Diszkrét matematika II. feladatok

Ötödik alkalom

Bemelegítő feladatok

1. Oldja meg az alábbi kongruneciákat az Euler-Fermat tétel segítségével:

   a) $2x \equiv 1 \pmod 7$; b) $3x \equiv 2 \pmod{11}$; c) $5x \equiv 3 \pmod 8$; d) $3x \equiv 2 \pmod{11}$
   e) $6x \equiv 3 \pmod{15}$; f) $14x \equiv 2 \pmod{13}$; g) $5x \equiv 3 \pmod{33}$; h) $15x \equiv 12 \pmod{42}$

   Megoldás: Az Euler-Fermat tétel szerint $a^{\varphi(m)} \equiv 1 \pmod m$, ha a és m relaív prímek, ezért ilyenkor $a^{-1} \equiv a^{\varphi(m)-1} \pmod m$ az a reciproka (multiplikatív inverze) modulo m.

   a) $2x \equiv 1 \pmod 7$; $\varphi(7) = 6$, $\gcd(2,7) = 1$, ezért $2^{-1} \equiv 2^5 \equiv 32 \equiv 4 \pmod 7$. És tényleg: $4 \cdot 2 = 8 \equiv 1 \pmod 7$.

   Tehát $4 \cdot 2x \equiv 4 \cdot 1 \pmod 7$, vagyis $x \equiv 4 \pmod 7$.

   b) $3x \equiv 2 \pmod{11}$; $\varphi(11) = 10$, $\gcd(3,11) = 1$, ezért $3^{-1} \equiv 3^9 \pmod{11}$.

   $3^3 = 27 \equiv 5 \pmod{11}$, így $3^{-1} \equiv 3^9 \equiv (3^3)^3 \equiv 5^3 \equiv 125 \equiv 4 \pmod{11}$. És tényleg: $4 \cdot 3 = 12 \equiv 1 \pmod{11}$.

   Tehát $4 \cdot 3x \equiv 4 \cdot 2 \pmod{11}$, vagyis $x \equiv 8 \pmod{11}$.

   c) $5x \equiv 3 \pmod 8$; $\varphi(8) = 4$, $\gcd(5,8) = 1$, ezért $5^{-1} \equiv 5^3 \equiv 125 \equiv 5 \pmod 8$. És tényleg: $5 \cdot 5 = 25 \equiv 1 \pmod 8$.

   Tehát $5 \cdot 5x \equiv 5 \cdot 3 \pmod 8$, vagyis $x \equiv 15 \equiv 7 \pmod 8$.

   e) $6x \equiv 3 \pmod{15}$; $\varphi(15) = 8$, de a 6 és 15 NEM relatív prímek! NEM HASZNÁLHATÓ az Euler-Fermat tétel! Először $\gcd(6,15) = 3$-mal egyszerűsíteni kell: osztani mindkét oldalt és a modulust is:

   $2x \equiv 1 \pmod 5$; $\varphi(5) = 4$, $\gcd(2,5) = 1$, ezért $2^{-1} \equiv 2^3 = 8 \equiv 3 \pmod 5$. És tényleg: $3 \cdot 2 = 6 \equiv 1 \pmod 5$.

   Tehát $3 \cdot 2x \equiv 3 \cdot 1 \pmod 5$, vagyis $x \equiv 3 \pmod 5$. De ez modulo 5 megoldás, és a feladat modulo 15 maradékosztályokként kéri a megoldásokat! $x \equiv 3 \pmod 5 \iff x = 3 + 5k : k \in \mathbb{Z}$, ami modulo 15 tekintve: $x \equiv 3 \pmod{15}$, $x \equiv 8 \pmod{15}$, $x \equiv 13 \pmod{15}$.

   f) $14x \equiv 2 \pmod{13}$; mivel $14 \equiv 1 \pmod{13}$, ezért $14x \equiv 2 \pmod{13} \iff x \equiv 2 \pmod{13}$, így itt nem is kell használni az Euler-Fermat tételt.

   g) $5x \equiv 3 \pmod{33}$; $\varphi(33) = 33 \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{11}) = 33 \cdot \frac{2}{3} \cdot \frac{10}{11} = 20$, $\gcd(5,33) = 1$, ezért $5^{-1} \equiv 5^{19} \pmod{33}$. Nem ússzuk meg a gyorshatványozást: A kitevő $19 = 16 + 2 + 1$ bináris alakja 10011.

