Adatstruktúrák és Algoritmusok

4. gyakorlat

Kibővített Euklidészi algoritmus
A lineáris kongruencia egyenlet megoldása
Multiplikatív inverz fogalma

Bináris legnagyobb közös osztó algoritmus

Legyenek $a, b \in \mathbb{Z}_+ \cup \{0\}$

$$\mathrm{lnko}(a,b) = \begin{cases} a, & \text{ha } b = 0 \\ b, & \text{ha } a = 0 \\ c, & \text{egyébként,} \end{cases}$$

ahol a c szám az alábbi táblázatban van definiálva:

$a \setminus b$	*ps*	*pt*
ps	$2\mathrm{lnko}\left(\frac{a}{2}, \frac{b}{2}\right)$	$\mathrm{lnko}\left(\frac{a}{2}, b\right)$
pt	$\mathrm{lnko}\left(a, \frac{b}{2}\right)$	$\mathrm{lnko}\left(\frac{a-b}{2}, b\right)$

Feladat

A bináris közös osztó algoritmussal számoljuk ki a 90 és a 24 legnagyobb közös osztóját.

Mo.:

$$\begin{aligned}\mathrm{lnko}(90,24) &= 2\mathrm{lnko}(45,12) = 2\mathrm{lnko}(45,6) = \\ &= 2\mathrm{lnko}(45,3) = 2\mathrm{lnko}(21,3) = \\ &= 2\mathrm{lnko}(18,3) = 2\mathrm{lnko}(9,3) = \\ &= 2\mathrm{lnko}(3,3) = 2\mathrm{lnko}(0,3) = 2 \cdot 3 = 6\end{aligned}$$

A kibővített euklideszi algoritmus rekurzív változata

Két nemnegatív egész szám a és b legnagyobb közös osztóját $d^* = \mathrm{lnko}(a, b)$ módon jelöljük. A reprezentációs tétel alapján d^* előállítható az a és b számok lineáris kombinációjaként, ahol az együtthatók $\mathbb{Z}$-beliek, azaz

$$\exists(x^* \in \mathbb{Z})\exists(y^* \in \mathbb{Z}) : d^* = x^* a + y^* b.$$

A kibővített euklideszi algoritmus a d^*-ot és az x^* és $y*$ együtthatókat is szolgáltatja.

	KREUK(a,b $\|$ d^*, x^*, y^*)
INPUT	$a, b \in \mathbb{Z}_+ \cup \{0\}$
OUTPUT	$d^* \in \mathbb{Z}_+ \cup \{0\}, x^*, y^* \in \mathbb{Z} : d^* = \mathrm{lnko}(a, b)$, $d^* = x^* a + y^* b$
1.	IF $(b = 0)$
2.	THEN $d^* \longleftarrow a$
3.	$x^* \longleftarrow 1$
4.	$y^* \longleftarrow 0$
5.	ELSE KREUK $(b, a \mod b, d^*, x^*, y^*)$
6.	$\binom{x^*}{y^*} \longleftarrow \binom{y^*}{x^* - \lfloor \frac{a}{b} \rfloor y^*}$
7.	RETURN(d^*, x^*, y^*)

1. Feladat

Futtassuk a kibővített euklideszi algoritmust az $(a, b) = (133, 157)$ számpáron.
E: $(-72)133 + 61 \cdot 157 = 1$.

k	a_k	b_k	q_k	r_k	d	x_k	y_k
0	133	157	0	133	1	-72	$61 - 0 \cdot (-72) = 61$
1	157	133	1	24	1	61	$-11 - 1 \cdot 61 = -72$
2	133	24	5	13	1	-11	$6 - 5 \cdot (-11) = 61$
3	24	13	1	11	1	6	$-5 - 1 \cdot 6 = -11$
4	13	11	1	2	1	-5	$1 - 1 \cdot (-5) = 6$
5	11	2	5	1	1	1	$0 - 5 \cdot 1 = -5$
6	2	1	2	0	1	0	$1 - 2 \cdot 0 = 1$
7	1	0	-	-	1	1	0

2. Feladat

$(a, b) = (90, 24)$.
E: $(-1) \cdot 90 + 4 \cdot 24 = 6$.

k	a_k	b_k	q_k	r_k	d	x_k	y_k
0	90	24	3	18	6	-1	$1 - 3 \cdot (-1) = 4$
1	24	18	1	6	6	1	$0 - 1 \cdot 1 = -1$
2	18	6	3	0	6	0	$1 - 3 \cdot 0 = 1$
3	6	0	-	-	6	1	0

3. Feladat

$(a, b) = (628, 44)$
E: $(-19) \cdot 628 + 27 \cdot 442 = 2$.

