5. POSLEDNÉ ČÍSLICE MOCNÍN

Pripomíname, že pod poslednými číslicami nejakého prirodzeného čísla vždy myslíme posledné číslice jeho dekadického zápisu, pokiaľ výslovne neuvedieme iný základ. Ani pri zmene základu však nemeníme význam číslic 0 až 9.

Úloha 5.1. Nájdite poslednú číslicu čísla $A = 4^{1234567}$.

Riešenie I. Indukciou dokážeme, že pre každé $n \in \mathbb{N}$ končí 4^{2n+1} číslicou 4. Pre $n = 0$ to zrejme platí. Ak už vieme, že 4^{2n+1} končí číslicou 4, t. j. že platí $4^{2n+1} \equiv 4 \pmod{10}$, tak ľahko zistíme (počítame modulo 10)

$$4^{2(n+1)+1} = 4^{2n+1}.16 \equiv 4.6 \equiv 4 \pmod{10},$$

teda aj $4^{2(n+1)+1}$ končí číslicou 4. Tým je dôkaz indukciou ukončený. Podľa práve dokázaného tvrdenia, ktoré použijeme pre $n = \lfloor 1234567/2 \rfloor = 617283$, končí aj A číslicou 4. □

Riešenie II. Dokážeme, že $10|(A - 4)$. Pretože A je párne, platí $2|(A - 4)$, a treba ešte dokázať $5|(A - 4)$. Počítajme modulo 5

$$A - 4 \equiv (-1)^{1234567} - 4 = -1 - 4 =$$
$$= -5 \equiv 0 \pmod{5},$$

teda skutočne $5|(A - 4)$. Potom $10|(A - 4)$, a teda A končí číslicou 4. □

Táto úloha bola taká ľahká, že ju čitateľ zaiste vedel vyriešiť spamäti. Pravdepodobne pritom postupoval podľa prvého riešenia, ale indukciu urobil intuitívne: všimol si pravidelné striedanie číslic 4, 6 v postupnosti mocnín štvorky. Uvedené riešenia, najmä prvé z nich mali skôr upozorniť čitateľa na princípy, ktoré sám používa, než naučiť ho niečo nové. V ďalších úlohách už nevypisujeme riešenia tak podrobne.

Úloha 5.2. Nájdite poslednú číslicu čísla $B = 7^{4567890}$.

Riešenie. Čísla 7, 10 sú nesúdeliteľné, $\varphi(10) = 4$, a preto podľa Eulerovej vety platí (počítame modulo 10)

$$B \equiv 7^{4567890 \bmod 4} = 7^2 \equiv 9 \pmod{10}.$$

Teda posledná číslica čísla B je 9. $\square$

Úloha 5.3. Nájdite poslednú číslicu čísla $C = 13^{17^{19}}$.

Riešenie. Použijeme Eulerovu vetu a počítame modulo 10

$$C \equiv 3^{17^{19}} \equiv 3^{17^{19} \bmod 4} = 3^{1^{19} \bmod 4} = 3^1 = 3 \pmod{10}.$$

Teda posledná číslica čísla C je 3. $\square$

Úloha 5.4. Nájdite poslednú číslicu čísla $D = 17^{15^{13^{11}}}$.

Riešenie. Použijeme Eulerovu vetu a počítame modulo 10. Platí

$$D \equiv 7^{15^{13^{11}} \bmod 4} = 7^{3^{13^{11} \bmod 2} \bmod 4} = 7^{3^1 \bmod 4} =$$
$$= 7^3 \equiv 3 \pmod{10}.$$

Teda hľadaná posledná číslica je 3. $\square$

Nechâme čitateľovi na rozmyslenie, že výsledok by sa nezmenil, keby sme k „štvorposchodovej mocnine", ktorou je dané číslo D, na ďalšie „poschodia" pridali napríklad 9, 7, 5.

Úloha 5.5. Nájdite posledné dvojčíslie čísla 7^{1986}.

