

## Kurzusinformáció 2019\_20\_II.

<b>Tantárgy neve</b>	Diszkrét matematika
<b>Tantárgy kódja</b>	BPI1207
<b>Meghirdetés féléve</b>	2
<b>Kreditpont</b>	6
<b>Óraszám (ea+gyak)</b>	Nappali: 2+2 / hét
<b>Félévi követelmény</b>	gyakorlati jegy
<b>Előfeltétel</b>	nincs

### Előadások anyaga:

A matematika alapfogalmai. Halmazok, relációk, függvények, műveletek, struktúrák.

A halmazelmélet alapfogalmai. Halmazműveletek és tulajdonságaik.

Számhalmazok és azok jellemzői. Teljes indukció.

A számfogalom kiépítése a természetes számoktól a komplex számokig. Műveletek a komplex számok körében.

Algebrai műveletek és tulajdonságaik. Algebrai struktúrák. Nevezetes struktúrátípusok. Félcsoport, csoport, gyűrű. Az asszociativitás és a disztributivitás következményei. Boole-algebra.

Számelméleti alapismeretek. Oszthatóság és maradékos osztás egész számok körében.

A számelmélet alaptétele. Prímszámok. Számelméleti függvények.

Számrendszerek.

Lineáris kétismeretlenes diofantoszi egyenlet. Kongruencia, Euler-Fermat tétele. Egyismeretlenes lineáris kongruenciák.

Polinomgyűrűk. Oszthatóság és maradékos osztás polinomok körében. Prím és irreducibilis polinomok. A polinomelmélet alaptétele.

Testek. A racionális számok, tizedes tört alakjuk. A valós és komplex számok teste. Az algebra alaptétele. Másod- és harmadfokú egyenletek megoldása.

Kombinatorikai alapfogalmak, alaptulajdonságok. Leszámlálás. Alapvető kombinatorikai konstrukciók, szitaformula, permutáció, kombináció, variáció, ismétlés nélküli, ismétléses.

### Kötelező ill. ajánlott irodalom.

1. Fried Ervin: ALgebra I, II. Nemzeti Tankönyvkiadó, Budapest, 2002, ISBN 963 18 9754 0

2. J. Kurdics: Diszkrét matematika, Bessenýiei Kiadó, Nyíregyháza, 2006, -

3. Kurdics, J: „Algebra. Part I., LAP Lambert Academic Publishing, Saarbrücken (2014), pp. viii + 203, ISBN 978-3-659-62092-8, zbMATH06370129, <http://doi.org/10.13140/2.1.2645.6644>

4. J. Kurdics: Diszkrét matematika, elektronikus tananyag, moodle.nyf.hu

5. Dr. Szendrei János: Algebra és számelmélet. Nemzedékek Tudása Tankönyvkiadó, Budapest, 2001, ISBN: 9789631924015

2020. február 07.

Nyilas József  
adjunktus

## **Osztthatóság**

Az **osztthatóság** egy matematikai reláció, melynek tulajdonságait a számelmélet vizsgálja.

Hagyományos értelemben akkor mondjuk, hogy az  $a$  és  $b$  **természetes** számok között (ebben a sorrendben) fennáll az osztthatósági reláció; röviden a  $b$  szám **osztója** az  $a$  számnak, vagy az  $a$  szám **osztható** a  $b$ -vel, ha van olyan egész szám, melyet  $b$ -vel szorozva  $a$ -t kapunk, vagyis, más szóval, ha az  $a$  szám **többszöröse** a  $b$ -nek. A  $b$  osztó **valódi osztó**, ha nem azonos  $a$ -val vagy 1-gyel.

Egy  $a$  egész szám osztója egy  $b$  egész számnak, ha van olyan  $n$  egész szám, melyre  $a \cdot n = b$ . Jele:  $a|b$  ( $a$  osztója  $b$ -nek).

