Diszkrét modellek alkalmazásai 5. gyakorlat

2020. 10. 05.

1 A gyakorlat anyaga

Ezen a gyakorlaton - különböző példákon keresztül - ismerkedünk meg a diofantikus egyenletekkel, kongruencia-rendszerekkel, a kínai maradéktétellel, valamint nézünk olyan feladatokat, amik olyan fogalmak ismereteit igénylik, mint oszthatóság, egység, felbonthatatlan szám, prímszám, illetve az összetett szám.

1.1 diofantikus egyenletek - lineáris egyenletek

A matematikában a diofantoszi egyenlet vagy diofantikus egyenlet olyan egész együtthatós, általában többismeretlenes algebrai egyenlet, amelynek megoldásait az egész, ritkábban a természetes számok, illetve racionális számok körében keressük.
Az $ax + by = m$ egyenlet egész számokban akkor és csak akkor oldható meg, ha $lnko(a, b)|m$. Ha kikötjük, hogy a, b, m pozitív egész legyen és $(a, b) = 1$, akkor pontosan $(a - 1)(b - 1)/2$ darab olyan m szám van, ami nem állítható elő nemnegatív x-szel és y-nal $ax + by$ alakban, a legnagyobb közülük $(a - 1)(b - 1) - 1$. Általában az $a_1x_1 + ... + a_nx_n = m$ egyenlet pontosan akkor oldható meg egészekben, ha $(a_1, ..., a_n)|m$.

1.2 kongruencia rendszerek

Akárcsak az egyenleteknél, itt is beszélhetünk több kongruenciából álló kongruenciarendszerről. Ekkor egy olyan maradékosztályt keresünk, ami minden kongruenciát kielégít. A páronként relatív prím modulusú kongruenciarendszerek megoldásáról szól a kínai maradéktétel, mely kimondja hogy a megoldás létezik és egyértelmű.

1.3 kínai maradéktétel

A kínai maradéktétel a több kongruenciából álló szimultán kongruenciarendszerek megoldhatóságára ad választ. A tétel tulajdonképpen a következő feladatra ad választ (továbbá kimondja, hogy a megoldás egyértelmű maradékosztály): keressük azt az egész számot (maradékosztályt), ami bizonyos számokkal osztva, amelyek páronként relatív prímek, meghatározott maradékot ad.
Legyenek m_1,m_2,...,$m_k > 0$ páronként relatív prímek, c_1,c_2,....,c_k pedig tetszőleges egészek. Ekkor az
$x \equiv c_1 \quad (m_1)$
$x \equiv c_2 \quad (m_2)$
$x \equiv c_3 \quad (m_3)$
...
$x \equiv c_k \quad (m_k)$
kongruencia-rendszer megoldható, és a megoldás egyetlen maradékosztály lesz $\mod M$, ahol $M = m_1m_2 \dots m_k$.

1.4 oszthatóság

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

1.5 egység

Az egységek olyan számok, melyek osztói minden aktuális egész számhalmazbeli számnak.

1.6 felbonthatatlan számok

A a számtól (és nullától) különböző számot felbonthatatlan számnak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység, azaz: $(a = bc)$ => b vagy c egység.

1.7 prímszámok

Az a egységtől és nullától különböző számot prímszámnak (vagy röviden prímnek) nevezzük, ha csak úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója, azaz: $a|bc$ => $a|b$ vagy $a|c$.

1.8 összetett számok

Összetett számnak nevezzük az olyan 1-nél (szigorúan) nagyobb számokat, amelyeknek kettőnél több osztója van (, azaz van legalább egy valódi osztójuk). Másképp fogalmazva, az összetett szám nem lehet nulla, egység, vagy felbonthatatlan szám.

