

## SZÁMELMÉLETI FELADATOK

1. Az  $1 = 1$ ,  $3 = 1 + 2$ ,  $6 = 1 + 2 + 3$ ,  $10 = 1 + 2 + 3 + 4$  számokat a pitagoreusok *háromszög számoknak* nevezték, mert az összeadandóknak megfelelő számú pont szabályos háromszög alakban is elrendezhető. Bizonyítsa be az alábbi állításokat:
  - (a) Egy természetes szám pontosan akkor háromszögszám, ha  $n(n + 1)/2$  alakú valamilyen  $n \in \mathbf{N}$ -re (Pithagoras kb. i.e. 550).
  - (b) Egy  $n \in \mathbf{N}$  pontosan akkor háromszögszám, ha  $8n + 1$  négyzetszám (Plutarchos kb. i.sz. 100).
  - (c) Két egymás utáni háromszögszám összege teljes négyzet (Nikomachosz kb. i.sz. 100).
  - (d) Ha  $n$  háromszögszám, akkor  $9n + 1$ ,  $25n + 3$ ,  $49n + 6$  is az (Euler 1775).
2. Ha  $t_n$  jelöli az  $n$ -edik háromszögszámot, akkor  $t_n = \binom{n+1}{2}$ ,  $n \geq 1$ .
3. Igazolja Aryabhata (kb. i.sz. 500) formuláját

$$t_1 + t_2 + \dots + t_n = \frac{n(n+1)(n+2)}{6}.$$

[Használja az 1(c) feladat eredményét].

4. Maradékos osztás segítségével igazolja, hogy
  - (a) minden négyzetszám  $3k$  vagy  $3k + 1$  alakú;
  - (b) minden köbszám  $9k$ ,  $9k + 1$  vagy  $9k + 8$  alakú;
  - (c)  $3a^2 - 1$  sohasem négyzetszám;
  - (d)  $n(n + 1)(2n + 1)/6$  mindig egész.
5. Igazolja, hogy ha egy egész szám egyidejűleg négyzetszám és köbszám, akkor  $7k$  vagy  $7k + 1$  alakú [pl.  $64 = 8^2 = 4^3$ ].
6. Igazolja, hogy tetszőleges  $a$ ,  $b$  ( $b \neq 0$ ) egészekhez vannak olyan  $q$ ,  $r$  egészek, hogy

$$a = bq + r \text{ valamint } -\frac{1}{2}|b| < r \leq \frac{1}{2}|b|,$$

s ezen  $q$ ,  $r$  egyértelműen meghatározott.

7. Igazolja, hogy a

$$11, 111, 1111, 11111, \dots$$

sorozatban nincs négyzetszám.

[Vegyék észre, hogy  $111 \dots 111 = 111 \dots 108 + 3 = 4k + 3$ .]

