. \end{array}$$

Tudjuk, hogy ekkor

$$\begin{aligned} F(a) &= f(a_1)+f(a_2)+\ldots+f(a_r) \\ F(b) &= f(b_1)+f(b_2)+\ldots+f(b_s) \\ F(ab) &= f(a_1b_1)+f(a_2b_1)+\ldots+f(a_rb_s). \end{aligned}$$

A multiplikativitás miatt tetszőleges i és j esetén $f(a_ib_j)=f(a_i)f(b_j)$ (hiszen $(a,b)=1$ miatt $(a_i,b_j)=1$). Így a jobb oldalt átalakítva a következőket kapjuk:

$$\begin{aligned} F(ab) &= f(a_1)f(b_1)+f(a_2)f(b_1)+\ldots+f(a_r)f(b_s)= \\ &= (f(a_1)+f(a_2)+\ldots+f(a_r))(f(b_1)+f(b_2)+\ldots+f(b_s))= \\ &= F(a)F(b). \end{aligned}$$

Vagyis ha $f(n)$ multiplikatív, akkor $F(n)$ is az.

Most tegyük fel, hogy $F(n)$ multiplikatív, vagyis hogy ha $(a,b)=1$, akkor $F(a)F(b)=F(ab)$. Felhasználva, hogy

$$F(a)F(b)=f(a_1)f(b_1)+f(a_2)f(b_1)+\ldots+f(a_r)f(b_s)$$

és

$$F(ab)=f(a_1b_1)+f(a_2b_1)+\ldots+f(a_rb_s),$$

azt kapjuk, hogy

$$\begin{aligned} &f(a_1)f(b_1)+f(a_2)f(b_1)+\ldots+f(a_r)f(b_s)= \\ &=f(a_1b_1)+f(a_1b_2)+f(a_1b_3)+\ldots+f(a_2b_1)+f(a_2b_2)+\ldots+f(a_rb_s). \end{aligned}$$

Azt szeretnénk bizonyítani, hogy $f(a)f(b)=f(ab)$, vagyis a fenti jelölésekkel $f(a_r)f(b_s)=f(a_rb_s)$. Ezt teljes indukcióval bizonyítjuk.

Ha $n=1$, akkor $F(n)$ multiplikativitása és $F(n)\neq 0$ miatt $F(1)=1$, így $F(1)=f(1)$ miatt teljesül, hogy $f(1)f(1)=f(1)=1$.

Tegyük fel, hogy az állítás minden ab-nél kisebb szám esetén igaz. Ekkor $f(a_i)f(b_j) = f(a_ib_j)$ teljesül az ab szorzat minden olyan a_ib_j osztójára, ahol $i < r$ vagy $j < s$.

(Vagyis a 12.17. ábrán szemléltetett szorzatok az indukciós feltevés alapján az utolsó kivételével átírhatók a 12.18. ábrán jelölt alakra.)

Ez azt jelenti, hogy a fenti egyenlőségben szereplő összegek az utolsó tagok kivételével tagonként egyenlők. Mivel azonban a két összeg egyenlő, így az utolsó tagoknak is egyenlőknek kell lenniük – ami a bizonyítandó állítás volt. □

	$f(a_1)$	+ $f(a_2)$	+ $f(a_3)$	+ ...	+ $f(a_r)$
$f(b_1)$	$f(a_1)f(b_1)$	$f(a_2)f(b_1)$	$f(a_3)f(b_1)$	...	$f(a_r)f(b_1)$
+					
$f(b_2)$	$f(a_1)f(b_2)$	$f(a_2)f(b_2)$	$f(a_3)f(b_2)$	...	$f(a_r)f(b_2)$
+					
$f(b_3)$	$f(a_1)f(b_3)$	$f(a_2)f(b_3)$	$f(a_3)f(b_3)$	...	$f(a_r)f(b_3)$
+					
⋮					
+					
$f(b_s)$	$f(a_1)f(b_s)$	$f(a_2)f(b_s)$	$f(a_3)f(b_s)$	...	$f(a_r)f(b_s)$

12.17. ábra.

	$f(a_1)$	+ $f(a_2)$	+ $f(a_3)$	+ ...	+ $f(a_r)$
$f(b_1)$	$f(a_1b_1)$	$f(a_2b_1)$	$f(a_3b_1)$	...	$f(a_rb_1)$
+					
$f(b_2)$	$f(a_1b_2)$	$f(a_2b_2)$	$f(a_3b_2)$	...	$f(a_rb_2)$
+					
$f(b_3)$	$f(a_1b_3)$	$f(a_2b_3)$	$f(a_3b_3)$	...	$f(a_rb_3)$
+					
⋮					
+					
$f(b_s)$	$f(a_1b_s)$	$f(a_2b_s)$	$f(a_3b_s)$	...	$f(a_r)f(b_s)$

12.18. ábra.

Az f függvényből összegzéssel kapjuk az összegzési függvényét. Érdekes kérdés, hogy miként kapható meg az F összegzési függvényből az f megfordítási függvény.

Megjegyzés. Mivel egy multiplikatív függvény összegzési függvénye is multiplikatív, így ha az összegzési függvényét keressük, azt is elegendő csak a prímhatvány helyeken meghatározni.

Egy $f(n)$ multiplikatív számelméleti függvény összegzési függvénye a p^α (prímhatvány) helyen az osztókon felvett függvényértékek összegét, vagyis az

$$f(1) + f(p) + f(p^2) + \ldots + f(p^\alpha)$$

értéket veszi fel.

Ha például a $\varphi(n)$ függvény összegzési függvényére vagyunk kíváncsiak, akkor ezt a következőképpen kaphatjuk meg: Legyen p^α egy prímhatvány. Ekkor

$$F(p^\alpha) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^\alpha) =$$
$$= 1 + (p-1) + (p^2 - p) + \ldots + (p^\alpha - p^{\alpha-1}) = p^\alpha.$$

Mivel $\varphi(n)$ multiplikatív, az összegzési függvénye is multiplikatív, így a fentiek alapján $F(n) = \sum_{d|n} \varphi(d) = n$.

Megfordítva, ha egy adott $F(n)$ multiplikatív függvény megfordítási függvényét keressük, akkor a mellett ezt is meghatározhatjuk annak ismeretében, hogy a multiplikatív függvény megfordítási függvénye is multiplikatív.

$$F(p^\alpha) = f(1) + f(p) + f(p^2) + \ldots + f(p^\alpha)$$

és

$$F(p^{\alpha-1}) = f(1) + f(p) + f(p^2) + \ldots + f(p^{\alpha-1})$$

miatt

$$f(p^\alpha) = F(p^\alpha) - F(p^{\alpha-1}).$$

Ebből már $f(n)$ multiplikativitása miatt tetszőleges helyen meghatározható $f(n)$ értéke.

Ha például az $F(n) = n$ függvény megfordítási függvényét keresnénk, akkor

$$f(p^\alpha) = F(p^\alpha) - F(p^{\alpha-1}) = p^\alpha - p^{\alpha-1} = \varphi(p^\alpha),$$

amiből a multiplikativitás miatt már következik, hogy a keresett függvény a $\varphi(n)$.

A 12.6. Tétel egyébként arra is alkalmas, hogy azzal bizonyos függvények multiplikativitását bizonyítsuk. Konkrétan: tudjuk, hogy a konstans 1

függvény multiplikatív, az összegzési függvénye az p^α prímhatvány helyen $\alpha + 1 = d(p^\alpha)$, ebből pedig következik, hogy összegzési függvénye a $d(n)$ függvény, és hogy $d(n)$ multiplikatív.

Hasonlóan, mivel az $n \mapsto n$ függvény multiplikatív, akkor ebből következik, hogy megfordítási függvénye – azaz $\varphi(n)$ – is, valamint az összegzési függvénye – azaz $\sigma(n)$ – is multiplikatív.

De nemcsak multiplikatív függvények megfordítására lehetünk kíváncsiak.

12.4. Állítás. *Egy tetszőleges F számelméleti függvényből az f megfordítási függvényt az alábbiak szerint kapjuk meg:*

$$f(n) = \sum_{d|n} \mu(d) \cdot F\left(\frac{n}{d}\right).$$

Bizonyítás. Mivel $F\left(\frac{n}{d}\right) = \sum_{d_1|\frac{n}{d}} f(d_1)$, ezt behelyettesítjük a bizonyítandó kifejezés jobb oldalába.

$$\sum_{d|n} \mu(d) \cdot \sum_{d_1|\frac{n}{d}} f(d_1).$$

A összegzés során n osztópárjait vesszük: $dd_1 = n$. Az egyik tényezőn a μ, a másikon az f függvényt hajtuk végre. Így az összegzést átcsoportosíthatjuk (1.3. Állítás) úgy, hogy az ugyanahhoz az f értékekhez tartozó μ függvényértékeket összegezzük:

$$\sum_{d|n} \mu(d) \cdot \sum_{d_1|\frac{n}{d}} f(d_1) = \sum_{d_1|n} f(d_1) \sum_{d|\frac{n}{d_1}} \mu(d)$$

A jobb oldalon a második összeg egyetlen esettől (amikor $d = 1$, vagyis $d_1 = n$) eltekintve 0 (lásd a 12.1. Megjegyzést követő 4. példa). Vagyis az marad, hogy

$$\sum_{d_1|n} f(d_1) \sum_{d|n} \mu(d) = \sum_{d_1=n} f(d_1) = f(n),$$

ami éppen a tétel állítása. □

Feladatok

(A d, a φ és a σ számelméleti függvények értékeinek kiszámításához használhatja a http://www.cs.elte.hu/~kfried/algebra1/DividorsNum.jard, http://www.cs.elte.hu/~kfried/algebra1/Phi.jarfí, http://www.cs.elte.hu/~kfried/algebra1/DividorSum.jarszigma programokat.)