2 Feladatok és megoldásaik

2.1 Oldja meg a következő lineáris diofantikus egyenleteket!

- 3x + 10y = 9:
3x + 10y = 9 (lnko(3,10) | 9 igaz) $\iff$ 3x = 9 - 10y. Most pedig maradékosan osszuk le mind a két oldalt 10-zel:
3x = 9 - 10y $\iff$ 3x mod 10 = (9 - 10y) mod 10 $\iff$ 3x mod 10 = 9 mod 10 (mert -10y mod 10 = 0)
3x mod 10 = 9 mod 10 $\iff$ $3x \equiv 9 \quad (10)$. Innentől a megszokott módon oldjuk meg a feladatot.
A $3x$ miatt le akarunk osztani 3-mal, mert $x \equiv y \quad (z)$ formátumú kongruenciát akarunk, ehhez megvizsgáljuk a modulus és az 3 legnagyobb közös osztóját, mert a modulus osztása a korábban tanult képlet alapján zajlik, míg a két oldalt oszthatjuk 3-mal, mert 3 | 3 és 3 | 9. Így lnko(10,3) = 1. Ezek után:
$3x \equiv 9 \quad (10) \iff x \equiv 3 \quad (10/lnko(10,3)) \iff x \equiv 3 \quad (10)$
Melyek azok az x számok, amelyek 10-való osztáskor 3 maradékot adnak? x $\in (..., -17, -7, 3, 13, 23, ...)$
$x \in (3 + 10k_1|k_1 \in \mathbb{Z})$, de ezzel még nincs vége a feladatnak, hiszen egy kétismeretlenes egyenletből indultunk ki, így meg kell határoznunk y értékét is:
3 (3 + 10k_1) + 10y = 9 $\iff$ 9 + 30k_1 + 10y = 9 $\iff$ 30k_1 + 10y = 0 $\iff$ 10y = -30k_1
$\iff$ y = -3k_1 $\iff$ $y \in (-3k_1|k_1 \in \mathbb{Z})$
A megoldás így: $x \in (3 + 10k_1|k_1 \in \mathbb{Z})$ és $y \in (-3k_1|k_1 \in \mathbb{Z})$.

- 15x + 33y = 40:
15x + 33y = 40 (lnko(15,33) | 40 hamis) $\iff$ 15x = 40 - 33y. Most pedig maradékosan osszuk le mind a két oldalt 33-mal:
15x = 40 - 33y $\iff$ 15x mod 33 = (40 - 33y) mod 33 $\iff$ 15x mod 33 = 40 mod 33 (mivel -33y mod 33 = 0), így 15x mod 33 = 40 mod 33 $\iff$ $15x \equiv 40 \pmod{33}$. Innentől a megszokott módon oldjuk meg a feladatot, azaz törekszünk a $x \equiv y \pmod{z}$ formára, elsőként ezért 5-tel osztunk le, mert mind a 15, mind a 40 öttel osztható, ami meg a modulust illeti, azt lnko(33,5) = 1-gyel osztjuk le:
$15x \equiv 40 \pmod{33} \iff 3x \equiv 8 \pmod{33}$
A bal oldali x 3-mal osztható, azonban a jobb oldali 8-hoz nem tudok annyi 33-at hozzáadni vagy kivonni, hogy a végén egy 3-mal osztható számot kapjak jobb oldalt, így x-re nincs helyes megoldás, ezt alátámasztja a megoldhatósági feltétel: 33 | 3x - 8, így ennek a feladatnak nem létezik megoldása.

2.2 Bontsuk fel a 812-t két egész, illetve két természetes szám összegére úgy, hogy az egyik szám osztható legyen 12-vel, a másik pedig osztható legyen 32-vel!