8. Ha  $a$  páratlan, akkor  $32|(a^2 + 3)(a^2 + 7)$ .

9. Ha  $a$  és  $b$  közül legalább az egyik nemzéró, akkor  $\text{ln.k.o.}(2a - 3b, 4a - 5b) | b$  és így  $\text{ln.k.o.}(2a + 3, 4a + 5) \sim 1$ .
10. Igazolja, hogy négy egymás utáni egész szám szorzata osztható 24-gyel, míg öté 120-szal.
11. Igazolja, hogy
- $6 | a(a^2 + 11)$  bármely  $a \in \mathbf{Z}$ -re.
  - $24 | a(a^2 - 1)$  bármely páratlan  $a \in \mathbf{Z}$ -re.
  - $8 | a^2 - b^2$  bármely páratlan  $a, b \in \mathbf{Z}$ -re.
  - $24 | a^2 + 23$ , ha  $a \in \mathbf{Z}$ , de  $2, 3 \nmid a$ .
  - $360 | a^2(a^2 - 1)(a^2 - 4)$  bármely  $a \in \mathbf{Z}$ -re.
12. Fölhasználva, hogy  $\mathbf{Z}$  főideálgyűrű igazolja a legnagyobb közös osztó alábbi tulajdonságait:
- Ha  $\text{ln.k.o.}(a, b) \sim \text{ln.k.o.}(a, c) \sim 1$ , akkor  $\text{ln.k.o.}(a, bc) \sim 1$ .
  - Ha  $\text{ln.k.o.}(a, b) \sim 1$  és  $c | a$ , akkor  $\text{ln.k.o.}(b, c) \sim 1$ .
  - Ha  $\text{ln.k.o.}(a, b) \sim 1$  és  $c | a + b$ , akkor  $\text{ln.k.o.}(a, c) \sim \text{ln.k.o.}(b, c) \sim 1$ .
13. Bizonyítsa be, hogy valahányszor  $d | n$  mindannyiszor  $2^d - 1 | 2^n - 1$ .
14. Euklideszi algoritmussal igazolja, hogy  $\text{ln.k.o.}(ka, kb) \sim k \cdot \text{ln.k.o.}(a, b)$ .
15. Bizonyítsa be, hogy ha  $a, b$  relatív prím egészek, akkor  $a + b$  és  $ab$  is azok.
16. Oldja meg az alábbi diophantoszi egyenleteket:
- $$14x + 35y = 93$$
- $$56x + 72y = 40$$
- $$221x + 35y = 11$$
- $$158x - 57y = 7$$
17. Ha  $a, b$  relatív prím egészek, akkor az  $ax - by = c$  diophantoszi egyenletnek végtelen sok természetes szám tesz eleget. Igazolja.
18. Bizonyítsa be, hogy az  $ax + by + cz = d$  diophantoszi egyenlet pontosan akkor oldható meg (az egész számok körében), ha  $\text{ln.k.o.}(a, b, c) | d$ .
19. Mr. Smith beváltott egy csekket készpénzre bankjában, s a pénztáros véletlenül fölcserélte a dollárok és a centek számát. Mr. Smith ezt csak azután vette észre, miután 68 centet elköltvén azt tapasztalta, hogy kétszer annyi pénze van, mint amennyi eredetileg a csekken szerepelt. Határozza meg azt a legkisebb összeget, amely szerepelhetett a csekken.
20. Fejtse meg az alábbi rejtvényeket:
- 100 véka gabonát osztunk szét 100 személy között úgy, hogy minden férfi 3, minden nő 2, s minden gyermek  $1/2$  vékányit kap. Hány férfi, nő és gyermek volt? (yorki Alcuin kb. 775)

