Diszkrét matematika II. feladatok

Hatodik alkalom

Gyakorló feladatok

1. Az RSA titkosításnál legyen $p = 11$, $q = 13$ és $e = 7$. a) Mi lesz d? b) Az $m = 4$ üzenetet szeretnénk titkosítani, mi lesz a titkosított üzenet?

   Megoldás: A nyilvános modulus $n = p \cdot q = 11 \cdot 13 = 143$, a redukált maradékosztályok száma $\varphi(n) = \varphi(143) = (p-1) \cdot (q-1) = 10 \cdot 12 = 120$, és és azt a kongruenciát kell megoldani, ami szerint $e \cdot d \equiv 1 \mod \varphi(n)$, vagyis $7 \cdot d \equiv 1 \pmod{120}$.

   Bővített euklideszi algoritmussal (vagy annak észrevételével, hogy $7 \cdot 17 = 119$) kijön, hogy $120 \cdot (1) + 7 \cdot (-17) = 1$. Ebből tehát: $7 \cdot (-17) \equiv 1 \pmod{120}$, azaz $d \equiv -17 \pmod{120}$, tehát $d = 103$, mivel ez a legkisebb pozitív egész eleme a megoldásként kijött maradékosztálynak.

   b) Az $c = m^e = 4^7 \bmod 143$ érték lesz a titkosított üzenet. $4^7 = (4^2 \cdot 4)^2 \cdot 4 = (16 \cdot 4)^2 \cdot 4 = 64^2 \cdot 4 = 4096 \cdot 4 \equiv 92 \cdot 4 \equiv 184 \cdot 2 \equiv 41 \cdot 2 \equiv 82 \pmod{143}$. Tehát $c = 82$ a titkosított üzenet.

2. Az RSA titkosításnál legyen $p = 7$, $q = 13$ és $e = 5$. A $c = 2$ titkosított üzenetet kaptuk. Mi az eredeti üzenet?

   Megoldás: A nyilvános modulus $n = p \cdot q = 7 \cdot 13 = 91$, a redukált maradékosztályok száma $\varphi(n) = \varphi(91) = (p-1) \cdot (q-1) = 6 \cdot 12 = 72$, és és azt a kongruenciát kell megoldani, ami szerint $e \cdot d \equiv 1 \mod \varphi(n)$, vagyis $5 \cdot d \equiv 1 \pmod{72}$.

   Bővített euklideszi algoritmussal (vagy annak észrevételével, hogy $5 \cdot 29 = 145$ és $72 \cdot 2 = 144$) kijön, hogy $72 \cdot (-2) + 5 \cdot (29) = 1$. Ebből tehát: $5 \cdot 29 \equiv 1 \pmod{72}$, azaz $d \equiv 29 \pmod{72}$, tehát $d = 29$, mivel ez a legkisebb pozitív egész eleme a megoldásként kijött maradékosztálynak.

   Mivel $c = m^e \bmod n$, ezért $c^d = (m^e)^d = m^{e \cdot d} \equiv m^1 \pmod{n}$, tehát $m = c^d \bmod n$, tehát $m = 2^{29} \bmod 91$ az eredeti üzenet. $2^{29} = 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2$, a kitevő bináris alakja tehát 11101, gyorshatványozással:

$$2^{29} = \left(\left(\left(\left(2^1\right)^2 \cdot 2^1 \right)^2 \cdot 2^1 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv \left(\left(\left(4 \cdot 2^1 \right)^2 \cdot 2^1 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv$$

$$\equiv \left(\left(\left(8 \right)^2 \cdot 2^1 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv \left(\left(64 \cdot 2^1 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv \left(\left(128 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv$$

$$\equiv \left(\left(37 \right)^2 \cdot 2^0 \right)^2 \cdot 2^1 \equiv \left(1369 \right)^2 \cdot 2^1 \equiv \left(-4 \right)^2 \cdot 2^1 \equiv 16 \cdot 2^1 \equiv 32 \pmod{91}$$

   Tehát $m = 32$ az eredeti üzenet.

