Diszkrét matematika II. feladatok

Negyedik alkalom

Bemelegítő feladatok

1. Oldja meg az alábbi kongruenciákat a *bővített euklideszi algoritmus* segítségével:

   a) $3x \equiv 1 \mod 7$; b) $3x \equiv 1 \mod 8$; c) $2x \equiv 1 \mod 8$; d) $4x \equiv 2 \mod 8$
   e) $31x \equiv 4 \mod 17$; f) $31x \equiv 4 \mod 117$; g) $5x \equiv 10 \mod 15$; h) $17x \equiv 4 \mod 2024$

   Megoldások: A bővített euklideszi algoritmust az előző feladatsorokon alaposan begyakoroltuk, itt már csak az eredményét közöljük.

   a) $3x \equiv 1 \mod 7 \iff \exists y \in \mathbb{Z} : 3x + 7y = 1$, bővített euklideszi algoritmussal kijön, hogy $3 \cdot (-2) + 7 \cdot (1) = 1$ és $3 \cdot (7k) + 7 \cdot (-3k) = 0$. A kettő összegéből: $3 \cdot (7k-2) + 7 \cdot (1-3k) = 1$, ezt modulo 7 tekintve: $3 \cdot (7k-2) \equiv 1 \pmod 7$, azaz $x = 7k - 2 : k \in \mathbb{Z}$, vagyis modulo 7 maradékosztályként megadva a megoldást: $x \equiv -2 \equiv 5 \pmod 7$.

   b) $3x \equiv 1 \mod 8 \iff \exists y \in \mathbb{Z} : 3x + 8y = 1$, bővített euklideszi algoritmussal kijön, hogy $3 \cdot (3) + 8 \cdot (-1) = 1$ és $3 \cdot (8k) + 8 \cdot (-3k) = 0$, a kettő összegéből: $3 \cdot (3+8k) + 8 \cdot (-1-3k) = 1$, ezt modulo 8 tekintve $3 \cdot (3 + 8k) \equiv 1 \pmod 8$, azaz $x = 3 + 8k : k \in \mathbb{Z}$, maradékosztályként megadva a megoldást: $x \equiv 3 \pmod 8$.

   Megjegyzés: Még nem látszik, hogy miért szükséges a 0-t előállító végtelen sok megoldás hozzáadásával a diophantoszi egyenlet összes megoldását megadni, de most kicsit előre ugorva látni fogjuk:

   g) $5x \equiv 10 \mod 15 \iff \exists y \in \mathbb{Z} : 5x + 15y = 10$, bővített euklideszi algoritmussal kijön, hogy $5 \cdot (-2) + 15 \cdot (1) = 5$ és $5 \cdot (3k) + 15 \cdot (-k) = 0$. Az első egyenletet kettővel szorozva $5 \cdot (-4) + 15 \cdot (2) = 10$ egy partikuláris megoldás, ehhez hozzáadjuk a (0-t előállító) második egyenletet: $5 \cdot (3k-4) + 15 \cdot (2-k) = 10$, ezt modulo 15 tekintve $5 \cdot (3k - 4) \equiv 10 \pmod{15}$, azaz $x = 3k - 4 : k \in \mathbb{Z}$, maradékosztályokként megadva a megoldást most $k = 2, 3, 4, 5, 6$ esetén különböző megoldásokat kapunk: $x \equiv 2 \pmod{15}$, $x \equiv 5 \pmod{15}$, $x \equiv 8 \pmod{15}$, $x \equiv 11 \pmod{15}$, $x \equiv 14 \pmod{15}$.

