Kötelező házi feladat(ok)

7. Határozzuk meg a $7x \equiv 5 \pmod{23}$ kongruencia megoldásait.

8. Határozzuk meg a $\varphi(n) = 6$ egyenlet valamennyi megoldását.

Házi feladat(ok)

10. Legyen m természetes szám.

(a) Milyen m-ek esetén alkotnak a $0 + \cdots + i$ $(0 \leqslant i \leqslant m-1)$ számok teljes maradékrendszert modulo m?

(a) Milyen m-ek esetén létezik olyan $a_1, \ldots, a_m$ teljes maradékrendszer modulo m, amelyre az $a_1 + \cdots + a_i$ $(1 \leqslant i \leqslant m)$ számok is teljes maradékrendszert alkotnak modulo m?

11. Legyen f tetszőleges egész együtthatós polinom. Definiáljuk a ψ leképezést az alábbi módon:

$$\psi \colon \mathbb{N} \to \mathbb{N},\ \psi(n) = \{k : 0 \leqslant k \leqslant n-1,\ \text{ln.k.o.}(n, f(k)) = 1\}.$$

(a) Igazoljuk, hogy $\psi(mn) = \psi(m)\psi(n)$, ha $m, n \in \mathbb{N}$ és ln.k.o.$(m, n) = 1$;

(b) Határozzuk meg $\psi(p^\alpha)$ értékét, ahol p prímszám és $\alpha \in \mathbb{N}$.

Kongruenciareláció, maradékosztályok

54. Bizonyítsuk be, hogy $23 \mid 61^{k+1} + 2^{5k+3}3^{3k}7^{2k}11^k$, ahol k teszőleges természetes szám.

55. Melyek igazak az alábbi állítások közül, ahol $a, b \in \mathbb{Z}$ és $k, n \in \mathbb{N}$?

(a) Ha $k \mid n$, $a \equiv b \pmod{n}$, akkor $a \equiv b \pmod{k}$.

(b) Ha $k \mid n$, $a \equiv b \pmod{k}$, akkor $a \equiv b \pmod{n}$.

(c) Ha $a \equiv b \pmod{k}$ és $a \equiv b \pmod{n}$, akkor $a \equiv b \pmod{kn}$.

(d) Ha $ka \equiv kb \pmod{kn}$, akkor $a \equiv b \pmod{n}$.

56. Igaz-e, hogy ha $m \mid a - b$, akkor $m^2 \mid a^m - b^m$?

57. Legyenek a és b egészek számok. Tegyük fel, hogy $3 \nmid a$, ln.k.o.$(6, n) = 1$ és $a^n \equiv b^n \pmod{3^n}$. Mutassuk meg, hogy ekkor $a \equiv b \pmod{3^n}$.

58. Legyen k, n természetes szám és p prímszám. Bizonyítsuk be, hogy

(a) $\binom{n}{p} \equiv \left[\frac{n}{p}\right] \pmod{p}$, (b) $\binom{n}{kp} \equiv \binom{[n/p]}{k} \pmod{p}$.

59. Megoldhatók-e az alábbi egyenletek $\mathbb{Z}_5$-ben, illetve $\mathbb{Z}_8$-ban?

(a) $\overline{3}x + \overline{12}^2 = \overline{2}^{-1}$; (b) $\overline{13}x^2 = \overline{1}$;

(c) $\overline{3}x^2 + \overline{2}x - \overline{4} = \overline{0}$; (d) $x^{2008} = \overline{2}$.

Lineáris kongruenciák és kongruenciarendszerek

60. Oldjuk meg az alábbi kongruenciákat:

(a) $24x \equiv 60 \pmod{51}$; (b) $100x \equiv 88 \pmod{116}$;

(c) $555x \equiv 5555 \pmod{55555}$; (d) $13x^{41} \equiv 27 \pmod{100}$.

61. Határozzuk meg azt a két legkisebb pozitív egészet, amelynek 13-szorosát hetes számrendszerben felírva az utolsó előtti jegy 4, az utolsó jegy pedig 3.

62. Egy százlábú meg akarja számolni a lábait. Tudja, hogy legfeljebb 250 lába van. Ha 11-esével számolja őket, akkor 5 marad ki, ha 15-ösével, akkor 3. Hánylábú a százlábú.

63. Legyenek a és b páronként relatív prím, 1-nél nagyobb egészek. Milyen maradékot ad ab-vel osztva $a^{\varphi(b)} + b^{\varphi(a)}$.

64. Mennyi lesz a pontos idő éjfél után $39^{38^{37}}$ perccel?

65. Bizonyítsuk be, hogy tetszőleges p prímszámra és n egész számra $n^{p^p} - n$ osztható p-vel.

66. Az m egész számról tudjuk, hogy m^{100} 57, m^{101} pedig 11 maradékot ad 73-mal osztva. Milyen maradékot ad maga az m egész 73-mal osztva?

