Diszkrét matematika II. feladatok

Harmadik alkalom

Bemelegítő feladatok

1. A bővített euklideszi algoritmus segítségével oldja meg az $ax + by = (a, b)$ $(x, y \in \mathbb{Z})$ egyenletet adott a, b számok esetében

   a) $a = 13, b = 14$; b) $a = 16, b = 37$; c) $a = 90, b = -111$; d) $a = -168, b = 219$
   e) $a = 39, b = 55$; f) $a = 51, b = 91$; g) $a = 105, b = 154$; h) $a = -63, b = -70$

Megoldás: Amikor az $b > a > 0$, akkor a legelső sort (ami 0 hányadossal a-t adja maradékul) lespórolhatjuk, de akkor vigyázni kell, hogy melyik az alfák és melyik a béták oszlopa, ezért ezt most nem tesszük meg.

a)

$a = 13$	$\alpha_{-1} = 1$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_{-1} = 0$		$a = 1 \cdot a + 0 \cdot b$
$b = 14$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$		$b = 0 \cdot a + 1 \cdot b$
$r_1 = 13$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$		
$r_2 = 1$	$\alpha_2 = -1$	$q_2 = 13$	$\beta_2 = 1$	azaz	$\gcd(a, b) = a \cdot (-1) + b \cdot (1) = 1$
$r_3 = 0$	$\alpha_3 = 14$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_3 = -13$	azaz	$a \cdot (14k) + b \cdot (-13k) = 0$

Összegezve: $13 \cdot (14k - 1) + 14 \cdot (1 - 13k) = \gcd(13, 14)$, vagyis $x = 14k - 1$ és $y = 1 - 13k$.

b)

$a = 16$	$\alpha_{-1} = 1$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_{-1} = 0$		$a = 1 \cdot a + 0 \cdot b$
$b = 37$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$		$b = 0 \cdot a + 1 \cdot b$
$r_1 = 16$	$\alpha_1 = 1$	$q_1 = 2$	$\beta_1 = 0$		
$r_2 = 5$	$\alpha_2 = -2$	$q_2 = 3$	$\beta_2 = 1$		
$r_3 = 1$	$\alpha_3 = 7$	$q_3 = 5$	$\beta_3 = -3$	azaz	$\gcd(a, b) = a \cdot (7) + b \cdot (-3) = 1$
$r_4 = 0$	$\alpha_4 = -37$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_4 = 16$	azaz	$a \cdot (-37k) + b \cdot (16k) = 0$

Összegezve: $16 \cdot (7 - 37k) + 37 \cdot (16k - 3) = \gcd(16, 37)$, vagyis $x = 7 - 37k$ és $y = 16k - 3$.

c) Hogy a maradékos osztás nemnegatív számok körében fusson, a negatív b helyett a pozitív $-b$-vel írjuk fel a táblázatot (és a végén az együtthatóra visszük majd át az előjelet):

$a = 90$	$\alpha_{-1} = 1$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_{-1} = 0$	$a = 1 \cdot a + 0 \cdot (-b)$
$-b = 111$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$-b = 0 \cdot a + 1 \cdot (-b)$
$r_1 = 90$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 21$	$\alpha_2 = -1$	$q_2 = 4$	$\beta_2 = 1$	
$r_3 = 6$	$\alpha_3 = 5$	$q_3 = 3$	$\beta_3 = -4$	
$r_4 = 3$	$\alpha_4 = -16$	$q_4 = 2$	$\beta_4 = 13$	$\gcd(a, -b) = a \cdot (-16) + (-b) \cdot (13) = 3$
$r_5 = 0$	$\alpha_5 = 37$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_5 = -30$	$a \cdot (37k) + (-b) \cdot (-30k) = 0$