Érdekes feladatok

3. Az RSA titkosításnál legyen $n = 221$ és $e = 5$. A $c = 2$ titkosított üzenetet hallgattuk le. Mi lehet az eredeti üzenet?

   Megoldás: Ha sikerül faktorizálni a nyilvános modulust, akkor könnyű dolgunk van: $n = 221 = 13 \cdot 17 = p \cdot q$, tehát $p = 13$, $q = 17$, és így $\varphi(n) = (p-1) \cdot (q-1) = 12 \cdot 16 = 192$.

$$e \cdot d \equiv 1 \mod \varphi(n), \text{ azaz } 5 \cdot d \equiv 1 \mod 192 \iff \begin{cases} 5 \cdot d \equiv 1 \mod 3 \iff 2d \equiv 4 \mod 3 \\ 5 \cdot d \equiv 1 \mod 64 \iff 5d \equiv 65 \mod 64 \end{cases}$$

   tehát $d \equiv 2 \equiv 77 \pmod{3}$ és $d \equiv 13 \equiv 77 \pmod{64}$, azaz $d = 77$.

(Vagy úgy is kijön, hogy $5 \cdot d \equiv 1 \equiv 192+192+1 \equiv 385 \mod 192$, $d \equiv 77 \mod 192$.)

Tehát $m = 2^{77} \bmod 221$ értéket kell kiszámolnunk:

$$\begin{aligned}2^{77} =& 2^{64+8+4+1} = \left(2^8\right)^8 \cdot 2^8 \cdot 2^4 \cdot 2 = \left(\left(\left(2^8 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 = \left(\left(\left(512\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \\ \equiv& \left(\left(\left(70\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(9800\right)^2\right)^2 \cdot 2 \equiv \left(\left(76\right)^2\right)^2 \cdot 2 \equiv \left(5776\right)^2 \cdot 2 \equiv \\ \equiv& \left(30\right)^2 \cdot 2 \equiv 900 \cdot 2 \equiv 16 \cdot 2 \equiv 32 \pmod{221}\end{aligned}$$

Megjegyzés: Ha ismerjük a modulus prímfelbontását, akkor a gyorshatvánmyozást is gyorsíthatjuk azzal, hogy külön $p = 13$ és külön $q = 17$ modulusok szerint gyorshatványozunk:

$$\begin{aligned}2^{77} =& 2^{64+8+4+1} = \left(2^8\right)^8 \cdot 2^8 \cdot 2^4 \cdot 2 = \left(\left(\left(2^8 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 = \left(\left(\left(\left(\left(2^2\right)^2\right)^2 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \\ \equiv& \left(\left(\left(\left(16\right)^2 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(\left(\left(3\right)^2 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(\left(18\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \\ \equiv& \left(\left(\left(5\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(25 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(-1 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(4\right)^2 \cdot 2 \equiv 16 \cdot 2 \equiv \\ \equiv& 3 \cdot 2 \equiv 6 \pmod{13} \\ 2^{77} \equiv& \left(\left(\left(\left(16\right)^2 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(\left(\left(-1\right)^2 \cdot 2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(\left(2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \\ \equiv& \left(\left(4 \cdot 2\right)^2\right)^2 \cdot 2 \equiv \left(\left(8\right)^2\right)^2 \cdot 2 \equiv \left(64\right)^2 \cdot 2 \equiv \\ \equiv& \left(-4\right)^2 \cdot 2 \equiv 16 \cdot 2 \equiv -1 \cdot 2 \equiv 15 \pmod{17} \qquad \text{Tehát } \begin{cases} m \equiv \ \ 6 \equiv 26 + \ \ 6 & \bmod 13 \\ m \equiv 15 \equiv 17 + 15 & \bmod 17 \end{cases}\end{aligned}$$

És a kínai maradéktétellel kijön az $m \equiv 32 \pmod{13 \cdot 17}$ megoldás.