A 812 szám felbontása két olyan számra, ami 12-vel illetve 32-vel osztható, egy diofantikus egyenletet eredményez, hiszen x, y változók esetén 812 = 12x + 32y. Innentől az előző feladatban látott módon oldjuk meg ezt az egyenletet:
812 = 12x + 32y $\iff$ 12x + 32y = 812 $\iff$ 12x = 812 - 32y $\iff$ 12x mod 32 = (812 - 32y) mod 32 $\iff$ 12x mod 32 = (812) mod 32, mivel -32y mod 32 = 0 $\iff$ $12x \equiv 812 \pmod{32}$
$12x \equiv 812 \pmod{32} \iff 3x \equiv 203 \pmod{8}$, mert a 4 osztója a 12-nek és a 812-nek, valamint lnko(32,4) = 4.
A $3x \equiv 203 \pmod{8}$ akkor megoldható, ha 8 | 3x - 203. Ez igaz (pl x = 1), így folytathatjuk a feladatot. (Természetesen ezt az ellenőzést a kongruenciaegyenlet elején is elvégezhettük volna, de így valamivel kisebb számokkal kellett dolgoznunk a feltétel vizsgálata során.)
$3x \equiv 203 \pmod{8}$: azt látjuk, hogy 203 nem osztható 3-mal, de tudunk-e annyi 8-ast hozzáadni/kivonni, hogy az eredmény osztható legyen 3-mal? Igen, tudunk, ha pl kétszer adunk hozzá 8-at:
$3x \equiv 203 \pmod{8} \iff 3x \equiv 219 \pmod{8} \iff x \equiv 73 \pmod{8}$, mivel 3 osztója 3-nak és 219-nek, valamint lnko(8,3) = 1, így megkaptunk egy egyszerű kongruenciát.
$x \equiv 73 \pmod{8}$, azaz ha x-et maradékosztok 8-cal, akkor ugyanazt kapom, mintha 73-at maradékosztanám 8-cal. Mivel 73 mod 8 = 65 mod 8 = 57 mod 8 = ... = 1 mod 8, ezért ezt egyszerűbb alakra is felírhatjuk: $x \equiv 1 \pmod{8}$.
Így a megoldás x-re: $x \in (1 + 8k | k \in \mathbb{Z})$. Keressük meg ehhez a megfelelő y-okat:
812 = 12 (1 + 8k) + 32y $\iff$ 812 = 12 + 96k + 32y $\iff$ 800 = 96k + 32y $\iff$ 800 - 96k = 32y
800 - 96k = 32y $\iff$ 25 - 3k = y, azaz $y \in (25 - 3k | k \in \mathbb{Z})$.
Ha az egész számokat keressük, akkor az $x \in (1 + 8k | k \in \mathbb{Z})$ és $y \in (25 - 3k | k \in \mathbb{Z})$ teljes megoldás. Amennyiben csupán természetes számokat keresünk, úgy szűkítenünk kell ezt a megoldáshalmazt a következőképpen:
$x \in (1 + 8k | 1 + 8k \geq 0) \iff x \in (1 + 8k | 1 \geq -8k) \iff x \in (1 + 8k | 1/8 \geq -k)$
$\iff x \in (1 + 8k | -1/8 \leq k) \iff x \in (1 + 8k | k \in \mathbb{N})$
$y \in (25 - 3k | 25 - 3k \geq 0) \iff y \in (25 - 3k | 25 \geq 3k) \iff y \in (25 - 3k | 25/3 \geq k) \iff y \in (25 - 3k | k \in [0, 8])$ Mivel mind a két változónál ugyanazon k-ról van szó, így:
$k = (k | k \in \mathbb{N}) \cap (k | k \in [0, 8]) = (k | k \in [0, 8])$.
Vagyis, ha x, y természetes számok, akkor $x \in (1 + 8k | k \in [0, 8])$ és $y \in (25 - 3k | k \in [0, 8])$.