   ($k = 7$ esetén $x \equiv 17 \equiv 2 \pmod{15}$, ami már nem új megoldás, innentől a már megkapott megoldádok ismétlődnek, ugyanígy $k = 1$-re és $k = 0$-ra és negatív k értékekre sem kapuk újabb megoldásokat.)

   c) $2x \equiv 1 \mod 8 \iff \exists y \in \mathbb{Z} : 2x + 8y = 1$, bővített euklideszi algoritmussal kijön, hogy $2 \cdot (-3) + 8 \cdot (1) = 2$ és $2 \cdot (4k) + 8 \cdot (-k) = 0$, a kettő összegéből: $2 \cdot (-3 + 4k) + 8 \cdot (1-k) = 2$ a két együttható legnagyobb közös osztója. Mivel $2x + 8y$ minden egész x és minden egész y esetén páros szám, így semmilyen egész számpár esetén nem lehet egyenlő 1-gyel, tehát NINCS megoldás.

   d) $4x \equiv 2 \mod 8 \iff \exists y \in \mathbb{Z} : 4x + 8y = 2$, bővített euklideszi algoritmussal kijön, hogy $4 \cdot (-1) + 8 \cdot (1) = 4$ és $4 \cdot (2k) + 8 \cdot (-k) = 0$, a kettő összegéből: $4 \cdot (-1 + 4k) + 8 \cdot (1-k) = 4$ a két együttható legnagyobb közös osztója. Mivel $4x + 8y$ minden egész x és minden egész y esetén néggyel osztható szám, így semmilyen egész számpár esetén nem lehet egyenlő 2-vel, tehát NINCS megoldás.

   e) $31x \equiv 4 \mod 17 \iff \exists y \in \mathbb{Z} : 31x + 17y = 4$. Bővített euklideszi algoritmussal kijön, hogy $31 \cdot (-6) + 17 \cdot (11) = 1$ és $31 \cdot (17k) + 17 \cdot (-31k) = 0$. Az első egyenletet néggyel szorozva kapunk egy partikuláris megoldást $31 \cdot (-24) + 17 \cdot (44) = 4$, ehhez adjuk hozzá a 0-t előállító második egyenletet: $31 \cdot (17k - 24) + 17 \cdot (44 - 31k) = 4$. Ezt modulo 17 tekintve: $31 \cdot (17k - 24) \equiv 4 \pmod{17}$, azaz $x = 17k - 24 : k \in \mathbb{Z}$, maradékosztályként megadva a megoldást $x \equiv -24 \equiv 10 \pmod{17}$.

f) $31x \equiv 4 \mod 117 \iff \exists y \in \mathbb{Z} : 31x + 117y = 4$, bővített euklideszi algoritmussal kijön, hogy $31 \cdot (34) + 117 \cdot (-9) = 1$ és $31 \cdot (-117k) + 117 \cdot (31k) = 0$. Az első egyenletet néggyel szorozva kapunk egy partikuláris megoldást $31 \cdot (136) + 177 \cdot (-36) = 4$, ehhez adjuk hozzá a 0-t előállító második egyenletet: $31 \cdot (136 - 117k) + 177 \cdot (31k - 36) = 4$. Ezt modulo 117 tekintve: $31 \cdot (136 - 117k) \equiv 4 \pmod{117}$, azaz $x = 136 - 117k : k \in \mathbb{Z}$, maradékosztályként megadva a megoldást $x \equiv 19 \pmod{117}$.

h) $17x \equiv 4 \mod 2024 \iff \exists y \in \mathbb{Z} : 17x + 2024y = 4$, bővített euklideszi algoritmussal kijön, hogy. $17 \cdot (-119) + 2024 \cdot (1) = 1$ és $17 \cdot (2024k) + 2024 \cdot (-17k) = 0$. Az első egyenletet néggyel szorozva kapunk egy partikuláris megoldást $17 \cdot (-476) + 2024 \cdot (4) = 4$, ehhez adjuk hozzá a 0-t előállító második egyenletet: $17 \cdot (2024k - 476) + 2024 \cdot (4 - 17k) = 4$. Ebből $x = 2024k - 476 : k \in \mathbb{Z}$, vagyis $x \equiv 1548 \pmod{2024}$.