$$\left(\left(\left((5^1)^2 \cdot 5^0\right)^2 \cdot 5^0\right)^2 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 = \left(\left(\left(25\right)^2 \cdot 5^0\right)^2 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 =$$
$$\left(\left(\left(-8\right)^2 \cdot 5^0\right)^2 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 = \left(\left(64 \cdot 5^0\right)^2 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 =$$
$$\left(\left(-2\right)^2 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 = \left(4 \cdot 5^1\right)^2 \cdot 5^1 \bmod 33 =$$
$$\left(20\right)^2 \cdot 5^1 \bmod 33 = 400 \cdot 5^1 \bmod 33 = 4 \cdot 5 \bmod 33 = 20$$

Tehát $5^{-1} \equiv 20 \pmod{33}$. És tényleg: $20 \cdot 5 \equiv 100 \equiv 99 + 1 \equiv 1 \pmod{33}$.

Ezért $20 \cdot 5x \equiv 20 \cdot 3 \pmod{33}$, azaz $100x \equiv 60 \pmod{33}$, azaz $x \equiv 27 \pmod{33}$.

h) $15x \equiv 12 \pmod{42}$; Mivel $\gcd(15, 42) = 3$, egyszerűsítés nélkül NEM HASZNÁLHATÓ az Euler-Fermat tétel! $15x \equiv 12 \pmod{42} \iff 5x \equiv 4 \pmod{14}$; $\varphi(14) = 6$, $\gcd(5, 14) = 1$, ezért $5^{-1} \equiv 5^5 \equiv 25 \cdot 25 \cdot 5 \equiv (-3) \cdot (-3) \cdot 5 \equiv 45 \equiv 3 \pmod{14}$. És tényleg: $3 \cdot 5 \equiv 1 \pmod{14}$.

Tehát $3 \cdot 5x \equiv 3 \cdot 4 \pmod{14}$, azaz $x \equiv 12 \equiv -2 \pmod{14}$, de ez még nem modulo 42 megoldás! $x \equiv -2 \pmod{14} \iff x = 14k - 2 : k \in \mathbb{Z}$, amit modulo 42 tekintve három különböző megoldás lesz: $x \equiv 12 \pmod{42}$, $x \equiv 26 \pmod{42}$, $x \equiv 40 \pmod{42}$.

2. Oldja meg az alábbi lineáris diofantikus egyenleteket kongruenciák segítségével:

   a) $27x + 35y = 3$; b) $33x + 23y = 2$; c) $33x + 15y = 6$; d) $18x + 14y = 16$.

   Megoldás:

   a) $27x + 35y = 3 \implies 27x \equiv 3 \pmod{35} \bigwedge 35y \equiv 3 \pmod{27}$; azaz $27x \equiv 3 \pmod{35}$ és $8y \equiv 3 \equiv 30 \pmod{27}$; az első egyszerűsíthető 3-mal (mert 3 relatív prím 35-höz), a második 2-vel (mert 2 relatív prím 27-hez): $9x \equiv 1 \equiv 36 \pmod{35}$ és $4y \equiv 15 \equiv -12 \pmod{27}$; az első egyszerűsíthető 9-cel (mert 9 relatív prím 35-höz), a második 4-gyel (mert 4 relatív prím 27-hez): $x \equiv 4 \pmod{35}$ és $y \equiv -3 \equiv 24 \pmod{27}$; azaz $x = 35k + 4$ és $y = 27\ell - 3$, $k, \ell \in \mathbb{Z}$.

   Kell még az ℓ és a k közötti összefüggés, hiszen a eredeti egyenletet megoldó egész számpárok kellenek megoldásként. $27 \cdot (35k + 4) + 35 \cdot (27\ell - 3) = 945 \cdot (k + \ell) + 3 = 3$. Ez akkor teljesül, ha $k = -\ell$; azaz $(x, y) = (4 - 35\ell, 27\ell - 3) : \ell \in \mathbb{Z}$.