Tehát $\gcd(a, -b) = \gcd(a, b) = 3 = a \cdot (-16) + (-b) \cdot (13) = a \cdot (-16) + b \cdot (-13)$, továbbá $a \cdot (37k) + b \cdot (30k) = 0$. Összegezve: $90 \cdot (37k - 16) + (-111) \cdot (30k - 13) = \gcd(90, -111)$, vagyis $x = 37k - 16$ és $y = 30k - 13$.

d) Hogy a maradékos osztás nemnegatív számok körében fusson, a negatív a helyett a pozitív $-a$-val írjuk fel a táblázatot (és a végén az együtthatóra visszük majd át az előjelet):

$-a = 168$	$\alpha_{-1} = 1$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_{-1} = 0$	$-a = 1 \cdot (-a) + 0 \cdot b$
$b = 219$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$b = 0 \cdot (-a) + 1 \cdot b$
$r_1 = 168$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 51$	$\alpha_2 = -1$	$q_2 = 3$	$\beta_2 = 1$	
$r_3 = 15$	$\alpha_3 = 4$	$q_3 = 3$	$\beta_3 = -3$	
$r_4 = 6$	$\alpha_4 = -13$	$q_4 = 2$	$\beta_4 = 10$	
$r_5 = 3$	$\alpha_5 = 30$	$q_5 = 2$	$\beta_5 = -23$	$\gcd(-a, b) = (-a) \cdot (30) + b \cdot (-23) = 3$
$r_6 = 0$	$\alpha_6 = -73$	$\boxtimes\boxtimes\boxtimes\boxtimes$	$\beta_6 = 56$	$(-a) \cdot (-73k) + b \cdot (56k) = 0$

Tehát $\gcd(-a,b) = \gcd(a,b) = 3 = (-a)\cdot(30) + b\cdot(-23) = a\cdot(-30) + b\cdot(-23)$, továbbá $a\cdot(73k) + b\cdot(56k) = 0$. Összegezve $-168\cdot(73k-30) + 219\cdot(56k-23) = \gcd(-168,219)$, vagyis $x = 73k - 30$ és $y = 56k - 23$.

e)

$a = 39$	$\alpha_{-1} = 1$	⊠⊠⊠⊠	$\beta_{-1} = 0$	$a = 1\cdot a + 0\cdot b$
$b = 55$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$b = 0\cdot a + 1\cdot b$
$r_1 = 39$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 16$	$\alpha_2 = -1$	$q_2 = 2$	$\beta_2 = 1$	
$r_3 = 7$	$\alpha_3 = 3$	$q_3 = 2$	$\beta_3 = -2$	
$r_4 = 2$	$\alpha_4 = -7$	$q_4 = 3$	$\beta_4 = 5$	
$r_5 = 1$	$\alpha_5 = 24$	$q_5 = 2$	$\beta_5 = -17$	azaz $\gcd(a,b) = a\cdot(24) + b\cdot(-17) = 1$
$r_6 = 0$	$\alpha_6 = -55$	⊠⊠⊠⊠	$\beta_6 = 39$	azaz $a\cdot(-55k) + b\cdot(39k) = 0$

Összegezve: $39\cdot(24-55k)+55\cdot(39k-17) = \gcd(39,55) = 1$, vagyis $x = 24-55k$ és $y = 39k-17$.

f)

$a = 51$	$\alpha_{-1} = 1$	⊠⊠⊠⊠	$\beta_{-1} = 0$	$a = 1\cdot a + 0\cdot b$
$b = 91$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$b = 0\cdot a + 1\cdot b$
$r_1 = 51$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 40$	$\alpha_2 = -1$	$q_2 = 1$	$\beta_2 = 1$	
$r_3 = 11$	$\alpha_3 = 2$	$q_3 = 3$	$\beta_3 = -1$	
$r_4 = 7$	$\alpha_4 = -7$	$q_4 = 1$	$\beta_4 = 4$	
$r_5 = 4$	$\alpha_5 = 9$	$q_5 = 1$	$\beta_5 = -5$	
$r_6 = 3$	$\alpha_6 = -16$	$q_6 = 1$	$\beta_6 = 9$	
$r_7 = 1$	$\alpha_7 = 25$	$q_7 = 3$	$\beta_7 = -14$	azaz $\gcd(a,b) = a\cdot(25) + b\cdot(-14) = 1$
$r_8 = 0$	$\alpha_8 = -91$	⊠⊠⊠⊠	$\beta_8 = 51$	azaz $a\cdot(-91k) + b\cdot(51k) = 0$