2. Számolja ki az a lehetséges hatványait modulo m, ha

   a) $a = 2, m = 4$; b) $a = 3, m = 5$; c) $a = 2, m = 7$; c) $a = 3, m = 7$; e) $a = 7, m = 8$

   Megoldások:

   a) $2^1 = 2 \equiv 2 \pmod 4$, $2^2 = 4 \equiv 0 \pmod 4$, $2^3 = 8 \equiv 0 \pmod 4$, $2^4 = 16 \equiv 0 \pmod 4$, és általában 2^n osztható 4-gyel, ha $n \geq 2$.

   Megjegyzés: Általában egy gyűrűben "nilpotens" elemnek nevezünk egy olyan (nemnulla) elemet, aminek valamilyen hatványa már a nulla. A fenti példa azt mutatja, hogy $\mathbb{Z}_4$-ben az $a = 2$ egy nilpotens elem, mert a négyzete (és innentől minden magasabb hatványa) már nullával kongruens. Általában, ha a modulus NEM "négyzetmentes" (azaz m prímosztói közül legalább az egyiknek, pl. p-nek a négyzete is osztja m-et, azaz $m = p^n \cdot q$, ahol q most nem feltélenül prím, hanem p-hez relatív prím egész, és $n > 1$), akkor például $a = p \cdot q \not\equiv 0 \pmod m$, de $a^n = p^n \cdot q^n \equiv 0 \pmod m$.

   De már a mátrixok körében is találkozhattunk nilpotens mátrixokkal. Például $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ mátrix négyzete $M^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, a köbe $M^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathbf{0}$, azaz $M^n = \mathbf{0}$, ha $n > 2$.

   b) $3^1 = 3 \equiv 3 \pmod 5$, $3^2 = 9 \equiv 4 \pmod 5$, $3^3 = 27 \equiv 2 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $3^5 = 81 \cdot 3 \equiv 3 \pmod 5$, $3^6 = 81 \cdot 9 \equiv 9 \equiv 4 \pmod 5$, és általában $3^{4n+k} \equiv 3^k \pmod 5$.

   c) $2^1 = 2 \equiv 2 \pmod 7$, $2^2 = 4 \equiv 4 \pmod 7$, $2^3 = 8 \equiv 1 \pmod 7$, $2^4 = 16 \equiv 2 \pmod 7$, $2^5 = 32 \equiv 4 \pmod 7$, $2^6 = 64 \equiv 1 \pmod 7$, és általában $2^{3n+k} \equiv 2^k \pmod 7$.

   d) $3^1 = 3 \equiv 3 \pmod 7$, $3^2 = 9 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 2 \cdot 3 \equiv 6 \pmod 7$, $3^4 = 81 \equiv 6 \cdot 3 = 18 \equiv 4 \pmod 7$, $3^5 = 243 \equiv 4 \cdot 3 = 12 \equiv 5 \pmod 7$, $3^6 = 729 \equiv 5 \cdot 3 = 15 \equiv 1 \pmod 7$, $3^7 = 2187 \equiv 1 \cdot 3 \equiv 3 \pmod 7$, $3^8 = 6561 \equiv 3 \cdot 3 \equiv 2 \pmod 7$, $3^9 = 19683 \equiv 2 \cdot 3 \equiv 6 \pmod 7$, és általában $3^{6n+k} \equiv 3^k \pmod 7$.

   e) $7^1 = 7 \equiv 7 \pmod 8$, $7^2 = 49 \equiv 1 \pmod 8$, $7^3 = 343 \equiv 7 \pmod 8$, $7^4 = 2401 \equiv 1 \pmod 8$, $7^5 \equiv 1 \cdot 7 \equiv 7 \pmod 8$, $7^6 \equiv 7 \cdot 7 \equiv 1 \pmod 8$, $7^7 \equiv 1 \cdot 7 \equiv 7 \pmod 8$, $7^8 \equiv 7 \cdot 7 \equiv 1 \pmod 8$, és általában $7^{2n} \equiv 1 \pmod 8$ és $7^{2n+1} \equiv 7 \pmod 8$.

