Bevezetés a számításelméletbe II.
MEGOLDÁSOK
10. gyakorlat: Kongruencia, Euler-Fermat tétel

1. A $3, 8, 17, -17, 120, 54, -40, 236, 227$ számok
   (a) legkisebb nem negatív maradékai sorrendben:$3, 8, 6, 5, 10, 10, 4, 5, 7$
   (b) abszolutértékben legkisebb maradékai sorrendben:$3, -3, -5, 5, -1, -1, 4, 6, -4$
   (c) így $-17 \equiv 236$ és $120 \equiv 54 \pmod{11}$.

2. A lineáris kongruenciák megoldásai:
   (a) $(11, 18) = 1$, $\exists$ 1db mo.
   $11x \equiv 12 \pmod{18} / \cdot 5$
   $55x \equiv 60 \pmod{18}$
   $x \equiv 6 \pmod{18}$
   (b) $(5, 35) = 5 \mid 5$, $\exists$ 5db mo.
   $5x \equiv 5 \pmod{35} / : 5$
   $x \equiv 1 \pmod 7$, ebből
   $x \equiv 1, 8, 15, 22, 29 \pmod{35}$
   (c) $(6, 35) = 1$, $\exists$ 1db mo.
   $6x \equiv 5 \pmod{35} / \cdot 6$
   $36x \equiv 30 \pmod{35}$
   $x \equiv 30 \pmod{35}$
   (d) $(7, 35) = 7 \nmid 5$, $\nexists$ mo.
   (e) $6x + 1 \equiv 10 \pmod{15} / - 1$
   $6x \equiv 9 \pmod{15}$
   $(6, 15) = 3 \mid 9$, $\exists$ 3db mo.
   $6x \equiv 9 \pmod{15} / : 3$
   $2x \equiv 3 \pmod 5 / \cdot 3$
   $6x \equiv 9 \pmod 5$
   $x \equiv 4 \pmod 5$, ebből
   $x \equiv 4, 9, 14 \pmod{15}$
   (f) $14x - 4 \equiv 80 \pmod{21}$
   $14x \equiv 84 \pmod{21} / + 4$
   $(14, 21) = 7 \mid 84$, $\exists$ 7db mo.
   $14x \equiv 84 \pmod{21} / : 7$
   $2x \equiv 12 \pmod 3$
   $2x \equiv 0 \pmod 3$
   $x \equiv 0 \pmod 3$, ebből
   $x \equiv 0, 3, 6, 9, 12, 15, 18 \pmod{21}$

3. A lineáris kongruenciák megoldása:
   (a) $202x \equiv 157 \pmod{203} / - 203x$
   $-x \equiv 157 \pmod{203} / \cdot (-1)$
   $x \equiv -157 \pmod{203} / + 203$
   $x \equiv 46 \pmod{203}$
   (b) $309x \equiv 451 \pmod{617} / \cdot 2$
   $618x \equiv 902 \pmod{617}$
   $x \equiv 285 \pmod{617}$
   (c) $5x \equiv 561 \pmod{1968} / + (3 \cdot 1968)$
   $5x \equiv 6465 \pmod{1968} / : 5$
   $x \equiv 1293 \pmod{1968}$
   (d) $105x \equiv 761 \pmod{809} / + 809$
   $105x \equiv 1570 \pmod{809} / : 5$
   $21x \equiv 314 \pmod{809} / + (2 \cdot 809)$
   $21x \equiv 1932 \pmod{809} / : 21$
   $x \equiv 92 \pmod{809}$

4. A szimultán kongruenciák megoldásai:
   (a) $x \equiv 3 \pmod 5$-ből $x = 5k + 3$
   így: $5k + 3 \equiv 4 \pmod 7$
   $5k \equiv 1 \pmod 7 / \cdot 3$
   $15k \equiv 3 \pmod 7 / \cdot 3$
   $k \equiv 3 \pmod 7$-ből $k = 7l + 3$
   így $x = 5(7l + 3) + 3 = 35l + 18$
   vagyis $x \equiv 18 \pmod{35}$
   (b) nem oldható meg.
   (c) $3x \equiv 2 \pmod 4 / \cdot 3$
   $x \equiv 2 \pmod 4$ből $x = 4k + 2$
   $2x \equiv 3 \pmod 5 / \cdot 3$
   $x \equiv 4 \pmod 5$
   így: $4k + 2 \equiv 4 \pmod 5 / - 2$
   $4k \equiv 2 \pmod 5 / - 5k$
   $-k \equiv 2 \pmod 5 / \cdot (-1)$
   $k \equiv 3 \pmod 5$-ből $k = 5l + 3$
   így $x = 4(5l + 3) + 2 = 20l + 14$
   vagyis $x \equiv 14 \pmod{20}$
   (d) nem oldható meg.

5. Oldjuk meg a megoldhatóakat az alábbi lineáris diofantikus egyenletek közül!
   (a) $15x + 13y = 19$-el ekvivalens:
   $15x \equiv 19 \pmod{13}$
   $2x \equiv 6 \pmod{13} / : 2$
   $x \equiv 3 \pmod{13}$,
   vagyis $x = 13t + 3$,
   ebből $t = 0$-ra $y_0 = -2$
   így $y = -2 - 15t$
   (b) $17x + 11y = 22$-el ekvivalens:
   $17x \equiv 22 \pmod{11}$
   $x \equiv 0 \pmod{11}$,
   vagyis $x = 11t$,
   ebből $t = 0$-ra $y_0 = 2$
   így $y = 2 - 17t$
   (c) $12x + 30y = 26 / : 2$
   $3(2x + 5y) \neq 13$, nincs megoldás.
   (d) $18x + 28y = 10 / : 2$
   $9x + 14y = 5$-el ekvivalens:
   $9x \equiv 5 \pmod{14} / \cdot 3$
   $27x \equiv 15 \pmod{14}$
   $-x \equiv 1 \pmod{14} / \cdot (-1)$
   $x \equiv -1 \pmod{14}$,
   vagyis $x = 14t - 1$,
   ebből $t = 0$-ra $y_0 = 1$
   így $y = 1 - 9t$

6. A prímtényezős felbontásokból behelyettesítve a képletekbe:

   (a) $12 = 2^2 \cdot 3$-ból:
   $d(12) = (2+1)(1+1) = 6$,
   $\phi(12) = (2^2-2)(3-1) = 4$,
   $\sigma(12) = (1+2+2^2)(1+3) = 28$

   (b) $2004 = 2^2 \cdot 3 \cdot 167$-ből:
   $d(2004) = (2+1)(1+1)(1+1) = 12$,
   $\phi(2004) = (2^2-2)(3-1)(167-1) = 664$,
   $\sigma(2004) = (1+2+2^2)(1+3)(1+167) = 4704$

7. $9 = 3^2$, $133 = 7 \cdot 19$, $540 = 2^2 \cdot 3^3 \cdot 5$, $7! = 2^4 \cdot 3^2 \cdot 5$
   $\phi(9) = 3^2 - 3 = 6$,
   $\phi(133) = \phi(7)\phi(19) = 6 \cdot 18 = 108$,
   $\phi(540) = (2^2-2)(3^3-3^2)(5-1) = 144$,
   $\phi(7!) = (2^4-2^3)(3^2-3)(5-1) = 192$.

8. $\phi(n)$ páratlan, akkor és csak akkor, ha minden $(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ tényező páratlan. Ez csak $p_i = 2$ első hatványára lehet páratlan. Tehát csak $n = 2$ lehet megoldás.
   $d(n)$ páratlan, akkor és csak akkor, ha minden $(\alpha_i + 1)$ tényező páratlan, vagyis α_i páros. Ez azt jelenti, hogy n négyzetszám.

9. Az Euler-Fermat tételt használva,

   (a) $n^{11} + 10n = n^{10}n + 10n \equiv n + 10n = 11n \equiv 0 \pmod{11}$,

   (b) $n^{16} \equiv 1 \pmod{17}$-ből következik, hogy $17 \mid n^{16} - 1 = (n^8+1)(n^8-1)$. Mivel 17 prím, ezért vagy $p \mid (n^8+1)$ vagy $p \mid (n^8-1)$.

   (c) $108^{182} = (5 \cdot 19 + 13)^{182} \equiv 13^{182} = 13^{18 \cdot 10 + 2} = (13^{18})^{10} \cdot 13^2 \equiv 13^2 = 169 \equiv 17 \pmod{19}$
   $5^{17} = 5^{18} \cdot 5^{-1} \equiv 5^{-1} \equiv 4 \pmod{19}$

   (d) $42 \mid n^7 - n$-hez belátjuk, hogy $2 \mid n^7 - n$, $3 \mid n^7 - n$ és $7 \mid n^7 - n$. Az első kettő egyszerű oszthatósági feltételek következménye, az utolsó pedig a kis-Fermat tétel.

10. Az Euler-Fermat tételt használva...

    (a) $39^{14} = (7 \cdot 5 + 4)^{14} \equiv 4^{14} = 4^{3 \cdot 4 + 2} \equiv 4^2 = 16 \equiv 1 \pmod{5}$

    (b) $333^{444} + 444^{333} = (7 \cdot 47 + 4)^{444} + (7 \cdot 63 + 3)^{333} \equiv 4^{444} + 3^{333} = 4^{6 \cdot 74} + 3^{330+3} \equiv 1 + 3^3 = 28 \equiv 0 \pmod{7}$

    (c) $4^{90} = 4^{2 \cdot 45} = 16^{45} = (17-1)^{45} \equiv (-1)^{45} = -1 \pmod{17}$

11. $\phi(49) = 7^2 - 7 = 42$.
    Így az Euler-Fermat tétel miatt:
    $(((43)^{43})^{43})^{43} = (((43)^{42+1})^{43})^{43} \equiv (((43)^1)^{43})^{43} = ((43)^{43})^{43} \equiv \cdots \equiv 43 \pmod{49}$.

12. Felhasználva, hogy $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$ és $\phi(100) = (2^2-2)(5^2-5) = 40$:

    (a) $49^{49} = (45+4)^{49} \equiv 4^{49} = 4^{6 \cdot 8 + 1} \equiv 4 \pmod{15}$,

    (b) $3^{80} = (3^{40})^2 \equiv 1 \pmod{100}$ miatt $x \equiv 23 \pmod{100}$

13. Felhasználva, hogy
    $\phi(1000) = (2^3-2^2)(5^3-5^2) = 400$,
    $\phi(100) = (2^2-2)(5^2-5) = 40$ és
    $\phi(10) = (2-1)(5-1) = 4$:

    (a) $403^{402} = 403^{400+2} \equiv 403^2 \equiv 409 \pmod{1000}$

    (b) $29^{39^{49}} = 29^{40-1^{49}} \equiv 29^{-1^{49}} = 29^{-1} \equiv 69 \pmod{100}$

    (c) $7^{6^{5^{4^{3^2}}}} = 7^{4k} \equiv 1 \pmod{10}$.

14. Mindkét állítás egyszerű oszthatósági megfontolások következménye:

    (a) Ha $2^m + 1$ prím, akkor m 2-hatvány. Tegyük fel, hogy nem így van, tehát $m = 2^n k$, ahol k páratlan szám. Ekkor $2^{2^n} + 1$ osztja $(2^{2^n})^k + 1$-et.

    (b) Ha $2^p - 1$ prím, akkor p prím. Tegyük fel, hogy nem az, vagyis $\exists\ 1 < a, b < p$ egészek, hogy $a \cdot b = p$. Ekkor $2^{a \cdot b} - 1$ osztható $2^a - 1$-el.