Összegezve: $51\cdot(25-91k)+91\cdot(51k-14) = \gcd(51,91) = 1$, vagyis $x = 25-91k$ és $y = 51k-14$.

g)

$a = 105$	$\alpha_{-1} = 1$	⊠⊠⊠⊠	$\beta_{-1} = 0$	$a = 1\cdot a + 0\cdot b$
$b = 154$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$b = 0\cdot a + 1\cdot b$
$r_1 = 105$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 49$	$\alpha_2 = -1$	$q_2 = 2$	$\beta_2 = 1$	
$r_3 = 7$	$\alpha_3 = 3$	$q_3 = 7$	$\beta_3 = -2$	azaz $\gcd(a,b) = a\cdot(3) + b\cdot(-2) = 7$
$r_4 = 0$	$\alpha_4 = -22$	⊠⊠⊠⊠	$\beta_4 = 15$	azaz $a\cdot(-22k) + b\cdot(15k) = 0$

Összegezve: $105\cdot(3-22k) + 154\cdot(15k-2) = \gcd(105,154) = 7$, vagyis $x = 3-22k$ és $y = 15k-2$.

h) Hogy a maradékos osztás nemnegatív számok körében fusson, a negatív a helyett a pozitív $-a$-val és negatív b helyett pozitív $-b$-vel írjuk fel a táblázatot (és a végén az együtthatóra visszük majd át az előjelet):

$-a = 63$	$\alpha_{-1} = 1$	⊠⊠⊠⊠	$\beta_{-1} = 0$	$-a = 1\cdot(-a) + 0\cdot(-b)$
$-b = 70$	$\alpha_0 = 0$	$q_0 = 0$	$\beta_0 = 1$	$-b = 0\cdot(-a) + 1\cdot(-b)$
$r_1 = 63$	$\alpha_1 = 1$	$q_1 = 1$	$\beta_1 = 0$	
$r_2 = 7$	$\alpha_2 = -1$	$q_2 = 9$	$\beta_2 = 1$	azaz $\gcd(-a,-b) = -a\cdot(-1) + (-b)\cdot(1) = 7$
$r_3 = 0$	$\alpha_3 = 10$	⊠⊠⊠⊠	$\beta_3 = -9$	azaz $-a\cdot(10k) + (-b)\cdot(-9k) = 0$

Tehát $\gcd(-a,-b) = \gcd(a,b) = -a\cdot(-1) + (-b)\cdot(1) = a\cdot(1) + b\cdot(-1) = 7$, és $a\cdot(-10k) + b\cdot(9k) = 0$. Összegezve: $-63\cdot(1-10k) + (-70)\cdot(9k-1) = \gcd(-63,-70) = 7$, vagyis $x = 1-10k$ és $y = 9k-1$.

2. A bővített euklideszi algoritmus segítségével oldja meg az $ax + by = c$ $(x, y \in \mathbb{Z})$ egyenletet adott a, b, c számok esetében

   a) $a = 13, b = 14, c = 5$; b) $a = 16, b = 37, c = -2$; c) $a = 90, b = -111, c = 13$;
   d) $a = -168, b = 219, c = 12$; e) $a = 39, b = 102, c = 10$; f) $a = 51, b = 114, c = -9$

Megoldás: Az előző feladatban elvégzett algoritmusok eredményét felhasználjuk.

