Primitív gyök, diszkrét logaritmus, gyökvonás mod p

Összefoglaló: Végig $p > 2$ prím és $(c, p) = 1$.

g primitív gyök mod $p \iff o_p(g) = p - 1 \iff 1, g, g^2, \ldots, g^{p-2}$ redukált maradékrendszer mod p. Ekkor $g^r \equiv g^t \pmod p \iff r \equiv s \pmod{p-1}$.

Index def: $\operatorname{ind}_g c = s$, ha $g^s \equiv c \pmod p$ és $0 \le s \le p-2$.

$x^k \equiv c \pmod p$ megoldható $\iff c^{(p-1)/(k,p-1)} \equiv 1 \pmod p \iff (k, p-1) \mid \operatorname{ind}_g c$. A kongruencia "logaritmálással" egy lineáris kongruenciára vezethető vissza. A megoldások száma $(k, p-1)$.

10. Adjunk meg egy-egy primitív gyököt modulo (a) 11; (b) 17; (c) 23. Van-e olyan szám, amely egyszerre primitív gyök mindhárom modulusra?

11. Igaz vagy hamis? ($p > 2$ rögzített prím.)
(a) Ha g primitív gyök, akkor g^3 is az.
(b) Ha g^3 primitív gyök, akkor g is az.
(c) Ha g primitív gyök, akkor kvadratikus nem-maradék.
(d) Ha g kvadratikus nem-maradék, akkor primitív gyök.
(e) Ha $p = 257$ és g kvadratikus nem-maradék, akkor primitív gyök.

12. Adjunk új bizonyítást a Wilson-tételre a primitív gyök segítségével.

13. Mennyi $1^k + 2^k + \ldots + p^k$ maradéka mod p?

14. Készítsünk indextáblázatot mod (a) 11; (b) 17.

15. $\operatorname{ind}_g 1 + \operatorname{ind}_g 2 + \ldots + \operatorname{ind}_g (p-1) =?$

16. Számítsuk ki: (a) $\operatorname{ind}_g 1$; (b) $\operatorname{ind}_g (-1)$; (c) $\operatorname{ind}_2 3 \bmod 11$; (d) $\operatorname{ind}_3 6 \bmod 17$.

17. Fogalmazzuk meg és bizonyítsuk be a szorzat és hatvány logaritmusára vonatkozó azonosságok indexes megfelelőit.

18. Oldjuk meg: (a) $3x^4 \equiv 5 \pmod{11}$; (b) $3x^{700} \equiv 5 \pmod{71}$; (c) $3x^{699} \equiv 5 \pmod{71}$; (d) $x^{24} \equiv 1 \pmod{107}$.

19. Bizonyítsuk be, hogy ha $p = 4n + 3$ alakú prím és az $x^2 \equiv c \pmod p$ kongruencia megoldható, akkor az $x^4 \equiv c \pmod p$ kongruencia is megoldható. Mi a helyzet $p = 4n + 1$ esetén?