k	a_k	b_k	q_k	r_k	d	x_k	y_k
0	628	442	1	186	2	-19	$8 - 1 \cdot (-19) = 27$
1	442	186	2	70	2	8	$-3 - 2 \cdot 8 = -19$
2	186	70	2	46	2	-3	$2 - 2 \cdot (-3) = 8$
3	70	46	1	24	2	2	$-1 - 1 \cdot 2 = -3$
4	46	24	1	22	2	-1	$1 - 1 \cdot (-1) = 2$
5	24	22	1	2	2	1	$0 - 1 \cdot 1 = -1$
6	22	2	11	0	2	0	$1 - 11 \cdot 0 = 1$
7	2	0	-	-	2	1	0

A kongruenciareláció fogalma és tulajdonságai

A kongruencia fogalma

Legyenek $a, b \in \mathbb{Z}$, $m > 1$. *Definiáljuk az* m *modulus szerinti* ***kongruencia relációt*** *az alábbi módon*

$$a \equiv b \mod (m) \qquad :\Longleftrightarrow \qquad m|b-a.$$

Megjegyzés *Könnyű látni, hogy* $a \equiv b \mod (m)$ *akkor és csak akkor, ha* a *és* b m*-mel maradékosan osztva ugyanazt a nemnegatív maradékot adja.*

Tulajdonságok

Tétel ***A kongruencia reláció tulajdonságai***

1. $a \equiv a \mod (m)$;
2. $a \equiv b \mod (m) \quad \Rightarrow \quad b \equiv a \mod (m)$;
3. $a \equiv b \mod (m)$ *és* $b \equiv c \mod (m)$, *akkor* $a \equiv c \mod (m)$.

Az 1.,2.,3., tulajdonságok azt fejezik ki, hogy rögzített m modulus esetén a kongruencia reláció egy ekvivalencia reláció $\mathbb{Z}$-n. Ennek hatására $\mathbb{Z}$ ekvivalencia osztályokra esik szét.

4. $a \equiv b \mod (m)$ és $c \equiv d \mod (m)$, akkor $(a + c) \equiv (b + d) \mod (m)$.
5. $a \equiv b \mod (m)$ és $c \equiv d \mod (m)$, akkor $ac \equiv bd \mod (m)$.

A 4.,5. tulajdonságok azt fejezik ki, hogy az ekvivalencia reláció kompatibilis a műveletekkel, így a faktorhalmazon művelet definiálható a reprezentáns elemek segítségével.

Példa

Legyen $m = 6$. *Ekkor* $\mathbb{Z}_6 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}\}$, *ahol*

$$\begin{aligned}
\underline{0} &= \{\ldots, -12, -6, 0, \ 6, 12, \ldots\} = \{0 + 6k \mid k \in \mathbb{Z}\}, \\
\underline{1} &= \{\ldots, -11, -5, 1, \ 7, 13, \ldots\} = \{1 + 6k \mid k \in \mathbb{Z}\}, \\
\underline{2} &= \{\ldots, -10, -4, 2, \ 8, 14, \ldots\} = \{2 + 6k \mid k \in \mathbb{Z}\}, \\
\underline{3} &= \{\ldots, \ -9, -3, 3, \ 9, 15, \ldots\} = \{3 + 6k \mid k \in \mathbb{Z}\}, \\
\underline{4} &= \{\ldots, \ -8, -2, 4, 10, 16, \ldots\} = \{4 + 6k \mid k \in \mathbb{Z}\}, \\
\underline{5} &= \{\ldots, \ -7, -1, 5, 11, 17, \ldots\} = \{5 + 6k \mid k \in \mathbb{Z}\}.
\end{aligned}$$

A műveletek Cayley táblázata $\mathbb{Z}_6$-ban

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Absztrakt algebrai fogalmak

Műveleti tulajdonságok

Azt mondjuk, hogy a $*$ *művelet*

- ***Kommutatív****, ha* $x * y = y * x$ *minden* $x, y \in X$ *esetén;*
- ***Asszociatív****, ha* $x * (y * z) = (x * y) * z$ *minden* $x, y, z \in X$ *esetén;*

Egységelem és elem inverze

Egy $X = (X, *)$ struktúra $e \in X$ elemét ***egységelem****nek nevezzük, ha minden $x \in X$ esetén*

$$e * x = x * e = x.$$

Ha egy struktúrának van egységeleme, akkor az egyértelműen létezik.
Legyen $X = (X, *)$ egy egységelemes struktúra (e az egységelemmel). Ha egy $x \in X$ elemhez létezik olyan $y \in X$ elem, amelyre

$$x * y = y * x = e,$$

akkor azt mondjuk, hogy az y elem az x ***elem inverze****.*
Ha az $X = (X, *)$ struktúrában a $*$ művelet asszociatív és egy $x \in X$ elemnek van inverze, akkor az egyértelműen létezik.