a) $13x+14y=5$. Tudjuk, hogy $\gcd(13,14)=13\cdot(-1)+14\cdot(1)=1$, és $13\cdot(14k)+14\cdot(-13k)=0$. Az első egyenlőséget 5-tel szorozva és hozzáadva a másodikat: $13\cdot(14k-5)+14\cdot(5-13k)=5$. Azaz $x=14k-5$ és $y=5-13k$.

b) $16x+37y=-2$. Mivel $16\cdot(7)+37\cdot(-3)=\gcd(16,37)=1$, és $16\cdot(-37k)+37\cdot(16k)=0$, ezért az első egyenlőséget -2-vel szorozva és hozzáadva a másodikat: $16\cdot(-14-37k)+37\cdot(16k+6)=-2$, vagyis $x=-14-37k$ és $y=16k+6$.

c) $90x-111y=13$. Tudjuk, hogy $90\cdot(-16)+(-111)\cdot(-13)=\gcd(90,-111)=3$, és mivel 3 NEM osztója 13-nak, viszont mindig osztója $90x-111y$-nak minden egész x és minden egész y esetén, ezért NINCS egész megoldás.

d) $-168x+219y=12$. Mivel $-168\cdot(-30)+219\cdot(-23)=3$, és $-168\cdot(73k)+219\cdot(56k)=0$, az első egyenlőséget 4-gyel szorozva, a másodikat hozzáadva: $-168\cdot(73k-120)+219\cdot(56k-92)=12$, vagyis $x=73k-120$ és $y=56k-92$.

e) $39x+102y=10$; Tudjuk, hogy $39x+102y$-nak minden egész x és minden egész y esetén osztója a 3, míg 10 nem osztható 3-mal, ezért NINCS egész megoldás.

f) $51x+114y=-9$, egyszerűsítsünk 3-mal: $17x+38y=-3$.

$b=38$	$\beta_{-1}=1$	$\boxtimes$	$\alpha_{-1}=0$
$a=17$	$\beta_0=0$	$q_0=2$	$\alpha_0=1$
$r_1=4$	$\beta_1=1$	$q_1=4$	$\alpha_1=-2$
$r_2=1$	$\beta_2=-4$	$q_2=4$	$\alpha_2=9$
$r_3=0$	$\beta_3=17$	$\boxtimes$	$\alpha_3=-38$

Vagyis $17\cdot(9)+38\cdot(-4)=1$, ezt -3-mal szorozva: $17\cdot(-27)+38\cdot(12)=-3$, ehhez $17\cdot(-38k)+38\cdot(17k)=0$-t hozzáadva: $17\cdot(-27-38k)+38\cdot(12+17k)=0$, vagyis $x=-27-38k$ és $y=12+17k$.

Gyakorló feladatok

3. Pajkos százlábúak futkároznak a ládában. Az egyik fajtának 14 lába van, a másiknak 20. Összesen 232 lábat számoltunk meg. Hány százlábú van a ládában?

   Megoldás: x darab húszlábú és y darab tizennégylábú állatnak összesen $20x+14y$ lába van. A feladat szerint $20x+14y=232$. Ez egy diophantoszi egyenlet azzal a plusz feltétellel, hogy a egész x és az egész y is nemnegatív.

$a=20$	$\alpha_{-1}=1$	$\boxtimes$	$\beta_{-1}=0$
$b=14$	$\alpha_0=0$	$q_0=1$	$\beta_0=1$
$r_1=6$	$\alpha_1=1$	$q_1=2$	$\beta_1=-1$
$r_2=2$	$\alpha_2=-2$	$q_2=3$	$\beta_2=3$
$r_3=0$	$\alpha_3=7$	$\boxtimes$	$\beta_3=-10$

   Vagyis $20\cdot(-2)+14\cdot(3)=2$ a legnagyobb közös osztó. Ez osztja 232-t, a hányados 116, amivel a legnagyobb közös osztót előállító lineáris kombinációt beszorozva: $20\cdot(-232)+14\cdot(348)=232$, ehhez hozzá kell adni a 0 összes lehetséges előállítását: $20\cdot(7k)+14\cdot(-10k)=0$, amiből azt kapjuk, hogy: $20\cdot(7k-232)+14\cdot(348-10k)=232$, azaz $(x=7k-232, y=348-10k)$ az általános megoldás.

