Diszkrét matematika II. feladatok

Második alkalom

Bemelegítő feladatok

1. Az euklideszi algoritmussal számolja ki az alábbi számpárok legnagyobb közös osztóját, és adja meg a legkisebb közös többszörösüket is.

   a) $a = 13, b = 14$; b) $a = 16, b = 37$; c) $a = 90, b = 111$; d) $a = 168, b = 219$;
   e) $a = 180, b = 219$; f) $a = 756, b = 795$; g) $a = 1440, b = 1587$; h) $a = 3048, b = 4611$.

   Megoldás:

a)

$a = 13$	⊠⊠⊠⊠	
$b = 14$	$q_0 = 0$	
$r_1 = 13$	$q_1 = 1$	
$r_2 = 1$	$q_2 = 13$	
$r_3 = 0$	⊠⊠⊠⊠	

azaz $\gcd(13, 14) = r_2 = 1$, $\quad [13, 14] = \dfrac{13 \cdot 14}{\gcd(13, 14)} = 182$

b)

$a = 16$	⊠⊠⊠⊠	
$b = 37$	$q_0 = 0$	
$r_1 = 16$	$q_1 = 2$	
$r_2 = 5$	$q_2 = 3$	
$r_3 = 1$	$q_3 = 5$	
$r_4 = 0$	⊠⊠⊠⊠	

azaz $\gcd(16, 37) = r_3 = 1$, $\quad [16, 37] = \dfrac{16 \cdot 37}{\gcd(16, 37)} = 592$

c)

$a = 90$	⊠⊠⊠⊠	
$b = 111$	$q_0 = 0$	
$r_1 = 90$	$q_1 = 1$	
$r_2 = 21$	$q_2 = 4$	
$r_3 = 6$	$q_3 = 3$	
$r_4 = 3$	$q_4 = 2$	
$r_5 = 0$	⊠⊠⊠⊠	

azaz $\gcd(90, 111) = r_4 = 3$, $\quad [90, 111] = \dfrac{90 \cdot 111}{\gcd(90, 111)} = 3330$

d)

$a = 168$	⊠⊠⊠⊠	
$b = 219$	$q_0 = 0$	
$r_1 = 168$	$q_1 = 1$	
$r_2 = 51$	$q_2 = 3$	
$r_3 = 15$	$q_3 = 3$	
$r_4 = 6$	$q_4 = 2$	
$r_5 = 3$	$q_5 = 2$	
$r_6 = 0$	⊠⊠⊠⊠	

azaz $\gcd(168, 219) = r_5 = 3$,

$[168, 219] = \dfrac{168 \cdot 219}{\gcd(168, 219)} = 12\ 264$

e)

$a = 180$	⊠⊠⊠⊠	
$b = 219$	$q_0 = 0$	
$r_1 = 180$	$q_1 = 1$	
$r_2 = 39$	$q_2 = 4$	
$r_3 = 24$	$q_3 = 1$	
$r_4 = 15$	$q_4 = 1$	
$r_5 = 9$	$q_5 = 1$	
$r_6 = 6$	$q_6 = 1$	
$r_7 = 3$	$q_7 = 2$	
$r_8 = 0$	⊠⊠⊠⊠	

azaz $\gcd(180, 219) = r_7 = 3$,

$[180, 219] = \dfrac{180 \cdot 219}{\gcd(90, 111)} = 13\ 140$

f)

$a = 756$	⊠⊠⊠⊠	
$b = 795$	$q_0 = 0$	
$r_1 = 756$	$q_1 = 1$	
$r_2 = 39$	$q_2 = 19$	
$r_3 = 15$	$q_3 = 2$	
$r_4 = 9$	$q_4 = 1$	
$r_5 = 6$	$q_5 = 1$	
$r_6 = 3$	$q_6 = 2$	
$r_7 = 0$	⊠⊠⊠⊠	

azaz $\gcd(756, 795) = r_6 = 3$,

$$[756, 795] = \frac{756 \cdot 795}{\gcd(756, 795)} = 200\ 340$$

g)