**Osztthatóság.** Ha a maradékos osztásnál a maradék  $q=0$ , akkor azt mondjuk, hogy „ $a$ ” a „ $b$ ”-nek osztója, vagy hogy „ $b$ ” az „ $a$ ”-nak többsége. Ezt így jelöljük:  $a|b$ . Vegyük észre, hogy maradékos osztásnál és az osztthatóságnál, bármely természetes számról szoltunk, tehát a 0-t nem zártuk ki. Ez nem azt jelenti, hogy 0-val osztani lehetne! De jelenti azt, hogy a 0 bármely szám többsége, mert létezik a  $0=p \cdot a+q$  egyenletet igazgató számok bármely „ $a$ ”-ra, csak azok:  $p=q=0$ , de ezt a definíció nem tiltja. Fordítva:  $b=p \cdot 0+q$  esetén nyilván minden érték 0, ami szintén nem azt jelenti, hogy 0-t 0-val sikerült elosztani, hanem azt, hogy 0-t szorzással csak 0-ból kaphatunk.

## **Prímszámok**

**Definíció:** Azt mondjuk, hogy egy  $p$  egynél nagyobb természetes szám **prímszám**, ha minden olyan esetben amikor  $p$  két természetes szám szorzatának osztója, akkor  $p$  a szorzat legalább egyik tényezőjének is osztója. Azaz tetszőleges  $a$  illetve  $b$  természetes számra:

Ugyanennek a tulajdonságnak egy másik fontos megfogalmazása a *felbonthatatlan tulajdonság*:

**Definíció:** Azt mondjuk, hogy egy  $f$  egynél nagyobb természetes szám **felbonthatatlan**, ha minden olyan esetben, amikor előáll két természetes szám szorzataként, a szorzatnak legalább az egyik tényezője 1. Azaz tetszőleges  $a$  illetve  $b$  természetes számra:

Azokat az egynél nagyobb természetes számokat, melyek nem felbonthatatlanok, összetett számoknak nevezzük.

*Azokat a természetes számokat, amelyeknek pontosan két osztójuk van, prímszámoknak (vagy másképp törzsszámoknak) nevezzük.*

*Összetett számoknak nevezzük azokat a természetes számokat, amelyeknek 2-nél több, de véges számú **osztója** van.*

**Tétel:** Két szomszédos prímszám között tetszőlegesen nagy különbség lehet; másképp megfogalmazva: tetszőleges  $n$ -re található  $n$  darab egymást követő összetett szám. Adott  $n$ -re például  $(n+1)!+2$  nyilván osztható 2-vel,  $(n+1)!+3$  osztható hárommal, és így tovább egészen

$(n+1)!+n+1$ -ig, ami osztható  $n+1$ -gyel. Ezért  $(n+1)!+2$ ,  $(n+1)!+3$ , ...,  $(n+1)!+n+1$   $n$  darab egymást követő összetett szám.

**Tétel:** Bármely egytől különböző pozitív egész szám és a kétszerese közt van prímszám.

**Prímszámok és számosságuk.** Megvizsgálhatjuk, hogy egy természetes számnak hány osztója lehet. Itt van mindjárt a 0. Ennek, mint azt az előbb láttuk, végtelen sok osztója van. A következő a sorban az 1. Hát ennek pontosan 1 darab osztója van. A két véglet itt foglal helyet a sorban, szépen egymás mellett. A 2-nek, a 3-nak két osztója van, (az 1 és önmaguk), míg a 4-nek már három: 1,2,4. Azokat a természetes számokat, amelyeknek pontosan 2 osztója van prímszámoknak, vagy másképpen törzsszámoknak nevezzük. Azokat, amelyeknek kettőnél több osztója van, összetett számoknak nevezzük. Így a 0 összetett szám, hiszen végtelen sok osztója van, az 1 viszont sem nem prím, sem nem összetett szám (önmaga egy külön csoportot alkot, oszthatóság szempontjából). Az első néhány prímszám: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Érdekes kérdés lehet, hogy hogyan helyezkednek el a prímszámok a természetes számok között, mekkora hézagokat találunk, azaz lehet-e nagyon sok összetett szám egymás után. Bebizonyítható, hogy tetszőleges  $N$  pozitív egész számhoz létezik  $N$  egymást követő pozitív egész szám, amelynek egyike sem prím. Bizonyításként előállítjuk ezeket a számokat. Jelölje „ $p$ ” az  $N$ -nél nagyobb, legkisebb prímszámot. Képezzük a következő számokat:

$$2*3*5*7*... *p+2$$

$$2*3*5*7*... *p+3$$

$$2*3*5*7*... *p+4$$

$$2*3*5*7*... *p+N$$

$$2*3*5*7*... *p+(N+1).$$

A felírt számok nyilván  $N$  darab egymást követő egész számok, ahol 2,3,5,7, ...  $p$  a prímszámokat jelenti 2-től  $p$ -ig. Mivel a számok szorzat részében, a hozzáadott rész legkisebb prímosztója szerepel (ezáltal kiemelhető), így mindegyik szám összetett szám. Ezzel a tételt bebizonyítottuk.