1. Legyen t olyan totálisan multiplikatív függvény, amely minden prímszámhoz (és 1-hez is) 1-et rendel. Mivel egyenlő $t(n)$ tetszőleges n-re?

2. Legyen r olyan totálisan additív függvény, amely 0-hoz 0-t, továbbá minden prímszámhoz 1-et rendel. Mivel egyenlő $r(n)$ tetszőleges n-re?

3. Legyen s olyan totálisan multiplikatív számelméleti függvény, amely 1-ben 1-et, p_n-ben (az n-edik prímszám helyen) pedig n-et vesz fel. Írja fel, hogy tetszőleges n-hez mit rendel!

4. Egy tetszőleges n számhoz hozzárendeljük a 2-vel való osztási maradékát. Additív-e, multiplikatív-e ez a függvény?

5. Van-e olyan természetes szám, amelyre $d(n) = \sigma(n)$?

6. Ha $\sigma(n) = n + 1$, akkor mennyi lehet a lehet $\varphi(n)$? Mennyi lehet az n?

7. Legalább mennyi $\sigma(n)$?

8. Van-e olyan szám, amelyre $\sigma(n) = n + 2$?

9. Hány megoldása van a következő egyenleteknek a természetes számok halmazán?

   - $\sigma(n) = n + 3$
   - $\sigma(n) = n + 4$
   - $\sigma(n) = n + 5$
   - $\sigma(n) = n + 6$

10. Igazolja, hogy ha $0 \leq k \leq n$ relatív prím n-hez, akkor $n - k$ is relatív prím hozzá!

11. Legfeljebb mennyi lehet $\varphi(n)$?

    Lehet-e valamely n-re $\varphi(n) = n - 2$?

12. Igazolja, hogy tetszőleges n természetes szám esetén $d(n) + \varphi(n) \leq n + 1$!

13. Keressen olyan n természetes számot, amelyre $\sigma(n) - n = d(n)$!

14. Legyen $f(n)$ az a számelméleti függvény, amely minden számhoz a 3-mal való osztási maradékát rendeli. Határozza meg f értékeit az $n = 1, 2, \ldots, 40$ helyeken!

    Határozza meg f összegzési függvényének értékeit az $n = 1, 2, \ldots, 40$ helyeken!

    Határozza meg f megfordítási függvényének értékeit az $n = 1, 2, \ldots, 40$ helyeken!

13. fejezet

Tökéletes számok

Vizsgáljuk meg különböző számok esetén az n szám n-nél kisebb (pozitív) osztóinak összegét:

$2\colon 1$	$3\colon 1$
$4\colon 1+2=3$	$5\colon 1$
$6\colon 1+2+3=6$	$7\colon 1$
$8\colon 1+2+4=7$	$9\colon 1+3=4$
$10\colon 1+2+5=8$	$11\colon 1$
$12\colon 1+2+3+4+6=16$	$13\colon 1$
$14\colon 1+2+7=10$	$15\colon 1+3+5=9$
$16\colon 1+2+4+8=15$	$17\colon 1$
$18\colon 1+2+3+6+9=21$	$19\colon 1$
$20\colon 1+2+4+5+10=22$	

Az összeg a számok egy részénél kisebb, mint maga a szám – az ilyen számokat szokás *hiányos* számoknak nevezni –, egy másik részénél nagyobb mint maga a szám – ezek a *bővelkedő* számok –, bizonyos számok esetén pedig az összeg megegyezik magával a számmal. Az ilyen számokat már az ókori görögök is különösen érdekesnek tekintették.

Az, hogy egy szám nála kisebb pozitív osztóinak összege magát a számot adja, azt jelenti, hogy magát a számot is beleszámolva az összegbe, vagyis a szám összes pozitív osztóját összeadva, a szám kétszeresét kapnánk:

13.1. Definíció. Az n szám *tökéletes*, ha $\sigma(n) = 2n$ (vagyis ha $\sigma(n) - n = n$).

Tökéletes szám például a 6 és a 28: $6 = 1+2+3$, $28 = 1+2+4+7+14$.

Minden eddig talált tökéletes szám páros, ezekről szól a következő tétel:

13.1. Tétel. *Minden $n = 2^{p-1}(2^p - 1)$ alakú szám tökéletes, ha p is és $(2^p - 1)$ is prímszám; és megfordítva, minden páros tökéletes szám felírható ilyen alakban.*

Bizonyítás. 1. Először belátjuk, hogy a fenti alakú számok tökéletesek. Ehhez összeadjuk az osztóikat.

Mivel $(2^{p-1}, 2^p - 1) = 1$ (az egyik egy kettő hatványa, a másik páratlan prímszám), ezért a $\sigma(n)$ függvény multiplikativitása miatt

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Felhasználva, hogy $\sigma(2^{p-1}) = 2^p - 1$, továbbá hogy ha $2^p - 1$ prímszám, akkor $\sigma(2^p - 1) = 2^p$, azt kapjuk, hogy

$$\sigma(2^{p-1}(2^p - 1)) = (2^p - 1)2^p = 2n.$$

Ezzel beláttuk, hogy a fenti alakú számok tökéletesek.

2. Most tegyük fel, hogy az n páros szám tökéletes, vagyis $\sigma(n) = 2n$.

Írjuk fel n-et $2^k \cdot m$ alakban, ahol m páratlan.

Ekkor természetesen $(2^k, m) = 1$, tehát $\sigma(n)$ a tényezők σ-értékének szorzata, másrészt $\sigma(n) = 2n = 2^{k+1} \cdot m$, így

$$2^{k+1} \cdot m = \sigma(n) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Vagyis

$$2^{k+1} \cdot m = 2^{k+1}\sigma(m) - \sigma(m).$$

Átrendezve

$$\sigma(m) = 2^{k+1}(\sigma(m) - m). \tag{13.1}$$

Eszerint $\sigma(m) - m \mid \sigma(m)$.

Tudjuk, hogy $\sigma(m)$ az m osztóinak összege, ezek között ezek szerint szerepel az 1, az m, a $\sigma(m) - m$. Igen ám, de $\sigma(m) - m + m$ már $\sigma(m)$-et ad, ez csak úgy lehet, hogy $\sigma(m) - m$ maga az 1. Vagyis m-nek mindössze két osztója van: 1 és m, tehát prímszám; és $\sigma(m) - m = 1$.

Ekkor viszont (13.1)-ből $1 + m = 2^{k+1}$, tehát $m = 2^{k+1} - 1$ prímszám.

Egy $2^{k+1} - 1$ alakú szám viszont a 7.14. Tétel (Mersenne prímek) szerint csak úgy lehet prím, ha a kitevőben prímszám van, vagyis ha $k + 1 = p$ prímszám. Ezt felhasználva azt kapjuk, hogy ha az n páros szám tökéletes, akkor $n = 2^k m = 2^{p-1}(2^p - 1)$ alakú, amit bizonyítani akartunk. □

Megjegyzés. Eszerint a tétel szerint minden olyan p prímszám meghatároz egy páros tökéletes számot, amelyre $2^p - 1$ is prímszám, vagyis a páros tökéletes számok és a Mersenne-prímek között kölcsönösen egyértelmű megfeleltetés létesíthető. Így pontosan ugyanannyi páros tökéletes számot ismerünk, mint ahány Mersenne-prímet, és az olyasfajta kérdésekre, mint például hogy hány tökéletes szám van, van-e végtelen sok stb., pontosan ugyanazok a válaszok, mint a Mersenne-prímekkel kapcsolatos hasonló kérdésekre.

Az első néhány páros tökéletes számot a következő táblázat tartalmazza:

p prímszám	$2^p - 1$ Mersenne-prím	$2^{p-1}(2^p - 1)$ tökéletes
2	3	6
3	7	28
5	31	496
7	127	8128
13	8191	33 550 336
⋮	⋮	⋮

Megjegyzés. Páratlan tökéletes számot eddig még senki nem talált. *Megoldatlan probléma,* hogy egyáltalán létezik-e, és hogy létezhet-e végtelen sok. Ennek ellenére nagyon sok eredmény született a páratlan tökéletes számokról, pontosabban sok szükséges feltétel gyűlt össze: ha létezik páratlan tökéletes szám, akkor ez milyen bizonyos tulajdonságokkal kell rendelkezzék, illetve a páratlan tökéletes számok rengeteg tulajdonságát sorolták fel.