3. Számolja ki a $\varphi(m)$ értékeket $1 \leq m \leq 16$ esetén!

   Megoldások: $\varphi(m)$ a $\{1, \ldots, m\}$ halmazban az m-hez relatív prímek darabszáma.

   $\varphi(1) = 1$, hiszen az $\{1\}$ halmazban az 1 relatív prím az 1-hez.

   $\varphi(2) = 1$, hiszen az $\{1, 2\}$ halmazban az 1 relatív prím az 2-höz (a 2 nem relatív prím saját magához).

$\varphi(3) = 2$, hiszen az $\{1, 2, 3\}$ halmazban az 1 és 2 relatív prímek az 3-hoz (a 3 nem relatív prím saját magához).

Megjegyzés: Mivel $m > 1$ esetén az m saját magához nem relatív prím ($m = 1$ viszont relatív prím saját magához), így $m > 1$ esetén a $\varphi(m)$ definícióját úgy is fogalmazhatjuk, hogy a $\{1, \dots, m-1\}$ halmazban az m-hez relatív prímek darabszáma. (De $m = 1$ esetén ez nem lenne jó definíció, hiszen üres lenne a halmaz.)

$\varphi(4) = 2$, hiszen az $\{1, 2, 3\}$ halmazban az 1 és 3 relatív prímek az 4-hez.

$\varphi(5) = 4$, hiszen az $\{1, 2, 3, 4\}$ halmazban az 1, 2, 3, és 4 relatív prímek az 5-höz.

$\varphi(6) = 2$, hiszen az $\{1, 2, 3, 4, 5\}$ halmazban az 1 és 5 relatív prímek az 6-hoz.

$\varphi(7) = 6$, hiszen az $\{1, 2, 3, 4, 5, 6\}$ halmazban az 1, 2, 3, 4, 5, 6 relatív prímek az 7-hez.

$\varphi(8) = 4$, hiszen az $\{1, 2, 3, 4, 5, 6, 7\}$ halmazban az 1, 3, 5 és 7 relatív prímek az 8-hoz.

$\varphi(9) = 6$, hiszen az $\{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazban az 1, 2, 4, 5, 7, 8 relatív prímek az 9-hez.

Megjegyzés: Nagyobb m-ek esetén, ha ismerjük m összes prímosztóját, kényelmesebb a

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

képletet használni. Prímekre $\varphi(p) = p - 1$.

$\varphi(10) = 10 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 4.$

$\varphi(11) = 11 - 1 = 10.$

$\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4.$

$\varphi(13) = 13 - 1 = 12.$

$\varphi(14) = 14 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{7}\right) = 6.$

$\varphi(15) = 15 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 8.$

$\varphi(16) = 16 \cdot \left(1 - \frac{1}{2}\right) = 8.$

4. Határozza meg a következő értékeket az Euler-Fermat tétel segítségével

   a) $2^6 \mod 7$; b) $2^7 \mod 7$; c) $2^8 \mod 7$; d) $2^9 \mod 7$
   e) $2^{12} \mod 13$; f) $2^{13} \mod 13$; g) $2^{13} \mod 11$; h) $2^{10} \mod 9$

   Megoldások: Az Euler-Fermat tétel szerint ha a és m relatív prímek, akkor $a^{\varphi(m)} \equiv 1 \pmod m$. Az előbb kiszámoluk, hogy $\varphi(7) = 6$, $\varphi(13) = 12$, $\varphi(11) = 10$, $\varphi(9) = 6$.

   2 és 7 relatív prímek, ezért $2^6 \equiv 1 \pmod 7$. 2 és 13 relatív prímek, ezért $2^{12} \equiv 1 \pmod{13}$. 2 és 11 relatív prímek, ezért $2^{10} \equiv 1 \pmod{11}$. 2 és 9 is relatív prímek, ezért $2^6 \equiv 1 \pmod 9$.

   a) $2^6 \equiv 1 \pmod 7$; **b)** $2^7 \equiv 2^6 \cdot 2 \equiv 2 \pmod 7$; **c)** $2^8 \equiv 2^6 \cdot 2^2 \equiv 4 \pmod 7$;
   d) $2^9 \equiv 2^6 \cdot 2^3 \equiv 8 \equiv 1 \pmod 7$; **e)** $2^{12} \equiv 1 \pmod{13}$; **f)** $2^{13} \equiv 2^{12} \cdot 2 \equiv 2 \pmod{13}$;
   g) $2^{13} \equiv 2^{10} \cdot 2^3 \equiv 8 \pmod{11}$; **h)** $2^{10} \equiv 2^6 \cdot 2^4 \equiv 7 \pmod 9$.