   Megjegyzés: Ha mindkét kongruenciának a legkisebb pozitív megoldásával számoltunk volna, azaz: $x = 35k+4$ és $y = 24+27\ell$, $k, \ell \in \mathbb{Z}$, akkor $27\cdot(35k+4)+35\cdot(24+27\ell) = 945\cdot(k+\ell)+948 = 3$, ekkor $k + \ell = -1$, vagyis $k = -\ell - 1$, és így $(x, y) = (-31 - 35\ell, 27\ell + 24) : \ell \in \mathbb{Z}$.

   b) $33x + 23y = 2 \implies 33x \equiv 2 \pmod{23} \bigwedge 23y \equiv 2 \pmod{33}$; azaz $10x \equiv 2 \pmod{23}$ és $-10y \equiv 2 \pmod{33}$; kettővel lehet egyszerűsíteni: $5x \equiv 1 \equiv 70 \pmod{23}$ és $5y \equiv -1 \equiv 65 \pmod{33}$; öttel is lehet egyszerűsíteni: $x \equiv 14 \equiv -9 \pmod{23}$ és $y \equiv 13 \pmod{33}$; vagyis $x = 23k - 9$ és $y = 33\ell + 13$.

   $33 \cdot (23k - 9) + 23 \cdot (33\ell + 13) = 759 \cdot (k + \ell) + 2 = 2$, azaz $k + \ell = 0$, vagyis $\ell = -k$. $(x, y) = (23k - 9, 13 - 33k) : k \in \mathbb{Z}$.

   c) $33x + 15y = 6 \implies 33x \equiv 6 \pmod{15} \bigwedge 15y \equiv 6 \pmod{33}$; mindkét kongruencia egyszerűsíthető 3-mal (de a modulusokat is osztani kell!): $11x \equiv 2 \pmod{5}$ és $5y \equiv 2 \pmod{11}$; azaz $6x \equiv 2 \equiv 12 \pmod{5}$ és $5y \equiv 2 \equiv 35 \pmod{11}$; és mivel $\gcd(6, 5) = 1 = \gcd(5, 11)$, ezért $x \equiv 2 \equiv -3 \pmod{5}$ és $y \equiv 7 \equiv -4 \pmod{11}$. Számoljuk végig a négy lehetséges módszerrel:

   $33 \cdot (5k + 2) + 15 \cdot (11\ell + 7) = 165 \cdot (k + \ell) + 171 = 6$, ekkor $k + \ell = -1$, azaz $\ell = -k - 1$.

   $33 \cdot (5k - 3) + 15 \cdot (11\ell + 7) = 165 \cdot (k + \ell) + 6 = 6$, ekkor $k + \ell = 0$, azaz $\ell = -k$.

   $33 \cdot (5k - 3) + 15 \cdot (11\ell - 4) = 165 \cdot (k + \ell) - 159 = 6$, ekkor $k + \ell = 1$, azaz $\ell = 1 - k$.

   $33 \cdot (5k + 2) + 15 \cdot (11\ell - 4) = 165 \cdot (k + \ell) + 6 = 6$, ekkor $k + \ell = 0$, azaz $\ell = -k$.

   Bármelyiket használhatjuk, vegyük például a legutolsót: $(x, y) = (5k + 2, -4 - 11k) : k \in \mathbb{Z}$, vagy a másodikat: $(x, y) = (5k - 3, 7 - 11k) : k \in \mathbb{Z}$.

   d) $18x + 14y = 16 \implies 18x \equiv 16 \pmod{14} \bigwedge 14y \equiv 16 \pmod{18}$; azaz $4x \equiv 2 \pmod{14}$ és $-4y \equiv -2 \pmod{18}$; azaz $2x \equiv 1 \equiv 8 \pmod{7}$ és $2y \equiv 1 \equiv 10 \pmod{9}$; azaz $x \equiv 4 \pmod{7}$ és $y \equiv 5 \pmod{9}$; azaz $x = 4 + 7k$ és $y = 5 + 9\ell$, $k, \ell \in \mathbb{Z}$.

   $18 \cdot (4 + 7k) + 14 \cdot (5 + 9\ell) = 72 + 126k + 70 + 126\ell = 142 + 126 \cdot (k + \ell) = 16 \iff (k + \ell) = -1$, vagyis $\ell = -k - 1$. Tehát $x = 4 + 7k$ és $y = -9k - 4$.

   Megjegyzés: Tehát érdemes a két kongruencia közül az egyiket negatív, a másikat pozitív reprezentánselemmel megadni a további számoláshoz.