Ennek a kutatásnak – bár még nem találtunk páratlan tökéletes számot – az az egyik értelme, hogy amennyiben ellentmondásos tulajdonságokra lelünk, biztosak lehetünk benne, hogy nincsnek páratlan tökéletes számok, a másik pedig az, hogy ha elég sok tulajdonságát megismerjük, akkor esetleg mégis rábukkanunk egyre.

Péter Rózsa neves magyar matematikus is sok energiát áldozott páratlan tökéletes számok kutatására.

Egy ilyen típusú megoldatlan problémának kétféle lezárása lehet.

1. Valaki talál páratlan tökéletes számot. (Ha például a sok feltételezett tulajdonság alapján sikerül találni egyet.)

2. Valaki bebizonyítja, hogy nincs páratlan tökéletes szám. (Például úgy, hogy feltételezve, hogy van tökéletes szám, ellentmondásra jut.)

És akkor marad harmadiknak az a lehetőség, hogy a problémának soha nem lesz lezárása: soha nem derül ki, hogy van-e páratlan tökéletes szám, a probléma megoldatlan marad.

[A XX. század elején, Gödel matematikai logikában elért eredménye alapján kiderült, hogy egyes állítások – az úgynevezett „Gödel-féle" állítások – esetén előfordulhat, hogy azok igazsága az adott axiómarendszerben nem igazolható és nem is cáfolható. Esetleg meg is lehet mutatni, hogy egy állítás ilyen. Aposztolosz Doxiadisz „Petrosz bácsi és a Goldbach-sejtés" című regénye (Aposztolosz Doxiadisz: Petrosz bácsi és a Goldbach-sejtés, Európa Könyvkiadó, ISBN 963 07 7518 2) is ezt a kérdést feszegeti, míg a tétel matematikáját részletesebben mutatja be R. Smullyan könyve (Raymond Smullyan: Gödel nemteljességi tétele, Typotex, 2006.)]

A matematikusok kutatómunkáját manapság nagyban segíti a számítógép. Számítógépes algoritmussal is kereshető páratlan tökéletes szám, de vagy nincs még alkalmas algoritmus egy (esetleg létező) páratlan tökéletes szám megtalálására, vagy valóban nincs ilyen szám, és akkor hiába is keresik gyors számítógépes algoritmussal. Az nem valószínű, hogy még senki sem kísérletezett ezzel. Azt gondolhatnánk, hogy ennyi idő alatt kellett volna már találni egy páratlan tökéletes számot. Az a tény, hogy a nagy sebességű számítógépek és a jó fél évszázada elterjedt számítástechnikai matamatikai kutatási módszerek ellenére sem sikerült páratlan tökéletes számot találni, azt a gyanút erősíti, hogy nincs ilyen. Természetesen ezt bizonyítani kellene, amit szintén lehetne számítógéppel, de egyelőre még ezt sem sikerült.

Barátságos számok

A tökéletes számok mintájára olyan számokat is kereshetünk, amelyek osztóinak összege – magát a számot nem beleszámolva – a szám kétszeresével, háromszorosával stb. egyenlő.

Számláncokat is készíthetünk úgy, hogy kiindulunk egy pozitív egész számból, összeadjuk a nála kisebb pozitív osztóit, majd az így kapott számmal elvégezzük ugyanezt és így tovább. A számok egy részénél előbb-utóbb eljutunk az 1-hez, ekkor nem tudjuk folytatni a láncot.

Például: 12–16–15–9–4–3–1

Tökéletes számok esetén konstans sorozatot kapunk, de vajon létrejöhete olyan ciklikus sorozat, ahol a ciklus hossza (a benne foglalt számok száma) 2, 3, ... stb.?

Az, hogy a ciklus hossza 2, azt jelentené, hogy találtunk két olyan számot, amelyekre az egyik szám nála kisebb pozitív osztóinak összege a másik szám, a másik szám nála kisebb pozitív osztóinak összege pedig az első szám.

13.2. Definíció. Az a, b számokat *barátságos számpárnak* nevezzük, ha $\sigma(a) - a = b$ és $\sigma(b) - b = a$.

Például: A 220 nála kisebb osztóinak összege:

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284,$$

a 284 nála kisebb osztóinak összege pedig:

$$1 + 2 + 4 + 71 + 142 = 220.$$

A következő barátságos számpár az 1184 és 1210, amelynek érdekessége, hogy egy Nicolo Paganini nevű 16 éves diák találta meg 1867-ben, amikor már számos nagyobb barátságos számpár volt ismert. Az, hogy van-e végtelen sok barátságos számpár, megoldatlan probléma.

Barátságos számhármasokat (amelyekre $\sigma(a) - a = b$, $\sigma(b) - b = c$ és $\sigma(c) - c = a$) még nem találtak, a legkisebb barátságos számnégyes a következő:

$$1\,264\,460, \qquad 1\,547\,860, \qquad 1\,727\,636, \qquad 1\,305\,184.$$

Feladatok

1. Miért nem lehet prímszám tökéletes szám?
2. Van-e négyzetszám a páros tökéletes számok között?
3. Lehetne-e négyzetszám egy páratlan tökéletes szám?
4. Igaz-e, hogy két, egymáshoz relatív prím tökéletes szám szorzata is tökéletes szám?

   Tud-e példát mondani rá? Miért nem?

14. fejezet

Függelék (A racionális számok tizedes tört alakja)

Racionális számnak nevezzük azokat a valós számokat, amelyek előállnak két egész szám hányadosaként. Ugyanaz a racionális szám sokféleképpen felírható tört alakban (két egész szám hányadosaként), azonban a számláló és a nevező legnagyobb közös osztójával egyszerűsítve a törtet, mindig eljutunk egy olyan $\frac{a}{b}$ alakhoz, ahol $(a, b) = 1$. Ezt az alakot a tört *redukált alak*jának nevezik.

Vizsgáljuk meg néhány racionális szám tizedes tört alakját:

$\frac{1}{2} = 0{,}5\dot{0}$	$\frac{3}{2} = 1{,}5\dot{0}$	$\frac{5}{2} = 2{,}5\dot{0}$	$\frac{7}{2} = 3{,}5\dot{0}$
$\frac{1}{3} = 0{,}\dot{3}$	$\frac{2}{3} = 0{,}\dot{6}$	$\frac{4}{3} = 1{,}\dot{3}$	$\frac{5}{3} = 1{,}\dot{6}$
$\frac{1}{4} = 0{,}25\dot{0}$	$\frac{3}{4} = 0{,}75\dot{0}$	$\frac{5}{4} = 1{,}25\dot{0}$	$\frac{7}{4} = 1{,}75\dot{0}$
$\frac{1}{5} = 0{,}2\dot{0}$	$\frac{2}{5} = 0{,}4\dot{0}$	$\frac{3}{5} = 0{,}6\dot{0}$	$\frac{4}{5} = 0{,}8\dot{0}$
$\frac{1}{6} = 0{,}1\dot{6}$	$\frac{5}{6} = 0{,}8\dot{3}$	$\frac{7}{6} = 1{,}1\dot{6}$	$\frac{11}{6} = 1{,}8\dot{3}$
$\frac{1}{7} = 0{,}\dot{1}42857\dot{7}$	$\frac{2}{7} = 0{,}\dot{2}85714\dot{4}$	$\frac{3}{7} = 0{,}\dot{4}28571\dot{1}$	$\frac{4}{7} = 0{,}\dot{5}71428\dot{8}$
$\frac{1}{8} = 0{,}125\dot{0}$	$\frac{3}{8} = 0{,}375\dot{0}$	$\frac{5}{8} = 0{,}625\dot{0}$	$\frac{7}{8} = 0{,}875\dot{0}$
$\frac{1}{9} = 0{,}\dot{1}$	$\frac{2}{9} = 0{,}\dot{2}$	$\frac{4}{9} = 0{,}\dot{4}$	$\frac{5}{9} = 0{,}\dot{5}$
$\frac{1}{10} = 0{,}1\dot{0}$	$\frac{3}{10} = 0{,}3\dot{0}$	$\frac{7}{10} = 0{,}7\dot{0}$	$\frac{9}{10} = 0{,}9\dot{0}$
$\frac{1}{11} = 0{,}\dot{0}\dot{9}$	$\frac{2}{11} = 0{,}\dot{1}\dot{8}$	$\frac{3}{11} = 0{,}\dot{2}\dot{7}$	$\frac{4}{11} = 0{,}\dot{3}\dot{6}$

$$\frac{1}{12} = 0{,}08\dot{3} \qquad \frac{5}{12} = 0{,}41\dot{6} \qquad \frac{7}{12} = 0{,}58\dot{3} \qquad \frac{11}{12} = 0{,}91\dot{6}$$
$$\frac{1}{13} = 0{,}\dot{0}76923\dot{} \qquad \frac{2}{13} = 0{,}\dot{1}53846\dot{} \qquad \frac{3}{13} = 0{,}\dot{2}30769\dot{} \qquad \frac{4}{13} = 0{,}\dot{3}07692\dot{}$$