- (b) Volt 63 egyenlő rakás gyümölcs és még 7 db. Ezt 23 vándor között osztották szét egyenlő arányban. Hány gyümölcs volt egy-egy rakásban? (Mahavira kb. 850)
- 21.** Azt sejtik, hogy végtelen sok  $n^2 - 2$  alakú prímszám van. Adjon meg öt ilyen prímszámot.
- 22.** Ellenpéldával cáfolja meg azon sejtést, hogy minden pozitív egész szám  $p + a^2$  alakban írható, ahol  $p$  vagy prím, vagy 1, továbbá  $a \in \mathbf{Z}$ .
- 23.** Igazolja a következő állításokat:
- (a) Minden  $3n + 1$  alakú prímszám  $6m + 1$  alakú is.
- (b) Minden  $3n + 2$  alakú egész számnak van ugyanilyen alakú prímosztója.
- 24.** Mutassa meg, hogy ha  $p \geq 5$  prím, akkor  $p^2 + 2$  összetett szám.
- 25.** Bizonyítsa be:
- (a) Minden  $n^4 + 4$  alakú egész, ha  $n > 1$  összetett szám.
- (b) Ha  $n > 4$  összetett, akkor  $n|(n-1)!$ .
- (c) Minden  $8^n + 1$  alakú egész összetett, ha  $n > 1$ .
- 26.** Adja meg  $50!$  összes prímosztóját.
- 27.** Ha  $p$  és  $q$  olyan prímek, hogy  $p \geq q \geq 5$ , akkor  $24|p^2 - q^2$ . Igazolja.
- 28.** Ha  $p \neq 5$  páratlan prím, akkor mutassa meg, hogy  $p^2 - 1$  vagy  $p^2 + 1$  osztható 10-zel.
- 29.** Mutassa meg, hogy ha  $p \nmid n$  minden  $p \leq \sqrt[3]{n}$ , akkor  $n$  vagy prím vagy két prím szorzata. [Indirekt úton: tegye föl, hogy  $n$  legalább három prímszám szorzata.]
- 30.** Igazolja, hogy ha  $p_n$  az  $n$ -edik prímszám, akkor
- (a)  $p_n > 2n - 1$  ha  $n \geq 5$ .
- (b) Egyetlen  $P_n = p_1 p_2 \cdots p_n + 1$  sem teljes négyzet.
- (c)  $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$  sohasem egész.
- 31.** Adjon meg olyan  $a$ ,  $b$ ,  $n$  egészeket, hogy  $a^2 \equiv b^2 \pmod{n}$  de  $a \not\equiv b \pmod{n}$ .
- 32.** Ha  $a \equiv b \pmod{n}$ , akkor  $\ln.k.o.(a, n) \sim \ln.k.o.(b, n)$ . Igazolja.
- 33.** (a) Milyen maradékot ad  $2^{50}$  és  $41^{65} 7 - tel$  osztva?
- (b) Mi lesz a maradék, ha

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5 - t$$

elosztjuk 4-gyel?

- 34.** Mutassa meg, hogy  $39|53^{103} + 103^{53}$  és  $7|111^{333} + 333^{111}$ .
- 35.** Kongruenciákat használva igazolja a következő állításokat:
- (a)  $7|5^{2n} + 3 \cdot 2^{5n-2}$ ;
- (b)  $13|3^{n+2} + 4^{2n+1}$ ;
- (c)  $27|2^{5n+1} + 5^{n+2}$ ;

(d)  $43|6^{n+2} + 7^{2n+1}$ .

36. Ha  $p$  olyan prímszám, hogy  $n < p < 2n$ , akkor

$$\binom{2n}{n} \equiv 0 \pmod{p}.$$

Igazolja.

37. Ha  $a_1, a_2, \dots, a_n$  teljes maradékrendszer modulo  $n$ , továbbá  $\text{ln.k.o.}(a, n) \sim 1$ , akkor  $aa_1, aa_2, \dots, aa_n$  is teljes maradékrendszer modulo  $n$ .

38. Bizonyítsa be az alábbi állításokat:

(a) Ha  $\text{ln.k.o.}(a, n) \sim 1$ , akkor a

$$c, c + a, c + 2a, c + 3a, \dots, c + (n - 1)a$$

egészek egy teljes maradékrendszert alkotnak modulo  $n$ .

(b) Bármely egymás utáni  $n$  egész szám teljes maradékrendszert alkot modulo  $n$ .

39. Mutassa meg, hogy ha  $ab \equiv cd \pmod{n}$  és  $b \equiv d \pmod{n}$  továbbá  $\text{ln.k.o.}(b, d) \sim 1$ , akkor  $a \equiv c \pmod{n}$ .

40. Igazolja következő állításokat:

(a) Tetszőleges  $a$  egészre  $a^2$  utolsó jegye 0, 1, 4, 5, 6 vagy 9.

(b) Egy köbszám akármilyen jegyre végződik.

(c) Ha  $a$  egész, akkor  $a^4$  utolsó jegye 0, 1, 5 vagy 6.