Szintén könnyen bizonyítható a következő állítás: a prímszámok száma végtelen. Ezt indirekt módon bizonyíthatjuk be. (Az indirekt bizonyítás lényege: feltételezzük az eredeti állítással ellentétes állítás igaz voltát, majd különböző logikai lépések után nyilvánvaló ellentmondásra jutunk, mely az eredeti tagadásának lehetetlenségét igazolja, a harmadik kizárt logikai elv alapján.) Tehát állításunkkal ellentétben tegyük fel, hogy csak véges sok ( $n$  darab) prímszám létezik. Legyenek ezek  $p_1$ ,  $p_2$ ,  $p_3$ . ...,  $p_n$ . Ezeknek a számoknak a szorzatához adjunk hozzá egyet, és vizsgáljuk meg, hogy milyen számot kapunk. Megállapíthatjuk, hogy ha bármely általunk felsorolt prímszámmal osztjuk ezt a számot, mindig 1-et kapunk maradékkul, azaz egyetlen prímszámmal sem osztható. Ebből két dolog következhet: vagy az, hogy egy prímszámot állítottunk elő, hiszen

pontosan két osztója van, (1 és önmaga), ekkor viszont nem soroltuk fel az előbb az összes prímszámot. A másik lehetőség az, hogy az előállított szám összetett szám, azaz legalább három osztója van, akkor viszont kell még legalább egy prímszámnak lenni, ami az előző véges felsorolásból kimaradt, és olyan, ami osztja az előállított összetett számot. Mivel minden lehetőséget megvizsgáltunk, nyilvánvaló, hogy semmi módon nem sorolhattuk fel az összes prímszámot, ellentmondásra jutottunk, azaz a prímszámok száma végtelen.

**Oszthatósági szabályok.** Függvénytáblázatokban gyakran bizonyos értékig felsorolják a prímszámokat, vagy a 2,3 és 5-el nem osztható számok prímtényezői felbontását, amelyből egyrészt a prímszámok, másrészt a nem könnyen felfedezhető prímtényezői felbontás kiolvasható. Néhány egyszerű szabályt említenénk meg, mely tetszőleges számról elárulja, hogy osztható-e egy adott számmal. Egyetlen páros prímszámunk van a 2. A kettővel való oszthatóság feltétele, az hogy az utolsó számjegye páros legyen, azaz osztható legyen kettővel. Ugyanez a szabály érvényes az 5-tel való oszthatóságra is (mármint az, hogy az utolsó számjegye osztható legyen 5-tel, mely ugye csak 0 és 5 esetén teljesül), hiszen a tízes számrendszer alapszámát mindkettő (a 2 és az 5 is) osztja. A hárommal való oszthatóság feltétele: a számjegyek összege osztható legyen 3-al. Ez annak a következménye, hogy a 10-es számrendszer alapjának 3-as maradéka 1. Ugyanez érvényes 9-re is. Ha egy szám osztható két egymáshoz képest relatív prímszámmal, akkor osztható azok szorzatával is. Így például a páros, 9-el osztható számok 18-al is oszthatók. A 11-el való oszthatóság: osszuk fel kétjegyű számokra a vizsgálandó számot az egyes helyi-értéktől kezdődően. Vegyük a keletkezett minden kétjegyű (és az esetleg legelöl keletkezett egyjegyű) szám 11-es maradékát, adjuk össze, ha 11-el osztható számot kapunk, akkor az eredeti szám is osztható volt 11-el, ha nem, akkor nem osztható. Egy másik szabály a 11-el való oszthatóságra: a vizsgálandó szám számjegyeit váltakozó előjellel adjuk össze, ha 11-el osztható összeget kapunk, akkor az eredeti is osztható volt 11-el (ha az összevonás eredménye negatív, oszthatóság szempontjából ugyanúgy járunk el, mintha pozitív volna). A számrendszer alapjával és annak hatványaival való oszthatósági feltételre, illetve a 25 vagy 50-nel való oszthatóságra egyszerűsége miatt nem térünk ki.