Alternatív megoldások: Mindig csak az *egyik* kongruenciát oldjuk meg a kettő közül (például azt, amelyik könnyebbnek tűnik), és annak az általános megoldását helyettesítjük vissza.

a) $27x + 35y = 3 \implies 27x \equiv 3 \pmod{35} \bigwedge 35y \equiv 3 \pmod{27}$; azaz $27x \equiv 3 \pmod{35}$ és $8y \equiv 3 \equiv 30 \equiv -24 \pmod{27}$; koncentráljunk csak a második konruenciára! $8y \equiv -24 \pmod{27}$, 8-cal egyszerűsítve: $y \equiv -3 \pmod{27}$, azaz $y = 27k - 3$.

$27x + 35 \cdot (27k - 3) = 945k - 105 = 3$, átrendezve: $27x = 108 - 945k$, azaz $x = 4 - 35k$.

b) $33x + 23y = 2 \implies 33x \equiv 2 \pmod{23} \bigwedge 23y \equiv 2 \pmod{33}$; azaz $10x \equiv 2 \pmod{23}$ és $-10y \equiv 2 \pmod{33}$; most csak az első kongruenciát oldjuk meg: $5x \equiv 1 \pmod{23}$, azaz $5x \equiv 1 \equiv 70 \pmod{23}$, azaz $x \equiv 14 \equiv -9 \pmod{23}$, azaz $x = 23k - 9$.

$33x \cdot (23k - 9) + 23y = 33 \cdot 23 \cdot k - 297 + 23y = 2$; átrendezve: $23y = -33 \cdot 23 \cdot k + 299$, azaz $y = 13 - 33k$.

c) $33x + 15y = 6 \implies 33x \equiv 6 \pmod{15} \bigwedge 15y \equiv 6 \pmod{33}$; azaz $18x \equiv 6 \pmod{15}$ és $15y \equiv 6 \pmod{33}$. Csak az első kongruenciát oldjuk meg; mivel a 6 NEM relatív prím a modulushoz, így két lépésben egyszerűsítünk: $18x \equiv 6 \pmod{15} \iff 9x \equiv 3 \pmod{15} \iff 3x \equiv 1 \pmod{5}$. $3x \equiv 1 \equiv 6 \pmod{5} \iff x \equiv 2 \pmod{5} \iff x = 5k + 2$.

$33 \cdot (5k + 2) + 15y = 165k + 66 + 15y = 6$, átrendezve: $15y = -165k - 60$, azaz $y = -11k - 4$.

d) $18x + 14y = 16 \implies 18x \equiv 16 \pmod{14} \bigwedge 14y \equiv 16 \pmod{18}$; azaz $4x \equiv 2 \pmod{14}$ és $-4y \equiv -2 \pmod{18}$; csak az első kongruenciát oldjuk meg: $4x \equiv 2 \pmod{14} \iff 2x \equiv 1 \equiv 8 \pmod{7} \iff x \equiv 4 \pmod{7} \iff x = 7k + 4$.

$18 \cdot (7k + 4) + 14y = 126k + 72 + 14y = 16$, átrendezve: $14y = -56 - 126k$, azaz $y = -4 - 9k$.

3. a) Számolja ki a 4 ill. 5 hatványait modulo 7! b) Ellenőrizze, hogy 4 ill. 5 generátor-e modulo 7! c) Legyen g egy generátor modulo 7, és adja meg a $\log_g(6)$ értékét!

   Megoldás: $4^2 = 16 \equiv 2 \pmod{7}$, $4^3 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$, $4^4 \equiv 1 \cdot 4 \pmod{7}$, $4^5 = 4^3 \cdot 4^2 \equiv 2 \pmod{7}$, $4^6 = (4^3)^2 \equiv 1 \pmod{7}$; tehát a 4 NEM generátor modulo 7, mert hatványaiként nem áll elő minden redukált maradékosztály ($3 < 6 = \varphi(7)$, de már $4^3 = 64 \equiv 1 \mod 7$).

   $5^2 = 25 \equiv 4 \pmod{7}$, $5^3 = 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6 \pmod{7}$, $5^4 = 5^3 \cdot 5 \equiv 6 \cdot 5 \equiv 30 \equiv 2 \pmod{7}$, $5^5 = 5^4 \cdot 5 \equiv 2 \cdot 5 \equiv 10 \equiv 3 \pmod{7}$, $5^6 = 5^5 \cdot 5 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$; tehát az 5 viszont generátor modulo 7, mert hatványaiként előáll minden redukált maradékosztály ($n = \varphi(7) = 6$ a legkisebb pozitív egész kitevő, amire $5^n \equiv 1 \mod 7$).