Gyakorló feladatok

5. Határozza meg azt a *két* legkisebb pozitív egész számot, mely

   a) 13-szorosát felírva 7-es számrendszerben az utolsó előtti jegy 4, az utolsó jegy pedig 3;

   b) 12-szorosát felírva 8-as számrendszerben az utolsó előtti jegy 2, az utolsó jegy pedig 1;

   c) 14-szorosát felírva 16-os számrendszerben az utolsó előtti jegy 3, az utolsó jegy pedig 4!

Megoldás: $13x \equiv 3 \pmod 7$, sőt $13x \equiv (4\cdot 7)+3 \pmod{49}$. Igazából a második kongruencia implikálja az elsőt, azaz elég csak a másodikat megoldani. $13x \equiv 31 \pmod{49}$, mivel $13 \equiv -36 \pmod{49}$ és $31 \equiv -18 \pmod{49}$, ezért $-36x \equiv -18 \pmod{49}$, és mínusz 18 relatív prím 49-hez, ezért lehet vele egyszerűsíteni: $2x \equiv 1 \pmod{49}$. Mivel $1 \equiv 50 \pmod{49}$, $2x \equiv 50 \pmod{49}$, és 2-vel is lehet egyszerűsíteni: $x \equiv 25 \pmod{49}$, ebben a maradékosztályban a két legkisebb pozitív szám $x = 25$ és $x = 25 + 49 = 74$.

Alternatív megoldás: Két lépcsőben, először csak az utolsó számjegyre vonatkozó feltételt megoldani, és az ezt kielégítők körében az utoldó előtti számjegyre vonatkozó feltételt teljesítőket megkeresni. Az első kongruencia redukálva: $6x \equiv 3 \pmod 7$, és mivel a 3 és 7 relatív prímek, tovább egyszerűsíhető: $2x \equiv 1 \equiv 8 \pmod 7$, és mivel a 2 és 7 is relatív prímek, tovább egyszerűsíhető: $x \equiv 4 \pmod 7$, vagyis $x = 7n + 4$ valamilyen egész n-re.

Ezt beírva a második kongruenciába: $13(7n+4) \equiv (4\cdot 7)+3 \pmod{49}$, elvégezve a műveleteket: $91n + 52 \equiv 31 \pmod{49}$, redukálva: $42n + 3 \equiv 31 \pmod{49}$, azaz $42n \equiv 28 \pmod{49}$, 7-tel egyszerűsítve (a modulust is!): $6n \equiv 4 \pmod 7$, vagyis $-n \equiv 4 \pmod 7$, vagyis -1-gyel egyszerűsítve $n \equiv -4 \equiv 3 \pmod 7$, vagyis $n = 7k + 3$.

Tehát $x = 7n + 4 = 7\cdot(7k + 3) + 4 = 49k + 25$. A két legkisebb ilyen pozitív egészt a $k = 0, 1$ helyettesítés adja: $x = 25$ és $x = 74$ a két keresett megoldás.

b) $12x \equiv 1 \pmod 8$, és $12x \equiv 2\cdot 8 + 1 \pmod{64}$. Az első kongruencia: $4x \equiv 1 \pmod 8$, aminek NINCS megoldása. (Bármilyen egész számnak a 12-szerese az egy páros szám, míg 8-as számrendszerben ha az utolsó jegy páratlan, akkor a szám maga is páratlan.)

c) $14x \equiv 4 \pmod{16}$ és $14x \equiv 3\cdot 16 + 4 \pmod{256}$. Az első kongruencia: $-2x \equiv 4 \pmod{16}$, 2-vel egyszerűsítve (a modulust is!): $-x \equiv 2 \pmod 8$, azaz $x \equiv -2 \equiv 6 \pmod 8$, vagyis $x = 8n + 6$.