Vegyes gyakorló feladatok

4. Számolja ki a $(3^{13}-1, 3^8-1)$ ill. $(3^{15}-1, 3^9-1)$ legnagyobb közös osztókat!

Megoldás: $(3^{13}-1, 3^8-1) = (3^{13}-3^8, 3^8-1) = (3^8(3^5-1), 3^8-1) = (3^5-1, 3^8-1) = (3^5-1, 3^8-3^5) = (3^5-1, 3^5(3^3-1)) = (3^5-1, 3^3-1) = (3^5-3^3, 3^3-1) = (3^3(3^2-1), 3^3-1) = (3^2-1, 3^3-1) = (3^2-1, 3^3-3^2) = (3^2-1, 3^2(3-1)) = (3^2-1, 3-1) = (3^2-3, 3-1) = (3(3-1), 3-1) = (3-1, 3-1) = 3-1 = 2$. Illetve:

$(3^{15}-1, 3^9-1) = (3^{15}-3^9, 3^9-1) = (3^9(3^6-1), 3^9-1) = (3^6-1, 3^9-1) = (3^6-1, 3^9-3^6) = (3^6-1, 3^6(3^3-1)) = (3^6-1, 3^3-1) = (3^6-3^3, 3^3-1) = (3^3(3^3-1), 3^3-1) = (3^3-1, 3^3-1) = 3^3-1 = 27-1 = 26$.

Alternatív megoldás: Az euklideszi algoritmust is alkalmazhatjuk, a következő maradékos osztásokat elvégezve: $3^a-1 = 3^{a-b} \cdot (3^b-1) + 3^{a-b}-1$, azaz $3^a-1 \bmod (3^b-1) = 3^{a-b}-1$, ezért $(3^a-1, 3^b-1) = (3^a-1 \bmod (3^b-1), 3^b-1) = (3^{a-b}-1, 3^b-1)$. Tehát:

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

Hasonlóan: $(3^{15}-1, 3^9-1) = (3^{15-9}-1, 3^9-1) = (3^6-1, 3^9-1) = (3^6-1, 3^{9-6}-1) = (3^6-1, 3^3-1) = (3^{6-3}-1, 3^3-1) = (3^3-1, 3^3-1) = 3^3-1 = 27-1 = 26$.

Megjegyzés: Ha $(3^{13}+1, 3^8-1)$ ill. $(3^{15}-1, 3^9+1)$ lett volna a feladat, akkor is hasonló a módszer. A módszer hasonló, az eredmény nem olyan szép (nincs köze a kitevők legnagyobb közös osztójához):

$(3^{13}+1, 3^8-1) = (3^{13}+3^8, 3^8-1) = (3^8(3^5+1), 3^8-1) = (3^5+1, 3^8-1) = (3^5+1, 3^8+3^5) = (3^5+1, 3^5(3^3+1)) = (3^5+1, 3^3+1) = (3^5-3^3, 3^3+1) = (3^3(3^2-1), 3^3+1) = (3^2-1, 3^3+1) = (3^2-1, 3^3+3^2) = (3^2-1, 3^2(3+1)) = (3^2-1, 3+1) = (3^2+3, 3+1) = (3(3+1), 3+1) = (3+1, 3+1) = 3+1 = 4$. Illetve:

$(3^{15}-1, 3^9+1) = (3^{15}+3^9, 3^9+1) = (3^9(3^6+1), 3^9+1) = (3^6+1, 3^9+1) = (3^6+1, 3^9-3^6) = (3^6+1, 3^6(3^3-1)) = (3^6+1, 3^3-1) = (3^6+3^3, 3^3-1) = (3^3(3^3+1), 3^3-1) = (3^3+1, 3^3-1) = (3^3+3^3, 3^3-1) = (2\cdot 3^3, 3^3-1) = (2, 3^3-1) = (2, 26) = 2$.

És, mint a fenti megoldások során elő is fordult részletszámításnál, akkor is hasonló a módszer, ha mindkét oldalon plusz egy van.

Ahol a megoldási módszer azonos a korábbi feladatsorokon már ismertetett módszerrel, ott egyes esetekben csak az eredményt közöljük, hogy ellenőrizhessed magadat.