   $n = \log_g(6)$ az az $0 < n < 7$ kitevő, amire $g^n \equiv 6 \equiv -1 \pmod{7}$. Azt az Euler-Fermat tételből tudjuk, hogy $g^6 \equiv 1 \pmod{7}$. Ha g primitív elem (generátor) modulo 7, akkor az is igaz, hogy $0 < n < 6 \implies g^n \not\equiv 1 \pmod{7}$, sőt, mivel $g^n \equiv g^{n \bmod 6} \pmod{7}$, ezért az is igaz, hogy $6 \nmid n \implies g^n \not\equiv 1 \pmod{7}$. Mivel $g^{2n} \equiv (g^n)^2 \equiv 6^2 \equiv 36 \equiv 1 \pmod{7}$, ezért a fentiek szerint $6 \mid 2n$, vagyis $0 < 2n = 6k < 14 : k \in \mathbb{Z}$. Tehát $0 < n = 3k < 7 : k \in \mathbb{Z}$, azaz $n = 3$.

   Megjegyzés: Általában is igaz, hogy ha p páratlan prím, és $g \in \mathbb{Z}_p$ primitív elem (más szóval g generátor modulo p), akkor $g^{\frac{p-1}{2}} \equiv -1 \equiv p - 1 \pmod{p}$, és így $\log_g(p-1) = \frac{p-1}{2}$. Ennek belátására a fenti $p = 7$ speciális esetre vonatkozó gondolatmenet általánosítható.

Gyakorló feladatok

4. Igazolja, hogy $g = 2$ generátor modulo 11. Számolja ki továbbá a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!

   a) $\log_2(2)$; b) $\log_2(4)$; c) $\log_2(5)$; d) $\log_2(10)$ e) $\log_2(9)$; f) $\log_2(7)$

   Megoldás: $2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^4 \equiv 16 \equiv 5 \pmod{11}$, $2^5 \equiv 2 \cdot 2^4 \equiv 2 \cdot 5 \equiv 10 \pmod{11}$, $2^6 \equiv 2 \cdot 2^5 \equiv 2 \cdot 10 \equiv 20 \equiv 9 \pmod{11}$, $2^7 \equiv 2 \cdot 2^6 \equiv 2 \cdot 9 \equiv 18 \equiv 7 \pmod{11}$, $2^8 \equiv 2 \cdot 2^7 \equiv 2 \cdot 7 \equiv 14 \equiv 3 \pmod{11}$, $2^9 \equiv 2 \cdot 2^8 \equiv 2 \cdot 3 \equiv 6 \pmod{11}$, $2^{10} \equiv 2 \cdot 2^9 \equiv 2 \cdot 6 \equiv 12 \equiv 1 \pmod{11}$; tehát a 2 által reprezentált maradékosztály hatványaiként

az összes modulo 11 redukált maradékosztály (mind a tíz) előáll, mert $n = \varphi(11) = 10$ a legkisebb olyan pozitív egész n kitevő, amire $2^n \equiv 1 \pmod{11}$. Ez pont azt jelenti, hogy a 2 generátor modulo 11.

a) $\log_2(2) = 1$; hiszen $\log_g(g) = 1$. És tényleg: $2^1 \equiv 2 \pmod{11}$.

b) $\log_2(4) = \log_2(2^2) = 2$; hiszen $\log_g(a^n) \equiv n \cdot \log_g(a) \pmod{p-1}$ általában $g \in \mathbb{Z}_p$ generátor esetén ($p - 1 = \varphi(p)$, hiszen p prím). És tényleg: $2^2 \equiv 4 \pmod{11}$.

c) $\log_2(5) = \log_2(16) = \log_2(2^4) = 4$; hiszen $16 \equiv 5 \pmod{11}$, és a logaritmusazonosság itt is használható. És tényleg: $2^4 \equiv 16 \equiv 5 \pmod{11}$.

d) $\log_2(10) = \log_2(-1) = \dfrac{\varphi(11)}{2} = \dfrac{10}{2} = 5$ az előző feladat szerint (hiszen $10 \equiv -1 \mod 11$). És tényleg: $2^5 \equiv 32 \equiv 10 \pmod{11}$.

