Diszkrét modellek alkalmazásai 4. gyakorlat

2020. 09. 28.

1 A gyakorlat anyaga

Ezen a gyakorlaton - különböző példákon keresztül - vizsgáljuk két szám legnagyobb közös osztóit, foglalkozunk az euklideszi algoritmussal, megismerkedünk a kongruenciával, valamint megnézzük, hogy miként oldunk meg egy tetszőleges lineáris kongruenciaegyenletet.

1.1 legnagyobb közös osztó

Egy a $\in \mathbb{Z}$ és b $\in \mathbb{Z}$ számoknak a d $\in \mathbb{Z}^+$ akkor a legnagyobb közös osztója, ha a d mindkét számnak közös osztója és minden közös osztónak a többszöröse.

1.2 euklideszi algoritmus

Az euklideszi algoritmus egy olyan számelméleti algoritmus, amellyel két szám legnagyobb közös osztója határozható meg.
$a = q_1 * b + r_1$
$b = q_2 * r_1 + r_2$
$r_1 = q_3 * r_2 + r_3$
...
$r_{n-2} = q_n * r_{n-1} + r_n$
$r_{n-1} = q_{n+1} * r_n + 0$
A fenti metódus a következő folyamatot írja le:
- az a számot felírjuk a b szám valahányszorosaként, melyhez hozzáadódik a hiányzó maradék
- ezután felírjuk a b számot a fentebb kapott maradékszám valahányszorosaként, amihez hozzáadódik egy új maradék
- a fenti folyamatot addig folytatjuk, amíg a maradék 0 nem lesz

Amint megkaptuk (véges számú lépésen belül) a 0 maradéktagot, úgy azt mondhatjuk, hogy a két szám legnagyobb közös osztója, a d szám a 0 maradéktagot közvetlenül megelőző maradéktag.
Hogyha nem jutunk el eddig a lépésig, úgy a két szám relatív prím, azaz a legnagyobb közös osztó az 1.
Hogyha létezik ez a d szám, akkor ez a legnagyobb közös osztó előállítható a két szám segítségével a következőképpen: $d = \alpha * a + \beta * b$
Hogy hogyan jön ki az α és a β érték, ahhoz a következő leírás adhat absztrakt magyarázatot:
$a - q_1 * b = r_1$ és $b - q_2 * r_1 = r_2$ és $r_1 = q_3 * r_2 + r_3$
$=> b - q_2 * (a - q_1 * b) = r_2$ és $(a - q_1 * b) = q_3 * (b - q_2 * (a - q_1 * b)) + r_3$
... $=> d = \alpha * a + \beta * b$

1.3 kongruencia

Legyen a, b tetszőleges egész szám, m pedig egy nullától különböző természetes szám. Azt mondjuk, hogy a kongruens b-vel modulo m, azaz hogy a és b egészek m-mel vett osztási maradéka egyenlő, ha $m|a-b$, azaz $\exists k \in \mathbb{Z}$: a = km + b. Jelölése: $a \equiv b \pmod{m}$ vagy $a \equiv b \quad (m)$. Ha a nem kongruens b-vel modulo m, azt mondjuk, inkongruens vele, és $a \not\equiv b \pmod{m}$ vagy $a \not\equiv b \quad (m)$ alakban jelöljük.

1.4 lineáris kongruenciaegyenlet megoldhatósága

Az $a * x \equiv b \quad (n)$ egyenletet, ahol a, b tetszőleges egész számok, n pedig egy pozitív egész szám, x egész szám pedig az ismeretlen, lineáris kongruencia egyenletnek nevezzük.
A lineáris kongruencia egyenlet megoldhatósági tétele:
Legyen a fenti egyenletre $d^* = lnko(a, n) = a * x^* + n * y + *$. A lineáris kongruencia egyenletnek akkor és csak akkor van megoldása, ha $d^*|b$. Ha van megoldás, akkor végtelen sok van, de ezeket egy d^* számú megoldást tartalmazó megoldás alaprendszerből megkaphatjuk az n egész számú többszöröseinek a hozzáadásával. Az alaprendszer elemeit a $0 \leq x \leq n$ intervallumból választjuk ki. Az alaprendszer megoldásai az alábbi módon írhatók fel:
$x_0 = x^* * (b/d^*) \bmod n$,
$x_i = x_0 + i * (n/d^*) \bmod n$ (i = 1,2,...,d^*-1)