Észrevehetjük, hogy a racionális számok tizedes tört alakjában a tizedes jegyek sorozata valahonnan kezdve mindig periodikus lesz, amit úgy is szokás mondani, hogy a racionális számok tizedes tört alakja szakaszos. Ez azért van, így, mert az $\frac{a}{b}$ $(a, b \in \mathbb{N}^+)$ racionális szám $q_0{,}q_1q_2q_3\ldots$ tizedes tört alakja maradékos osztások következő sorozatával kapható meg:

$$\begin{aligned}
a &= bq_0 + r_0 \quad (\text{ahol } 0 \le r_0 < b), \quad \text{vagyis } q_0 = \left[\frac{a}{b}\right];\\
10r_0 &= bq_1 + r_1 \quad (\text{ahol } 0 \le r_1 < b), \quad \text{vagyis } q_1 = \left[\frac{10r_0}{b}\right];\\
10r_1 &= bq_2 + r_2 \quad (\text{ahol } 0 \le r_2 < b), \quad \text{vagyis } q_2 = \left[\frac{10r_1}{b}\right];\\
10r_2 &= bq_3 + r_3 \quad (\text{ahol } 0 \le r_3 < b), \quad \text{vagyis } q_3 = \left[\frac{10r_2}{b}\right];
\end{aligned}$$

stb., ahol az a, r_0, r_1, r_2, r_3, ... számok b-vel való osztási maradéka legfeljebb b-féle lehet, így előbb-utóbb egy olyan r_k maradékot kapunk, amely megegyezik valamelyik korábban kapott r_i maradékkal. Ha viszont $r_k = r_i$ akkor $10r_k = 10r_i$, így

$$10r_k = bq_{k+1} + r_{k+1} \qquad (0 \le r_{k+1} < b)$$

és

$$10r_i = bq_{i+1} + r_{i+1} \qquad (0 \le r_{i+1} < b)$$

miatt $q_{k+1} = q_{i+1}$ és $r_{k+1} = r_{i+1}$. Abból pedig, hogy $r_{k+1} = r_{i+1}$ a fentiekhez hasonlóan következik, hogy $q_{k+2} = q_{i+2}$ és $r_{k+2} = r_{i+2}$ és így tovább, minden a-ra igaz lesz, hogy a $k + a$-adik tizedes jegy meg fog egyezni az $i + a$-adik tizedes jeggyel. (Példáinkban az első ismétlődő szakasz első és utolsó számjegyét a számjegy fölé írt ponttal jelöltük.)

Fenti észrevételünk megfordítása is igaz: minden szakaszos tizedes tört valamelyik racionális számnak a tizedes tört alakja. A korrekt bizonyításhoz analitikus ismeretekre van szükség. Egy végtelen szakaszos tizedestört végtelen numerikus sor, amely megfelelő feltételek mellett konvergens.

Az alábbiakban ennek a korrektül megalapozott elven működő módszernek egy szemléletes levezetését ismertetjük. Tekintsük az

$$x = q_0{,}q_1q_2\ldots q_i\dot{q}_{i+1}\ldots\dot{q}_k$$

szakaszos tizedes törtet. Ekkor (felülvonással jelölve az „egymás mögé írás”-t)

$$10^i x = \overline{q_0q_1q_2\ldots q_i}{,}\dot{q}_{i+1}\ldots\dot{q}_k$$

és

$$10^k x = \overline{q_0 q_1 q_2 \dots q_i q_{i+1} \dots q_k},\dot{q}_{i+1} \dots \dot{q}_k$$

(ahol $\overline{q_0 q_1 q_2 \dots q_i}$ és $\overline{q_0 q_1 q_2 \dots q_i q_{i+1} \dots q_k}$ egész számok), így

$$10^k x - 10^i x = \overline{q_0 q_1 q_2 \dots q_i q_{i+1} \dots q_k} - \overline{q_0 q_1 q_2 \dots q_i} \in \mathbb{Z},$$

vagyis

$$x = \frac{\overline{q_0 q_1 q_2 \dots q_i q_{i+1} \dots q_k} - \overline{q_0 q_1 q_2 \dots q_i}}{10^k - 10^i},$$

ahol a számláló is és a nevező is egész szám, így x racionális.

Megjegyzés. Meg kell jegyezzük, hogy miért mondtuk, hogy a fenti módszer csak szemléletes, és nem korrekt. Azért, mert nem adtunk korrekt definíciót arra, hogy végtelen tizedes törtekkel hogyan lehet műveleket végezni, különösen gyanús lépés a végtelen rész *levágása* a $10^i x - 10^k x$ esetben.

A matematikailag precíz levezetést az analízis adja.

Megjegyzés. Egy másik – még az előzőnél is kevésbé precíz, de talán még intuitívabb (a gyerekek számára is elfogadható és megközelíthető) levezetés a következő:

Megfigyelhetjük, hogy:

$$\frac{1}{9} = 0,\dot{1}$$
$$\frac{1}{99} = 0,\dot{0}\dot{1}$$
$$\frac{1}{999} = 0,\dot{0}0\dot{1}$$
$$\frac{1}{9999} = 0,\dot{0}\,00\dot{1}$$
$$\frac{1}{99\,999} = 0,\dot{0}0\,00\dot{1}$$

stb. (Ez egyébként a mértani sor összegére vonatkozó összefüggésből le is vezethető.)

Ekkor tetszőleges a esetén ha $10^{k-1} < a < 10^k$, akkor az $\dfrac{a}{10^k - 1}$ tört végtelen szakaszos tizedestört alakja $0,\overline{aa}\dots$ lesz. Ezt az eredmény megfordítva is felhasználhatjuk: az $0,\overline{aa}\dots$ alakú végtelen szakaszos tizedestört alakja $\dfrac{a}{10^k - 1}$.

Az előző eredményeink alapján megfogalmazhatjuk a következő (bizonyítást nyert) tételt:

14.1. Tétel. *Egy valós szám tizedes tört alakja akkor és csak akkor szakaszos, ha a szám racionális.*

14.1. Definíció. Azokat a szakaszos tizedes törteket, amelyekben az ismétlődő szakasz rögtön a tizedes vessző után kezdődik – vagyis a $q_0{,}\dot{q}_1q_2\dots\dot{q}_k$ alakúakat – *tiszta szakaszos tizedes tört*eknek nevezzük, a többit pedig *vegyes szakaszos tizedes tört*eknek. Amennyiben az ismétlődő szakasz pusztán a 0 számjegyből áll, véges tizedes törtről beszélünk. (Véges tizedes törtek esetén a $\dot{0}$ szakaszt általában nem szoktuk kiírni.)

Megjegyzés. A tizedes tört fogalmának hátterében – mint azt korábban említettük – a végtelen sor fogalma húzódik meg: a $q_0{,}q_1q_2q_3\dots$ tizedes tört alak, a $q_0+q_110^{-1}+q_210^{-2}+q_310^{-3}+\dots$ végtelen összeget jelenti. A fentiek során kihasználtuk, hogy ha $0\le q_1,q_2,q_3,\dots<10$, akkor ez a sor konvergens; továbbá hogy két konvergens sor összege és különbsége is konvergens, és határértéke a két sor határértékének összege, illetve különbsége.

Érdemes megjegyezni, hogy bár minden valós szám előáll $x=q_0+q_110^{-1}+q_210^{-2}+q_310^{-3}+\dots$ $(0\le q_1,q_2,q_3,\dots<10)$ alakban, ez az előállítás nem minden racionális szám esetén egyértelmű, így ha az ebben az előállításban szereplő együtthatók segítségével felírt $q_0{,}q_1q_2q_3\dots$ alakot tekintjük a szám tizedes tört alakjának, akkor bizonyos racionális számok nem csak egyféleképpen írhatók fel tizedes tört alakban.

Meggondolható, hogy például a $0{,}4\dot{9}$ és a $0{,}5\dot{0}$ ugyanannak a racionális számnak – az $\frac{1}{2}$ -nek – kétféle tizedes tört alakja. Bizonyítható, hogy bármelyik racionális szám ennek megfelelően legfeljebb kétféleképpen írható fel tizedes tört alakban, és ezen belül pontosan azok írhatók fel kétféleképpen, amelyek felírhatók véges tizedes törtként. Az összes többi racionális (és az összes irracionális) szám tizedes tört alakja egyértelmű. (Az olyan tizedes tört felírásokat, amelyekben egy helyiérték után csak 9-es szerepel, nem tekintjük korrekt tizedes tört felírásnak.)