$a = 1440$	⊠⊠⊠⊠	
$b = 1587$	$q_0 = 0$	
$r_1 = 1440$	$q_1 = 1$	
$r_2 = 147$	$q_2 = 9$	
$r_3 = 117$	$q_3 = 1$	
$r_4 = 30$	$q_4 = 3$	
$r_5 = 27$	$q_5 = 1$	
$r_6 = 3$	$q_6 = 9$	
$r_7 = 0$		

azaz $\gcd(1440, 1587) = r_7 = 3$,

$$[1440, 1587] = \frac{1440 \cdot 1587}{\gcd(1440, 1587)} = 761\ 760$$

h)

$a = 3048$	⊠⊠⊠⊠	
$b = 4611$	$q_0 = 0$	
$r_1 = 3048$	$q_1 = 1$	
$r_2 = 1563$	$q_2 = 1$	
$r_3 = 1485$	$q_1 = 1$	
$r_1 = 78$	$q_1 = 19$	
$r_1 = 3$	$q_1 = 26$	
$r_3 = 0$	⊠⊠⊠⊠	

azaz $\gcd(3048, 4611) = r_6 = 3$,

$$[3048, 4611] = \frac{3048 \cdot 4611}{\gcd(3048, 4611)} = 4\ 684\ 776$$

Gyakorló feladatok

2. Milyen $x \in \mathbb{Z}$ egészek elégítik ki a következő kongruenciákat:

   a) $x \equiv 1 \mod 3$; b) $2x \equiv 1 \mod 3$; c) $2x \equiv 1 \mod 4$; d) $2x \equiv 2 \mod 4$
   e) $x(x-2) \equiv 0 \mod 8$; f) $x^2 \equiv 1 \mod 5$; g) $x^2 \equiv 1 \mod 6$; h) $x^4 \equiv 1 \mod 5$

   Megoldás: a) $x \equiv 1 \pmod 3$, azaz $x = 3k + 1 : k \in \mathbb{Z}$

   b) $2x \equiv 1 \equiv 4 \pmod 3$. Mivel 2 relatív prím a 3-hoz, ezért egyszerűsíthetünk: $x \equiv 2 \pmod 3$, azaz $x = 3k + 2 : k \in \mathbb{Z}$

   c) $2x \equiv 1 \pmod 4$, mivel $2x$ mindig páros, nem lehet a néggyel vett osztási maradéka 1, ezért NINCS megoldás.

   Alternatív megoldás: $2x \equiv 1 \pmod 4 \iff \exists k \in \mathbb{Z} : (2x - 1) = 4k \iff \exists k \in \mathbb{Z} : 2x - 4k = 2(x - 2k) = 1$, de $2(x - 2k)$ minden egész k és minden egész x esetén páros, ami ellentmondás.)

   d) $2x \equiv 2 \pmod 4 \iff \exists k \in \mathbb{Z} : 2x - 2 = 4k \iff \exists k \in \mathbb{Z} : x - 1 = 2k$, azaz $x = 2k + 1 : k \in \mathbb{Z}$.

   Alternatív megoldás: $2x \equiv 2 \pmod 4 \iff x \equiv 1 \pmod 2$, azaz $x = 2k + 1 : k \in \mathbb{Z}$.

   e) $x(x - 2) \equiv 0 \pmod 8$, nézzünk végig egy teljes maradékrendszert modulo 8, például az $x \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ elemeket: $1 \cdot (1 - 2) = -1 \equiv 7 \pmod 8$, $2 \cdot (2 - 2) = 0 \equiv 0 \pmod 8$, $3 \cdot (3 - 2) \equiv 3 \pmod 8$, $4 \cdot (4 - 2) = 8 \equiv 0 \pmod 8$, $5 \cdot (5 - 2) = 15 \equiv 7 \pmod 8$, $6 \cdot (6 - 2) = 24 \equiv 0 \pmod 8$, $7 \cdot (7 - 2) = 35 \equiv 3 \pmod 8$, $8 \cdot (8 - 2) = 48 \equiv 0 \pmod 8$.

   Tehát $x \in \{2, 4, 6, 8\}$ számok, és nyilván az összes ezekkel modulo 8 kongruens szám elégíti ki az $x \cdot (x - 2) \equiv 0 \pmod 8$ nemlineáris kongruenciát, vagyis a páros számok.