Ezt beírva a második kongruenciába: $14\cdot(8n+6) \equiv 3\cdot 16+4 \pmod{256}$, elvégezve a műveleteket: $112n + 84 \equiv 48 + 4 \pmod{256}$, átrendezve $112n \equiv -32 \equiv 224 \pmod{256}$.

Vigyázat! Hiába csábító a 112-vel való egyszerűsítés, a modulus ehhez NEM relatív prím, de nem is a többszöröse! $112 = 16 \cdot 7$.

Először 16-tal egyszerűsítünk, a modulust is: $7n \equiv 14 \pmod{16}$, ezután 7-tel egyszerűsítünk: $n \equiv 2 \pmod{16}$, vagyis $n = 16k + 2$.

Tehát $x = 8n+6 = 8\cdot(16k+2)+6 = 128k+22$. A két legkisebb ilyen pozitív egészt a $k = 0, 1$ helyettesítés adja: $x = 22$ és $x = 150$ a két keresett megoldás.

(Valóban, a $14 \cdot 150 = 2100$ hexadecimális alakja 834 és $14 \cdot 22 = 308$ hexadecimális alakja 134)

Alternatív megoldás: Itt is igaz, hogy a második kongruencia implikálja az elsőt, azaz elég csak a másodikat megoldani. $14x \equiv 3\cdot 16+4 \pmod{256}$, azaz $14x \equiv 52 \pmod{256}$. Először 2-vel egyszerűsítve (a modulust is!): $7x \equiv 26 \pmod{128}$. Ha észrevesszük, hogy $26+128 = 154 = 7\cdot 22$, akkor bővített euklideszi algoritmus nélkül is meg tudjuk oldani: $7x \equiv 154 \pmod{128}$, és a 7 relatív prím a modulushoz, ezért: $x \equiv 22 \pmod{128}$. Ebben a maradékosztályban a két legkisebb pozitív egész $x = 22$ és $x = 22 + 128 = 150$.

6. Számolja ki az következő értékeket

   a) $3^{10} \bmod 7$; b) $3^{15} \bmod 7$; c) $3^{115} \bmod 7$; d) $3^{1155} \bmod 7$
   e) $2^{3^{12}} \bmod 11$; f) $2^{7^{122}} \bmod 11$; g) $2^{5^{11}} \bmod 13$; h) $2^{3^{1111}} \bmod 17$

   Megoldások: Itt is használhajuk az Euler-Fermat tételt, mert minden fenti hatvány alapja mindegyik modulushoz relatív prím. Mivel $\varphi(7) = 6$, ezért az első négy hatvány kitevője annak hattal vett osztási maradékával helyettesíthető: **a)** $3^{10} \equiv 3^4 \equiv 9^2 \equiv 2^2 \equiv 4 \pmod 7$; **b)** $3^{15} \equiv 3^3 \equiv 9\cdot 3 \equiv 2\cdot 3 \equiv 6 \pmod 7$; **c)** $3^{115} \equiv 3^1 \equiv 3 \pmod 7$; **d)** $3^{1155} \equiv 3^3 \equiv 6 \pmod 7$.

   Mivel $\varphi(11) = 10$, ezért a következő két hatvány kitevője annak tízzel vett osztási maradékával helyettesíthető: **e)** $2^{3^{12}} \pmod{11}$ meghatározásához előbb $3^{12} \pmod{10}$ meghatározása kell.