2.3 Oldja meg a következő kongruencia-rendszereket (a kínai maradéktétellel)!

- $x \equiv 1 \pmod{4}$, $x \equiv 3 \pmod{4}$
Mivel azonos a két kongruenciaegyenlet modulusa, ezért az egyik feltétel a megoldás létezésére az, hogy

a két egyenlet jobboldala közti különbség néggyel osztható szám legyen. Mivel $4 \nmid |1\text{-}3|$, (azaz (4 | x - 1) $\neq$ (4 | x - 3)) így nem létezik az egyenletrendszernek közös megoldása.
- $x \equiv 10 \quad (3)$, $x \equiv 4 \quad (7)$
Mivel a modulusok (3, 7) páronként relatív prímek, így - a kínai maradéktétel alapján - létezik megoldás. Így M = $m_1 * m_2$ = 3 * 7 = 21, valamint M_1 = M / m_1 = 21/3 = 7, M_2 = M / m_2 = 21/7 = 3 és c_1 = 10, c_2 = 4. Ekkor, felhasználjuk a $M_i * y \equiv 1 \quad (m_i)$ formulát és létrehozzuk az alábbi kongruenciarendszert: $7y \equiv 1 \quad (3)$; $3y \equiv 1 \quad (7)$.
Ha megoldjuk az egyes kongruenciákat, azt a leegyszerűsített egyenlethármast kapjuk, hogy:
$y \equiv 1 \quad (3)$; $y \equiv 5 \quad (7)$.
Innen, az egyes y értékek, azaz egy biztos megoldás az egyes egyenleteknél: $y_1 = 1$, $y_2 = 5$. Végül, használjuk fel az alábbi képletet a megoldás megtalálásához:
$x \equiv c_1 * M_1 * y_1 + c_2 * M_2 * y_2 \quad (M) \iff x \equiv 10 * 7 * 1 + 4 * 3 * 5 \quad (21)$
$\iff x \equiv 130 \quad (21) \iff x \equiv 4 \quad (21)$ = 4-es maradékosztály modulo 21.

- $x \equiv -2 \quad (4)$, $x \equiv 1 \quad (3)$, $x \equiv 3 \quad (7)$
Mivel a modulusok (4, 3, 7) páronként relatív prímek, így - a kínai maradéktétel alapján - létezik megoldás. Így M = $m_1 * m_2 * m_3$ = 4 * 3 * 7 = 21 * 4 = 84, valamint M_1 = M / m_1 = 84/4 = 21, M_2 = M / m_2 = 84/3 = 28 és M_3 = M / m_3 = 84/7 = 12 és c_1 = -2, c_2 = 1, c_3 = 3. Ekkor, felhasználjuk a $M_i * y \equiv 1 \quad (m_i)$ formulát és létrehozzuk az alábbi kongruenciarendszert:
$21y \equiv 1 \quad (4)$; $28y \equiv 1 \quad (3)$; $12y \equiv 1 \quad (7)$.
Ha megoldjuk az egyes kongruenciákat, azt a leegyszerűsített egyenlethármast kapjuk, hogy:
$y \equiv 1 \quad (4)$; $y \equiv 1 \quad (3)$; $y \equiv 3 \quad (7)$.
Innen, az egyes y értékek, azaz egy biztos megoldás az egyes egyenleteknél: $y_1 = 1$, $y_2 = 1$ és $y_3 = 3$. Végül, használjuk fel az alábbi képletet a megoldás megtalálásához:
$x \equiv c_1 * M_1 * y_1 + c_2 * M_2 * y_2 + c_3 * M_3 * y_3 \quad (M) \iff x \equiv -2 * 21 * 1 + 1 * 28 * 1 + 3 * 12 * 3 \quad (84)$
$\iff x \equiv 94 \quad (84) \iff x \equiv 10 \quad (84)$ = 10-es maradékosztály modulo 84.

- $9x \equiv 3 \quad (6)$, $5x \equiv -1 \quad (3)$, $-x \equiv 4 \quad (5)$
Mivel a modulusok (6, 3, 5) páronként nem relatív prímek (3 többszöröse 6), így a kínai maradéktétel alapján nem lehet megoldani ezt a kongruenciarendszert.