   Alternatív megoldás: Páratlan x esetén $x-2$ is páratlan, és így nyilván $x \cdot (x-2)$ is páratlan, azaz nem lehet osztható nyolccal.

Páros $x = 2k$ esetén $x \cdot (x-2) = 2k \cdot (2k-2) = 4 \cdot k \cdot (k-1)$. Mivel két szomszédos szám közül az egyik mindig páros, ezért $k \cdot (k-1)$ szorzat páros, ennek négyszerese nyolccal is osztható.

f) $x^2 \equiv 1 \pmod 5$, nézzünk végig egy teljes maradékrendszer négyzeteit modulo 5, például az $x \in \{1,2,3,4,5\}$ elemekét: $1^2 = 1 \equiv 1 \pmod 5$, $2^2 = 4 \equiv 4 \pmod 5$, $3^2 = 9 \equiv 4 \pmod 5$, $4^2 = 16 \equiv 1 \pmod 5$, $5^2 = 25 \equiv 0 \pmod 5$. Tehát modulo 5 két inkongruens megoldás van: $x \equiv 1 \pmod 5$ és $x \equiv 4 \pmod 5$, más szavakkal $x = 5k \pm 1 : k \in \mathbb{Z}$.

g) $x^2 \equiv 1 \pmod 6$, nézzünk végig egy teljes maradékrendszer négyzeteit modulo 6, például az $x \in \{1,2,3,4,5,6\}$ elemekét: $1^2 = 1 \equiv 1 \pmod 6$, $2^2 = 4 \equiv 4 \pmod 6$, $3^2 = 9 \equiv 3 \pmod 6$, $4^2 = 16 \equiv 4 \pmod 6$, $5^2 = 25 \equiv 1 \pmod 6$, $6^2 \equiv 0 \pmod 6$.

Vagyis $x \equiv 1 \pmod 6$ és $x \equiv 5 \pmod 6$ elégíti ki a kongruenciát, azaz $x = 6k \pm 1 : k \in \mathbb{Z}$.

h) $x^4 \equiv 1 \pmod 5$, nézzünk végig egy teljes maradékrendszer négyzeteit modulo 5, például az $x \in \{1,2,3,4,5\}$ elemekét: $1^4 = 1 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$, $5^4 = 0 \equiv 0 \pmod 5$. Azaz az öttel NEM osztható számok mindegyike megoldás. (Aki ismeri az Euler-Fermat tételt vagy a "Kis" Fermat tételt, azt ez nem lepi meg.)

Érdekes feladatok

3. Legyenek $z = i$ és $w = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ komplex számok. Mely n egészekre teljesül, hogy $z^n = w^n = 1$? Válaszát indokolja!

   Megoldás: Trigonometrikus alakban $z = i = 1 \cdot (\cos 90^\circ + i \cdot \sin 90^\circ)$, tehát z egy primitív negyedik egységgyök, azaz $z^n = 1 \Longleftrightarrow n = 4k : k \in \mathbb{Z}$.

   Hasonlóan $w = \frac{1}{2} + \frac{\sqrt{3}}{2}i = 1 \cdot (\cos 60^\circ + i \cdot \sin 60^\circ)$, tehát w egy primitív hatodik egységgyök, azaz $w^n = 1 \Longleftrightarrow n = 6k : k \in \mathbb{Z}$.

   Tehát $z^n = w^n = 1$ pontosan azokra az egész n számokra teljesül, amikre egyszerre teljesül, hogy n a 4-nek is többszöröse és a 6-nak is többszöröse, vagyis a 4 és 6 közös többszöröseire. A 4 és 6 legkisebb közös többszöröse $[4,6] = 12$, azaz $z^n = w^n = 1 \Longleftrightarrow n = 12k : k \in \mathbb{Z}$.

4. Mutassa meg, hogy $(ca, cb) = c(a,b)$ ill. $(a,b) = (a-b,b)$. Az összefüggések segítségével számolja ki a $(2^{13}-1, 2^8-1)$ ill. $(2^{15}-1, 2^9-1)$ legnagyobb közös osztókat!

   Megoldás: Az első két egyenlőség volt előadáson. Ezeken felül az is szükséges a megoldáshoz, hogy $\gcd(c,b) = 1 \Longrightarrow \gcd(a \cdot c, b) = \gcd(a,b)$.