**Az aritmetika alaptétele.** Az aritmetika alaptétele azt mondja ki, hogy bármely 1-nél nagyobb természetes szám vagy prímszám, vagy egyértelműen bontható fel (a tényezők sorrendjétől eltekintve) prímszámok szorzatára. A természetes számok **kanonikus alakját**, azaz törzstényezői (prímtényezői) felbontását, prímszámok szorzataként való felírásának nevezzük. Ez a felbontás a számelmélet alaptétele szerint (a sorrendtől eltekintve) egyértelmű.

**Legnagyobb közös osztó.** Két szám legnagyobb közös osztója alatt azt a számot értjük, mely mindkét számot osztja, és amely minden közös osztónak többsége (természetes számok között – mivel rendezett halmazról van szó – egyúttal a legnagyobb). Meghatározása a prímtényezői felbontás segítségével: mindkét számot bontsuk fel prímtényezőkre, válasszuk ki a közösen szereplő

prímtényezőket a közösen szereplő legnagyobb multiplicitással (ismétlődéssel, kitevővel), és szorozzuk őket össze. Ekkor a legnagyobb közös osztót kapjuk. (Informatikában alkalmazása kissé nehézkes, meghatározáshoz az Euklideszi algoritmus alkalmazása ajánlott.) A legnagyobb közös osztót gyakran így jelölik:  $(a,b)$ . Több szám legnagyobb közös osztójának definíciója és a prímtényezős felbontásból való meghatározása ugyanaz, mint két szám esetén.

**Legkisebb közös többszörös.** Két szám legkisebb közös többszöröse alatt azt a számot értjük, mely mindkét számnak többszöröse, és amely minden közös többszörösnek osztója (természetes számok között – mivel rendezett halmazról van szó – egyúttal a legkisebb). Meghatározása a prímtényezős felbontás segítségével: mindkét számot bontsuk fel prímtényezőkre, válasszuk ki az egyáltalán szereplő prímtényezőket a legnagyobb multiplicitással és szorozzuk őket össze. Ekkor a legkisebb közös többszöröst kapjuk. A legkisebb közös többszöröst gyakran így jelölik:  $[a,b]$ . (A törzstényezős felbontáson alapuló alkalmazása az informatikában kissé nehézkes, meghatározáshoz az Euklideszi algoritmus, és a következő összefüggés ajánlott:  $a*b = (a,b)*[a,b]$ , azaz a két szám szorzat egyenlő a legnagyobb közös osztó és a legkisebb közös többszörös szorzatával. Ez utóbbi összefüggés a törzstényezős felbontáson alapuló meghatározásokból szinte triviálisan következik.) Több szám legkisebb közös többszörösének definíciója és a prímtényezős felbontásból való meghatározása ugyanaz, mint két szám esetén.

**Euklideszi algoritmus.** Euklidesztől maradt ránk, két szám legnagyobb közös osztójának meghatározása, a prímszámfogalom felhasználásának kikerülésével. Éppen ez teszi könnyen algoritmizálhatóvá, sőt ha még azt is megemlítyük, hogy az eljárásban szereplő osztás ismételt kivonással helyettesíthető, akkor könnyen gépi kódú algoritmust is készíthetünk a módszerre. Az algoritmus a maradékos osztáson alapul.

1. lépés: Osszuk el maradékosan az egyik számot a másikkal.
2. lépés: Az osztandó szerepét vegye át az előbbi osztó, az osztó szerepét pedig, az előbbi maradék, ha az nem 0. Mindaddig ismételjük a műveletet (térjünk vissza az 1. lépéshez), amíg 0 maradékot nem kapunk.
3. lépés: Az utolsó nem 0 maradék lesz a két szám legnagyobb közös osztója.

