Bsc Algebra és számelmélet gyakorlat

A 11. és 12. előadás-diákhoz tartozó feladatsor feladatainak megoldásai

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?

□

Az első kérdésben az egyenlet $7x+11y = 75$. A megoldás során kifejezzük azt az ismeretlent, amelynek az együtthatója kisebb abszolút értékű: $x = (75 - 11y)/7$, majd elvégezzük a maradékos osztást: $11 = 7 * 2 - 3$. *Fontos:* azt az osztást választottuk, ahol a maradék abszolút értéke a lehető legkisebb, tehát nem azt, ahol a maradék 4 (mert így az eljárás gyorsabban véget ér). Az eredmény $x = 11 - 2y + (-2 + 3y)/7$. Ekkor $z = (-2 + 3y)/7$ is egész szám, megismételjük az eljárást: $7z - 3y = -2$, tehát $y = 2z + 1 + (z - 1)/3$. Így $u = (z - 1)/3$, ahonnan $z = 3u + 1$. A maradékos osztás véget ért, most u segítségével kifejezzük a korábbi ismeretleneket: $y = 2z + 1 + u = 2(3u + 1) + 1 + u = 7u + 3$, végül $x = 11 - 2y + z = 6 - 11u$. Ellenőrzés: $7(6 - 11u) + 11(7u + 3) = 75$ tényleg azonosság. Mivel a feladat szerint $x, y \geq 0$, ezért $6 \geq 11u$ és $7u \geq -3$. Innen $u = 0$, $x = 6$, $y = 3$.

A második kérdés egyenlete $7x+11y = 59$. Hasonlóan számolva $x = 10-11u$ és $y = 7u-1$. Tehát $u \leq 10/11 < 1$ és $u \geq 1/7 > 0$, így nincs megoldás.

A harmadik kérdés esetében az egyenlet $6x + 10y = 40$, azaz $3x + 5y = 20$. Itt rögtön látszik, hogy $x = 5z$, ahonnan $3z + y = 4$, tehát $y = 4 - 3z$ és $x = 5z$ az általános megoldás, nem kellett használni az algoritmust. Két megoldás van: $(x, y) = (0, 4) = (5, 1)$. (Vitatható, hogy a feladat szövege megengedi-e az első megoldást, amikor nincs 7 fejű sárkány.)

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

A $3x \equiv 5\ (17)$ egy *lineáris kongruencia,* azt jelenti, hogy $17 \mid 3x - 5$. Visszavezethetjük az előző feladatban tanult *lineáris diofantikus egyenletre,* ha ezt az oszthatóságot $17y = 3x - 5$ formában írjuk. A fenti algoritmussal megoldva $y = 5 - 3z$ és $x = 30 - 17z$.

A harmadik kongruencia a $26x - 65y = 5$ egyenletre vezet. Ennek nincs megoldása, mert a bal oldal osztható 13-mal a jobb pedig nem. Ha ezt nem vesszük észre, és elvégezzük az algoritmust, akkor az $x = 2y+(13y+5)/26$, majd az $y = 2z-(5/13)$ ellentmondásra jutunk (hiszen y és $2z$ is egész szám, de $5/13$ nem).

Összefoglalva: Az $ax + by = c$ egyenlet pontosan akkor oldható meg, ha $(a, b) \mid c$, az $ax \equiv b\ (m)$ kongruencia pedig ha $(a, m) \mid b$. Utóbbi általános megoldása $x = d + um/(a, m)$ alakú lesz, ahol u tetszőleges egész. Ez egy $a/(a, m)$ szerinti *maradékosztály.*

A $19^{39}x \equiv 7\ (100)$ esetében először ki kellene számolnunk 19^{39} maradékát 100-zal osztva, vagyis a két utolsó számjegyét. De az Euler–Fermat-tétel szerint $19^{40} \equiv 1\ (100)$, mert $\varphi(100) = 40$. Ezért szorozzuk be az eredeti kongruenciát 19-cel: $x \equiv 19^{40}x \equiv 133 \equiv 33\ (100)$.

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? □

Az $x \equiv 4\ (5)$ és $x \equiv 6\ (7)$ kongruenciarendszert megoldhatjuk úgy, hogy mindkettőt átírjuk diofantikus egyenletre: $x = 5y + 4$, illetve $x = 7z + 6$, majd megoldjuk az $5y + 4 = 7z + 6$ egyenletet. A megoldás $z = 5v - 1$, ahonnan $x = 35v - 1$. Vagyis az utolsó két feltétel helyettesíthető az $x \equiv -1\ (35)$ kongruenciával. Ezt ismételhetjük, két kongruenciát mindig eggyel helyettesítve. A végső megoldás $x \equiv -1\ (210)$, a legkisebb ilyen pozitív szám a 209.