Mivel 3 relatív prím a 10-hez, ezért ennek a kitevőjét $\varphi(10) = 4$ szerint redukálhatjuk: $3^{12} \equiv 3^0 \equiv 1 \pmod{10}$, tehát $2^{3^{12}} \equiv 2^1 \pmod{11}$.

f) $2^{7^{122}} \pmod{11}$ meghatározásához előbb $7^{122} \pmod{10}$ meghatározása kell. Mivel 7 relatív prím a 10-hez, ezért ennek a kitevőjét $\varphi(10) = 4$ szerint redukálhatjuk: $7^{122} \equiv 7^2 \equiv 9 \pmod{10}$, tehát $2^{7^{122}} \equiv 2^9 \pmod{11}$.

Ezt a hatványozást még el kell végeznünk, például gyorshatványozással. A kitevőt írjuk fel kettes számrendszerben: $9 = 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 1$, azaz a kitevő bináris alakja: 1001.

$$2^9 = \left(\left((2^1)^2 \cdot 2^0\right)^2 \cdot 2^0\right)^2 \cdot 2^1 \equiv \left(\left(4 \cdot 2^0\right)^2 \cdot 2^0\right)^2 \cdot 2^1 \equiv \left(5 \cdot 2^0\right)^2 \cdot 2^1 \equiv 3 \cdot 2^1 \equiv 6 \pmod{11}$$

g) $2^{5^{11}} \pmod{13}$ meghatározásához először $5^{11} \pmod{12}$ értékét kell meghatározni. Mivel 5 relatív prím 12-höz, itt is használható az Euler-Fermat tétel, használva a $\varphi(12) = 4$ értéket: $5^{11} \equiv 5^3 \pmod{12}$. Mivel $5^2 = 24 + 1 \equiv 1 \pmod{12}$, ezért $5^{11} \equiv 5^3 \equiv 5 \pmod{12}$.

Tehát $2^{5^{11}} \equiv 2^5 \equiv 32 \equiv 6 \pmod{13}$.

h) $2^{3^{1111}} \pmod{17}$ meghatározásához először $3^{1111} \pmod{16}$ értékét kell meghatározni. Mivel 3 relatív prím 16-hoz, itt is használható az Euler-Fermat tétel, használva a $\varphi(16) = 8$ értéket: $1111 \equiv 7 \pmod 8$, tehát $3^{1111} \equiv 3^8 \pmod{16}$. Ezt gyorshatványozással lehet meghatározni, azon belül is különösen egyszerűen, mert a kitevő maga egy 2-hatvány:

$$3^{1111} \equiv 3^8 \equiv \left((3^2)^2\right)^2 \equiv \left((9)^2\right)^2 \equiv \left(81\right)^2 \equiv \left(1\right)^2 \equiv 1 \pmod{16}$$

Tehát $2^{3^{1111}} \equiv 2^1 \pmod{17}$.

Érdekes feladatok

7. Egy a egész esetén legyen $a^{-1} \mod m$ az *a multiplikatív inverze modulo* m, azaz az az elem, hogy $a^{-1} \cdot a \equiv 1 \mod m$. Döntse el, hogy az alábbiak közül melyek léteznek, és azokat számolja ki

   a) $3^{-1} \mod 7$; b) $3^{-1} \mod 8$; c) $0^{-1} \mod 8$; d) $2^{-1} \mod 8$
   e) $2^{-1} \mod 7$; f) $1^{-1} \mod 7$; g) $2^{-1} \mod 3$; h) $31^{-1} \mod 17$

   Megoldások: Tehát a következő kongruenciákat kell megoldani:

   a) $3x \equiv 1 \mod 7$; b) $3x \equiv 1 \mod 8$; c) $0x \equiv 1 \mod 8$; d) $2x \equiv 1 \mod 8$
   e) $2x \equiv 1 \mod 7$; f) $1x \equiv 1 \mod 7$; g) $2x \equiv 1 \mod 3$; h) $31x \equiv 1 \mod 17$

