Bsc Algebra és számelmélet gyakorlat

A 11. és 12. előadás-diához tartozó feladatsor

1. Egy szigeten 7- és 11-fejű sárkányok élnek. Egy királyfi le akarta győzni az összeset, ezért megszámolta, hány feje van a sárkányoknak összesen (hogy tudja, mire vállalkozik).

(1) Hány sárkány van, ha 75 fejet számolt?
(2) 59 fejet számolt. Igazoljuk, hogy elszámolta.
(3) Most számolás előtt levágta az összes sárkánynak 1-1 fejét és ezután 40 fejet számolt. Hány sárkány lehetett összesen?

2. Oldjuk meg az alábbi kongruenciákat: $3x \equiv 5\ (17)$; $19^{39}x \equiv 7\ (100)$; $26x \equiv 5\ (65)$.

3. Melyik az a legkisebb természetes szám, amely 2-vel osztva 1, 3-mal osztva 2, 5-tel osztva 4, 7-tel osztva 6 maradékot ad?

4. Határozzuk meg 2^{1526} maradékát mod 17.

5. Határozzuk meg $777777^{7654321}$ utolsó két számjegyét.

6. Tegyük fel, hogy $11 | a^{100} + b^{100} + c^{100}$. Igazoljuk, hogy $11^{100} | a^{100} + b^{100} + c^{100}$.

7. Bizonyítsuk be, hogy $n^8 - 1$, n^8 és $n^8 + 1$ valamelyike osztható 17-tel.

8. Igazoljuk, hogy az $x^{12} + y^{24} - z^{36} = t^{48} + 3$ diofantikus egyenletnek nincs megoldása.

9. Redukált maradékrendszert alkot-e a $\{15, 35, 55, \dots, 315\}$ halmaz mod 32?

10. Adjunk meg egy-egy teljes maradékrendszert mod 11, amely csupa páros számból, illetve csupa prímszámból áll.

11. ***(*)*** Legyen m páros, és $a_1, a_2, \dots, a_m$ illetve $b_1, b_2, \dots, b_m$ egy-egy teljes maradékrendszer mod m. Igazoljuk, hogy $a_1 + b_1, a_2 + b_2, \dots, a_m + b_m$ nem teljes maradékrendszer mod m.

12. Az $1, 2, \dots, 2n$ számok közül maximum hány választható ki úgy, hogy bármely kettő nem relatív prím?

13. Igazoljuk, hogy ha m prím, akkor a kongruenciákból négyzetgyököt vonhatunk: ha $a^2 \equiv b^2\ (m)$, akkor $a \equiv b$ vagy $a \equiv -b$ mod m. Igaz-e ez minden összetett m modulusra?

14. Hány nullára végződik a 100! szám?

15. Oldjuk meg az $x^{1000} + 2y^{1000} = 5z^{1000}$ diofantikus egyenletet.

16. Milyen maradékot adhat 5-tel osztva $1^k + 2^k + 3^k + 4^k$? Bizonyítsuk be, hogy ha k és n tetszőleges páratlan számok, akkor $1^k + 2^k + \cdots + (n-1)^k$ osztható n-nel.

17. ***(*)*** Mi az utolsó két számjegye $73^{73} + 37^{37}$-nek?

18. Mutassuk meg, hogy minden $n > 2$-re $\varphi(n)$ páros.

19. ***(**)*** Igazoljuk, hogy ha p prím és $a^p \equiv b^p\ (p)$, akkor $a^p \equiv b^p\ (p^2)$.

20. ***(*)*** Bizonyítsuk be, hogy 561 álprím, azaz nem prímszám, mégis teljesül rá a kis-Fermat tétel: $\forall a$-ra: $a^{561} \equiv a\ (561)$.

21. ***(*)*** Legyen p egy prímszám, $r_1, \dots, r_p$ pedig egy teljes maradékrendszer mod p. Igazoljuk, hogy $r_1^{2p-3}, \dots, r_p^{2p-3}$ is teljes maradékrendszer mod p.

22. ***(**)*** Igazoljuk, hogy $n^2 + 1$ alakú szám minden páratlan osztója $4k + 1$ alakú. Mutassuk meg, hogy végtelen sok $4k + 1$ alakú prím van.