2 Feladatok és megoldásaik

2.1 Számítsa ki a következő számok legnagyobb közös osztóját euklideszi algoritmus használatával!

- 18, 24:
Határozzuk meg az $lnko(18, 24)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: 24 = 1 * 18 + 6. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 18 = 3 * 6 + 0. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(18, 24) = 6$.
- 30, 70:
Határozzuk meg az $lnko(30, 70)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: 70 = 2 * 30 + 10. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 30 = 3 * 10 + 0. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(30, 70) = 10$.
- 231, 105:
Határozzuk meg az $lnko(231, 105)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: 231 = 2 * 105 + 21. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 105 = 5 * 21 + 0. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(231, 105) = 21$.
- 33, 21:
Határozzuk meg az $lnko(33, 21)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: 33 = 1 * 21 + 12. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 21 = 1 * 12 + 9. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 12 = 1 * 9 + 3. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: 9 = 3 * 3 + 0. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(33, 21) = 3$.

- 126, 150:
Határozzuk meg az $lnko(126, 150)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: $150 = 1 * 126 + 24$. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: $126 = 5 * 24 + 6$. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: $24 = 4 * 6 + 0$. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(126, 150) = 6$.
- 275, 132:
Határozzuk meg az $lnko(275, 132)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: $275 = 2 * 132 + 11$. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: $132 = 12 * 11 + 0$. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(275, 132) = 11$.
- 31, 11:
Határozzuk meg az $lnko(31, 11)$-et! Vegyük a nagyobbik értéket és nézzük meg, hogy a kisebbik hányszor van meg benne, milyen maradékkal: $31 = 2 * 11 + 10$. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: $11 = 1 * 10 + 1$. Mivel van (nemnulla, pozitív, egész) maradék, így a képlet alapján folytatjuk a számítást: $10 = 10 * 1 + 0$. Mivel a maradék itt 0, így meg is állhatunk. A megoldás így: $lnko(31, 11) = 1$.

2.2 Igazak-e az alábbi kongruenciák?

- $7 \equiv 3 \quad (3)$
$m|a - b => 3|7 - 3 = 3|4 =>$ hamis
- $7 \equiv 3 \quad (2)$
$m|a - b => 2|7 - 3 = 2|4 =>$ igaz
- $7 \equiv 3 \quad (1)$
$m|a - b => 1|7 - 3 = 1|4 =>$ igaz
- $8 \equiv 10 \quad (5)$
$m|a - b => 5|8 - 10 = 5| - 2 =>$ hamis
- $2 \equiv -1 \quad (3)$
$m|a - b => 3|2 - -1 = 3|3 =>$ igaz
- $6 \equiv 6 \quad (100)$
$m|a - b => 100|6 - 6 = 100|0 =>$ igaz
- $6 \equiv 2 \quad (4)$
$m|a - b => 4|6 - 2 = 4|4 =>$ igaz
- $3 \equiv -5 \quad (4)$
$m|a - b => 4|3 - -5 = 4|8 =>$ igaz
- $11 \equiv 8 \quad (3)$
$m|a - b => 3|11 - 8 = 3|3 =>$ igaz
- $18 \equiv -10 \quad (4)$
$m|a - b => 4|18 - -10 = 4|28 =>$ igaz
- $160 \equiv 80 \quad (16)$
$m|a - b => 16|160 - 80 = 16|80 =>$ igaz
- $11 \equiv 5 \quad (3)$
$m|a - b => 3|11 - 5 = 3|6 =>$ igaz
- $16 \equiv 8 \quad (8)$
$m|a - b => 8|16 - 8 = 8|8 =>$ igaz
- $8 \equiv 5 \quad (3)$
$m|a - b => 3|8 - 5 = 3|3 =>$ igaz