   Most alkalmazzuk, hogy $x=7k-232\geq 0$ és $y=348-10k\geq 0$, vagyis $7k\geq 232$ és $348\geq 10k$, amiből $k\geq 33\frac{1}{7}$ és $34,8\geq k$, vagyis k olyan egész szám, amire $34,8\geq k\geq 33\frac{1}{7}$. Ezt csak $k=34$ elégíti ki az egészek közül, tehát $x=7\cdot 34-232=6$ és $y=348-10\cdot 34=8$.

   Tehát hat darab húszlábú és nyolc darab tizennégylábú állat futkározik a ládában.

4. A boltban a vásárlás során 100 forint a visszajáró. Hányféleképpen kaphatjuk meg a visszajárót, ha a pénztárgépben csak 20 és 50 forintosok vannak?

Megoldás: Lehet józan paraszti ésszel is megoldani, aszerinti esetszétválasztással, hogy ötvenest egyáltalán kapok-e vissza. Ha kapok legalább egy ötvenest, akkor a fennmaradó 50 forintot nem kaphatom csupa huszasokban, hiszen a 20 nem osztója az 50-nek. De ekkor a fennmaradó 50 forintot is csak egy mási ötvenessel kaphatom vissza: vagyis ebben az esetben két ötvenest kapok. Ha nem kapok vissza övenest, akkor csupa huszasokban kaptam a visszajárót. Azaz *kétféleképpen* kaphatjuk a visszajárót: vagy két ötvenes, vagy öt huszas.

Másik megoldás: Akinek ez nem jut eszébe, visszavezetheti a feladatot diophantoszi egyenletre is: x darab övenes és y darab huszas esetén $50x + 20y = 100$ forintot kell visszakapnom. Most is (a százlábús feladathoz hasonlóan) csak nemnegatív egész megoldásokat keresünk.

Mivel $50 \cdot (1) + 20 \cdot (-2) = 10$ az ötven és a húsz legnagyobb közös osztójának előállítása (ránézésre is kitalálható, de a bővített euklideszi algoritmus is ezt adná), és a tíz az a száznak osztója, ezért $50 \cdot (10) + 20 \cdot (-20) = 100$ egy partikuláris megoldás.

Mivel az öt és a kettő (50 és 20 osztva a legnagyobb közös osztójukkal) relatív prímek, belőlük a nulla csak $5\cdot(-2k)+2\cdot(5k) = 0$ módon állítható elő nemtriviálisan, ezért $50\cdot(-2k)+20\cdot(5k) = 0$ a homogén feladat általános megoldása, amit hozzá kell adni a partikuláris megoldáshoz:

$50 \cdot (10 - 2k) + 20 \cdot (5k - 20) = 100$, vagyis $x = 10 - 2k$ és $y = 5k - 20$ az általános megoldások. A plusz nemnegativitási feltételekből $10 \geq 2k$ és $5k \geq 20$ adódik, azaz $5 \geq k$ és $k \geq 4$. Tehát most *kettő különböző* megoldásunk is lesz: $k = 4$ és $k = 5$. $k = 4$ esetén $x = 2, y = 0$ és $k = 5$ esetén $x = 0, y = 5$.