Félcsoport, csoport

Egy $X = (X, *)$ *struktúrát*

- ***Félcsoport****nak nevezzük, ha a* $*$ *művelet asszociatív;*
- ***Csoport****nak nevezzük, ha asszociatív, létezik egységeleme és minden elemének van inverze.*

Additív és multiplikatív írásmód

- Ha a műveletet $+$ módon jelöljük, akkor **additív írásmód**ról beszélünk.
  Additív írásmód esetén az egységelemet 0-val jelöljük és nullának, vagy zérusnak nevezzük.
  Egy x elem additív inverzét $-x$ módon jelöljük.
- Ha a műveletet $\cdot$ módon jelöljük, akkor **multiplikatív írásmód**ról beszélünk.
  Multiplikatív írásmód esetén az egységelemet 1-gyel jelöljük és egynek olvassuk.
  Egy x (zérustól különböző) elem inverzét x^{-1} módon jelöljük.

További műveleti tulajdonságok

Ha $X = X(+, \cdot)$ egy kétműveletes algebrai struktúra, akkor a azt mondjuk, hogy

- ***A szorzás az összeadásra nézve balról disztributív**, ha $x(y + z) = xy + xz$ minden $x, y, z \in X$ esetén.*
- ***A szorzás az összeadásra nézve balról disztributív**, ha $(x + y)z = xz + yz$ minden $x, y, z \in X$ esetén.*

Mivel gyakran találkozunk olyan kétműveletes struktúrákkal, amelyekben a szorzás kommutatív, így ha az egyik irányú disztributivitás teljesül, akkor a másik is, így na kettő között nem teszünk különbséget és csak annyit mondunk, hogy a szorzás disztributív az összeadásra nézve.

Gyűrű

*Egy $R = R(+, \cdot)$ kétműveletes algebrai struktúrát **gyűrű**nek nevezünk, ha rendelkezik a következő tulajdonságokkal:*

- $R(+)$ *(kommutatív) csoport;*
- $R(\cdot)$ *egy félcsoport;*
- *A szorzás az összeadásra nézve disztributív.*

Test

Egy $F = F(+, \cdot)$ kézműveletes algebrai struktúrát ***test****nek nevezzük, ha*

- *F egy kommutatív egységelemes gyűrű;*
- *F minden nemzérus elemének van multiplikatív inverze.*

A modulo m maradékosztálygyűrű

A $(\mathbb{Z}, +, \cdot)$ *(egész számok gyűrűje) egy gyűrű. Ha* $m \in \mathbb{Z}_+$, $m > 1$, *akkor* $(\mathbb{Z}_m, +, \cdot)$ *szintén gyűrű, amit* $\mod(m)$ *maradékosztály gyűrűnek nevezünk.*

Ha az m modulus reducibilis (azaz összetett szám), akkor a $\mathbb{Z}_m$ maradékosztálygyűrű nem zérusosztómentes. Például $\mathbb{Z}_6$-ban a $\underline{2}$ és a $\underline{3}$ zérusosztók.

Feladat

Keressük meg az invertálható elemek $\mathbb{Z}_6$-ban és határozzuk meg az inverzeiket.

x	0	1	2	3	4	5
x^{-1}	-	1	-	-	-	5

Két invertálható elem van, az 1 *és az* 5. $1^{-1} = 1$, $5^{-1} = 5$.

- *Általában elmondható, hogyha $\mathbb{Z}_m$ maradékosztálygyűrűben $\underline{a}$ elemnek pontosan akkor létezik multiplikatív inverze, ha* $\mathrm{lnko}(a, m) = 1$.
- *A most bevezetett multiplikatív inverz fogalma azonos a azzal a multiplikatív inverz fogalommal, amelyet a későbbiekben a lineáris kongruenciaegyenlet segítségével fogunk bevezetni.*
- *A Zh-ban ez utóbbi fogalmat kérjük. (Némileg kevesebb előkészületet igényel.)*

Tétel *Ha p prím, akkor $\mathbb{Z}_p$ test.*

A fenti tétel alkalmat ad arra, hogy véges testeket konstruáljunk. A legkisebb elemszámú test a kételemű $\{0, 1\}$ amelyben a műveletek $\mod 2$ szerint vannak definiálva.

A műveletek Cayley táblázata $\mathbb{Z}_5$-ben

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Lineáris kongruencia egyenletek

A lineáris kongruencia egyenlet

Legyenek $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}_+$ *úgy, hogy* $m > 1$. *Ekkor az*

$$ax \equiv b \mod (m) \qquad \text{(LKE)}$$

egyenletet lineáris kongruencia egyenletnek nevezzük.