41. Adja meg  $9^{9^9}$  utolsó két jegyét.

42. Modulo 9 vagy 11 kongruenciák segítségével keresse meg az alábbi számolásokban a hiányzó számjegyeket:

(a)  $51840 \cdot 273581 = 1418243x040$ ;

(b)  $2x99561 = (3(523 + x))^2$ ;

(c)  $2784x = x \cdot 493$ .

43. Milyen maradékot ad  $4444^{4444}$ , ha elosztjuk 9-cel

44. Határozza meg  $7^{999}$  utolsó három jegyét.

45. Jelölje  $t_n$  az  $n$ -edik háromszögszámot. Mutassa meg, hogy  $t_{n+2k} \equiv t_n \pmod{k}$ ; s így  $t_n$  és  $t_{n+20}$  ugyanarra a jegyre végződik.

46. Adja meg azon  $n > 1$  értékeket, amelyekre

$$1! + 2! + 3! + \dots + n!$$

teljes négyzet.

47. Adjon meg szabályt a 7, 11 és 13-mal való oszthatóságra. Megfogalmazható e ilyen szabály bármely  $p$  prímszámra?
48. *Palindromnak* nevezik az olyan számot, amely visszafelé olvasva is ugyanaz (például: 373, 521125). Bizonyítsa be, hogy minden páros sok jegyű palindrom osztható 11-gyel.
49. Oldja meg az alábbi lineáris kongruenciákat:
- (a)  $25x \equiv 15 \pmod{29}$ .  
 (b)  $5x \equiv 2 \pmod{26}$ .  
 (c)  $6x \equiv 15 \pmod{21}$ .
50. Kongruenciák segítségével oldja meg a következő diophantoszi egyenleteket:
- (a)  $4x + 51y = 9$ .  
 (b)  $5x - 53y = 17$ .
51. Adja meg  $3x - 7y \equiv 11 \pmod{13}$  összes megoldását.
52. Oldja meg az alábbi kongruencia-rendszereket:
- (a)  $x \equiv 1 \pmod{3}$ ,  $x \equiv 2 \pmod{5}$ ,  $x \equiv 3 \pmod{7}$ .  
 (b)  $x \equiv 5 \pmod{11}$ ,  $x \equiv 14 \pmod{29}$ ,  $x \equiv 15 \pmod{31}$ .  
 (c)  $2x \equiv 1 \pmod{5}$ ,  $3x \equiv 9 \pmod{6}$ ,  $4x \equiv 1 \pmod{7}$ ,  $5x \equiv 9 \pmod{11}$ .
53. Ha egy kosár tojást 2, 3, 4, 5 vagy 6-osával ürítünk ki, rendre 1, 2, 3, 4, 5 tojás marad benne. Ha azonban 7-esével vesszük ki a tojásokat, akkor egy sem marad benne. Adja meg a kosárban levő tojások minimális számát. (Brahmagupta i.sz. VII.sz.)
54. Egy 17 tagú kalózcsoport egy zsák aranypénzt lopott. Amikor megpróbálták egyenlően elosztani azt tapasztalták, hogy három arany kimaradt. A kimaradt aranyak fölötti vitában egy kalózt megöltek. Ezután újraosztották egyenlő arányban a zsákmányt, s most 10 arany maradt ki. Az e fölötti vitában egy újabb kalózt öltek meg, s ezután már el tudták osztani a lopott aranyat úgy, hogy mindenki ugyanannyit kapott. Határozza meg a lopott aranypénzek minimális számát. (Ókori kínai probléma.)
55. Bizonyítsa be, hogy az

$$x \equiv a \pmod{n} \quad x \equiv b \pmod{m}$$

kongruencia-rendszer pontosan akkor oldható meg, ha  $\text{ln.k.o.}(n, m) \mid a - b$ ; és amennyiben megoldható, az  $\text{mod}(\text{lk.k.t.}(n, m))$  kongruencia erejéig egyértelmű.