Példáink közül a következő racionális számok tizedes tört alakja volt véges:

$$\begin{array}{cccccccccc}
\frac{1}{2}, & \frac{3}{2}, & \frac{5}{2}, & \frac{7}{2}, & \frac{1}{4}, & \frac{3}{4}, & \frac{5}{4}, & \frac{7}{4}, & \frac{1}{5}, & \frac{2}{5},\\
\frac{3}{5}, & \frac{4}{5}, & \frac{1}{8}, & \frac{3}{8}, & \frac{5}{8}, & \frac{7}{8}, & \frac{1}{10}, & \frac{3}{10}, & \frac{7}{10}, & \frac{9}{10},\\
\frac{1}{3}, & \frac{2}{3}, & \frac{4}{3}, & \frac{5}{3}, & \frac{1}{7}, & \frac{2}{7}, & \frac{3}{7}, & \frac{4}{7}, & \frac{1}{9}, & \frac{2}{9},\\
\frac{4}{9}, & \frac{5}{9}, & \frac{1}{11}, & \frac{2}{11}, & \frac{3}{11}, & \frac{4}{11}, & \frac{1}{13}, & \frac{2}{13}, & \frac{3}{13}, & \frac{4}{13}
\end{array}$$

a következőké vegyes szakaszos:

$$\frac{1}{6},\quad \frac{5}{6},\quad \frac{7}{6},\quad \frac{11}{6},\quad \frac{1}{12},\quad \frac{5}{12},\quad \frac{7}{12},\quad \frac{11}{12}.$$

A továbbiakban azt fogjuk megvizsgálni, hogy a és b megválasztásától függően, milyen lesz az $\frac{a}{b}$ $(a, b \in \mathbb{Z})$ tört tizedes tört alakja. Mivel minket most csak az $\frac{a}{b}$ szám törtrésze érdekel, elegendő, ha vizsgálatainkban a $0 < a < b$ esetre szorítkozunk. Azt is fel fogjuk tételezni, hogy $\frac{a}{b}$ már a redukált alakja a vizsgált törtnek.

14.2. Tétel. *Legyen $a < b$ és $(a, b) = 1$ $(a, b \in \mathbb{N}^+)$. Ekkor az $\frac{a}{b}$ törtnek akkor és csak akkor van véges tizedes tört alakja, ha $b = 2^s 5^t$ alakú $(s, t \in \mathbb{N})$.*

Bizonyítás. Tegyük fel, hogy $\frac{a}{b}$ véges tizedes tört alakba írható, vagyis

$$\frac{a}{b} = 0, q_1 q_2 \dots q_i \dot{0}.$$

Ekkor

$$10^i \frac{a}{b} = \overline{q_1 q_2 \dots q_i} \ (\in \mathbb{N}),$$

így

$$10^i a = \overline{q_1 q_2 \dots q_i} \cdot b.$$

Mivel b nyilvánvalóan osztója az egyenlőség jobb oldalának, osztania kell a balt is, tehát $b \mid 10^i a$. Ez csak úgy lehetséges, ha $b \mid 10^i$, hiszen $(a, b) = 1$. Ekkor viszont (a 6.3 tétel miatt) b prímtényezős alakjában csak 2-es és 5-ös prímtényezők szerepelhetnek.

Megfordítva, tegyük fel, hogy $b = 2^s 5^t$, ahol mondjuk $(0 \leq) s \leq t$. Ekkor

$$\frac{a}{b} = \frac{a}{2^s 5^t} = \frac{2^{t-s} a}{10^t},$$

márpedig egy egész számot tíz egy hatványával osztva véges tizedes törtet kapunk. □

14.3. Tétel. *Legyen $a < b$ és $(a, b) = 1$ $(a, b \in \mathbb{N}^+)$. Ekkor az $\frac{a}{b}$ tört tizedes tört alakja akkor és csak akkor tiszta szakaszos, ha $(b, 10) = 1$.*

Bizonyítás. Ha $\frac{a}{b}$ tizedes tört alakja tiszta szakaszos, vagyis

$$\frac{a}{b} = 0, \dot{q}_1 q_2 \dots \dot{q}_k,$$

akkor

$$10^k \frac{a}{b} = \overline{q_1 q_2 \dots q_k}, \dot{q}_1 q_2 \dots \dot{q}_k$$

így

$$(10^k - 1)\frac{a}{b} = \overline{q_1 q_2 \dots q_k},$$

vagyis

$$(10^k - 1)a = \overline{q_1 q_2 \dots q_k} \cdot b.$$

Ekkor viszont $b \mid (10^k - 1)a$, amiből $(a, b) = 1$ miatt következik, hogy $b \mid (10^k - 1)$. Mivel $10^k - 1$ relatív prím a 10-hez, minden osztója, így b is relatív prím a 10-hez.

Megfordítva, tegyük fel, hogy $(b, 10) = 1$, és

$$\frac{a}{b} = 0, q_1 q_2 \dots q_i \dot{q}_{i+1} \dots \dot{q}_k,$$

ahol az

$$\begin{aligned}
a &= b \cdot 0 + a && (\text{ahol } 0 \le a < b),\\
10a &= bq_1 + r_1 && (\text{ahol } 0 \le r_1 < b),\\
10r_1 &= bq_2 + r_2 && (\text{ahol } 0 \le r_2 < b),\\
10r_2 &= bq_3 + r_3 && (\text{ahol } 0 \le r_3 < b),\\
&\vdots\\
10r_{i-1} &= bq_i + r_i && (\text{ahol } 0 \le r_i < b),\\
&\vdots\\
10r_{k-1} &= bq_k + r_k && (\text{ahol } 0 \le r_k < b),\\
&\vdots
\end{aligned}$$

maradékos osztássorozat során fellépő a, r_1, r_2, r_3, … maradékok közül r_k az első olyan, amely megegyezik valamelyik korábban kapott maradékkal (mondjuk r_i-vel). Ha viszont $r_k = r_i$, akkor

$$10(r_{k-1} - r_{i-1}) = b(q_k - q_i) + \underbrace{r_k - r_i}_{0} \qquad (0 \le r_{k-1}, r_{i-1} < b),$$

vagyis $b \mid 10(r_{k-1} - r_{i-1})$, amiből $(b, 10) = 1$ miatt következik, hogy

$$b \mid r_{k-1} - r_{i-1}.$$

Mivel $(0 \le r_{k-1}, r_{i-1} < b)$ és így $(0 \le |r_{k-1} - r_{i-1}| < b)$, ez csak úgy lehetséges, hogyha $|r_{k-1} - r_{i-1}| = 0$, vagyis $r_{k-1} = r_{i-1}$. Ez viszont azt

jelenti, hogy ha r_k nem az elsőnek kapott maradékkal (a-val) egyezne meg, akkor nem lehetne ő az elsőként megismétlődő maradék, hiszen ekkor már r_{k-1} is megegyezne egy korábban kapott maradékkal (r_{i-1}-gyel).

Ezek szerint $r_k = r_i = a$, emiatt $r_{k+1} = r_{i+1} = q_1$, tehát az ismétlődő szakasz első tizedes jegye q_1, a tizedes tört tiszta szakaszos. □

Megjegyzés. Könnyen meggondolható, hogy $\frac{a}{b}$ $((a,b)=1)$ tizedes tört alakja akkor és csak akkor lesz tiszta szakaszos, ha b-nek van 10^k-1 alakú többszöröse. Azt, hogy ez akkor és csak akkor teljesül, ha $(b,10)=1$, egyrészt a fenti tétel bizonyítja, másrészt a következőképpen is meggondolhatjuk:

Ha $(b,10)=1$, akkor az Euler–Fermat-tétel (8.13. Tétel) értelmében $10^{\varphi(b)} \equiv 1 \pmod{b}$, vagyis $k=\varphi(b)$ esetén $b \mid 10^{\varphi(b)}-1$; ha pedig $(b,10)\neq 1$, akkor b minden többszöröse páros vagy 5-tel osztható, így egyik sem végződhet 9-esre.

Megjegyzés. A 14.3. Tételből az következik, hogy az $\frac{a}{b}$ $((a,b)=1)$ racionális szám tizedes tört alakja akkor és csak akkor vegyes szakaszos, ha b prímtényezői között olyan is szerepel, amely relatív prím a 10-hez, és olyan is, amely nem. Könnyen meggondolható, hogy azoknak a – nem egész – racionális számoknak, amelyeknek kétféle (egy véges és egy végtelen) tizedes tört alakja is van, mindkét alakja vegyes szakaszosnak tekinthető.

Összefoglalva: az $\frac{a}{b}$ $(a,b\in\mathbb{Z},\ (a,b)=1)$ racionális szám tizedes tört alakja mindig szakaszos. Ezen belül lehet véges vagy végtelen, illetve tiszta szakaszos vagy vegyes szakaszos. Azoknak a racionális számoknak, amelyeknek van véges tizedes tört alakjuk (az ismétlődő szakasz a 0 számjegyből áll), van végtelen is (ahol az ismétlődő szakasz a 9-es számjegyből áll). Ezen belül az egész számok (mindkét) tizedes tört alakja tiszta szakaszos, a nem egész számoké vegyes szakaszos.