- $x \equiv -10 \quad (3)$, $x \equiv 6 \quad (5)$, $x \equiv 3 \quad (8)$
Mivel a modulusok (3, 5, 8) páronként relatív prímek, így - a kínai maradéktétel alapján - létezik megoldás. Így M = $m_1 * m_2 * m_3$ = 3 * 5 * 8 = 120, valamint M_1 = M / m_1 = 120/3 = 40, M_2 = M / m_2 = 120/5 = 24 és M_3 = M / m_3 = 120/8 = 15 és c_1 = -10, c_2 = 6, c_3 = 3. Ekkor, felhasználjuk a $M_i * y \equiv 1 \quad (m_i)$ formulát és létrehozzuk az alábbi kongruenciarendszert:
$40y \equiv 1 \quad (3)$; $24y \equiv 1 \quad (5)$; $15y \equiv 1 \quad (8)$.
Ha megoldjuk az egyes kongruenciákat, azt a leegyszerűsített egyenlethármast kapjuk, hogy:
$y \equiv 1 \quad (3)$; $y \equiv 4 \quad (5)$; $y \equiv 7 \quad (8)$.
Innen, az egyes y értékek, azaz egy biztos megoldás az egyes egyenleteknél: $y_1 = 1$, $y_2 = 4$ és $y_3 = 7$. Végül, használjuk fel az alábbi képletet a megoldás megtalálásához:
$x \equiv c_1 * M_1 * y_1 + c_2 * M_2 * y_2 + c_3 * M_3 * y_3 \quad (M) \iff x \equiv -10 * 40 * 1 + 6 * 24 * 4 + 3 * 15 * 7 \quad (120)$
$\iff x \equiv 491 \quad (120) \iff x \equiv 11 \quad (120)$ = 11-es maradékosztály modulo 120.

2.4 Bontsuk fel a 12-es számot felbonthatatlan számok szorzatára!

$12 = 4 \cdot 3 = 2 \cdot 2 \cdot 3$
vagy (-2) · (-2) · 3 vagy (-2) · 2 · (-3) vagy 2 · (-2) · (-3) vagy 2 · 3 · 2 vagy (-2) · (-3) · 2 vagy 3 · 2 · 2

vagy 2 · (-3) · (-2) vagy (-2) · 3 · (-2) vagy (-3) · (-2) · 2 vagy (-3) · 2 · (-2) vagy 3 · (-2) · (-2)

2.5 Lehet-e két prímszám különbsége 5? Keresse meg az összes lehetőséget!

Igen, lehet, pl. 2 és 7. Van-e több?
Tegyük fel, hogy p és q prímszámok és $q = p + 5$! Ekkor, ha p páratlan, akkor p felírható úgy, hogy $2x + 1$, ahol x egy egész szám. Ekkor $q = 2x + 1 + 5 = 2(x + 3)$, ami kettővel osztható, így q nem lehet páratlan.
Tehát, p-nek párosnak kell lennie, azonban az egyetlen páros prímszám a 2. Más páros prím nem létezik, mivelhogy egyszerre nem osztható kettővel és prím (kivéve magát a kettőt).
Így aztán a (2,7) számpár az egyetlen olyan prímszám-páros, amik különbsége 5.

2.6 Igaz vagy hamis?

- A pozitív egész számok halmazán egység az 1.

Igaz, hiszen minden pozitív egész szám osztója az 1.

- A páros pozitív egész számok halmazán egység az 1.

Igaz, mert minden pozitív páros egész szám osztója az 1 és az 1-nek nem kell elemének lennie ahhoz, hogy egysége lehessen a halmaznak.

- A legkisebb összetett szám a 4.

Igaz, mert $1 \mid 4$, $4 \mid 4$ és $2 \mid 4$.

- Minden összetett szám sorrendtől eltekintve egyértelműen felírható prímszámok szorzataként.

Igaz, ez a számelmélet alaptétele.

- Minden összetett szám prímtényezős alakjában pontosan egy prímszám szerepel.

Hamis, mert minden összetett szám prímtényezős alakjában egynél több, nem feltétlenül különböző prímszám szerepel.

- Ha $n > 5$ összetett szám, akkor $(n-1)! \equiv 0 \quad (n)$.

Igaz, ezt a Wilson-tétel mondja ki.