56. Igazolja, hogy  $18^6 \equiv 1 \pmod{7^k}$   $k = 1, 2, 3 - ra$ .
57. (a) Mutassa meg, hogy  $a^{12} \equiv 1 \pmod{35}$ , ha  $\text{ln.k.o.}(a, 35) \sim 1$ .  
 (b) Ha  $\text{ln.k.o.}(a, 42) \sim 1$ , akkor  $168 \mid a^6 - 1$ . Igazolja.
58. Bizonyítsa be, hogy végtelen sok olyan  $n$  összetett szám van, amelyre  $a^{n-1} \equiv a \pmod{n}$ . [Mi a helyzet, ha  $n = 2p$  valamilyen  $p$  páratlan prímre?]

59. Legyen  $a$  olyan egész, amelyre  $ln.k.o.(a, 30) \sim 1$ . Mutassa meg, hogy  $60|a^4 + 59$ .
60. (a) Fermat tétele segítségével határozza meg  $3^{100}$  utolsó jegyét.  
 (b) Igazolja, hogy bármely  $a$  egészre  $a^5$  és  $a$  utolsó jegye megegyezik.
61. Ha  $7 \nmid a$ , akkor vagy  $7|a^3 + 1$  vagy  $7|a^3 - 1$ .
62. A Halley üstökös három legutóbbi megjelenése 1835, 1910 és 1986-ban volt, legközelebb 2061-ben lesz látható. Igazolja, hogy

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}.$$

63. A Fermat tétel alapján mutassa meg, hogy  
 (a) ha  $p$  prím és  $ln.k.o.(a, p) \sim 1$ , akkor  $x \equiv a^{p-2}b \pmod{p}$  megoldása az  $ax \equiv b \pmod{p}$  lineáris kongruenciának.  
 (b) Az előző feladat alapján oldja meg a következő lineáris kongruenciákat:

$$2x \equiv 1 \pmod{31}, \quad 6x \equiv 5 \pmod{11} \quad \text{és} \quad 3x \equiv 17 \pmod{29}.$$

64. Föltéve, hogy  $a$  és  $b$  olyan egészek, amelyek nem oszthatók a  $p$  prímszámmal igazolja, hogy  
 (a)  $a^p \equiv b^p \pmod{p}$ , ha  $a \equiv b \pmod{p}$ .  
 (b)  $a^p \equiv b^p \pmod{p^2}$ , ha  $a^p \equiv b^p \pmod{p}$ .
65. Legyen  $p$  páratlan prím, valamint  $1 \leq k \leq p - 1$ . Igazolja, hogy

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

66. Tegyük föl, hogy  $p$  és  $q$  különböző páratlan prímelek, továbbá  $p-1|q-1$ . Mutassa meg, hogy valahányszor  $ln.k.o.(a, pq) \sim 1$ , mindannyiszor  $a^{q-1} \equiv 1 \pmod{pq}$ .
67. Legyenek  $p$  és  $q$  különböző prímelek. Igazolja, hogy

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

68. Ha  $M_p = 2^p - 1$  összetett, ahol  $p$  prím, akkor  $M_p$  pszeudoprím. Igazolja.
69. Mutassa meg, hogy az alábbi számok mindegyike abszolút pszeudoprím:  
 (a)  $1387 = 19 \cdot 73$ ,  
 (b)  $2821 = 7 \cdot 13 \cdot 31$ ,  
 (c)  $1905 = 3 \cdot 5 \cdot 127$ .
70. Igazolja, hogy 341 pszeudoprím, de nem abszolút pszeudoprím fölhasználva, hogy  $11^{341} \not\equiv 11 \pmod{341}$ . [Vegyük észre, hogy  $31 \nmid 11^{34} - 11$ .]

71. Ha  $n = 2p$ , ahol  $p$  páratlan prím, akkor  $a^{n-1} \equiv a \pmod{n}$  bármely  $a$  egészre. Igazolja.

72. Mutassa meg, hogy minden

$$n = (6k + 1)(12k + 1)(18k + 1)$$

alaku egész abszolút pszeudoprím, ha mindhárom faktor prím; s így  $1729 = 7 \cdot 13 \cdot 19$  egy abszolút pszeudoprím.