Az $\frac{a}{b}$ $(a,b\in\mathbb{Z},\ (a,b)=1)$ racionális szám tizedes tört alakja:

- véges és tiszta szakaszos akkor és csak akkor, ha $b=1$.
- véges és vegyes szakaszos, akkor és csak akkor, ha $b\neq 1$, és nincs 2-től és 5-től különböző prímtényezője.
- végtelen és tiszta szakaszos, akkor és csak akkor, ha $b\neq 1$, és $(b,10)=1$.
- végtelen és vegyes szakaszos, akkor és csak akkor, ha b-nek van 2-től és 5-től különböző prímtényezője, de $(b,10)\neq 1$.

Vesszős törtek

Egy tetszőleges x valós szám nemcsak

$$x = q_0 + q_1 10^{-1} + q_2 10^{-2} + q_3 10^{-3} + \dots \qquad (0 \le q_1, q_2, q_3, \dots < 10)$$

alakban írható fel, hanem tetszőleges $t \ge 2$ egész szám esetén

$$x = c_0 + c_1 t^{-1} + c_2 t^{-2} + c_3 t^{-3} + \dots$$

alakban is, ahol $0 \le c_1, c_2, c_3, \dots < t$. Az ebből kapott $c_0, c_1 c_2 c_3 \dots$ alakot, az x szám t számrendszerbeli vesszős tört alakjának nevezik.

Nézzük meg például az $\frac{1}{2}$, az $\frac{1}{3}$ és az $\frac{1}{6}$ vesszős tört alakját néhány számrendszerben (a tízes számrendszerben írt számok alsó, $_{10}$ indexét az egyszerűbb jelölés érdekében elhagyjuk):

$$\begin{array}{lllll}
t=2\colon & \frac{1}{2} = \frac{1}{10}_2 = 0{,}1_2 & \frac{1}{3} = \frac{1}{11}_2 = 0{,}\dot{0}\dot{1}_2 & \frac{1}{6} = \frac{1}{110}_2 = 0{,}0\dot{0}\dot{1}_2 \\
t=3\colon & \frac{1}{2}_3 = 0{,}\dot{1}_3 & \frac{1}{3} = \frac{1}{10}_3 = 0{,}1_3 & \frac{1}{6} = \frac{1}{20}_3 = 0{,}0\dot{1}_3 \\
t=4\colon & \frac{1}{2}_4 = 0{,}2_4 & \frac{1}{3}_4 = 0{,}\dot{1}_4 & \frac{1}{6} = \frac{1}{12}_4 = 0{,}0\dot{2}_4 \\
t=5\colon & \frac{1}{2}_5 = 0{,}\dot{2}_5 & \frac{1}{3}_5 = 0{,}\dot{1}\dot{3}_5 & \frac{1}{6} = \frac{1}{11}_5 = 0{,}\dot{0}\dot{4}_5 \\
t=6\colon & \frac{1}{2}_6 = 0{,}3_6 & \frac{1}{3}_6 = 0{,}2_6 & \frac{1}{6} = \frac{1}{10}_6 = 0{,}1_6 \\
t=7\colon & \frac{1}{2}_7 = 0{,}\dot{3}_7 & \frac{1}{3}_7 = 0{,}\dot{2}_7 & \frac{1}{6}_7 = 0{,}\dot{1}_7 \\
t=8\colon & \frac{1}{2}_8 = 0{,}4_8 & \frac{1}{3}_8 = 0{,}\dot{2}\dot{5}_8 & \frac{1}{6}_8 = 0{,}1\dot{2}\dot{5}_8 \\
t=8\colon & \frac{1}{2}_9 = 0{,}\dot{4}_9 & \frac{1}{3}_9 = 0{,}3_9 & \frac{1}{6}_9 = 0{,}1\dot{4}_9 \\
\vdots &&&
\end{array}$$

Megvizsgálva néhány racionális szám vesszős tört alakját különböző számrendszerekben, számos érdekességet fedezhetünk fel. Megállapíthatjuk például, hogy a racionális számok tizedes tört alakjával kapcsolatos állításainkhoz hasonlók tetszőleges számrendszerben teljesülnek, azaz:

14.4. Tétel. *Legyen $t \ge 2$ tetszőleges egész szám. Vizsgáljuk $a, b \in \mathbb{N}^+$ mellett az $\frac{a}{b}$ törtet.*

(i) Egy valós szám vesszős tört alakja t alapú számrendszerben akkor és csak akkor szakaszos, ha a szám racionális.

(ii) *Ha a vizsgált törtre $(a, b) = 1$, akkor t alapú számrendszerben akkor és csak akkor van véges vesszős tört alakja, ha b minden prímtényezője osztója t-nek.*

(iii) *Ha a vizsgált törtre $(a, b) = 1$, ekkor t alapú számrendszerben akkor és csak akkor tiszta szakaszos a vesszős tört alakja, ha $(b, t) = 1$.*

Az állítások a 14.1., a 14.2. és a 14.3. Tételekhez hasonlóan bizonyíthatóak.

Megjegyzés. A tizedes tört alakhoz hasonlóan a vesszős tört alak sem mindig egyértelmű. A $0{,}1_2$ és a $0{,}0\dot{1}_2$ például egyaránt az $\frac{1}{2}_{10}$ racionális szám 2-es számrendszerbeli vesszős tört alakja. Általában is igaz, hogy azoknak (és csak azoknak) a racionális számoknak, amelyeknek t alapú számrendszerben felírt vesszős tört alakjában az ismétlődő szakasz a $(t-1)$-es számjegyből áll, van – ugyanebben a számrendszerben – véges vesszős tört alakja is.

Feladatok

1. Írja fel a következő tizedestörteket tört alakban!

   - $0{,}\dot{1}\dot{6}$
   - $0{,}\dot{1}5\dot{3}$
   - $0{,}4\dot{3}\dot{1}$
   - $0{,}4\dot{3}2\dot{1}$
   - $1{,}30\dot{1}27\dot{6}$

2. Állapítsa meg a következő törtekről, hogy a tizedes tört alakjuk tiszta szakaszos-e vagy vegyes; véges vagy végtelen-e?

   - $\frac{2}{6}$
   - $\frac{3}{6}$
   - $\frac{6}{4}$
   - $\frac{16}{24}$
   - $\frac{105}{24}$

3. Igaz-e, hogy két tiszta szakaszos tizedes tört összege is tiszta szakaszos?

4. Igaz-e, hogy két vegyes szakaszos tizedes tört összege is vegyes szakaszos?

5. Igaz-e, hogy két véges tizedes tört összege is véges?

6. Igaz-e, hogy két végtelen szakaszos tizedes tört összege is végtelen szakaszos?

15. fejezet

TESZTEK

Az alábbi tesztkérdések mindegyikében egyetlen helyes választ kell megjelölni. (Megoldások a 214. oldalon.)

Alapok

1. Melyik nem ad meg relációt az alábbiak közül? Tetszőleges a, b elemek „álljanak relációban” egymással, ha

   (a) $a + b = 0$
   (b) $a = b$
   (c) $a \cdot b$
   (d) $a < b$

2. Az alábbiak közül melyik tulajdonsággal rendelkezik a $\leq$ reláció?

   (a) szimmetria
   (b) tranzitivitás
   (c) irreflexivitás
   (d) trichotómia

3. Melyik ekvivalenciareláció az alábbiak közül? Tetszőleges a, b elemek álljanak relációban egymással, ha

   (a) $a \neq b$
   (b) $a < b$
   (c) $a \leq b$
   (d) $a - b$ páros

4. Egy mértani sorozat első két eleme -1 és $-\frac{1}{2}$. Adja meg az első 10 eleme összegét!

   (a) $-\frac{341}{512}$

   (b) $\frac{1}{1024}$

   (c) 1

   (d) Nem létezik az összeg.

5. Egy mértani sorozat első két eleme -1 és 1. Adja meg az első 10 eleme összegét!

   (a) -1

   (b) 0

   (c) -10

   (d) Nem létezik az összeg.

6. Melyik tag nem fordul elő a $\sum_{i=5}^{8}\sum_{j=-2}^{-1}(i+j)$ összegben?

   (a) 3

   (b) 5

   (c) 7

   (d) 9

7. Mivel egyenlő a $\sum_{i=5}^{8}\sum_{j=-2}^{-1}(i+j)$ összeg?

   (a) 40

   (b) 18

   (c) 20

   (d) 8

Oszthatóság, maradékos osztás

1. Melyik számnak van pontosan 4 pozitív osztója az alábbi számok közül?

   (a) 0

   (b) 3

(c) 6
(d) 9

2. Melyik szám nem többszöröse az alábbiak közül a 24-nek?

(a) 0
(b) 24
(c) -24
(d) 12

3. 1. $(a+b)^n$, 2. $(a-b)^n$, 3. a^n+b^n, 4. a^n-b^n

A fentiek közül melyik osztható minden n természetes számra $(a-b)$-vel?

(a) 1. és 2.
(b) 1. és 3.
(c) 2. és 3.
(d) 2. és 4.