De ha nem vettük volna észre, hogy $10 \equiv -1 \pmod{11}$, akkor is $10 = 2 \cdot 5$, és így $\log_2(10) = \log_2(2 \cdot 5) \equiv \log_2(2) + \log_2(5) \equiv 1 + 4 \equiv 5 \pmod{10}$, használva a másik logaritusazonosságot, ami szerint $\log_g(a \cdot b) \equiv \log_g(a) + \log_g(b) \pmod{p-1}$.

e) Mivel $9 \equiv 20 \pmod{11}$, ezért $\log_2(9) \equiv \log_2(20) \equiv \log_2(4 \cdot 5) \equiv \log_2(4) + \log_2(5) \equiv 2 + 4 \equiv 6 \pmod{10}$; tehát $\log_2(9) = 6$. És tényleg: $2^6 = 64 = 55 + 9 \equiv 9 \pmod{11}$.

f) Mivel $7 \equiv 18 \pmod{11}$, ezért $\log_2(7) = \log_2(18) = \log_2(2 \cdot 9) \equiv \log_2(2) + \log_2(9) \equiv 1 + 6 \equiv 7 \pmod{10}$; tehát $\log_2(7) = 7$. És tényleg: $2^7 = 128 = 121 + 7 \equiv 7 \pmod{11}$.

5. A Diffie-Hellman kulcscsere protokollnál legyen $p = 11$ és $g = 2$. Legyen Alice *titkos* kulcsa $a = 3$ és Bob *titkos* kulcsa $b = 4$. Mi lesz a közös kulcsuk?

   Megoldás: A közös kulcsuk $g^{a \cdot b} \equiv 2^{3 \cdot 4} \equiv 2^{12} \equiv 2^{12 \bmod 10} \equiv 2^2 \equiv 4 \pmod{11}$.

6. A Diffie-Hellman kulcscsere protokollnál legyen $p = 13$ és $g = 2$. Legyen Alice *nyilvános* kulcsa 7 és Bob *titkos* kulcsa $b = 4$. Mi lesz a közös kulcsuk?

   Megoldás: A közös kulcsuk $(g^a)^b = 7^4 \equiv 49^2 \equiv (-3)^2 \equiv 9 \pmod{13}$.

Érdekes feladatok

7. Felhasználva, hogy $g = 2$ generátor modulo 13, számolja ki a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!

   a) $\log_2(2)$; b) $\log_2(4)$; c) $\log_2(3)$; d) $\log_2(6)$ e) $\log_2(5)$; f) $\log_2(10)$

   Megoldás: a) $\log_2(2) = 1$; És tényleg: $2^1 = 2$.

   b) $\log_2(4) = \log_2(2^2) = 2$; És tényleg: $2^2 = 4$.

   c) $\log_2(3) = \log_2(3 + 13) = \log_2(16) = \log_2(2^4) = 4$; És tényleg: $2^4 = 16 \equiv 3 \pmod{13}$.

   d) $\log_2(6) = \log_2(3 \cdot 2) \equiv \log_2(3) + \log_2(2) \equiv 4 + 1 \equiv 5 \pmod{12}$, tehát $\log_2(6) = 5$.

   És tényleg: $2^5 = 32 \equiv 6 \pmod{13}$.

   e) $\log_2(5) = \log_2(5 + 13) = \log_2(18) = \log_2(2 \cdot 3^2) \equiv \log_2(2) + 2 \cdot \log_2(3) \equiv 1 + 2 \cdot 4 \equiv 9 \pmod{12}$; tehát $\log_2(5) = 9$.

   És tényleg: $2^9 = 512 = 39 \cdot 13 + 5 \equiv 5 \pmod{13}$.

   f) $\log_2(10) \equiv \log_2(2) + \log_2(5) \equiv 1 + 9 \equiv 10 \pmod{13}$, azaz $\log_2(10) = 10$.

   És tényleg: $2^{10} = 1024 = 78 \cdot 13 + 10 \equiv 10 \pmod{13}$.

8. A Diffie-Hellman kulcscsere protokollnál legyen $p = 17$ és $g = 3$. Legyen Alice *nyilvános* kulcsa 7 és Bob *nyilvános* kulcsa 8. Mi lehet a közös kulcsuk?

   Megoldás: Ez elvileg egy *nagyon nehéz* feladat lenne (hiszen ettől titkosítás a titkosítás), de ilyen kis számok esetén persze még nyers erővel is megoldható.