Általában az $x \equiv a\ (m)$ és $x \equiv b\ (n)$ *szimultán kongruenciarendszer* pontosan akkor oldható meg, ha $(m, n) \mid b - a$, és a megoldás egy maradékosztály mod $[m, n]$ (azaz m és n legkisebb közös többszöröse). A *kínai maradéktétel* szerint ha az $m_1, \ldots, m_k$ számok páronként relatív prímek, akkor az $x \equiv a_i\ (m_i)$ rendszernek mindig egyetlen megoldása van modulo $m_1 m_2 \ldots m_k$. Mivel $2, 3, 5, 7$ páronként relatív prím, ezért már a tételből tudjuk, hogy a kongruenciarendszernek egyetlen megoldása van modulo 210. És mivel a -1 mindegyik kongruenciának megoldása, minden számolás nélkül látjuk, hogy $x \equiv -1\ (210)$ a megoldás.

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

A 2 hatványai nyolcasával periodikusak mod 17, ezért az eredmény 13.

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

Az Euler–Fermat-tétel miatt $77^{40} \equiv 1\ (100)$. Mivel $7654321 \equiv 1\ (40)$, ezért az eredmény 77.

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

Az Euler–Fermat miatt $(x, 11) = 1$ esetén $x^{10} \equiv 1\ (11)$, hiszen $\varphi(11) = 10$. Ha meg $(x, 11) \neq 1$, akkor $11 \mid x$, hiszen 11 prímszám. Ezért $x^{100} = (x^{10})^{10}$ maradéka 0 vagy 1 lehet, a háromtényezős összegé pedig 0, 1, 2 vagy 3. De 0 csak akkor, ha a, b, c mindegyike 0-t ad. Így mindhárom szám osztható 11-gyel és ezért 11^{100} osztja a 100-adik hatványukat.

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

Ha $17 \mid n$, akkor $17 \mid n^8$. Ha nem, akkor $17 \mid n^{16} - 1 = (n^8 + 1)(n^8 - 1)$ az Euler–Fermat miatt. Mivel 17 prím, valamelyik tényezőnek osztója.

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

Az Euler–Fermat miatt x^{12} maradéka 0 vagy 1 lehet mod 13, és ezért a hatványainak is. Vagyis az egyenletben mind a négy ismeretlent tartalmazó tag 0 vagy 1 mod 13.

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

Nem, $15 + 8 \cdot 20 = 175$ és 15 kongruensek mod 32. Az kellene, hogy $(20, 32) = 1$ legyen.

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

$0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20$, illetve $3, 5, 7, 11, 13, 17, 23, 31, 37, 41, 43$.

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

Kiválasztható így n darab: a párosak. Ennél több nem, mert akkor lenne két szomszédos.

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

Ha m prím és $m \mid a^2 - b^2 = (a-b)(a+b)$, akkor valamelyik tényezőnek osztója. Összetett modulusra nem mindig igaz, pl. $4^2 \equiv 1^2\ (15)$, de $4 \not\equiv 1\ (15)$ és $4 \not\equiv -1\ (15)$.

14. Hány nullára végződik a 100! szám? □

Lagrange képlete szerint az 5 kitevője $[100/5]+[100/25]+[100/125]+\ldots = 24$. A 2 kitevője ennél nyilvánvalóan nagyobb, ezért az eredmény 24.

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

Az Euler–Fermat miatt a^{10} (és így a^{1000}) maradéka 0 vagy 1 mod 11. Ezért az egyenlet csak úgy teljesülhet, ha $11 \mid x, y, z$. De akkor 11^{1000}-nel egyszerűsítve ugyanilyen egyenletet kaptunk. Ezt végtelen sokszor megtehetjük, és így $x = y = z = 0$ az egyetlen megoldás.

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. □

Az Euler–Fermat miatt $a^i \equiv a^{i+4}\ (5)$, így az első kérdésnél elég a $0, 1, 2, 3$ kitevőket nézni, a válasz rendre $4, 0, 0, 0$. A másodiknál párosítsuk j^k-t $(n-j)^k$-nal, ezek összege osztható $j + (n-j)$-vel, mert k páratlan. Mindenkinek van tőle különböző párja, mert n páratlan.

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

Párosítsuk a d számot $n-d$-vel, ahol $1 \le d < n$. Ekkor $1 \le n-d < n$ és $(d, n) = 1$ akkor és csak akkor, ha $(n-d, d) = 1$. Ha d párja önmaga, akkor $n = 2d$, és így ha d relatív prím n-hez, akkor $n = 2$. Továbbá $n > 1$ esetén n nem relatív n-hez, ezért $\varphi(n)$ definíciójában elég az n-nél kisebb pozitív számokat nézni. Így $n > 2$ esetén $\varphi(n)$ tényleg páros.

Második megoldás: a $\varphi(n)$ képlete szerint ha egy p páratlan prím osztója n-nek, akkor a (páros) $p - 1 \mid \varphi(n)$. Ha pedig $n = 2^k$, és $k \ge 2$, akkor $\varphi(n) = 2^{k-1}$ páros.

---

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

Teljes maradékrendszer elemeinek összege $\equiv (m/2)\ (m)$ (párosítsuk az elemeket a mod m ellentettjükkel). De akkor az $(m/2) + (m/2) \equiv (m/2)\ (m)$ ellentmondást kapjuk.

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

A végeredmény 50. A szám $4k+2$ alakú, mert $73 \equiv 1\ (4)$ és $37 \equiv 1\ (4)$, ezért elég megmutatni, hogy 25-tel osztható. Mod 25 vizsgálódva, ha $5 \nmid a$, akkor $a^{20} \equiv 1$, hiszen $\varphi(25) = 20$. Speciálisan $1 \equiv 37^{40} = 37^{37} \cdot 37^3$. Mivel $37 \cdot 2 \equiv -1$, ezért az előzőt $(-2)^3$-nel szorozva $-8 \equiv 37^{37} \cdot 1^3$. Másrészt $1 \equiv 73^{80} = 73^{73} \cdot 73^7$ és $73^7 \equiv (-2)^7 = -127 \equiv -3$. Ezt 8-cal szorozva 1-et kapunk mod 25, ezért $8 \equiv 73^{73} \cdot 1$. Így $37^{37} + 73^{73} \equiv -8 + 8 = 0$.

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

$561 = 3 \cdot 11 \cdot 17$, és ezek páronként relatív prímek, ezért elég belátni, hogy $a^{561} \equiv a \bmod 3$, 11 és 17. Mod 11 vizsgálva: ha $11 \mid a$, akkor teljesül; ha $11 \nmid a$, akkor $a^{10} \equiv 1\ (11)$, tehát $561 \equiv 1\ (10)$ miatt teljesül. A másik két modulusra is igaz, mert $3-1, 17-1 \mid 561-1$.

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. □

Ha $r_i^{2p-3} \equiv r_j^{2p-3} \not\equiv 0\ (p)$, akkor $r_i r_j$-vel szorozva $r_j \equiv r_i^{2p-2} r_j \equiv r_j^{2p-2} r_i \equiv r_i\ (p)$, hiszen az Euler–Fermat miatt $r \not\equiv 0\ (p) \implies r^{p-1} \equiv 1\ (p)$. A 0 maradék pedig csak egyszer szerepel.

---

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

A kis-Fermat miatt $a \equiv a^p \equiv b^p \equiv b\ (p)$. Ezért $b = a + pk$. A binomiális tételt $(a+pk)^p$-re felírva kapjuk, hogy $b^p \equiv a^p + \binom{p}{1} a^{p-1}(pk)\ (p^2)$ (a többi tagban $(pk)^m$ szerepel, ahol $m \geq 2$).

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

Legyen p páratlan prímosztója n^2+1-nek, ekkor $n^2 \equiv -1\ (p)$. Ezt $(p-1)/2$-edikre emelve $n^{p-1} \equiv (-1)^{(p-1)/2}\ (p)$. Az Euler–Fermat miatt $n^{p-1} \equiv 1\ (p)$. Mivel $1 \not\equiv -1\ (p)$, ezért $(-1)^{(p-1)/2} = 1$, azaz $(p-1)/2$ páros, és így $4 \mid p-1$. (Hasonlóan igazolhatjuk, hogy ha p páratlan prímosztója a^2+b^2-nek, akkor $p \equiv 1\ (4)$, vagy $p \mid a$ és $p \mid b$. Ezért két négyzetszám összegében minden $4k-1$ alakú prím páros kitevőn szerepel.)

Ha csak véges sok $4k+1$ alakú prím lenne, ezek $p_1, \dots, p_k$, akkor az $N = 4(p_1 \dots p_k)^2+1 > 1$ számnak nem lehetne prímosztója, ami ellentmondás.