4. 1. $(a+b)^n$, 2. $(a-b)^n$, 3. a^n+b^n, 4. a^n-b^n

A fentiek közül melyik osztható minden n természetes számra $(a+b)$-vel?

(a) Csak 1.
(b) 1. és 2.
(c) 1. és 3.
(d) 1. és 4.

5. Mi a maradék, ha -413-at maradékosan osztjuk 11-gyel?

(a) -5
(b) -6
(c) 6
(d) 5

6. Mi a hányados, ha -413-at maradékosan osztjuk 11-gyel?

(a) -38
(b) 36
(c) 37
(d) -37

Számrendszerek, osztható sági szabályok

1. Az alábbiak közül melyik a 247 szám 5-ös számrendszerbeli felírása

   (a) 2441
   (b) 1491
   (c) 1442
   (d) 1441

2. Melyik számrendszerben lehet felírva az 1661 szám, ha osztható 3-mal?

   (a) 5
   (b) 7
   (c) 9
   (d) 10

3. Az alábbiak közül melyik alapú számrendszerben nem lehet a 3-mal való oszthatóságról a számjegyek összege alapján dönteni?

   (a) 3
   (b) 4
   (c) 7
   (d) 10

4. Az alábbiak közül melyik alapú számrendszerben nem lehet a 2-vel való oszthatóságról az utolsó számjegy alapján dönteni?

   (a) 2
   (b) 4
   (c) 5
   (d) 8

5. Melyik nem lehetett egy olyan számrendszer alapszáma, amelyben az utolsó számjegy, valamint a számjegyek összege vagy váltott előjelű összege alapján eldönthető, hogy egy szám osztható-e 30_{10}-cal?

   (a) 5
   (b) 9
   (c) 11
   (d) 12

6. Melyek azok a számok az alábbiak közül, amelyekkel való oszthatóság tetszőleges alapú számrendszerben eldönthető az utolsó számjegy, valamint a számjegyek összege vagy váltott előjelű összege alapján?

(a) 2 és 5
(b) 3 és 5
(c) 2 és 3
(d) 3 és 9

Legnagyobb közös osztó, legkisebb közös többszörös

1. Az euklideszi algoritmus során hanyadik maradékos osztással adja meg 148 és 218 legnagyobb közös osztóját?

   (a) 1
   (b) 2
   (c) 3
   (d) 4

2. Mivel egyenlő $(126, 60)$?

   (a) 3
   (b) 4
   (c) 6
   (d) 12

3. Mivel egyenlő $[12, 50]$?

   (a) 120
   (b) 150
   (c) 240
   (d) 300

4. Két szám legnagyobb közös osztója 4, legkisebb közös többszöröse 24. Melyik nem lehet ez a két szám az alábbiak közül?

   (a) 4 és 24
   (b) 8 es 24
   (c) 6 és 24
   (d) 8 és 12

5. Legyen $(a, b) = 1$! Melyik állítás nem teljesül ekkor az alábbiak közül?

   (a) Ha $d \mid a$, $d \mid b$, akkor $|d| = 1$.
   (b) Ha $a \mid c$, akkor $(b, c) = 1$.

(c) Ha $c \mid a$, akkor $(b, c) = 1$.

(d) Ha $|d| > 1$, $d \mid a$, akkor $d \nmid b$.

6. Lehet-e két természetes szám legnagyobb közös osztója egyenlő a legkisebb közös többszörösével?

(a) Nem, mert a legnagyobb közös osztó mindig nagyobb, mint a legkisebb közös többszörös.

(b) Nem, mert a legnagyobb közös osztó mindig kisebb, mint a legkisebb közös többszörös.

(c) Igen, de csak ha mind a két szám 1-gyel egyenlő.

(d) Igen, de csak ha az egyik 1-gyel egyenlő, a másik meg nem.

Felbonthatatlan szám, prímszám

Az $a + b\sqrt{2}$ alakú számok (ahol a és b egész számok) körében ugyanúgy elvégezhető az összeadás, a kivonás és a szorzás, mint az egész számok körében, továbbá a szokásos műveleti tulajdonságok is teljesülnek. Nevezzük ezt a halmazt a megszokott műveletekkel és műveleti tulajdonságokkal H_2-nek. A többszörös szokásos definíciója (2.1. Definíció) értelmében van értelme két szám szorzatát mindkét szám többszörösének nevezni. Hasonlóan, az osztó fogalom is értelmezhető.

1. Melyik nem egység H_2-ben? (Vagy azért, mert nincs benne, vagy azért, mert nem osztója minden elemnek.)

(a) 1

(b) -1

(c) $3 - \sqrt{2}$

(d) $3 + 2\sqrt{2}$

2. Melyik nem osztható $2 - \sqrt{2}$-vel a következő H_2-beli számok közül?

(a) $2 + 2\sqrt{2}$

(b) $\sqrt{2}$

(c) $2 - 3\sqrt{2}$

(d) $3 - 2\sqrt{2}$

A számelmélet alaptétele

1. Melyik számnak nem 8 az osztói száma a következők közül?
   (a) $2^3 \cdot 5$
   (b) $3 \cdot 5 \cdot 7$
   (c) 7^7
   (d) $2 \cdot 3 \cdot 5 \cdot 7$
2. Melyik két számnak van ugyanannyi osztója?
   (a) 2^3 és 3^2
   (b) $2 \cdot 3 \cdot 5$ és 2^3
   (c) $2 \cdot 5$ és 2^3
   (d) $2 \cdot 3$ és 5^2
3. Melyik felírás helyes?
   (a) $d(2) \leq d(3) \leq d(4) \leq d(5)$
   (b) $d(3) \leq d(4) \leq d(5) \leq d(6)$
   (c) $d(7) \leq d(8) \leq d(9) \leq d(10)$
   (d) $d(13) \leq d(14) \leq d(15) \leq d(16)$

A prímszámokról

1. A nagy prímszámtétel alapján milyen nagyságrendi becslés adható a prímszámok számára 10^{10}-ig?
   (a) $10^9 \cdot \ln 10$
   (b) $10^9 \cdot \log_{10} e$
   (c) $\dfrac{10^9}{\log_{10} e}$
   (d) $\dfrac{10^9}{\ln 10}$

Kongruencia

1. Milyen modulus szerint lehet kongruens 5 és 17?
   (a) 4

(b) 5
(c) 10
(d) 12

2. Az alábbiak közül melyik modulus szerint nem kongruens az 5 és a 17?

(a) 4
(b) 6
(c) 9
(d) 12

3. Mivel kongruens a 45 modulo 13?

(a) 9
(b) 19
(c) 29
(d) 39

4. Melyik teljes maradékrendszer modulo 7?

(a) -3, 3, 13, 23, 33, 43, 53
(b) 7, 14, 21, 28, 35, 42, 49
(c) 1, 2, 3, 4, 5, 6
(d) 1, 9, 17, 25, 33, 41, 49

5. Melyik redukált maradékrendszer modulo 7?

(a) -3, 3, 13, 23, 33, 43, 53
(b) 1, 2, 3, 4, 5, 6, 7
(c) 1, 2, 3, 4, 5, 6
(d) 1, 9, 17, 25, 33, 41, 49

6. Ha $\varphi(n) = 6$, akkor az alábbiak közül melyik nem lehet az n?

(a) 7
(b) 9
(c) 14
(d) 21

7. Melyik értéket nem veszi fel a φ függvény?

(a) 1
(b) 2
(c) 3
(d) 4

Lineáris kongruenciák

1. Az alábbi lineáris kongruenciák közül válasszuk ki azt, amelyiknek nincsen megoldása!

   (a) $2x \equiv 13 \pmod{6}$

   (b) $2x \equiv 6 \pmod{13}$

   (c) $13x \equiv 6 \pmod{2}$

   (d) $13x \equiv 2 \pmod{6}$

2. Hány megoldása van a $16x \equiv 15 \pmod{20}$ kongruenciának?

   (a) 0

   (b) 1

   (c) 4

   (d) végtelen sok

3. Hány megoldása van a $16x \equiv 20 \pmod{15}$ kongruenciának?

   (a) 0

   (b) 1

   (c) 2

   (d) végtelen sok

4. Hány megoldása van a $24x \equiv 102 \pmod{30}$ kongruenciának?

   (a) 0

   (b) 1

   (c) 5

   (d) 6

Lineáris diofantoszi egyenletek

1. Melyik lineáris diofantoszi egyenlet vezethető vissza a $3x \equiv 4 \pmod{8}$ kongruenciára?

   (a) $3x + 8y = -4$

   (b) $3x + 4y = 8$

   (c) $3x + 8y = 4$

   (d) $3x - 4y = -8$

2. Melyik kongruencia nem feleltethető meg az $5a - 7b = 11$ lineáris diofantoszi egyenletnek? (A kongruencia akkor feleltethető meg a diofantoszi egyenletnek, ha ugyanazon egész számokra teljesülnek.)