   Ezek megoldásai (pl. ad hoc észrevétellel, hogy $1 + 2 \cdot 7 = 15$, $1 + 8 = 9$, 0 és 8 legnagyobb közös osztója a 8, ami nem osztja 1-et, 2 és 8 legnagyobb közös osztója a 2, ami nem osztja 1-et, $1 + 7 = 8$, $1 + 3 = 4$, és végül $31 \equiv -3 \pmod{17}$, míg $1 + 17 = 18$):

   a) $x \equiv 5 \mod 7$; b) $x \equiv 3 \mod 8$; c) nincs megoldása; d) nincs megoldása
   e) $x \equiv 4 \mod 7$; f) $x \equiv 1 \mod 7$; g) $x \equiv 2 \mod 3$; h) $x \equiv -6 \equiv 11 \mod 17$

   A fenti kongruenciák akár bővített euklideszi algoritmussal is megoldhatók, ha nem jut eszünkbe ad hoc ötlet.

   Másik megoldás: Euler-Fermat tétel segítségével. $3^6 \equiv 1 \pmod 7$, ezért $3^{-1} \equiv 3^5 \pmod 7$. (Ez például gyorshatványozással számolható.) $3^4 \equiv 1 \pmod 8$, ezért $3^{-1} \equiv 3^3 \pmod 8$. $2^6 \equiv 1 \pmod 7$, ezért $2^{-1} \equiv 2^5 \pmod 7$. $2^2 \equiv 1 \pmod 3$, ezért $2^{-1} \equiv 2^1 \pmod 3$. És végül $31^{16} \equiv 1 \pmod{17}$, ezért $31^{-1} \equiv 31^{15} \pmod{17}$, ezt viszont tényleg csak gyorshatványozással tudjuk kiszámítani.

8. Határozza meg az utolsó két számjegyét a $7^{3^{47}}$ hatványnak!

   Megoldás: Azaz $7^{3^{47}} \mod 100$ értékét kell meghatározni. Mivel $\varphi(100) = 40$, és a 7 relatív prím a 100-hoz, $3^{47} \mod 40$ értéke lesz a kitevő.

A 3 a 40-hez relatív prím, ezért újra használható az Euler-Fermat tétel: a 3 kitevőjét modulo $\varphi(40) = 40 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 16$ kell nézni. $47 \mod 16 = 15$, ezért $3^{47} \equiv 3^{15} \mod 40$.

Mivel 3^{15} igazából 3-nak a reciproka modulo 40, és $81 \equiv 1 \pmod{40}$, vagyis $3 \cdot 27 \equiv 1 \pmod{40}$, ezért gyorshatványozás nélkül is rájöhetünk arra, hogy $3^{47} \equiv 3^{15} \equiv 3^{-1} \equiv 27 \mod 40$.

Tehát $7^{3^{47}} \equiv 7^{27} \mod 100$. Most már nem ússzuk meg a gyorshatványozást. $27 = 16+8+2+1$ bináris alakja 11011.

$$7^{27} \equiv \left(\left(\left((7^1)^2 \cdot 7^1\right)^2 \cdot 7^0\right)^2 \cdot 7^1\right)^2 \cdot 7^1 \equiv \left(\left(\left(43\right)^2 \cdot 7^0\right)^2 \cdot 7^1\right)^2 \cdot 7^1 \equiv$$

$$\left(\left(49\right)^2 \cdot 7^1\right)^2 \cdot 7^1 \equiv \left(1 \cdot 7^1\right)^2 \cdot 7^1 \equiv \left(7\right)^2 \cdot 7^1 \equiv 49 \cdot 7^1 \equiv 343 \equiv 43 \pmod{100}$$

Tehát $7^{3^{47}}$ utolsó két számjegye: 43.

Szorgalmi feladatok

8. Írjon programot, mely egy adott n esetén kiszámolja a $\varphi(n)$ értékét. Írjon tesztet, hogy ha egy véletlen k bites n számot választ, akkor várhatóan mennyi idő alatt számolja ki $\varphi(n)$-et: minden $k = 50, 100, 150, 200, 250, 300, 350, 400$ esetén válasszon 10 darab k bites számot, számolja ki φ értéket minden esetben és átlagolja az időket.