5. Oldja meg az $ax + by = c$ $(x, y \in \mathbb{Z})$ egyenletet adott a, b, c számok esetében

   a) $a = 27, b = 14, c = 5$;   b) $a = 105, b = 40, c = 15$;   c) $a = 115, b = -50, c = 10$;
   d) $a = -135, b = 70, c = 12$;   e) $a = 117, b = -90, c = -6$;   f) $a = 78, b = 93, c = -10$

   Megoldások: Kétféle módszerünk is van: a bővített euklieszialgoritmus, és a kongruenciákra visszavezeés (ha azokat meg tudjuk oldani máshogy, mint bővített euklideszi algoritmussal). Bármelyiket bármelyikkel meg lehet oldani.

   a) $27x+14y = 5$; például bővített euklideszi algoritmussal: $\gcd(27, 14) = 27\cdot(-1)+14\cdot(2) = 1$. Így $27\cdot(-5) + 14\cdot(10) = 5$, így $27\cdot(14k-5) + 14\cdot(10-27k) = 5$, tehát $x = 14k-5$ és $y = 10-27k$.

   b) $105x + 40y = 15 \iff 21x - 8y = 3$; például kongruenciákkal: $21x \equiv 3 \pmod 8$, azaz $-3x \equiv 3 \pmod 8$, vagyis $x \equiv -1 \pmod 8$. Tehát $x = 8k-1$, ezért $21\cdot(8k-1) + 8y = 3$; átrendezve: $8y = 24 - 8\cdot 21k$, azaz $y = 3 - 21k$.

   c) $115x - 50y = 10 \iff 23x - 10y = 2$, ebből: $23x \equiv 2 \pmod{10}$, azaz $3x \equiv 12 \pmod{10}$, azaz $x \equiv 4 \pmod{10}$, tehát $x = 4 - 10k$.

   $23\cdot(4-10k) - 10y = 2$, azaz $10y = 90 - 230k$, vagyis $y = 9 - 23k$.

   d) $-135x + 70y = 12$; de mivel -135 és 70 is osztható öttel, míg 12 nem osztható öttel, ezért nem létezhet az egészek körében $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ megoldáspár.

   e) $117x - 90y = -6$; de mivel 117 és -90 is osztható kilenccel, míg -6 nem osztható kilenccel, ezért nem létezhet az egészek körében $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ megoldáspár.

   f) $78x+93y = -10$; de mivel 78 és 93 is osztható hárommal, míg -10 nem osztható hárommal, ezért nem létezhet az egészek körében $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ megoldáspár.

6. Pajkos százlábúak futkároznak a ládában. Az egyik fajtának 12 lába van, a másiknak 23. Összesen 152 lábat számoltunk meg. Hány százlábú van a ládában?

   Eredmény: $23x + 12y = 152$ diofantikus egyenlet nemnegatív megoldásai kellenek.

   $x = 4, y = 5$ az egyelen olyan megoldáspár, aminek mindkét koordinátája nemnegatív.

7. A boltban a vásárlás során 150 forint a visszajáró. Hányféleképpen kaphatjuk meg a visszajárót, ha a pénztárgépben csak 20 és 50 forintosok vannak?

Eredmény: Kétféleképpen; vagy három ötvenest kapunk, vagy öt huszast és egy ötvenest.

8. Oldja meg a következő egyenleteket egész számok körében!

a) $27^a \cdot 81^b = 1/9$; b) $32^a \cdot 128^b = 16$ c) $i^a \cdot \left(\frac{1+i}{\sqrt{2}}\right)^b = -i$.

Megoldás: a) $3^{3a} \cdot 3^{4b} = 3^{-2} \iff 3a + 4b = -2$; mivel $3 \cdot (1) + 4 \cdot (-1) = -1$, ezért $3 \cdot (2) + 4 \cdot (-2) = -2$, és így $3 \cdot (2 - 4k) + 4 \cdot (3k - 2) = -2$, vagyis $a = 2 - 4k$ és $b = 3k - 2$.

b) $2^{5a} \cdot 2^{7b} = 2^4 \iff 5a + 7b = 4$; mivel $7b \equiv 4 \pmod 5$, ezért $2b \equiv 4 \pmod 5$, ezt megoldva $b \equiv 2 \pmod 5$, tehát $b = 2 - 5k$. Behelyettesítve: $5a + 7 \cdot (2 - 5k) = 4$, azaz $5a = 35k - 10$, és így $a = 7k - 2$.