   (a) $5a \equiv 7b \pmod{11}$

   (b) $5x \equiv 11 \pmod{7}$

   (c) $7x \equiv 5 \pmod{11}$

   (d) $7x \equiv 11 \pmod{5}$

3. Hány megoldása van a $16a + 20b = 15$ diofantoszi egyenletnek?

   (a) 0

   (b) 1

   (c) 1-nél több, de véges sok

   (d) végtelen sok

4. Hány megoldása van a $16a + 12b = 32$ diofantoszi egyenletnek?

   (a) 0

   (b) 1

   (c) 1-nél több, de véges sok

   (d) végtelen sok

Néhány nevezetes diofantoszi probléma

1. Hány természetes (pozitív egész) szám nem lehet egy pitagoraszi számhármas egy tagja?

   (a) 0

   (b) 1

   (c) 2

   (d) 2-nél több

2. Az alábbiak közül melyik szám nem állhat elő két négyzetszám különbségeként?

   (a) 1

   (b) 3

   (c) 4

   (d) 6

3. Az alábbiak közül melyik szám nem állhat elő két négyzetszám különbségeként?

   (a) 8
   (b) 9
   (c) 10
   (d) 11

4. Az alábbiak közül melyik szám írható fel két négyzetszám összegeként?

   (a) 102
   (b) 103
   (c) 104
   (d) 105

Számelméleti függvények

1. Melyik, a φ számelméleti függvényre vonatkozó állítás igaz?

   (a) φ soha nem vehet fel páratlan értéket.
   (b) φ csak egyszer vesz fel páratlan értéket.
   (c) φ csak kétszer vesz fel páratlan értéket.
   (d) φ végtelen sokszor vesz fel páratlan értéket.

2. Melyik, a d számelméleti függvényre vonatkozó állítás hamis?

   (a) d soha nem vesz fel páros értéket.
   (b) d soha nem vesz fel páratlan értéket (csak az 1-ben az 1-et).
   (c) d tetszőleges természetes számot felvehet függvényértékként.
   (d) Van olyan természetes (pozitív egész) szám, amelyet d nem vehet fel függvényértékként.

3. Melyik állítás helyes a σ számelméleti függvényre?

   (a) $\sigma(n)$ soha nem lehet n-nél nagyobb.
   (b) $\sigma(n)$ soha nem lehet n-nél kisebb.
   (c) $\sigma(n)$ soha nem lehet n-nel egyenlő.
   (d) $\sigma(n)$ soha nem lehet $2n$-nel egyenlő.

4. Melyik állítás hamis?

   (a) Az $n \mapsto \varphi(n)$ összegzési függvénye n helyen n.

(b) Az $n \mapsto n$ összegzési függvénye n helyen $\sigma(n)$.

(c) Az $n \mapsto n^2$ függvénynek az összegzési függvénye az $n \mapsto \frac{n(n+1)(2n+1)}{6}$.

(d) Az $n \mapsto d(n)$ függvény megfordítási függvénye az $n \mapsto 1$ függvény.

Tökéletes számok

1. Az alábbiak közül melyikre teljesül, hogy $\sigma(n) < 2n$?

   (a) 6

   (b) 10

   (c) 12

   (d) 18

2. Az alábbiak közül melyik számra teljesül, hogy $\sigma(n) = 2n - 1$?

   (a) 6

   (b) 10

   (c) 14

   (d) 16

Függelék (A racionális számok tizedes tört alakja)

1. Az alábbiak közül melyik szám tizedes tört alakja nem véges?

   (a) $\frac{6}{10}$

   (b) $\frac{10}{6}$

   (c) $\frac{3}{12}$

   (d) $\frac{12}{3}$

2. Az alábbiak közül melyik szám tizedes tört alakja tiszta szakaszos?

   (a) $\frac{4}{36}$

   (b) $\frac{5}{6}$

   (c) $\frac{2}{12}$

(d) $\frac{2}{36}$

3. Melyik közönséges tizedes tört alakja a $0,\dot{3}4\dot{5}$

(a) $\frac{345}{9}$

(b) $\frac{345}{99}$

(c) $\frac{345}{999}$

(d) $\frac{345}{9999}$

4. Melyik tört lesz végtelen vesszős tört?

(a) $\frac{1}{3}$ a 3-as számrendszerben

(b) $\frac{1}{2}$ a 2-es számrendszerben

(c) $\frac{1}{2}$ a 3-as számrendszerben

(d) $\frac{2}{3}$ a 3-as számrendszerben

Irodalomjegyzék

[1] Bartha Gábor, Bogdán Zoltán, Csúri József, Duró Lajosné dr., dr. Gyapjas Ferencné, dr. Kálmán Sándorné, dr. Pintér Lajosné: *Matematika feladatgyűjtemény I. a középiskolák tanulói számára,* Nemzeti Tankönyvkiadó, 18. kiadás, 2004.

[2] Erdős Pál, Surányi János: *Válogatott fejezetek a számelméletből,* Polygon, Szeged, 1996.

[3] Korándi József, Török Judit, *Számelmélet,* Számelmélet és algebra sorozat, 1. kötet. NLV Nyomda, Budapest, 1996

[4] Laczkovich Miklós: Középiskolai Matematika Lapok, 1999, 7. szám, 385–398.

[5] Maurer I. Gyula: *Tizedes törtek és lánctörtek,* Dacia Könyvkiadó (Románia), 1981. (Magyar nyelvű)

[6] Sárközy András, Surányi János: *Számelmélet feladatgyűjtemény,* kézirat, Tankönyvkiadó, Budapest, 1986.

További érdekes olvasmányok, feladatgyűjtemények:

Fried Ervin: Oszthatóság és számrendszerek, Tankönyvkiadó, Budapest, 1982.

Freud Róbert: Prímszámok – ősi problémák, új eredmények, 2005. Előadás a Fazekasban, http://matek.fazekas.hu/portal/eloadas/2005/eloadas_2005_11_22_freud.html

Halmos Mária, Gábos Adél: Számelmélet, Műszaki Könyvkiadó Kft., 2000.

Lánczos Kornél: Számok mindenütt, Gondolat, 1972.

Matematikai érdekességek, Gondolat, Budapest, 1969, benne: Lánczi Ivánné: szórakozás számrendszerekkel, Surányi János: Érdekes számok.

Matematikai mozaik, Typotex, 1999 (Hódi Endre szerk.), benne: Surányi János: Érdekes számok, Rónyai Lajos: Egy igazán érdekes bizonyítás, Laczkovich Miklós: Prímképletek.

Otto Neugebauer: *Egzakt tudományok az Ókorban,* Gondolat, Budapest, 1984.

Oystein Ore: *Number Theory and Its History,* Dover Publications Ins., New York.

Pálfalvi Józsefné: Barátkozzunk a számokkal, Typotex, 1993.

Róka Sándor: 2000 feladat az elemi matematika köréből, Typotex, 2000.

Sain Márton: *Nincs királyi út!,* Gondolat, Budapest, 1986.

Sárközy András: Számelmélet, Bolyai könyvek sorozat, Műszaki Könyvkiadó, Budapest, 1976.

Waclaw Sierpinski: 200 feladat az elemi számelméletből, Középiskolai szakköri füzetek, Tankönyvkiadó, Budapest, 1972.

Simon Singh: A nagy Fermat-sejtés, Park Könyvkiadó, Budapest, 1999.

D. O. Sklarszkij, N. N. Csencov, I. M. Jaglom: Válogatott feladatok és tételek az elemi matematika köréből 1. Aritmetika és algebra, Typotex, 2000.

Raymond Smullyan: Gödel nemteljességi tétele, Typotex, 2006

Tárgymutató

A tesztek megoldása

Alapok 1. (c) 2. (b) 3. (d) 4. (a) 5. (b) 6. (d) 7. (a)

Oszthatóság, maradékos osztás 1. (c) 2. (d) 3. (d) 4. (a) 5. (d) 6. (a)

Számrendszerek, oszthatósági szabályok 1. (c) 2. (b) 3. (a) 4. (c) 5. (d) 6. (c)

Legnagyobb közös osztó, legkisebb közös többszörös 1. (c) 2. (c) 3. (d) 4. (c) 5. (b) 6. (c)

Felbonthatatlan szám, prímszám 1. (c) 2. (d)

A számelmélet alaptétele 1. (d) 2. (c) 3. (d)

A prímszámokról 1. (b)

Kongruencia 1. (d) 2. (c) 3. (b) 4. (d) 5. (c) 6. (d) 7. (c)

Lineáris kongruenciák 1. (a) 2. (a) 3. (b) 4. (d)

Lineáris diofantoszi egyenletek 1. (c) 2. (c) 3. (a) 4. (d)

Néhány nevezetes diofantoszi probléma 1. (c) 2. (d) 3. (c) 4. (c)

Számelméleti függvények 1. (c) 2. (c) 3. (b) 4. (c)

Tökéletes számok 1. (b) 2. (d)

Függelék (A racionális számok tizedes tört alakja) 1. (b) 2. (a) 3. (c) 4. (c)

A könyvhöz tartozó videó megtekintése: www.cs.elte.hu/~kfried/algebra1/kettedestort.avi