Bsc Algebra és számelmélet gyakorlat

A 28. előadás-diához tartozó feladatsor

1. Határozzuk meg az alábbi elemrendeket: $o_7(2)$, $o_7(3)$, $o_{17}(3)$, $o_{128}(5)$, $o_{25}(2)$, $o_{100}(3)$.

2. Adjunk meg olyan egész számot, ami egyszerre primitív gyök modulo 11 és modulo 14 is.

3. Keressünk primitív gyököt mod 23, készítsünk logaritmus-táblázatot, majd oldjuk meg a $11x^{17} \equiv 3\ (23)$ és a $4 \cdot 9^x \equiv 16\ (23)$ kongruenciákat.

4. Hány megoldása van az $x^{18} \equiv 6\ (29)$ kongruenciának?

5. Mely p prímszámokra és k és a természetes számokra teljesül, hogy az $x^k \equiv a\ (p)$ kongruenciának pontosan $p-2$ megoldása van?

6. Számítsuk ki az alábbi Jacobi-szimbólumokat:

$$\left(\frac{-99}{207}\right); \quad \left(\frac{1234567}{225}\right); \quad \left(\frac{31}{95}\right); \quad \left(\frac{589}{1999}\right); \quad \left(\frac{1113}{11131}\right).$$

7. Bizonyítsuk be, hogy ha a rendje 3 modulo p (prím), akkor $a+1$ rendje 6.

8. ***(*)*** Legyen $p > 2$ prím és $(a,p) = 1$. Igazoljuk, hogy $o_p(a)$ pontosan akkor páros, ha létezik olyan s, amelyre $a^s \equiv -1\ (p)$.

9. Igazoljuk az elemrend felhasználásával is, hogy $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

10. Legyenek $1 < a, n$ egészek. Igazoljuk, hogy $n \mid \varphi(a^n - 1)$.

11. Adjunk meg egy primitív gyököt modulo 625 és egy olyan számot is, ami modulo 5 primitív gyök, de modulo 625 nem.

12. ***(*)*** Legyen $\alpha \geq 3$. Igazoljuk, hogy $o_{2^\alpha}(5) = 2^{\alpha-2}$. Továbbá mutassuk meg, hogy a $\{\pm 5^k \mid 0 \leq k < 2^{\alpha-2}\}$ számok redukált maradékrendszert alkotnak modulo 2^α.

13. Oldjuk meg az alábbi kongruenciákat:

(1) $3x^2 + 5x + 5 \equiv 0\ (13)$;
(2) $7x^2 + 8x \equiv 5\ (17)$;
(3) $6x^{25} + x^5 + 5x \equiv 0\ (23)$;
(4) $2x^{17} + 5x + 1 \equiv 0\ (19)$.

14. ***(*)*** Számítsuk ki az

$$\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)$$

Legendre-szimbólumok összegét és szorzatát.

15. ***(*)*** Bizonyítsuk be, hogy ha $1999 \mid a^2 + 2b^2$, akkor $1999 \mid a$ és $1999 \mid b$.

16. ***(**)*** Igazoljuk, hogy $1 + a + a^2 + a^3 + a^4 + a^5 + a^6$ minden prímosztója 7 vagy $7k+1$ alakú. Vezessük le ebből, hogy végtelen sok $7k+1$ alakú prím van.

17. ***(*)*** Igaz-e, hogy egy pitagoraszi számhármas három tagjának a szorzata mindig osztható 60-nal?