c) Mivel $\left(\frac{1+i}{\sqrt{2}}\right)^2 = i$ és így $\left(\frac{1+i}{\sqrt{2}}\right)^6 = i$, és általában $\left(\frac{1+i}{\sqrt{2}}\right)^x = \left(\frac{1+i}{\sqrt{2}}\right)^y \iff x \equiv y \pmod 8$, ezért átírható: $i^a \cdot \left(\frac{1+i}{\sqrt{2}}\right)^b = -i \iff \left(\frac{1+i}{\sqrt{2}}\right)^{2a} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^b = \left(\frac{1+i}{\sqrt{2}}\right)^6 \iff 2a + b \equiv 6 \pmod 8$.

Tehát $2a + b = 6 + 8k : k \in \mathbb{Z}$. Vagyis $b = 6 - 2a + 8k = 2 \cdot (3 - a + 4k) : k \in \mathbb{Z}$. Minden $a \in \mathbb{Z}$ egészhez végelen sok b egész tartozik a fenti képlet szerint.

A b lehetséges értékeit nézve: $b \equiv 1 \pmod 8$, $b \equiv 3 \pmod 8$, $b \equiv 5 \pmod 8$ és $b \equiv 7 \pmod 8$ esetén NINCS hozzá tartozó a, amivel $2a + b \equiv 6 \pmod 8$ teljesülne: $2 \cdot (3 - a) \equiv b \pmod 8$ és $2 \mid 8$, azaz $b \equiv 0 \pmod 8$, $b \equiv 2 \pmod 8$, $b \equiv 4 \pmod 8$ és $b \equiv 8 \pmod 8$ jöhet szóba megodásként.

$$\begin{array}{llll}
b \equiv 0 \pmod 8 & \text{esetén:} & 2a + b \equiv 6 \pmod 8 \iff 2a \equiv 6 \pmod 8 \iff a \equiv 3 \pmod 4 \\
b \equiv 2 \pmod 8 & \text{esetén:} & 2a + b \equiv 6 \pmod 8 \iff 2a \equiv 4 \pmod 8 \iff a \equiv 2 \pmod 4 \\
b \equiv 4 \pmod 8 & \text{esetén:} & 2a + b \equiv 6 \pmod 8 \iff 2a \equiv 2 \pmod 8 \iff a \equiv 1 \pmod 4 \\
b \equiv 6 \pmod 8 & \text{esetén:} & 2a + b \equiv 6 \pmod 8 \iff 2a \equiv 0 \pmod 8 \iff a \equiv 0 \pmod 4
\end{array}$$

9. Legyen $a = 2^{13} - 1$ és $b = 2^8 - 1$. Határozza meg (számológép használata nélkül) azokat x, y egészeket, melyre $ax + by = (a, b)$.

Megoldás:

$a = 2^{13} - 1$	$\alpha_{-1} = 1$	⊠⊠⊠⊠⊠⊠	$\beta_{-1} = 0$	$a = 1 \cdot a + 0 \cdot b$
$b = 2^8 - 1$	$\alpha_0 = 0$	$q_0 = 2^5$	$\beta_0 = 1$	$b = 0 \cdot a + 1 \cdot b$
$r_1 = 2^5 - 1$	$\alpha_1 = 1$	$q_1 = 2^3$	$\beta_1 = -2^5$	
$r_2 = 2^3 - 1$	$\alpha_2 = -2^3$	$q_2 = 2^2$	$\beta_2 = 1 + 2^8$	
$r_3 = 2^2 - 1$	$\alpha_3 = 1 + 2^5$	$q_3 = 2^1$	$\beta_3 = -2^5 - 2^2 - 2^{10}$	
$r_4 = 2^1 - 1$	$\alpha_4 = -2^3 - 2 - 2^6$	$q_4 = 2^1 + 1$	$\beta_4 = 1 + 2^8 + 2^6 + 2^3 + 2^{11}$	
$r_5 = 0$	$\alpha_5 = 2^8 - 1$	⊠⊠⊠⊠⊠⊠	$\beta_5 = 1 - 2^{13}$	

Tehát $(2^{13} - 1) \cdot (-2^6 - 2^3 - 2 + k \cdot (2^{13} - 1)) + (2^8 - 1) \cdot (2^{11} + 2^8 + 2^6 + 2^3 + 1 - k \cdot (2^8 - 1)) = 1$.