2.3 Oldja meg az alábbi lineáris kongruenciaegyenleteket!

- $x \equiv 2 \quad (3)$
$m|a-b => 3|x-2 => (..., -4, -1, 2, 5, ...) = (2 + k * 3|k \in \mathbb{Z}) = \overline{2} \text{ mod } 3$
- $x \equiv 7 \quad (2)$
$m|a-b => 2|x-7 => (..., -9, -7, -5, -3, -1, 1, 3, 5, 7, 9...) = (7 + k * 2|k \in \mathbb{Z}) =$
$= (1 + k * 2|k \in \mathbb{Z}) = \overline{7} \text{ mod } 2 = \overline{1} \text{ mod } 2$
- $2x \equiv 3 \quad (4)$
$m|a-b => 4|2x-3 = ...$
Nincs olyan x egész szám, amelyre $2x-3$ néggyel osztható lenne, sőt, nincs olyan x se, amire páros lenne a $2x-3$ értéke, így ennek a feladatnak nincs megoldása.
- $12x \equiv 8 \quad (20)$
$m|a-b => 20|12x-8$
Ahhoz, hogy az x-es tagon egyszerűsíteni tudjunk, meg kell néznünk, hogy mennyivel oszthatunk le mind a két oldalon, így most keressük meg 12 és 20 legnagyobb közös osztóját!
$lnko(12, 20)$: $20 = 1 * 12 + 8 => 12 = 1 * 8 + 4 => 8 = 2 * 4 + 0 => lnko(12, 20) = 4$
Most, osszunk le mindkét oldalt ezzel az értékkel:
$12x/lnko(12, 20) \equiv 8/lnko(12, 20) \quad (20/lnko(20, 4)) = 3x \equiv 2 \quad (5)$
Látható, hogy a modulo leosztása nem a hagyományos módon történik. Ott a következő képletet alkalmaztuk: m => m / lnko(m,c), ahol c az adott osztószám.
$3x \equiv 2 \quad (5)$ - alakítsuk át a jobb oldalt úgy, hogy hárommal lehessen osztani vele! pl.: adjunk hozzá 10-et, azaz 2*5-öt:
$3x \equiv 12 \quad (5)$ - ezt megtehettük, mivel ugyanazon maradékosztály eleme a 12 és a 2, mert a modulo többszörösével növeltünk! Most osszunk le 3-mal:
$x \equiv 4 \quad (5/lnko(5, 4)) = x \equiv 4 \quad (5) => (4 + k * 5|k \in \mathbb{Z}) = (-1 + k * 5|k \in \mathbb{Z}) =$
$= \overline{-1} \text{ mod } 5 = \overline{4} \text{ mod } 5.$
DE nekünk 20-as modulo osztályok kellenek, ahogy az eredeti feladatban is volt! Így nekünk fel kell bontanunk ezt az osztályt olyan 20-as modulo osztályokra, amelyek együttesen lefedik ezt a $\overline{4}$ mod 5 osztályt:
$\overline{4}$ mod 5 = (...,-16,-11,-6,-1,4,9,14,19,...) =
$= (4 + k_1 * 20|k_1 \in \mathbb{Z}) \cup (9 + k_2 * 20|k_2 \in \mathbb{Z}) \cup (14 + k_3 * 20|k_3 \in \mathbb{Z}) \cup (19 + k_4 * 20|k_4 \in \mathbb{Z})$
- $22x \equiv 8 \quad (10)$
$m|a-b => 10|22x-8$
Ahhoz, hogy az x-es tagon egyszerűsíteni tudjunk, meg kell néznünk, hogy mennyivel oszthatunk le mind a két oldalon, így most keressük meg 10 és 22 legnagyobb közös osztóját!
$lnko(10, 22)$: $22 = 2 * 10 + 2 => 10 = 5 * 2 + 0 => lnko(10, 22) = 2$
Most, osszunk le mindkét oldalt ezzel az értékkel:
$22x/2 \equiv 8/2 \quad (10/lnko(10, 2)) = 11x \equiv 4 \quad (5)$
$11x \equiv 4 \quad (5)$ - alakítsuk át a jobb oldalt úgy, hogy 11-gyel lehessen osztani vele! pl.: adjunk hozzá 40-et, azaz 8*5-öt:
$11x \equiv 44 \quad (5)$- ezt megtehettük, mivel ugyanazon maradékosztály eleme a 4 és a 44, mert a modulo többszörösével növeltünk! Most osszunk le 11-gyel:
$x \equiv 4 \quad (5) => (4 + k * 5|k \in \mathbb{Z})$
DE nekünk 10-es modulo osztályok kellenek, ahogy az eredeti feladatban is volt! Így nekünk fel kell bontanunk ezt az osztályt olyan 10-es modulo osztályokra, amelyek együttesen lefedik ezt a $\overline{4}$ mod 5 osztályt:
$\overline{4}$ mod 5 = (...-16,-11,-6,-1,4,9,14,19,...) $= (4 + k_1 * 10|k_1 \in \mathbb{Z}) \cup (9 + k_2 * 10|k_2 \in \mathbb{Z})$