Érdekes feladatok

5. Oldja meg a következő egyenleteket egész számok körében!

   a) $8^a \cdot 16^b = 32$; b) $27^a \cdot 81^b = 9$ c) $16^a \cdot 128^b = 1024$; d) $64^a \cdot 512^b = 2048$

   Megoldás: Vegyük észre, hogy minden feladaton belül ugyananak a prímnek a hatványai szerepelnek! Minden egyenletnek vehetjük ezen prím alapú logaritmusát:

   a) $(2^3)^a \cdot (2^4)^b = 2^5$, vagyis $2^{3a+4b} = 2^5$, azaz $3a + 4b = 5$.

   Ezt a diophantoszi egyenletet kell megoldani. $3 \cdot (-1) + 4 \cdot (1) = 1$, azaz $3 \cdot (-5) + 4 \cdot (5) = 5$, ehhez adódik $3\cdot(4k)+4\cdot(-3k) = 0$, tehát $3\cdot(4k-5)+4\cdot(5-3k) = 5$. $a = 4k-5$ és $b = 5-3k$ adják a megoldáspárokat minden egész k-ra.

   b) $(3^3)^a \cdot (3^4)^b = 3^2$, vagyis $3^{3a+4b} = 3^2$, azaz $3a + 4b = 2$.

   Ezt a diophantoszi egyenletet kell megoldani, használva az előző feladatban kijött első egyenletet: $3\cdot(-2)+4\cdot(2) = 2$, ehhez adódik $3\cdot(4k)+4\cdot(-3k) = 0$, tehát $3\cdot(4k-2)+4\cdot(2-3k) = 2$. $a = 4k - 2$ és $b = 2 - 3k$ adják a megoldáspárokat minden egész k-ra.

   c) $(2^4)^a \cdot (2^7)^b = 2^{10}$, vagyis $2^{4a+7b} = 2^{10}$, azaz $4a + 7b = 10$.

   Ezt a diophantoszi egyenletet kell megoldani. $4\cdot(2)+7\cdot(-1) = 1$, azaz $4\cdot(20)+7\cdot(-10) = 10$, ehhez adódik $4 \cdot (-7k) + 7 \cdot (4k) = 0$, tehát $4 \cdot (20 - 7k) + 7 \cdot (4k - 10) = 10$. $a = 20 - 7k$ és $b = 4k - 10$ adják a megoldáspárokat minden egész k-ra.

   d) $(2^6)^a \cdot (2^9)^b = 2^{11}$, vagyis $2^{6a+9b} = 2^{11}$, azaz $6a + 9b = 11$. Ennek a diophantoszi egyenletnek viszont NINCS megoldása, mert a baloldal osztható hárommal, a jobboldal viszont nem.

6. Mutassa meg, hogy

   a) $3^{3n+1}5^{2n+1} + 2^{5n+1}11^n \equiv 0 \mod 17$; b) $61^{k+1} + 11^k 7^{2k} 3^{3k} 2^{5k+3} \equiv 0 \mod 23$

   Megoldás: Egy lehetséges gondolatmenet, ha észrevesszük, hogy $11 \equiv -6 \equiv -2 \cdot 3 \pmod{17}$, ezért $11^n \equiv (-2)^n \cdot 3^n \pmod{17}$, továbbá $2^{5n+1} = 2 \cdot (2^5)^n = 2 \cdot 32^n \equiv 2 \cdot (-2)^n \pmod{17}$, ezért $2^{5n+1} \cdot 11^n \equiv 2 \cdot (-2)^n \cdot (-2)^n \cdot 3^n \equiv 2^{2n+1} \cdot 3^n \pmod{17}$, kihasználva, hogy $(-2)^n \cdot (-2)^n = (-2)^{2n} = 2^{2n}$.

$3^{3n+1} \cdot 5^{2n+1} = 3^n \cdot 3^{2n+1} \cdot 5^{2n+1} = 3^n \cdot 15^{2n+1} \equiv 3^n \cdot (-2)^{2n+1} \equiv (-1) \cdot 3^n \cdot 2^{2n+1} \pmod{17}$, kihasználva, hogy $(-2)^{2n+1} = (-1) \cdot 2^{2n+1}$.