73. Wilson-tétele alapján adja meg, hogy

(a) milyen maradékot ad  $15!$ , ha 17-tel osztjuk;

(b) milyen maradékot ad  $2(26!)$ , ha 29-cel osztjuk.

74. Döntse el annak alapján, hogy a  $16! \equiv -1 \pmod{17}$  teljesül vagy nem, hogy 17 prímszám-e.

75. Rendezze el a  $2, 3, 4, \dots, 21$  egészeket  $a, b$  párokba úgy, hogy  $ab \equiv 1 \pmod{23}$ .

76. Legyen  $n > 1$  egész.

(a) Bizonyítsa be, hogy  $n$  akkor és csak akkor prím, ha  $(n-2)! \equiv 1 \pmod{n}$ .

(b)  $(n-1)! \equiv 0 \pmod{n}$  valahányszor  $n$  összetett és  $n \neq 4$ .

77. Legyen  $p$  egy prímszám. Mutassa meg, hogy

$$(p-1)! \equiv p-1 \pmod{1+2+3+\dots+(p-1)}.$$

78. Keressen két olyan  $p \leq 13$  prímszámot amelyre fönnáll a  $(p-1)! \equiv -1 \pmod{p^2}$  kongruencia.

79. Wilson-tétele segítségével igazolja, hogy

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

teljesül minden páratlan  $p$  prímre.

80. Igazolja az alábbi állításokat:

(a) Ha  $p = 4k + 3$  prím akkor

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \text{ vagy } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p};$$

és így  $((p-1)/2)!$  megoldása az  $x^2 \equiv 1 \pmod{p}$  kongruenciának.

(b) Az (a) rész fölhasználásával mutassa meg, hogy ha  $p = 4k + 3$  prím, akkor az összes  $p$ -nél kisebb páros szám szorzata kongruens  $\pm 1$ -gyel modulo  $p$ . [Fermat-tétele alapján  $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$ ].

81. Bizonyítsa be, hogy az  $n^2 + 1$  alakú egészek páratlan prímosztói  $4k + 1$  alakúak. [Mikor oldható meg az  $x^2 \equiv -1 \pmod{p}$  kongruencia?]
82. Ha  $p$  és  $p + 2$  ikerprímek, akkor

$$4((p - 1)! + 1) + p \equiv 0 \pmod{p(p + 2)}.$$

Igazolja.