10. Oldja meg az alábbi kongruenciákat:

a) $13x \equiv 1 \mod 17$; b) $12x \equiv 18 \mod 15$; c) $7x \equiv 21 \mod 42$; d) $51x \equiv 69 \mod 152$
e) $5x \equiv 1 \mod 25$; f) $31x \equiv 18 \mod 17$; g) $11x \equiv 21 \mod 120$; h) $65x \equiv 91 \mod 117$

Eredmények:

a) $x \equiv 4 \pmod{17}$ **b)** $x \equiv 4 \pmod 5$ **c)** $x \equiv 3 \pmod 6$ **d)** $x \equiv 207 \pmod{152}$
e) NINCS megoldás. **f)** $x \equiv 6 \pmod{17}$ **g)** $x \equiv 111 \pmod{120}$ **h)** $x \equiv 5 \pmod 9$

11. Határozza meg azt a *két* legkisebb pozitív egész számot, mely

a) 7-szeresét felírva 8-es számrendszerben az utolsó előtti jegy 4, az utolsó jegy pedig 3;

b) 13-szorosát felírva 4-es számrendszerben az utolsó előtti jegy 2, az utolsó jegy pedig 1;

c) 19-szorosát felírva 16-os számrendszerben az utolsó előtti jegy 1, az utolsó jegy pedig 2!

Megoldás: $7x \equiv 8 \cdot 4 + 3 \pmod{64}$, azaz $7x \equiv 35 \pmod{64}$, tehát $x \equiv 5 \pmod{64}$. A két legkisebb ezt teljesítő pozitív egész: $x_1 = 5$ és $x_2 = 64 + 5 = 69$.

b) $13x \equiv 2 \cdot 4 + 1 \pmod{16}$, azaz $-3x \equiv 9 \pmod{16}$, tehát $x \equiv -3 \pmod{16}$. A két legkisebb ezt teljesítő pozitív egész: $x_1 = -3 + 16 = 13$ és $x_2 = -3 + 16 + 16 = 29$.

c) $19x \equiv 1 \cdot 16 + 2 \pmod{256} \Longrightarrow 19x \equiv 2 \pmod{16}$. (Vigyázat: nem ekvivalens átalakítás.) $3x \equiv 18 \pmod{16}$, ezért $x \equiv 6 \pmod{16}$, azaz $x = 16k + 6$. Ezt beírva az eredeti kongruenciába: $19 \cdot (16k + 6) \equiv 1 \cdot 16 + 2 \pmod{256}$, azaz $19 \cdot 16k + 19 \cdot 6 \equiv 18 \pmod{256}$, azaz $19 \cdot 16k + 114 \equiv 18 \pmod{256}$, azaz $19 \cdot 16k \equiv -96 \equiv 160 \pmod{256}$, azaz $19k \equiv 10 \pmod{16}$, azaz $3k \equiv -6 \pmod{16}$, azaz $k \equiv -2 \equiv 14 \pmod{16}$.

Tehát $x \equiv 16 \cdot 14 + 6 \equiv 230 \pmod{256}$. A két legkisebb ezt teljesítő pozitív egész: $x_1 = 230$ és $x_2 = 486$.