Így $3^{3n+1} \cdot 5^{2n+1} + 2^{5n+1} \cdot 11^n \equiv (-1) \cdot 3^n \cdot 2^{2n+1} + 2^{2n+1} \cdot 3^n \equiv 0 \pmod{17}$

b) $61 \equiv -8 \pmod{23}$, ezért $61^{k+1} \equiv (-8)^{k+1} \equiv -8 \cdot (-8)^k \pmod{23}$. A másik tag végén $2^{5k+3} = 2^{5k} \cdot 2^3 = 32^k \cdot 8 \equiv 9^k \cdot 8 \pmod{23}$, azaz mindkét tagból 8-at ki tudunk emelni. Ez bíztató. $3^{3k} = 27^k \equiv 4^k \pmod{23}$, $7^{2k} = 49^k \equiv 3^k \pmod{23}$, tehát $7^{2k} \cdot 2^{5k+3} \equiv 3^k \cdot 9^k \cdot 8 \equiv 27^k \cdot 8 \equiv 4^k \cdot 8 \pmod{23}$, vagyis $7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} \equiv 4^k \cdot 4^k \cdot 8 \equiv 16^k \cdot 8 \pmod{23}$. Ami eddig megvan, abból: $61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} \equiv -8 \cdot (-8)^k + 11^k \cdot 16^k \cdot 8 \pmod{23}$.

$11 \cdot 16 = 176 = 115 + 61 \equiv 61 \equiv -8 \pmod{23}$, ezért $61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} \equiv -8 \cdot (-8)^k + (-8)^k \cdot 8 \equiv 0 \pmod{23}$.

7. Legyen $z = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$. Oldja meg a $z^{3x} = i$ egyenletet!

   Megoldás: Trigonometrikus alakban $z = 1 \cdot (\cos 45° + i \cdot \sin 45°)$, ez egy primitív 8-adik egységgyök (a 8 a legkisebb pozitív egész, ahányadik hatványa az 1). $z^2 = i$, $z^3 = i \cdot z$, $z^4 = -1$, $z^5 = -z$, $z^6 = -i$, $z^7 = -i \cdot z$, $z^8 = 1$, és innen újraindul a ciklus: $z^{k+8} = z^k$, és általában $z^k = z^n \iff k \equiv n \pmod{8}$.

   $z^{3x} = i \iff z^{3x} = z^2 \iff 3x \equiv 2 \pmod{8}$. Ezt a kongruenciát kell megoldani.

   $2 \equiv 2 + 16 \pmod{8}$, $3x \equiv 18 \pmod{8}$, a 3 relatív prím a 8-hoz, így $x \equiv 6 \pmod{8}$.

Szorgalmi feladatok

8. Bendegúz pontosan négy pint sört szeretne meginni a csütörtök esti buliban (jó a hangulat, de másnap reggel mégiscsak dimat előadás van). Sajnos csak egy 3 pintes és egy 5 pintes (mérőbeosztás nélküli) edény áll rendelkezésére, továbbá egy hordó sör. Legkevesebb hány pint sört kell engednie a hordóból, hogy pontosan a kívánt mennyiséget tudja elfogyasztani?

   Megoldás: Először megtölti a hárompintes korsót, azután annak tartalmát áttölti az ötpintesbe. Ekkor az ötpintesben még marad 2 pint üres hely. Ezután újra megtölti a hárompintes korsót, és csurig tölti belőle az ötpinteset (azaz 2 pintet áttölt.)

   Most van egy pint söre a kisebbik korsóban: azt megissza.

   Ezután az ötpintesből csurig tölti a hárompinteset (az ötpintesben 2 pint marad). Most is a kisebbik korsó tartalmár issza meg, ami most 3 pint. Ezzel összesen 4 pint sört ivott, és csak a nagyobbik korsóban maradt 2 pintet "pocsékolta" el.