83. Keresse meg a 2, 3 és 5 multiplikatív rendjét: (a) modulo 17, (b) modulo 19, (c) modulo 23.
84. Igazolja az alábbi állításokat:
- (a) Ha  $a$  rendje modulo  $p$   $2k$ , ahol  $p$  páratlan prím, akkor  $a^k \equiv -1 \pmod{p}$ .
  - (b) Ha  $a$  rendje modulo  $n$   $n - 1$ , akkor  $n$  prímszám.
85. Legyen  $p$  páratlan prím, az  $a$  egész rendje modulo  $p$  pedig 3. Bizonyítsa be, hogy  $a + 1$  rendje modulo  $p$  szükségképp 6. [ $a^2 + a + 1 \equiv 0 \pmod{p}$  alapján  $(a + 1)^2 \equiv a \pmod{p}$  és  $(a + 1)^3 \equiv -1 \pmod{p}$ ]
86. Igazolja a következő állításokat:
- (a) Az  $n^2 + 1$  minden páratlan prímosztója  $4k + 1$  alakú. [ $n^2 \equiv -1 \pmod{p}$  ekkor, így  $4 \mid \varphi(p)$ ]
  - (b)  $n^4 + 1$  páratlan prímosztói  $8k + 1$  alakúak.
  - (c) Az  $n^2 + n + 1$  alakú egészek minden 3-tól különböző páratlan prímosztója  $6k + 1$  alakú.
87. Mutassa meg, hogy végtelen sok  $4k + 1$ ,  $6k + 1$ ,  $8k + 1$  alakú prímszám van. [pl. ha  $p_1, p_2, \dots, p_r$  az összes  $4k + 1$  alakú prím, akkor alkalmazza az előző állítást  $(2p_1 p_2 \cdot \dots \cdot p_r)^2 + 1$ -re.]
88. Igazolja, hogy a 2 primitív gyök modulo 19, de modulo 17 már nem.
89. Legyen  $p$  egy páratlan prímszám. Mutassa meg, hogy
- (a) az  $x^2 \equiv 1 \pmod{p}$  kongruencia összes inkongruens megoldásai 1 és  $p - 1$ .
  - (b) az  $x^{p-2} + \dots + x^2 + x + 1 \equiv 0 \pmod{p}$  kongruenciának pontosan  $p - 2$  inkongruens megoldása van, s ezek a  $2, 3, \dots, p - 1$  egészek.
90. Tegyük föl, hogy  $r$  primitív gyök modulo  $p$ . Igazolja, hogy
- (a) az  $r^{(p-1)/2} \equiv -1 \pmod{p}$  kongruencia fõnnáll.
  - (b) ha  $r'$  szintén egy primitív gyök modulo  $p$ , akkor  $rr'$  már nem primitív gyök.
  - (c) ha  $r'$  olyan egész, hogy  $rr' \equiv 1 \pmod{p}$ , akkor  $r'$  primitív gyök modulo  $p$ .
91. Legyen  $p$  páratlan prím és  $r$  egy primitív gyök modulo  $p$ . Bizonyítsa be, hogy
- (a) ha  $p \equiv 1 \pmod{4}$ , akkor  $-r$  is egy primitív gyök.
  - (b) ha  $p \equiv 3 \pmod{4}$ , akkor  $-r$  rendje modulo  $p$   $(p - 1)/2$ .



- 92.** Igazolja az alábbi állításokat:
- Ha  $n$  páratlan egész, akkor  $\varphi(2n) = \varphi(n)$ .
  - Ha  $n$  egy páros egész, akkor  $\varphi(2n) = 2\varphi(n)$ .
  - $\varphi(3n) = 3\varphi(n)$  akkor és csak akkor, ha  $3|n$ .
  - $\varphi(3n) = 2\varphi(n)$  pontosan akkor, ha  $3 \nmid n$ .
- 93.** Igazolja, hogy a  $\varphi(n) = \varphi(n+2)$  egyenlőség teljesül  $n = 2(2p-1)$ -re, valahányszor  $p$  és  $2p-1$  prímszám.
- 94.** Mutassa meg, hogy
- tetszőleges pozitív egész  $n$ -re  $\frac{1}{2}\sqrt{n} \leq \varphi(n) \leq n$ . [Ha  $n = 2^{k_0} p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ , akkor  $\varphi(n) = 2^{k_0-1} p_1^{k_1-1} \cdot \dots \cdot p_r^{k_r-1} (p_1-1) \cdot \dots \cdot (p_r-1)$  és használja a  $p-1 > \sqrt{p}$ , valamint a  $k - \frac{1}{2} \geq \frac{k}{2}$  egyenlőtlenségeket.]
  - ha az  $n > 1$  egésznek  $r$  különböző prímfaktora van, akkor  $\varphi(n) \geq \frac{n}{2^r}$ .
- 95.** Bizonyítsa be, hogy ha  $n$ -nek  $r$  különböző páratlan prímfaktora van, akkor  $2^r | \varphi(n)$ .
- 96.** Ha minden olyan prím amely osztója  $n$ -nek az  $m$ -nek is osztója, akkor  $\varphi(nm) = n\varphi(m)$ , speciálisan,  $\varphi(n^2) = n\varphi(n)$ . Igazolja.
- 97.** Mutassa meg, hogy  $n \geq 1$  esetén  $\tau(n) \leq 2\sqrt{n}$ .
- 98.** Bizonyítsa be, hogy
- $\tau(n)$  pontosan akkor páratlan, ha  $n$  teljes négyzet.
  - $\sigma(n)$  pontosan akkor páratlan, ha  $n$  teljes négyzet, vagy egy teljes négyzet kétszerese.
- 99.** Mutassa meg, hogy bármely pozitív egész  $n$ -re  $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ .
- 100.** Legyen  $n$  négyzetmentes szám. Mutassa meg, hogy  $\tau(n) = 2^r$ , ahol  $r$  az  $n$  különböző prímtényezői száma.
- 101.** Legyen  $n = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$ , ahol  $p_i \neq p_j$ , ha  $i \neq j$ . Igazolja, hogy

