KÖTELEZŐ HÁZI FELADAT(OK)

9. Tudjuk, hogy a 2 egész szám primitív gyök modulo 13. Készítsünk indextáblázatot.

10. Határozzuk meg a $3x^7 \equiv 8 \pmod{13}$ kongruencia valamennyi megoldását.

HÁZI FELADAT(OK)

12. Legyen p prímszám és legyenek modulo p a prmitív gyökök

$$g_1 < \cdots < g_{\varphi(p-1)}.$$

Milyen maradékot ad p-vel osztva a $g_1 \cdots g_{\varphi(p-1)}$ szorzat?

13. Legyen p prímszám és legyenek modulo p a prmitív gyökök

$$g_1 < \cdots < g_{\varphi(p-1)}.$$

Milyen maradékot ad p-vel osztva a $g_1 + \cdots + g_{\varphi(p-1)}$ összeg, ha p és $(p-1)/2$ is prímszám?

REND, PRIMITÍV GYÖK, INDEX

86. Határozzuk meg az a elem rendjét modulo m.

(a) $a = 2$, $m = 7$;
(b) $a = 2$, $m = 41$;
(c) $a = 3$, $m = 41$;
(d) $a = 3$, $m = 32$;
(e) $a = 6$, $m = 41$;
(f) $a = 15$, $m = 32$.

87. Legyen n természetes szám.

(a) Határozzuk meg a 2 egész szám rendjét modulo 3^n.

(b) Határozzuk meg a 3 egész szám rendjét modulo 2^n.

88. Legyenek a és b egész számok, k és n természetes számok. Bizonyítsuk be a következőket.

(a) Ha $ab \equiv 1 \pmod{n}$, akkor $\mathfrak{o}_n(a) = \mathfrak{o}_n(b)$.

(b) Ha $\mathfrak{o}_n(a)$ létezik, akkor $\mathfrak{o}_n(a^k)$ is létezik, és a két rend között az

$$\mathfrak{o}_n(a^k) = \mathfrak{o}_n(a)/\text{ln.k.o.}(\mathfrak{o}_n(a), k)$$

összefüggés áll fenn.

89. Legyen $p > 2$ prímszám. Igazoljuk, hogy $\mathfrak{o}_p(a) = \mathfrak{o}_p(-a)$ pontosan akkor teljesül, ha $4 \mid \mathfrak{o}_p(a)$.

90. Legyenek a és b egész számok, m és n pedig természetes számok. Igazoljuk a következőket.

(a) Ha ln.k.o.$(a, m) = 1$ és $n \mid m$, akkor $\mathfrak{o}_n(a) \mid \mathfrak{o}_m(a)$.

(b) Ha ln.k.o.$(a, mn) = 1$, akkor

$$\mathfrak{o}_{\text{lk.k.t.}(m,n)}(a) = \text{lk.k.t.}(\mathfrak{o}_m(a), \mathfrak{o}_n(a)).$$

(c) Ha ln.k.o.$(a, n) = 1$ és ln.k.o.$(b, n) = 1$, akkor

$$\mathfrak{o}_n(ab) = \mathfrak{o}_n(a) \cdot \mathfrak{o}_n(b) \Longleftrightarrow \text{ln.k.o.}(\mathfrak{o}_n(a), \mathfrak{o}_n(b)) = 1.$$

91. Legyen $p > 2$ prímszám, a olyan egész szám, amelyre $p \nmid a$ teljesül, valamint legyen α természetes szám. Igazoljuk, hogy ha $\mathfrak{o}_{p^\alpha}(a) = 2t$, akkor $a^t \equiv -1 \pmod{p^\alpha}$.

92. Legyen $p > 2$ prímszám és a olyan egész szám, amelyre $a^t \equiv -1 \pmod{p^\alpha}$ teljesül, valamely α és t természetes számokra. Igazoljuk, hogy $\mathfrak{o}_{p^\alpha}(a) = 2u$, ahol $u \mid t$ és t/u páratlan.

93. Legyenek a és r természetes számok, $p > 2$ prímszám. Bizonyítsuk be, hogy ha $p \mid a^{2^r} + 1$, akkor $p \equiv 1 \pmod{2^{r+1}}$.

94. Legyenek $a, n \geqslant 2$ természetes számok. Bizonyítsuk, be hogy $n \mid \varphi(a^n - 1)$.

95. Az a, b egészekre és m természsetes számra teljesül, hogy

$$a^{\mathfrak{o}_m(b)} \equiv b^{\mathfrak{o}_m(a)} \pmod{m}.$$

Bizonyítsuk be, hogy $\mathfrak{o}_m(a) = \mathfrak{o}_m(b)$.