Egy ötlet: elkezdjük hatványozni g-t modulo p, és ha vagy Alíz vagy Bob nyilvános kulcsát megkapjuk, azzal már meg is tudtuk az egyik titkos kulcsot.

Érdemes keresni Alíz és Bob nyilvános kulcsának másik modulo 17 reprezentánselemét is, ami például négyzetszám vagy köbszám. $g^a = 7 \equiv 24 \pmod{17}$ ez nem négyzetszm és nem is köbszám, de $g^b = 8 \equiv 25 \equiv 5^2 \pmod{17}$, azaz ha az 5-öt sikerül $g = 3$ hatványaként előállítani, akkor is megállhatunk.

$3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 10 \equiv -7 \pmod{17}$, $3^4 \equiv 3 \cdot 3^3 \equiv 30 \equiv 13 \equiv -4 \pmod{17}$, $3^5 \equiv 3 \cdot 3^4 \equiv 3 \cdot 13 \equiv 39 \equiv 5 \pmod{17}$, itt megállhatunk! $(3^5)^2 \equiv 5^2 \equiv 25 \equiv 8 \equiv g^b \pmod{17}$, azaz $b = 5 \cdot 2 = 10$ Bob titkos kulcsa! Ebből és Alíz nyilvános kulcsából ugyanúgy határozzuk meg a közös kulcsot, ahogy Bob is teszi.

A közös kulcs $(g^a)^b \equiv 7^{10} \equiv (7^2)^5 \equiv (49)^5 \equiv (-2)^5 \equiv -32 \equiv -32 + 34 \equiv 2 \pmod{17}$.

Szorgalmi feladatok

9. Emlékeztető Dimat1-ből: „*Egy hotelba 100 fős társaság érkezik, akik közül kezdetben bármely két ember jóban van egymással. Esténként egyetlen nagy kerek asztal köré ül le mindenki. Sajnos egy vacsora alatt az egymás mellé került emberek örökre összevesznek egymással. A társaság minden vacsora előtt úgy ül le, hogy a szomszédjaival jóban legyen. Ha ez lehetetlen, akkor minden résztvevő aznap este hazamegy. Ekkor legalább 25 éjszakát a hotelben tölt a társaság!*" Feladat: mutsson módszert (ülésrendet), hogy hogyan tud a társaság $\varphi(100)/2 = 20$ éjszakát ott eltölteni.

   Megoldás: Legyen $1 \leq d \leq 99$ egy rögzített differencia, és tekintsük a $0 + k \cdot d \bmod 100 : k = 1 \dots 100$ számtani sorozatot $\mathbb{Z}_{100}$ maradékosztálygyűrűben. Ennek a sorozatnak pontosan akkor lesz száz különböző eleme, ha a d differencia relatív prím a 100-hoz.

   Egy ilyen sorozat felsorolja a gráf pontjait (ha a V csúcshalmazt megfeleltetjük a $\{0, 1, \dots, 99\}$ teljes maradékrendszernek), és ebben a sorrendben megad egy Hamilton-kört (a pontok közötti éleket értelemszerűen felsorolva), ha $\gcd(d, 100) = 1$. Viszont d és $100-d$ *ugyanazt* a Hamilton-kört adja meg, csak fordított sorrendben.

   De bármely *két különböző* ilyen Hamilton-körnek biztosan nincs közös éle, mert a gráf élei megcímkézhetők az általuk összekötött pontok sorszámainak különbségével (a nagyobb sorszámból a kisebbet vonjuk ki), és egy ilyen számtani sorozattal meghatározott Hamilton-körben minden él a d vagy a $100 - d$ címkével van megcímkézve.

   Ilyen módon találunk annyi éldiszjunkt Hamilton-kört, amennyi a 100-hoz relatív prímek száma 1-től 100-ig, de mindegyiket duplán kapjuk meg, azaz $\varphi(100)/2 = 20$ darab éldiszjunkt Hamilton-kör találunk így.

   Ez *gyengébb* eredmény, mint amit Dimat1-ben bizonyítottunk Dirac-tétellel, hiszent ott 25 Hamilton-kört találtunk.

   De ugyanezzel a módszerrel egy 101 csúcsú gráfban a Dimat1-beli módszerrel továbbra is csak 25 éldiszjunkt Hamilton-kört találnánk, ezzel a módszerrel viszont $\varphi(101)/2 = 50$-et.