A lineáris kongruencia egyenlet alaprendszere

- A lineáris kongruencia egyenletnek keressük az összes egész szám megoldását, ha egyáltalán megoldható. A megoldhatóság kritériuma viszonylag egyszerűen megoldható.
- Másrészt, ha megoldható a lineáris kongruencia egyenlet és egy z_1 egy egész megoldása, a z_2 pedig olyan, hogy $z_1 \equiv z_2 \mod (m)$, akkor z_2 is megoldás.
- Tehát elég megkeresnünk az egymással páronként modulo m inkongruens megoldásokat. Azt is előírhatjuk, hogy minden egyes ilyen megoldás nemnegatív, de $m-1$-nél kisebb vagy egyenlő legyen. Ezeket a számokat nevezzük **alaprendszernek**.
- Az alaprendszer birtokában az összes megoldást ismerjük, mivel ha találunk egy tetszőleges megoldást, akkor az az alaprendszer valamelyik tagjával lesz kongruens modulo m.

A(z) (LKE) megoldhatósága és a megoldás szerkezete

Tekintsük az $ax \equiv b \mod (m)$ *(LKE)-t.*

- ***A(z) (LKE) egyenlet megoldhatóságának a kritériuma:*** *A(z) (LKE) pontosan akkor oldható meg, ha* $\mathrm{lnko}(a, m) | b$.
- ***A megoldás szerkezete:*** *Megoldhatósága esetén a lineáris kongruencia egyenlet egy alaprendszere*

$$x_0 = x^* \cdot \frac{b}{d^*} \mod (m)$$

$$x_i = x_0 + i \cdot \frac{m}{d^*} \mod (m) \qquad (i = 1, 2, \ldots, d^* - 1),$$

ahol $d^* = \mathrm{lnko}(a, m)$ *és az* x^*, y^* *olyan egész számok, amelyekkel* $x^* a + y^* b = d^*$. *(Az* y^* *számot nem használjuk fel az alaprendszer felírásakor.)*
Ebből az is látszik, hogy az (LKE)-nek megoldhatósága esetén $d^* = \mathrm{lnko}(a, m)$ *elemű az alaprendszere.*

A multiplikatív inverz

Legyen $a \in \mathbb{Z}$, $m \in \mathbb{Z}_+$, $m > 1$ *olyanok, hogy* $\mathrm{lnko}(a, m) = 1$ *(azaz relatív prímek). Ekkor az* $ax \equiv 1 \mod (m)$ *lineáris kongruencia egyenlet modulo m egyértelműen létező megoldását az a szám m modulusra vonatkozó* ***multiplikatív inverz****ének nevezzük és* a^{-1} *módon jelöljük.*

Érdemes megjegyezni, hogy:

- *Amikor multiplikatív inverzről beszélünk, mindig meg kell mondani, hogy a multiplikatív inverz milyen modulusra vonatkozik.*
- *Multiplikatív inverz keresésekor is mindig a legkisebb pozitív egész multiplikatív inverzet keressük.*
- *Ha egy a egész szám multiplikatív inverze adott m modulusra a b pozitív egész, az azt jelenti, hogy létezik olyan k egész szám, amelyre* $ab = km + 1$.

Feladat

Oldjuk meg a $84x \equiv 16 \mod (44)$ *lineáris kongruencia egyenletet kibővített euklideszi algoritmussal.*

k	a	m	q	r	d	x^*	y^*
0	84	44	1	40	4	-1	$1 - 1 \cdot (-1) = 2$
1	44	40	1	4	4	1	$0 - 1 \cdot 1 = -1$
2	40	4	10	0	4	0	$1 - 10 \cdot 0 = 1$
3	4	0	-	-	4	1	0

Ellenőrzés: $(-1) \cdot 84 + 2 \cdot 44 = 4$.

Az alaprendszer

$$x_0 = x^* \cdot \frac{b}{d^*} = (-1) \cdot \frac{16}{4} = -4 \equiv 40 \mod (44)$$

$$x_i = x_0 + i\frac{m}{d^*} = 40 + i\frac{44}{4} = 40 + i \cdot 11 \mod (44) \quad (i = 1, 2, 3),$$

azaz $x_0 = 40$, $x_1 = 7$, $x_2 = 18$, $x_3 = 29$.

Záró megjegyzés

Tanultunk két hasonló fogalmat, a $\mathrm{mod}(\cdot,\cdot)$ *függvényt és az* $a \equiv b \mod (m)$ *relációt.*
Könnyű látni, hogy ha $a \equiv b \mod (m)$ *és* $0 \leqslant b < m$*, akkor* $\mathrm{mod}(a, m) = b$*.*

KÖSZÖNÖM A FIGYELMET!