12. Határozza meg (a tízes számrendszerben felírt) 143^{143} utolsó három jegyét hármas alapú számrendszerben.

Megoldás: Ehhez $143^{143} \bmod 27$ étékét kell kiszámolnunk (és hármas alapú számrendszerben megadnunk). $143^{143} \equiv 8^{143} \equiv 2^{429} \pmod{27}$, mivel $\gcd(2, 27) = 1$, használható az Euler-Fermat tétel: $2^{\varphi(27)} \equiv 1 \pmod{27}$. $\varphi(27) = 27 \cdot (1 - \frac{1}{3}) = 18$, ezért a kitevőt $429 \bmod 18 = 15$ értékre cserélhetjük: $143^{143} \equiv 2^{429} \equiv 2^{15} \equiv (2^5)^3 \equiv 5^3 \pmod{27}$, hiszen $2^5 = 32 = 27 + 5$.

$5^3 = 25 \cdot 5 \equiv -2 \cdot 5 \equiv -10 \equiv 17 \pmod{27}$. Ezt hármas alapú számrendszerbe írva: $17 \bmod 3 = 2$ az utolsó számjegy, $\frac{17-2}{3} = 5$, $5 \bmod 3 = 2$ az utolsó előtti számjegy, és $\frac{5-2}{3} = 1$, $1 \bmod 3 = 1$ a "kilences helyiértéken" álló számjegy. Tehát $143^{143} = k \cdot 3^3 + \mathbf{1} \cdot 3^2 + \mathbf{2} \cdot 3^1 + \mathbf{2} \cdot 3^0$.

13. Milyen maradékot ad 103-mal osztva a következő szám: $205^{206^{207}}$?

Megoldás: $205 \equiv -1 \pmod{103}$, ezért $205^{206^{207}} \equiv (-1)^{206^{207}} \pmod{103}$, a 206 páros szám, annak pozitív egész kitevős hatványa is páros, tehát 206^{207} páros, a -1 páros kitevős hatánya pedig 1. Ezért $205^{206^{207}} \equiv 1 \pmod{103}$.

14. Számolja ki az következő értékeket

a) $6^{13^{20}} \bmod 11$; b) $5^{15^{17}} \bmod 12$; c) $13^{7^{120}} \bmod 8$; d) $13^{9^{45}} \bmod 17$

Megoldás: Általában ha $\gcd(a, n) = 1$, akkor $a^{b^c} \bmod n = a^{\left(b^c \bmod \varphi(n)\right)} \bmod n$; és ha még az is igaz, hogy $\gcd\big(b, \varphi(n)\big) = 1$, akkor $b^c \bmod \varphi(n) = b^{\left(c \bmod \varphi\left(\varphi(n)\right)\right)} \bmod \varphi(n)$.

a) Mivel $\varphi(11) = 10$ és $\varphi(10) = 4$; továbbá $\gcd(6, 11) = 1$ és $\gcd(13, 10) = 1$, ezért használható az általános módszer:

$13^{20} \bmod 10 = 13^{(20 \bmod 4)} \bmod 10 = 13^0 \bmod 10 = 1$. Ezért $6^{13^{20}} \bmod 11 = 6^1 \bmod 11 = 6$.

b) Mivel $\varphi(12) = 4$ és $\varphi(4) = 2$; továbbá $\gcd(5, 12) = 1$ és $\gcd(15, 4) = 1$, ezért használható az általános módszer:

$15^{27} \bmod 4 = 15^{(17 \bmod 2)} \bmod 4 = 15^1 \bmod 4 = 3$. Ezért $5^{15^{17}} \bmod 12 = 5^3 \bmod 12 = 5$.

c) Mivel $\varphi(8) = 4$ és $\varphi(4) = 2$; továbbá $\gcd(13, 8) = 1$ és $\gcd(7, 4) = 1$, ezért használható az általános módszer:

$7^{120} \bmod 4 = 7^{(120 \bmod 2)} \bmod 4 = 7^0 \bmod 4 = 1$. Ezért $13^{7^{120}} \bmod 8 = 13^1 \bmod 8 = 5$.

d) Mivel $\varphi(17) = 16$ és $\varphi(16) = 8$; továbbá $\gcd(13, 17) = 1$ és $\gcd(9, 16) = 1$, ezért használható az általános módszer:

$9^{45} \bmod 16 = 9^{(45 \bmod 8)} \bmod 16 = 9^5 \bmod 16$. Mivel $9 = 3^2$ és $\gcd(3,16) = 1$, így tovább egyszerűsíthetünk: $9^5 \bmod 16 = 3^{10} \bmod 16 = 3^{(10 \bmod 8)} = 3^2 \bmod 16 = 9$.