Az algoritmus helyes volta könnyedén igazolható, melyről itt eltekintünk. Azt viszont megemlíteném, hogy az általános algoritmus fogalmára az Euklideszi algoritmus nagyon szép példa. Könnyen megmutathatók rajta az algoritmussal kapcsolatban általánosan megfogalmazott igényeink: minden lépésben egyértelmű, minden lehetséges esetre megoldással szolgál, véges sok lépésben véget ér (hiszen a pozitív maradékok csökkenő sorozata véges), és számtalan (nagyon sok), csak kezdeti feltételekben különböző (ezáltal nagyon hasonló) feladat megoldására alkalmas.

**Relatív prímszámok.** Két szám relatív prím, ha a legnagyobb közös osztójuk 1. Ekkor a legkisebb közös többszörösük, a szorzatuk. Több szám is lehet relatív prím, ha legnagyobb közös

osztójuk 1. Ebben az esetben még előfordulhat, hogy néhány szám-pár nem relatív prím az összesből. Például: 3,5,15 relatív príme, de közülük két pár is kiválasztható, amelyek nem relatív príme. Több számra vonatkoztatva a relatív prím fogalomnál van egy szigorúbb is: a páronként relatív prím fogalma. Ekkor a számhalmaz bármely két szám-párja relatív prím.

**Ikerprímek.** Ha két prímszám különbsége 2, akkor ikerprímeknek nevezzük őket. A prímszámok elején rögtön egy hármast ikerprímet találunk: 3, 5 és a 7. Könnyen belátható, hogy további hármast ikerprím nem létezhet, mert olyan számtani sorozat három egymást követő tagjai lennének, amelyek közül az egyik biztosan osztható lenne 3-al, azaz nem lehetne az egyik prímszám. További ikerprímek: (11,13); (17,19); (29,31); (41,43); (59,61); (71,73); (101,103); ... Az ikerprímek számosságával kapcsolatban semmi biztosat nem tudunk mondani. Találtak már igen nagy ikerprímeket is, de nem ismert, hogy számuk véges-e vagy végtelen.

**Az osztók száma.** Egy pozitív természetes szám osztóinak számát prímtényező felbontásából a legkönnyebb meghatározni. Szerepeljenek az  $N$  szám prímtényező felbontásában a  $p_1, p_2, p_3, \dots, p_k$  prímszámok az  $n_1, n_2, n_3, \dots, n_k$  kitevőkkel (megengedett a 0 is). Ekkor a  $N$  szám osztóinak számát az  $(n_1+1) \cdot (n_2+1) \cdot (n_3+1) \cdot \dots \cdot (n_k+1)$  szorzat adja. Indoklásnak csak annyit, hogy itt a prímtényezők ismétléses variációinak számát számoltuk össze, megengedve azt is, hogy egy prímszámot egyetlen egyszer sem, vagy az előforduló maximális kitevővel is figyelembe vegyünk, az osztók előállításakor. Példaként megemlítjük, hogy ha egy számról azt tudjuk, hogy pontosan három osztója van, akkor az egy prímszám négyzete.

Egy számnak (ha nem 1), akkor legalább két osztója van: az 1 és önmaga. Ezeket az osztókat szokás nem valódi osztóknak nevezni, minden más osztóját (ha létezik), valódi osztónak hívjuk. Ezek szerint a prímszámoknak nincs, az összetett számoknak van valódi osztója. Szokás az osztók felsorolásánál osztó-párokat feltüntetni, amelyek szorzata maga a szám. Minden összetett számnak van a szám négyzetgyökénél nem nagyobb prímosztója. (Az osztó-pároknál az egyik kisebb-egyenlő, mint a szám négyzetgyöke, a másik pedig, nagyobb-egyenlő. Ha egyenlők, akkor a szám négyzetszám volt.) Prímosztók keresésénél tehát csak a szám négyzetgyökéig kell a keresést végrehajtani. Ha addig nem volt prímosztó, akkor már nem is lesz, azaz a kérdéses szám prímszám (Eratosztenész szitája).