96. Igazoljuk, hogy a 2 egész szám nem primitív gyök modulo p, ha $p = 2^{2^n} + 1$ $(n \geqslant 2)$ Fermat-féle prímszám.

Legyen $n > 1$ természetes szám. Definiáljuk az A_n halmazt és $g(n)$ egészet a következőképpen:

$$A_n := \{a \in \mathbb{N} : a \leqslant n - 1 \text{ és } a \text{ primitív gyök modulo } n\},$$

és legyen $g(n) = \min A_n$.

97. Határozzuk meg $g(p)$ értékét, amennyiben

(a) $p = 5$;

(b) $p = 13$;

(c) $p = 19$;

(d) $p = 23$;

(e) p Fermat-féle prímszám;

(f) $p \equiv 3 \pmod 8$ prímszám, amelyre $(p-1)/2$ is prímszám.

98. Adjuk meg az A_n halmaz elemeit, ahol $n \in \{7, 10, 18, 24, 1973\}$.

99. Legyen q olyan páratlan prímszám, amelyre $p = 2q + 1$ is prímszám. Bizonyítsuk be, hogy

$$q + \frac{1 + (-1)^{(q-1)/2}}{2}$$

primitív gyök modulo p.

100. Legyen q olyan páratlan prímszám, amelyre $p = 2q + 1$ is prímszám. Bizonyítsuk be, hogy amennyiben $p \nmid a^3 - a$, akkor a vagy $-a$ primitív gyök modulo p.

101. Keressünk primitív gyököt modulo 47, illetve modulo 59.

102. Legyen p prímszám és n természetes szám. Milyen maradékot ad p-vel osztva a $\sum_{1 \leqslant i \leqslant p-1} i^n$ összeg?

103. Legyen p páratlan prímszám és a olyan egész szám, amely nem osztható p-vel, valamint legyen $t = \mathfrak{o}_p(a)$. Ekkor igazak a következők.

(a) Ha $t > 1$, akkor $\sum_{1 \leqslant k \leqslant t-1} a^k \equiv -1 \pmod{p}$.

(b) $\mathfrak{o}_{p^n}(a) = t \cdot p^{\max(0, n-z)}$, ahol $p^z \parallel a^t - 1$.

Legyen n természetes szám, g primitív gyök modulo n. Ekkor tetszőleges a-ra ($1 \leqslant a \leqslant n-1$, ln.k.o.$(a, n) = 1$) van egyetlen olyan $t = \operatorname{ind}_{n,\,g} a \in \{1, \ldots, \varphi(p)\}$ kitevő, amelyre $g^t \equiv a \pmod{n}$, ez a kitevő az a elem indexe modulo n (a g primitív gyökre vonatkozóan).

104. Határozzuk meg az alábbi indexeket.

(a) $\operatorname{ind}_{7,\,g(7)} 4$;

(b) $\operatorname{ind}_{9,\,5} 5$;

(c) $\operatorname{ind}_{49,\,10} 24$;

(d) $\operatorname{ind}_{27,\,g(27)} 25$.

105. Legyen p prímszám, g és h primitív gyökök modulo p. Igazoljuk, hogy $\operatorname{ind}_h a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_h g \pmod{p-1}$.

106. Tudjuk, hogy a 2 egész szám primitív gyök modulo 29. Készítsünk indextáblázatot.

107. Oldjuk meg az alábbi kongruenciákat:

(a) $17x \equiv 10 \pmod{29}$;

(b) $17x^2 \equiv 10 \pmod{29}$;

(c) $17x^2 - 3x + 10 \equiv 0 \pmod{29}$;

(d) $17x^2 - 4x + 10 \equiv 0 \pmod{29}$.

108. Melyik az a legkisebb pozitív egész, amelyre $p - 1 \mid s \cdot \operatorname{ind}_p a$?

109. Legyen $n > 1$ természetes szám és p prímszám, amelyekre $p > \dfrac{3^{2^n} - 1}{2^n}$ teljesül és $2^n p + 1$ prímszám. Mutassuk meg, hogy 3 primitív gyök modulo $2^n p + 1$.

110. Legyen p prímszám és M egész szám. A $p - 1$ egész szám különböző prímosztóinak a száma legyen k. Mutassuk meg, hogy ha $p > 4 \left(\dfrac{p-1}{\varphi(p-1)} \right)^2 \cdot 2^{2k}$, akkor az

$$M, M+1, \ldots, M + 2 \left[\frac{p-1}{\varphi(p-1)} 2^{2k} \sqrt{p} \right] - 1$$

sorozatban található modulo p primitív gyök.