67. Oldjuk meg az

(a) $\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{7}, \end{cases}$ (b) $\begin{cases} 3x \equiv 67 \pmod{77}, \\ 5x \equiv 20 \pmod{55}, \end{cases}$

(c) $\begin{cases} x \equiv 5 \pmod{6}, \\ x \equiv 6 \pmod{7}, \\ x \equiv 10 \pmod{11}, \end{cases}$ (d) $\begin{cases} 3x \equiv 1 \pmod{4}, \\ 5x \equiv 2 \pmod{7}, \\ 7x \equiv 8 \pmod{9}. \end{cases}$

kongruenciarendszereket.

Maradékrendszerek, az Euler-féle φ függvény

68. Milyen $m \geqslant 2$ egészek esetén létezik olyan teljes maradékrendszer, amelynek elemei

(a) páratlan számok; (b) összetett számok;

(c) négyzetszámok; (d) mértani sorozatot alkotnak.

69. Milyen $m \geqslant 2$ egészek esetén létezik olyan redukált maradékrendszer, amelynek elemei

(a) 15-tel osztható számok;

(b) 15-tel nem osztható számok;

(c) négyzetszámok;

(d) teljes hatványok.

70. Legyen m tetszőleges természetes szám.

(a) Milyen maradékot ad m-mel osztva egy modulo m teljes maradékrendszer elemeinek az összege?

(b) Tegyük fel, hogy m páros, valamint $a_1, \ldots, a_m$ és $b_1, \ldots, b_m$ egy-egy teljes maradékrendszer modulo m. Bizonyítsuk be, hogy az

$$a_1 + b_1, \ldots, a_m + b_m$$

elemek sohasem alkotnak teljes maradékrendszert modulo m.

71. Egy kör alakú tisztás mentén m darab fa áll, mindegyiken egy-egy mókussal. A mókusok össze szeretnének gyűlni egy fán, de csak úgy változtathatják a helyüket, hogy két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára. Ezt a lépést akárhányszor ismételhetik. Milyen m esetén tudnak összegyűlni a mókusok?

72. Legyen $r_1, \ldots, r_t$ redukált maradékrendszer modulo $m \in \mathbb{N}$.

(a) Melyek azok az a egész számok, amelyekre az $ar_1, \ldots, ar_t$ számok páronként inkongruensek modulo m?

(b) Adjuk meg az összes olyan b egész számot, amelyre az $r_1 + b, \ldots, r_t + b$ elemek is redukált maradékrendszert alkotnak modulo m.

73. Legyenek a és b tetszőleges természetes számok és legyen $d = \text{ln.k.o.}(a, b)$. Mutassuk meg, hogy $\varphi(ab) = \dfrac{d}{\varphi(d)}\varphi(a)\varphi(b)$.

74. Mutassuk meg, hogy ha $m \mid n$, akkor $\varphi(m) \mid \varphi(n)$.

75. Legyen $n > 1$ természetes szám és

$$\mathcal{R}_n = \{k \in \mathbb{N} : 0 \leqslant k < n,\ \text{ln.k.o.}(k, n) = 1\}.$$

Ekkor tetszőleges $k \in \mathcal{R}_n$-hez van olyan egyértelműen meghatározott $l \in \mathcal{R}_n$, amelyre $kl \equiv 1 \pmod{n}$ teljesül. Az $l \in \mathcal{R}_n$ elemet k inverzének nevezzük és k^{-1}-gyel jelöljük. Határozzuk meg az alábbi összegek értékét modulo n.

(a) $\displaystyle\sum_{k \in \mathcal{R}_n} k$;

(b) $\displaystyle\sum_{k \in \mathcal{R}_n} k^{-1}$.

76. Legyen n természetes szám. Határozzuk meg a $\varphi(x) = 4n + 2$ egyenlet gyökeit.

77. Oldjuk meg az alábbi egyenleteket a természetes számok körében.

(a) $\text{ln.k.o.}(n, \varphi(n)) = 1$;

(b) $n - \varphi(n) = k$, ahol $k \in \{1, 6, 10\}$;

(c) $\varphi(m^2) = \varphi(n^2)$;

(d) $\varphi(m!) = n!$.

78. Mutassuk meg, hogy ha az n természetes szám nem prímszám, akkor teljesül az

$$n - \varphi(n) \geqslant \sqrt{n}$$

egyenlőtlenség.

79. Mely m természetes számok esetén létezik olyan számtani sorozat, amely redukált maradékrendszert alkot modulo m.

80. Határozzuk meg 1793^{8642} utolsó két számjegyét (tizes számrendszeben).

81. Mutassuk meg, hogy

$$a^{1729} \equiv a \pmod{1729}$$

teljesül tetszőleges a egész számra.

82. Mutassuk meg, hogy

$$m \mid a^m - a^{m-\varphi(m)}$$

teljesül tetszőleges a egész számra és m természetes számra.

83. Legyen p egy $4k-1$ alakú prímszám. Bizonyítsuk be, hogy $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

84. Lássuk be, hogy bármely p prímszámra $p^p \mid (p^2-1)! - p^{p-1}$ teljesül.

85. Legyen $a_1, \ldots, a_{30}$ redukált maradékrendszer modulo 31. Igazoljuk, hogy $31 \mid (a_1 a_2 a_3)^3 + (a_4 a_5 \cdots a_{30})^{27}$.