Tehát $9^{45} \bmod 16 = 9$. Ezért $13^{9^{45}} \bmod 17 = 13^9 \bmod 17$. Mivel $13 \equiv -4 \pmod{17}$, ezért $13^9 \equiv (-4)^9 \equiv -(4^9) \equiv -(2^{18}) \equiv -\left(2^{(18 \bmod 16)}\right) \equiv -2^2 \equiv -4 \equiv 13 \pmod{17}$, ezt felhasználva: $13^{9^{45}} \bmod 17 = 13^9 \bmod 17 = 13$.

15. Felhasználva, hogy $g = 5$ generátor modulo 23, számolja ki a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!

a) $\log_5(5)$; b) $\log_5(2)$; c) $\log_5(10)$; d) $\log_5(20)$ e) $\log_5(4)$; f) $\log_5(9)$

Megoldás: A logaritmusértékeket nem mod23, hanem mod$\varphi(23)$ = mod22 kell érteni, azaz ahol 21-nél magasabb érték jönne ki, ott a 22-vel vett osztási maradékot kell venni helyette.

a) $\log_5(5) = 1$.

b) Mivel $2 \equiv 25 \pmod{23}$, ezért $\log_5(2) = \log_5(25) = \log_5(5^2) = 2 \cdot \log_5(5) = 2$.

c) $\log_5(10) = \log_5(5 \cdot 2) = \log_5(5) + \log_5(2) = 1 + 2 = 3$.

d) $\log_5(20) = \log_5(10 \cdot 2) = \log_5(10) + \log_5(2) = 3 + 2 = 5$.

e) $\log_5(4) = \log_5(2 \cdot 2) = \log_5(2) + \log_5(2) = 2 + 2 = 4$; úgy is kijön, hogy $\log_5(4) = \log_5(2^2) = 2 \cdot \log_5(2) = 2 \cdot 2 = 4$;

Alternatív megoldás: Mivel $5 = \log_5(20) = \log_5(4 \cdot 5) = \log_5(4) + \log_5(5) = \log_5(4) + 1$, ezért $\log_5(4) = 5 - 1 = 4$.

f) Mivel $9 \equiv 32 \pmod{23}$, ezért $\log_5(9) = \log_5(32) = \log_5(2^5) = 5 \cdot \log_5(2) = 5 \cdot 2 = 10$.

Alternatív megoldás: Mivel $27 \equiv 4 \pmod{23}$, ezért $4 = \log_5(4) = \log_5(27) = \log_5(3^3) \equiv 3 \cdot \log_5(3) \pmod{\varphi(23)}$, azaz $3x \equiv 4 \pmod{22}$ megoldása adja $\log_5(3)$ értékét.

$3x \equiv 4 \equiv 48 \pmod{22}$, azaz $x \equiv 16 \pmod{22}$, ezért $\log_5(3) = 16$, így $\log_5(9) = \log_5(3^2) \equiv 2 \cdot \log_5(3) \equiv 2 \cdot 16 \equiv 32 \pmod{22}$, vagyis $\log_5(9) = 32 \bmod 22 = 10$.

Szorgalmi feladatok

16. Legyen F_n az n-edik Fibonacci szám. Ekkor $(F_n, F_{n-1}) = 1$. Oldja meg a $F_n \cdot x + F_{n-1} \cdot y = 1$ lineáris diofantikus egyenletet!

17. Írjon programot egészek faktorizációjára! Tekintsük a következő k bites egészeket:

k	n
40	684793814603
60	603141140725829899
80	605165905583175532445917
100	634444622321125788536087345851
120	665263035897162070681897421870027857
140	697578852189910008270768723978535669599683
160	731464442511808404319136684547345616528481453723
180	766996059271257858790344715690184347937909872494372031
200	804253659846418472879149405411605577932569166668425013521027
220	843321085627118096604442632091346426470017620515795831183527030727

Mekkora k értékre tudja n-et faktorizálni?