   $(2^{13}-1, 2^8-1) = (2^{13}-2^8, 2^8-1) = (2^8 \cdot (2^5-1), 2^8-1) = (2^5-1, 2^8-1) = (2^5-1, 2^8-2^5) = (2^5-1, 2^5 \cdot (2^3-1)) = (2^5-1, 2^3-1) = (2^5-2^3, 2^3-1) = (2^3 \cdot (2^2-1), 2^3-1) = (2^2-1, 2^3-1) = (4-1, 8-1) = (3,7) = 1$.

   $(2^{15}-1, 2^9-1) = (2^{15}-2^9, 2^9-1) = (2^9 \cdot (2^6-1), 2^9-1) = (2^6-1, 2^9-1) = (2^6-1, 2^9-2^6) = (2^6-1, 2^6 \cdot (2^3-1)) = (2^6-1, 2^3-1) = (2^6-2^3, 2^3-1) = (2^3 \cdot (2^3-1), 2^3-1) = (2^3-1, 2^3-1) = 2^3 - 1 = 8 - 1 = 7$.

5. Legyen $F_1 = F_2 = 1$ és $n \geq 1$ esetén $F_{n+2} = F_{n+1} + F_n$. Ekkor az F_n sorozatot *Fibonacci sorozatnak* hívjuk, első néhány eleme: 1, 1, 2, 3, 5, 8, 13,... Mutassa meg, hogy $(F_{n+1}, F_n) = 1$

   Megoldás: Teljes indukcióval. $n = 1$ esetén $(F_{n+1}, F_n) = (F_2, F_1) = (1,1) = 1$ teljesül. Tegyük fel, hogy $\forall n \leq N : (F_{n+1}, F_n) = 1$ teljesül. Ekkor $n = N+1$ esetén $(F_{n+1}, F_n) = (F_{N+2}, F_{N+1})$. Mivel a rekurzív képlet szerint $F_{N+2} = F_{N+1} + F_N$, ezért $(F_{N+2}, F_{N+1}) = (F_{N+1} + F_N, F_{N+1})$. Tehát $(F_{N+2}, F_{N+1}) = (F_N, F_{N+1}) = 1$, az utolsó egyenlőség az indukciós feltevés miatt.

Szorgalmi feladatok

9. Legyen F_n az n-edik Fibonacci-szám! Mi lesz (F_{n+2}, F_n) ill. (F_{n+3}, F_n)?

Megoldás: $(F_{n+2}, F_n) = (F_{n+1} + F_n, F_n) = (F_{n+1}, F_n) = 1$.

A másikhoz is a rekurzív képletet használjuk, csak többször egymás után: $F_{n+3} = F_{n+2} + F_{n+1} = (F_{n+1} + F_n) + F_{n+1} = 2 \cdot F_{n+1} + F_n$

$(F_{n+3}, F_n) = (2 \cdot F_{n+1} + F_n, F_n) = (2 \cdot F_{n+1}, F_n)$. Mivel F_n és F_{n+1} relatív prímek, ezért $\gcd(c, b) = 1 \Longrightarrow \gcd(a \cdot c, b) = \gcd(a, b)$ miatt $\gcd(2 \cdot F_{n+1}, F_n) = \gcd(2, F_n)$. Tehát $(F_{n+3}, F_n) = (2, F_n)$, ami vagy 1 vagy 2, F_n paritásától függően.

F_n paritása is kiszámolható a rekuzív képletből: $F_1 = F_2 = 1$, $F_3 = 1 + 1 = 2$, azaz *van* páros Fibonacci szám. Mivel a szomszédos Fibonacci számok relatív prímek, ezért ha F_n páros, akkor F_{n+1} páratlan, és $F_{n+2} = F_{n+1} + F_n$ páros és páratlan összege, tehát szintén páratlan, viszont $F_{n+3} = F_{n+2} + F_{n+1}$ két páratlan összege, azaz páros. Indukcióval tehát F_n páros pontosan akkor, ha n hárommal osztható.

$(F_{n+3}, F_n) = (2, F_n) = 1$, ha n nem osztható 3-mal, és $(F_{n+3}, F_n) = (2, F_n) = 2$, ha $n = 3k$.