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right).$$

- 102.** Legyen  $k > 1$  egész. Mutassa meg, hogy végtelen sok olyan  $n \in \mathbf{N}$  van amelyre  $\tau(n) = k$ , de csak véges sok olyan, amelyre  $\sigma(n) = k$ .
- 103.** Bizonyítsa be, hogy ha  $n$  és  $n+2$  prímelek, akkor  $\sigma(n+2) = \sigma(n) + 2$  és ez igaz  $n = 434$  és  $8575$ -re is.
- 104.** Legyen  $n \in \mathbf{N}$ . Mutassa meg, hogy

$$\sum_{d|n} \tau(d)^3 = \left( \sum_{d|n} \tau(d) \right)^2$$

[Vegye észre, hogy az egyenlőség mindkét oldalán multiplikatív függvény szerepel.]

- 105.** Legyen  $x, y, z$  egy primitív pithagoraszi számhármast. Bizonyítsa be, hogy  $x + y$  és  $x - y$  1 vagy 7-tel kongruensek modulo 8.
- 106.** Igazolja, hogy bármely  $x, y, z$  primitív pithagoraszi számhármásra  $12|xy$  és  $60|xyz$ .
- 107.** Határozza meg az összes olyan pithagoraszi számhármast, amely
- (a) három egymás utáni egész szám.
  - (b) elemei számtani sorozatot alkotnak.
- 108.** Mutassa meg, hogy ha  $x, y, z$  olyan pithagoraszi számhármast amelyben  $z - y = 2$ ,

$$x = 2t, \quad y = t^2 - 1, \quad z = t^2 + 1$$

valamilyen  $t > 1$  egészre.

- 109.** Legyen  $n \in \mathbf{N}$ . Bizonyítsa be, hogy van olyan pithagoraszi számhármast, hogy az általa meghatározott háromszög beírt körének sugara  $n$ .
- 110.** Mutassa meg, hogy végtelen sok olyan pithagoraszi számhármast van, amelyben az első két szám egymás utáni egész. [Ha  $x, x + 1, z$  pithagoraszi akkor  $3x + 2z + 1, \dots$  is az.]
- 111.** Végtelen sok olyan pithagoraszi számhármast van, amelyben két egymás utáni háromszögszám szerepel. [Ha  $x, x + 1, z$  pithagoraszi számhármast, akkor tekintse a  $t_{2x}$ -szel kezdődő hármast.]
- 112.** Oldja meg az alábbi kongruenciákat:
- (a)  $3x^2 + 5x - 2 \equiv 0 \pmod{12}$
  - (b)  $14x^6 - 18x^5 + 31 \equiv 0 \pmod{63}$
  - (c)  $x^2 + 33x + 18 \equiv 0 \pmod{49}$
  - (d)  $x^3 + 2x^2 + 28 \equiv 0 \pmod{27}$
  - (e)  $x^{19} + 2x + 1 \equiv 0 \pmod{38}$
  - (f)  $x^{99} - 1 \equiv 0 \pmod{8}$