**Számelméleti függvény**nek nevezünk a [matematikában](#) egy olyan [függvényt](#), amelynek értelmezési tartománya a [természetes számok halmaza](#) (kivéve esetleg a nullát), értékkészlete pedig a [komplex számok](#) egy [részhalmaza](#). (általában az egész számok halmaza)

jel	név (nevek)	jelentés
$d(n)$	<a href="#">osztószám-függvény</a>	az argumentum <a href="#">osztóinak</a> száma
$\sigma(n)$	<a href="#">osztóösszeg-függvény</a> (szigma)	az argumentum osztóinak összege
$s(n)$	<a href="#">valódiosztóösszeg-függvény</a>	az argumentum valódi osztóinak összege
$\sigma_x(n)$	<a href="#">osztóhatványösszeg-függvény</a>	az argumentum osztóinak <a href="#">valós</a> , rögzített kitevőjű <a href="#">hatványának</a> összege
$P(n)$	<a href="#">osztószorzat-függvény</a>	az argumentum osztóinak szorzata
$v(n)$	nű-függvény	az argumentum <a href="#">prímtényezőinek</a> száma ( <a href="#">multiplicitással</a> számolva)
$\chi(n)$	khi-függvény	az argumentum különböző prímtényezőinek száma
$\varphi(n)$	<a href="#">Euler-függvény</a> (fi)	az argumentumhoz <a href="#">relatív prím</a> , nála nem nagyobb pozitív egészek száma
$\mu(n)$	<a href="#">Möbius-függvény</a> (mű)	egy, a számok <a href="#">négyzetmentességét</a> „mérő” függvény
$\pi(n)$	diszkrét <a href="#">prímszámláló függvény</a>	az argumentumnál nem nagyobb prímek száma
$g(n)$	lnko-összeg-függvény	az argumentumnál nem nagyobb pozitív egészek és az argumentum legnagyobb közös osztóinak összege

## Kongruenciák.

Legyen  $m$  egy pozitív egész szám, melyet modulusnak (vagy a modulus alapjának) fogunk nevezni.

Ha az egész számokat osztjuk  $m$ -mel, akkor a következő maradékok egyikét kaphatjuk:

$$0, 1, 2, \dots, m-1.$$

**Ha „a” és „b” két egész szám, továbbá,  $m$ -mel osztva ugyanazt a maradékot adják akkor mondjuk, hogy  $a$  és  $b$  kongruensek modulo  $m$ -re, jelölése:**

$$a \equiv b \pmod{m}.$$

Mivel „a” és „b” csak akkor adnak ugyanolyan maradékot  $m$ -mel való osztáskor, ha különbségük osztható  $m$ -mel, **a kongruenciát így is definiálhatjuk:  $a \equiv b \pmod{m}$ , ha  $m \mid a-b$ .**

A kongruencia egy ekvivalencia reláció. Ez pontosan azt jelenti, hogy a természetes számokat modulo  $m$ -re „ $m$ ” darab osztályba soroltuk, egy osztályba kerülve az egymással kongruens számok. Hogy a kongruencia ekvivalencia reláció, a következő tulajdonságai bizonyítják:

1. A kongruencia reflexív:  $a \equiv a \pmod{m}$  bármely  $a$ -ra. (Hiszen minden szám a 0-nak osztója.)
2. A kongruencia szimmetrikus, azaz: ha  $a \equiv b \pmod{m}$ , akkor  $b \equiv a \pmod{m}$  is igaz.
3. A kongruencia transzítív, azaz: ha  $a \equiv b \pmod{m}$  és  $b \equiv c \pmod{m}$  akkor  $a \equiv c \pmod{m}$  is igaz.

Márpedig azokat a relációkat, amelyekre igaz a fenti három (aláhúzással jelölt) tulajdonság, azt a relációt ekvivalencia relációnak nevezzük. További tulajdonságok, melyek az egyenlőséghez (azonossághoz) nagyon hasonlóvá teszik:

1. Szabad a kongruencia minkét oldalához ugyanazt az egész számot hozzáadni.
2. Kongruenciák (ugyanazon modulo mellett) összeadhatók, mint az egyenletek.
3. A kongruenciák kivonhatók, mint az egyenletek.
4. A kongruencia egyik oldalához hozzáadható a modulus többszöröse.
5. A kongruenciák mindkét oldala megszorozható ugyanazzal a számmal.
6. A kongruenciák összeszorozhatók (szintén ugyanazon modulo mellett).
7. Szabad a kongruenciák mindkét oldalát ugyanarra a hatványra (pozitív egész!) emelni.
8. Szabad a kongruenciában a benne lévő számok helyett velük kongruens számokat írni (természetesen ugyanazon modulo mellett).
9. A kongruencia mindkét oldalát szabad olyan számmal egyszerűsíteni, amely relatív prím a modulushoz.
10. Kongruens számoknak a modulussal ugyanaz a legnagyobb közös osztójuk, azaz ha  $a \equiv b \pmod{m}$ , akkor  $(a,m) = (b,m)$ .



## Lineáris diofantoszi egyenlet

Kétismeretlenes lineáris diofantikus egyenletek

**Definíció:** Az  $ax+by=c$  kétismeretlenes lineáris egyenletet diofantoszi egyenletnek nevezzük, ha  $a,b,c$  egész számok, ( $a=b=0$  esetet kizárjuk), és megoldások ( $x$  és  $y$ ) egész számokból álló számpárok.

**Tétel:** Legyenek  $a$ ,  $b$  és  $c$  rögzített egész számok, ahol  $a$  és  $b$  közül legalább az egyik nem nulla, és tekintsük az  $ax+by=c$  diofantikus egyenletet. Az egyenlet akkor és csak akkor oldható meg, ha  $(a,b)|c$ . Megoldhatóság esetén végtelen sok megoldás van. Ha  $x_0$ ,  $y_0$  (egy rögzített) megoldás, akkor az összes  $x'$ ,  $y'$  megoldást az alábbi képlet szolgáltatja:

$$x' = x_0 + t \frac{b}{(a,b)}, \quad y' = y_0 - t \frac{a}{(a,b)}, \text{ ahol } t=0, \pm 1, \pm 2, \dots$$

Az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg

**Példa:** Oldjuk meg az  $52x+23y=65$  diofantikus egyenletet.

A feladatot háromféleképpen is megoldjuk.

### 1) Kongruencia segítségével

Tudjuk, hogy két egész szám kongruens egymással modulo  $m$ , ha  $m$ -mel osztva ugyanazt a maradékot adják ( $m$  egész). A következő tételt használjuk fel a megoldásnál: Ha az  $ax+by=c$  egyenlőség fennáll, akkor  $ax \equiv c \pmod{b}$  és fordítva. Az egyenletünk tehát  $52x+23y=65$  ekvivalens a  $52x \equiv 65 \pmod{23}$  kongruencia megoldásával.

Mindkét oldalból levonjuk a 23 valahányszorosát úgy, hogy a legkisebb abszolút értékű számokat kapjuk a kongruencia mindkét oldalán.

$$6x \equiv -4 \pmod{23}, \quad \text{osztva 2-vel } 3x \equiv -2 \pmod{23}$$

Ha -2-höz hozzáadunk 23-at, a kongruencia jobb oldalán 21 fog állni. Osztva 3-mal:  $x \equiv 7 \pmod{23}$ .

Ha  $x=7$ , ebből  $y=-13$  adódik az  $x=7$  egyenletbe történő behelyettesítése után.

Kaptunk tehát egy  $x_0$ ,  $y_0$  megoldást.

A többi megoldást a tételből kapjuk meg az előző megoldásban leírtakkal azonos mód

### 2) A tétel felhasználásával

Próbálkozással keresünk egy  $x_0$ ,  $y_0$ s zámpárt, mely kielégíti az egyenletet, majd a tétel segítségével meghatározzuk az összes többi.

Próbálkozásaink során kiderül, hogy  $x_0=7$ ,  $y_0=-13$  kielégíti az egyenletet.

Ebből az összes megoldás:  $x=7+t \cdot 23$ ,  $y=-13+t \cdot 52$ , ahol  $t=0, \pm 1, \pm 2, \dots$

### 3) Egyszerű következtetéssel, középiskolában alkalmazott módon.

Fejezzük ki az egyenletből azt az ismeretlent, amelynek az együtthatója kisebb abszolút értékű, és a törtből válasszunk le olyan részeket, amelyek biztosan egész értékűek: