Diszkrét matematika II. feladatok

Kiegészítő feladatok — öt-és-feledik alkalom :)

Lineáris kongruenciarendszerek megoldása — Kínai maradéktétel (Szun Ce tétele) segítségével

1. Oldjuk meg a következő kongruenciarendszereket:

e) $\begin{cases} 5x \equiv 2 \mod 6 \\ 7x \equiv 3 \mod 10 \end{cases}$ b) $\begin{cases} 5x \equiv 3 \mod 7 \\ 3x \equiv 7 \mod 8 \end{cases}$ c) $\begin{cases} 3x \equiv 2 \mod 4 \\ 4x \equiv 3 \mod 5 \end{cases}$ d) $\begin{cases} 5x \equiv 1 \mod 6 \\ 7x \equiv 9 \mod 10 \end{cases}$

a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 1 \mod 5 \end{cases}$ f) $\begin{cases} 4x \equiv 2 \mod 3 \\ 3x \equiv 2 \mod 7 \\ 9x \equiv 7 \mod 11 \end{cases}$ g) $\begin{cases} 3x \equiv 1 \mod 4 \\ 7x \equiv 2 \mod 9 \\ 9x \equiv 3 \mod 13 \end{cases}$ h) $\begin{cases} 5x \equiv 3 \mod 6 \\ 3x \equiv 9 \mod 10 \\ 8x \equiv 9 \mod 15 \end{cases}$

Megoldások: Mindig meg kell vizsgálni, hogy a modulusok *páronként* relatív prímek-e, és ha nem, akkor előbb helyettesíteni kell az egyes kongruenciákat a velük ekvivalens (több kongruenciából álló) rendszerrel.

a) $\begin{cases} x \equiv 2 \mod 3 & \gcd(3,4)=1 \\ x \equiv 3 \mod 4 & \gcd(4,5)=1, \\ x \equiv 1 \mod 5 & \gcd(5,3)=1 \end{cases}$ tehát közvetlenül alkalmazható a kínai maradéktétel.

$3 \cdot (-1) + 4 \cdot (1) = 1$, $c_{1,2} = 3 \cdot (-1) \cdot 3 + 4 \cdot (1) \cdot 2 = -1$ az első két kongruenciának egy közös megoldása, így az első kettő kongruencia helyettesíthető $x \equiv -1 \pmod{12}$ kongruenciával. $\begin{cases} x \equiv -1 \mod 12 \\ x \equiv 1 \mod 5 \end{cases}$ $\begin{matrix} -1 \equiv 11 \pmod{12} \\ 1 \equiv 11 \pmod{5} \end{matrix}$ vagyis: $\begin{cases} x \equiv 11 \mod 12 \\ x \equiv 11 \mod 5 \end{cases}$ tehát $x = 11$ egy közös megoldása a két kongruenciának. Így az összes közös megoldás $x \equiv 11 \mod 60$.

Megjegyzés: Ha nem jöttünk volna rá, hogy $-1 \equiv 11 \pmod{12}$ és $1 \equiv 11 \pmod{5}$, akkor is meg tudtuk volna oldani: $12 \cdot (-2) + 5 \cdot (5) = 1$, $c_{1,2,3} = 12 \cdot (-2) \cdot 1 + 5 \cdot (5) \cdot (-1) = -49$ egy közös megoldás, tehát $x \equiv -49 \pmod{60}$, vagyis $x \equiv -49 + 60 \equiv 11 \pmod{60}$.

b) $\begin{cases} 5x \equiv 3 \mod 7 \\ 3x \equiv 7 \mod 8 \end{cases}$ $\gcd(7,8)=1$, tehát közvetlenül alkalmazható a kínai maradéktétel. De előtte külön-külön meg kell oldani az egyes kongruenciákat.

$\begin{cases} 5x \equiv 3 \mod 7 \iff 5x \equiv 10 \mod 7 \iff x \equiv 2 \mod 7 \\ 3x \equiv 7 \mod 8 \iff 3x \equiv 15 \mod 8 \iff x \equiv 5 \mod 8 \end{cases}$ $7 \cdot (-1) + 8 \cdot (1) = 1,$

$c_{1,2} = 7 \cdot (-1) \cdot 5 + 8 \cdot (1) \cdot 2 = -35 + 16 = -19$ egy közös megoldása a két kongruenciának. Így az összes közös megoldás $x \equiv -19 \mod 56$, vagyis $x \equiv 37 \mod 56$.

c) $\begin{cases} 3x \equiv 2 \mod 4 \\ 4x \equiv 3 \mod 5 \end{cases}$ $\gcd(4,5)=1$, tehát közvetlenül alkalmazható a kínai maradéktétel. De előtte külön-külön meg kell oldani az egyes kongruenciákat: $\begin{cases} 3x \equiv 6 \mod 4 \iff x \equiv 2 \mod 4 \\ 4x \equiv 8 \mod 5 \iff x \equiv 2 \mod 5 \end{cases}$

Most könnyű dolgunk van, hiszen $x = 2$ egy közös megoldása a két kongruenciának. Így az összes közös megoldás $x \equiv 2 \mod 20$.

d) $\begin{cases} 5x \equiv 1 \mod 6 \\ 7x \equiv 9 \mod 10 \end{cases}$ $\gcd(6,10) = 2$, tehát NEM alkalmazható a kínai maradéktétel. Előtte külön-külön megoldjuk az egyes kongruenciákat: $\begin{cases} 5x \equiv -5 \mod 6 \iff x \equiv -1 \mod 6 \\ 7x \equiv 49 \mod 10 \iff x \equiv 7 \mod 10 \end{cases}$

Az $x \equiv -1 \pmod 6$ kongruencia helyettesíthető: $x \equiv -1 \pmod 6 \iff \begin{cases} x \equiv -1 \mod 2 \\ x \equiv -1 \mod 3 \end{cases}$

Hasonlóan $x \equiv 7 \pmod{10} \iff \begin{cases} x \equiv 7 \mod 2 \\ x \equiv 7 \mod 5 \end{cases}$ Tehát az eredeti kongruenciarendszer ekvivalensen helyettesíthető egy négy kongruenciából állóval: $\begin{cases} x \equiv -1 \mod 2 \Leftrightarrow x \equiv 1 \mod 2 \\ x \equiv -1 \mod 3 \Leftrightarrow x \equiv 2 \mod 3 \\ x \equiv 7 \mod 2 \iff x \equiv 1 \mod 2 \\ x \equiv 7 \mod 5 \iff x \equiv 2 \mod 5 \end{cases}$

Az első és harmadik kongruencia ugyanazt állítja, a második és negyedik kongruencia közös megoldása az $x = 2$. Vagyis további ekvivalens rendszer: $\begin{cases} x \equiv 1 \mod 2 \iff x \equiv 17 \mod 2 \\ x \equiv 2 \mod 15 \iff x \equiv 17 \mod 15 \end{cases}$

Azaz $x = 17$ egy közös megoldás, tehát $x \equiv 17 \pmod{30}$.

Megjegyzés: Ha már ekkor: $\begin{cases} x \equiv -1 \mod 6 \iff x \equiv 18 - 1 \equiv 17 \mod 6 \\ x \equiv 7 \mod 10 \iff x \equiv 10 + 7 \equiv 17 \mod 10 \end{cases}$ megtalálunk egy közös megoldást ($x = 17$), akkor csak a közös modulust kell kitalálni, ami $[6, 10] = 30$, ezért $x \equiv 17 \pmod{30}$.

e) $\begin{cases} 5x \equiv 2 \mod 6 \\ 7x \equiv 3 \mod 10 \end{cases}$ $\gcd(6, 10) = 2$, tehát NEM alkalmazható a kínai maradéktétel. Előtte külön-külön megoldjuk az egyes kongruenciákat: $\begin{cases} -x \equiv 2 \mod 6 \iff x \equiv -2 \mod 6 \\ -3x \equiv 3 \mod 10 \iff x \equiv -1 \mod 10 \end{cases}$

Az $x \equiv -2 \pmod 6$ kongruencia helyettesíthető: $x \equiv -2 \pmod 6 \iff \begin{cases} x \equiv -2 \mod 2 \\ x \equiv -2 \mod 3 \end{cases}$

Hasonlóan $x \equiv -1 \pmod{10} \iff \begin{cases} x \equiv -1 \mod 2 \\ x \equiv -1 \mod 5 \end{cases}$ Tehát az eredeti kongruenciarendszer ekvivalensen helyettesíthető négy kongruenciából állóval: $\begin{cases} x \equiv -2 \mod 2 \iff x \equiv 0 \mod 2 \\ x \equiv -2 \mod 3 \iff x \equiv 1 \mod 3 \\ x \equiv -1 \mod 2 \iff x \equiv 1 \mod 2 \\ x \equiv -1 \mod 5 \iff x \equiv 4 \mod 5 \end{cases}$

Az első és a harmadik kongruencia ellentmond egymásnak, ezért NINCS közös megoldás.

f) $\begin{cases} 4x \equiv 2 \mod 3 & \gcd(3, 7) = 1 \\ 3x \equiv 2 \mod 7 & \gcd(7, 11) = 1, \\ 9x \equiv 7 \mod 11 & \gcd(11, 3) = 1 \end{cases}$ tehát közvetlenül alkalmazható a kínai maradéktétel.

Előtte külön-külön megoldjuk az egyes kongruenciákat: $\begin{cases} 4x \equiv 8 \mod 3 \iff x \equiv 2 \mod 3 \\ 3x \equiv 9 \mod 7 \iff x \equiv 3 \mod 7 \\ 9x \equiv 18 \mod 11 \iff x \equiv 2 \mod 11 \end{cases}$

Az első és a harmadik kongruencia egyik közös megoldása $x = 2$, ezért ez a két kongruencia ekvivalensen helyettesíthető az $x \equiv 2 \pmod{33}$ kongruenciával: $\begin{cases} x \equiv 2 \mod 33 \\ x \equiv 3 \mod 7 \end{cases}$

$33 \cdot (3) + 7 \cdot (-14) = 1$, ebből $x = c_{1,2} = 33 \cdot (3) \cdot 3 + 7 \cdot (-14) \cdot 2 = 101$ egy közös megoldás, ezért $x \equiv 101 \pmod{231}$ az eredeti kongruenciaendszer megoldása.

g) $\begin{cases} 3x \equiv 1 \mod 4 & \gcd(4, 9) = 1 \\ 7x \equiv 2 \mod 9 & \gcd(9, 13) = 1, \\ 9x \equiv 3 \mod 13 & \gcd(13, 4) = 1 \end{cases}$ tehát közvetlenül alkalmazható a kínai maradéktétel.

Előtte külön megoldjuk az egyes kongruenciákat: $\begin{cases} 3x \equiv 9 \mod 4 \iff x \equiv 3 \equiv -1 \mod 4 \\ -2x \equiv 2 \mod 9 \iff x \equiv -1 \equiv 8 \mod 9 \\ 3x \equiv 1 \equiv 27 \mod 13 \iff x \equiv 9 \mod 13 \end{cases}$

Először az első két kongruenciak keresünk közös megoldást: $4 \cdot (-2) + 9 \cdot (1) = 1$, ennek segítségével $x = c_{1,2} = 4 \cdot (-2) \cdot (-1) + 9 \cdot (1) \cdot 3 = 35$ egy közös megoldás, tehát az első ké kongruencia helyett ekvivalensen írható csak egy: $x \equiv 35 \pmod{36}$. Avagy $x \equiv -1 \pmod{36}$, ami rögtön látható lett volna. $\begin{cases} x \equiv -1 \mod 36 \\ x \equiv -4 \mod 13 \end{cases}$ Bővített euklideszi algoritmussal kijön, hogy $36 \cdot (4) + 13 \cdot (-11) = 1$, ennek segítséével $x = c_{1,2,3} = 36 \cdot (4) \cdot (-4) + 13 \cdot (-11) \cdot (-1) = -433$ egy közös megoldás. Vagyis $x \equiv -433 \equiv 35 \pmod{468}$.

Ez úgy is kijöhetett volna, ha észrevesszük, hogy $\begin{cases} x \equiv -1 \equiv 36 - 1 \equiv 35 \mod 36 \\ x \equiv -4 \equiv 39 - 4 \equiv 35 \mod 13 \end{cases}$

h) $\begin{cases} 5x \equiv 3 \mod 6 & \gcd(6, 10) = 2 \\ 3x \equiv 9 \mod 10 & \gcd(10, 15) = 5, \\ 8x \equiv 9 \mod 15 & \gcd(15, 6) = 3 \end{cases}$ ezért NEM alkalmazható a kínai maradéktétel. Előbb külön-külön megoldjuk az egyes kongruenciákat: $\begin{cases} 5x \equiv 15 \mod 6 \iff x \equiv 3 \mod 6 \\ 3x \equiv 9 \mod 10 \iff x \equiv 3 \mod 10 \\ 8x \equiv 24 \mod 15 \iff x \equiv 3 \mod 15 \end{cases}$ Így $x = 3$ egy közös megoldás, vagyis akkor sem vezetne ellentmondásra a rendszer, ha külön külön mod 2 és mod 3, mod 2 és mod 5, valamint mod 3 és mod 5, kongrenciákkal helyettesítenénk (ahogy akkor járnánk el, ha nem találtunk volna rögtön közös megoldást). A modulusok legisebb közös többszöröse $[6, 10, 15] = 2 \cdot 3 \cdot 5 = 30$, ezért a közös megoldás $x \equiv 3 \pmod{30}$.

2. Keressük meg a kínai maradéktétel alkalmazásával azokat az egész számokat, amelyek 3-mal osztva 1-et, 4-gyel osztva 2-t, 5-tel osztva 3-at adnak maradékul.

   Megoldás: $\begin{cases} x \equiv 1 \equiv -2 \mod 3 & \gcd(3, 4) = 1 \\ x \equiv 2 \equiv -2 \mod 4 & \gcd(4, 5) = 1, \\ x \equiv 3 \equiv -2 \mod 5 & \gcd(3, 5) = 1 \end{cases}$ tehát $x \equiv -2 \equiv 58 \pmod{60}$.

3. Adjuk meg azt a legkisebb természetes számot, amely 28-as alapú számrendszerben felírva 3-ra, 19-es alapú számrendszerben felírva pedig 4-re végződik. Oldjuk meg a feladatot kongruenciák segítségével.

   Megoldás: $\begin{cases} x \equiv 3 \mod 28 \\ x \equiv 4 \mod 19 \end{cases}$ Bővített euklideszi algoritmussal $28 \cdot (-2) + 19 \cdot (3) = 1$, ennek segítségével $28 \cdot (-2) \cdot 4 + 19 \cdot (3) \cdot 3 = -53$ egy közös megoldás, ezért $x \equiv -53 \equiv 479 \pmod{532}$. Tehát a 479 a legkisebb természetes szám a megoldások között.

Oszthatósággal kapcsolatos feladatok — használhatjuk a középiskolában tanultakat is:

4. Bizonyítsuk be, hogy 6 osztója az $n \cdot (n + 1) \cdot (2n + 1)$-nek, ahol n egész szám.

   Megoldás: Két szomszédos szám közül az egyik páros, ezért $n \cdot (n+1)$ osztható kettővel. Ha n hárommal osztható, vagy ha hárommal osztva 2 a maradék, akkor nyiván $n \cdot (n + 1)$ hárommal is osztható. Ha n hárommal osztva egyet ad maradékul, akkor $2n \equiv 2 \pmod{3}$, ezért ekkor $2n + 1$ lesz hárommal osztható. Így $n \cdot (n + 1) \cdot (2n + 1)$ biztosan páros és osztható hárommal, azaz hattal is osztható.

5. Jelöljön m egész számot. Bizonyítsuk be, hogy $m^5 - m$ osztható 30-cal.

   Megoldás: m^5 és m paritása megegyezik, így $m^5 - m \equiv 0 \pmod{2}$.

   $m^5 \equiv m \pmod{5}$, azaz $m^5 - m \equiv 0 \pmod{5}$ a kis-Fermat tétel szerint.

Szintén a kis-Fermat tétel szerint $m^3 \equiv m \pmod 3$, ezért $m^3 \cdot m^2 \equiv m \cdot m^2 \equiv m^3 \equiv m \pmod 3$, vagyis $m^5 - m \equiv 0 \pmod 3$.

Tehát $m^5 - m$ 2-nek, 3-nak és 5-nek is többszöröse, azaz 30-nak is többszöröse (ami ezek legkisebb közös többszöröse), vagyis $m^5 - m$ osztható 30-cal.

Másik megoldás: $m^5 - m = m \cdot (m^4 - m) = m \cdot (m^2 - 1) \cdot (m^2 + 1) = m \cdot (m-1) \cdot (m+1) \cdot (m^2+1)$.

Két szomszédos szám szorzata biztosan páros, három egymást követő szám közül az egyik biztosan hárommal osztható, tehát három egymást követő szám szorzata $(m-1) \cdot m \cdot (m+1)$ biztosan osztható hattal. Ha m öttel osztható, vagy öttel osztva 1, vagy 4 maradékot ad, ez a szorzat öttel is osztható.

Csak azokat az m-eket kell még megvizsgálni, amik öttel osztva 2 vagy 3 maradékot adnak. Ezek négyzete öttel osztva $2^2 = 4$ vagy $3^2 \bmod 5 = 4$ maradékot adnak, így ekkor $m^2 + 1$ öttel osztható lesz.

Tehát $m^5 - m$ 2-nek, 3-nak és 5-nek is többszöröse, azaz 30-nak is többszöröse (ami ezek legkisebb közös többszöröse), vagyis $m^5 - m$ osztható 30-cal.

6. Bizonyítsuk be, hogy ha a 4-gyel nem osztható páros szám, akkor

   $a \cdot (a^2 - 1) \cdot (a^2 - 4)$ osztható 960-nal.

   Megoldás: Ha a néggyel nem osztható páros szám, akkor $r = a \bmod 4$ maradék maga páros szám ($a = 4k + r$ páros), de r nem a nulla, azaz $r = a \bmod 4 = 2$.

   $a \cdot (a^2 - 1) \cdot (a^2 - 4) = (4k+2) \cdot ((4k+2)^2 - 1) \cdot ((4k+2)^2 - 4) =$
   $= (4k+2) \cdot (16k^2 + 16k + 4 - 1) \cdot ((16k^2 + 16k + 4 - 4) = (4k+2) \cdot (16k^2 + 16k + 3) \cdot (16k^2 + 16k) =$
   $= 2 \cdot (2k+1) \cdot (16k^2 + 16k + 3) \cdot 16 \cdot k \cdot (k+1) = 32 \cdot k \cdot (k+1) \cdot (2k+1) \cdot (16k^2 + 16k + 3)$.

   Azt korábban láttuk, hogy $k \cdot (k+1) \cdot (2k+1)$ osztható hattal, azaz $32 \cdot k \cdot (k+1) \cdot (2k+1)$ osztható 64-gyel és 3-mal is, vagyis 192-vel.

   $960 = 64 \cdot 15 = 2^6 \cdot 3 \cdot 5$, azaz már csak azt kell belátni, hogy öttel is osztható a teljes szorzat. Ha $k \equiv 0 \pmod 5$, ha $k \equiv 4 \pmod 5$, ha $k \equiv 2 \pmod 5$, akkor $k \cdot (k+1) \cdot (2k+1)$ osztható öttel is. Már csak $k \equiv 1 \pmod 5$ és $k \equiv 3 \pmod 5$ eseteket kell megnézni.

   $16k^2 + 16k + 3 \equiv k^2 + k + 3 \pmod 5$. Az első esetben $k^2 + k + 3 \equiv 1^2 + 1 + 3 \equiv 0 \pmod 5$. A második esetben $k^2 + k + 3 \equiv 3^2 + 3 + 3 \equiv 15 \equiv 0 \pmod 5$.

7. Bizonyítsuk be, hogy három egymás után következő egész szám köbének összege osztható

   a) a középső szám 3-szorosával; b) 9-cel.

   Megoldás: $(n-1)^3 + n^3 + (n+1)^3 = (n^3 - 3n^2 + 3n - 1) + n^3 + (n^3 + 3n^2 + 3n + 1) = 3n^3 + 6n = 3n \cdot (n^2 + 2)$. Ez tényleg a középső szám (n) háromszorosának ($3n$-nek) a többszöröse.

   b) Ha n osztható hárommal, akkor $3n$ kilenccel is osztható, és kész vagyunk. Ha $n \equiv \pm 1 \pmod 3$, akkor $n^2 \equiv 1 \pmod 3$, és így $n^2 + 2 \equiv 1 + 2 \equiv 0 \pmod 3$, és ekkor $3 \cdot (n^2 + 2)$ osztható kilenccel.

8. Bizonyítsuk be, hogy ha a tizes számrendszerben ábrázolt bármelyik háromjegyű természetes számot kétszer egymás mellé írjuk, akkor az így kapott hatjegyű szám osztható 7-tel, 11-gyel és 13-mal.

   Megoldás: $n = 100a + 10b + c$ esetén ($9 \geq a, b, c \geq 0$, $a > 0$) tehát a $10000a + 10000b + 1000c + 100a + 10b + c = 100100a + 10010b + 1001c = 1001 \cdot (100a + 10b + c) = 1001 \cdot n$ számról van szó. Mivel $999 \geq n \geq 100$ tetszőleges, ezért nyilván 1001-ről kell belátni, hogy az biztosan mindig osztható 7-tel, 11-gyel és 13-mal. És $1001 = 7 \cdot 11 \cdot 13$, azaz tényleg.

9. Lássuk be, hogy két páratlan szám négyzetének különbsége mindig osztható 8-cal.

   Megoldás: $(2k+1)^2-(2\ell+1)^2 = 4k^2+4k+1-4\ell^2-4\ell-1 = 4\cdot(k^2+k-\ell^2-\ell) = 4\cdot\big((k^2-\ell^2)+k-\ell\big) = 4\cdot\big((k-\ell)\cdot(k+\ell)+(k-\ell)\cdot 1\big) = 4\cdot(k-\ell)\cdot(k+\ell+1)$, ha k és ℓ azonos paritású, akkor $4\cdot(k-\ell)$ osztható nyolccal, ha különböző paritásúak, akkor pedig $4\cdot(k+\ell+1)$ osztható nyolccal.

10. Bizonyítsuk be, hogy

    a) n^6-1 osztható 7-tel, ha $\gcd(n,7)=1$;

    b) $n^{12}-1$ osztható 7-tel, ha $\gcd(n,7)=1$;

    c) $n^{6k}-1$ osztható 7-tel, ha $\gcd(n,7)=1$.

    Megoldás: Az első maga az Euler-Fermat tétel közvetlenül $m=7$ modulusra kimondva, hiszen $\varphi(7)=6$, ezért $n^6\equiv 1 \pmod 7$, $\gcd(n,7)=1$ esetén.

    b) Kihasználva az a) eredményét: $n^{12}=(n^6)^2\equiv 1^2\equiv 1 \pmod 7$, tehát $n^{12}-1\equiv 0 \pmod 7$.

    c) Kihasználva az a) eredményét: $n^{6k}=(n^6)^k\equiv 1^k\equiv 1 \pmod 7$, tehát $n^{6k}-1\equiv 0 \pmod 7$.

11. Bizonyítsuk be, hogy bármely egész x-re $x^7\equiv x \mod 42$.

    Megoldás: A kis-Fermat tétel szerint $\forall x\in\mathbb{Z}: x^7\equiv x \pmod 7$.

    Szintén a kis-Fermat tétel szerint $\forall x\in\mathbb{Z}: x^3\equiv x \pmod 3$; ezt egymás után többször használva: $x^7=x\cdot x^6=x\cdot(x^3)^2\equiv x\cdot x^2\equiv x^3\equiv x \pmod 3$. Tehát $\forall x\in\mathbb{Z}: x^7\equiv x \pmod 3$.

    Szintén a kis-Fermat tétel szerint $\forall x\in\mathbb{Z}: x^2\equiv x \pmod 2$. Vagy ezt többször egymás után használva, vagy rögtön belátva, hogy páros x hetedik hatványa is páros, páratlan x hetedik hatványa is páratlan, kijön hogy $\forall x\in\mathbb{Z}: x^7\equiv x \pmod 2$.

    Tehát $\forall x\in\mathbb{Z}: x^7-x$ osztható héttel is, hárommal is és kettővel is, azaz ezek legkisebb közös többszörösével, 42-vel is: $\forall x\in\mathbb{Z}: x^7-x\equiv 0 \pmod{42}$. Vagyis $\forall x\in\mathbb{Z}: x^7\equiv x \pmod{42}$.

12. Bizonyítsuk be, hogy $n^{13}-n$ minden n egészre osztható a $2,3,5,7$ és 13 számokkal.

    Megoldás: A kis-Fermat tétel szerint $\forall n\in\mathbb{Z}: n^{13}\equiv n \pmod{13}$ ez kész is, $n^2\equiv n \pmod 2$, $n^3\equiv n \pmod 3$, $n^5\equiv n \pmod 5$, $n^7\equiv n \pmod 7$. Az utóbbiakat egymás után többször alkalmazva:

    $n^{13}=n^{1+12}=n\cdot\Big(\big(n^2\big)^2\Big)^3\equiv n\cdot\Big(\big(n\big)^2\Big)^3\equiv n\cdot\Big(n\Big)^3\equiv n^4\equiv n^2\cdot n^2\equiv n\cdot n\equiv n^2\equiv n \pmod 2$.

    $n^{13}=n^{1+12}=n\cdot\big(n^3\big)^4\equiv n\cdot\big(n\big)^4\equiv n^5\equiv n^2\cdot n^3\equiv n^2\cdot n\equiv n^3\equiv n \pmod 3$.

    $n^{13}=n^{3+10}=n^3\cdot\big(n^5\big)^2\equiv n^3\cdot\Big(n\Big)^2\equiv n^5\equiv n \pmod 5$.

    $n^{13}=n^{6+7}=n^6\cdot n^7\equiv n^6\cdot n\equiv n^7\equiv n \pmod 7$.

13. Mutassuk meg, hogy $a^{1729}\equiv a \mod 1729$, habár az $1729=7\cdot 13\cdot 19$ NEM prím.

    Megoldás: Az eddigiekhez hasonlóan kis-Fermat tétellel: $a^7\equiv a \pmod 7$, $a^{13}\equiv a \pmod{13}$, $a^{19}\equiv a \pmod{19}$. Az előző feadatban azt is láttuk, hogy $n^{13}\equiv n \pmod 7$.

    $\Big(\big(a^7\big)^{13}\Big)^{19}\equiv\Big(\big(a\big)^{13}\Big)^{19}\equiv\Big(a\Big)^{19}\equiv a^{13+6}\equiv a^{13}\cdot a^6a\cdot a^6\equiv a^7\equiv a \pmod 7$.

    $\Big(\big(a^{13}\big)^{19}\Big)^7\equiv\Big(\big(a\big)^{19}\Big)^7\equiv\Big(\big(a\big)^{13+6}\Big)^7\equiv\Big(a^{13}\cdot a^6\Big)^7\equiv\Big(a\cdot a^6\Big)^7\equiv\Big(a^7\Big)^7\equiv a^{49}\equiv a^{13+13+13+10}\equiv a^{13}\cdot a^{13}\cdot a^{13}\cdot a^{10}\equiv a\cdot a\cdot a\cdot a^{10}\equiv a^{13}\equiv a \pmod{13}$.

    $\Big(\big(a^{19}\big)^{13}\Big)^7\equiv\Big(\big(a\big)^{13}\Big)^7\equiv\Big(a\Big)^{91}\equiv\Big(a\Big)^{19+19+19+19+15}\equiv a^{19}\cdot a^{19}\cdot a^{19}\cdot a^{19}\cdot a^{15}\equiv a\cdot a\cdot a\cdot a\cdot a^{15}\equiv a^{19}\equiv a \pmod{19}$.

Tehát $a^{1729} - a$ osztható 7-el is, 13-mal is, 19-cel is, azaz ezek legkisebb közös többszörösével is.