Riešenie. Treba vlastne určiť 7^{1986} MOD 100.
Pretože 7^4 MOD 100 = 2401 MOD 100 = 1, platí

$$7^{1986} \text{ MOD } 100 = 7^{4.496+2} \text{ MOD } 100 = (7^4 \text{ MOD } 100)^{496} .$$
$$.(7^2 \text{ MOD } 100) \text{ MOD } 100 = 1^{496} . 49 \text{ MOD } 100 = 49 .$$

Teda hľadané posledné dvojčíslie je 49. □

Keby sme hľadali posledné dvojčíslie čísla 7^{1988}, vyšlo by nám obdobným výpočtom číslo 1; hľadané dvojčíslie by potom bolo 01.

Úloha 5.6. Nájdite najmenšie celé kladné číslo n také, že

$$327^{n+1} \equiv 327 \pmod{1000} .$$

Riešenie. Pretože $D(327, 1000) = 1$, je uvedená kongruencia ekvivalentná s kongruenciou

$$327^n \equiv 1 \pmod{1000} .$$

Táto kongruencia je zasa ekvivalentná so systémom kongruencií

$$327^n \equiv 1 \pmod{8} , \quad 327^n \equiv 1 \pmod{125} ;$$

tu sme využili rozpis $1000 = 8 . 125$, pričom $D(8, 125) =$ $= 1$. Druhá kongruencia dáva

$$77^n \equiv 1 \pmod{125} . \tag{1}$$

Pretože $\varphi(125) = 100$, podľa Eulerovej vety dostávame

$$77^{100} \equiv 1 \pmod{125}.$$

Preto najmenšie kladné riešenie n kongruencie (1) je deliteľom čísla 100. Číslo n však nie je deliteľom čísla 20 ani čísla 50, pretože (počítame modulo 125)

$$77^{20} = (75 + 2)^{20} \equiv \binom{20}{1}.75.2^{19} + 2^{20} \equiv 0 + (2^{10})^2 \equiv$$

$$\equiv 24^2 \equiv 76 \not\equiv 1 \pmod{125},$$

$$77^{50} = (75 + 2)^{50} \equiv \binom{50}{1}.75.2^{49} + 2^{50} \equiv 0 + (2^{10})^5 \equiv$$

$$\equiv 24^5 \equiv (25 - 1)^5 \equiv + \binom{5}{1}.25.1^4 - 1^5 \equiv$$

$$\equiv -1 \not\equiv 1 \pmod{125}.$$

Teda najmenšie kladné riešenie kongruencie (1) je $n = 100$, a to zrejme vyhovuje aj prvej kongruencii (tej vyhovuje každé párne prirodzené n). Teda $n = 100$ je aj riešením úlohy. □

Úloha 5.7. Dokážte, že neexistuje celé kladné číslo n také, že 7516^{n+1} končí štvorčíslím 7516.

Riešenie. Platí $4 \mid 7516$, $8 \mid 4^2$, a teda $8 \mid 7516^{n+1}$ pre každé celé kladné n. Avšak žiadne číslo končiace štvorčíslím 7516 nie je deliteľné ôsmimi. □

Úloha 5.8. Určite posledných šesť číslic čísla $A = 5^{678901^{234}}$.

Riešenie. Treba určiť číslo A MOD 10^6, a na to najprv určíme A MOD 2^6, A MOD 5^6. Pretože $D(5, 64) = 1$

a $\varphi(64) = 32$, podľa Eulerovej vety platí $5^{32} \equiv 1 \pmod{64}$, a potom zrejme aj $A \equiv 1 \pmod{64}$. Ďalej zrejme platí $5^6 | A$, a preto pre $B = A \text{ MOD } 10^7$ platí

$$B \equiv 1 \pmod{64}, \qquad B \equiv 0 \pmod{15625}$$

(mocniny 2^6, 5^6 sme vypočítali). Tieto kongruencie spolu s nerovnosťou $0 \leqq B < 10^6$ jednoznačne určujú B. Z druhej kongruencie vieme $B = 15625x$ pre nejaké celé číslo x; ľahko zistíme $0 \leqq x < 64$. Dosadením do prvej kongruencie dostávame

$$\begin{aligned} 15625x &\equiv 1 \pmod{64}, \\ 9x &\equiv 1 \pmod{64}, \\ -63x &\equiv -7 \pmod{64}, \\ x &\equiv 57 \pmod{64}, \end{aligned}$$

teda vzhľadom na nerovnosť pre x dostávame $x = 57$, a potom

$$B = 57 . 15625 = 890625 .$$

Teda posledné šesťčíslie čísla A je 890625. □

Kongruenciu pre x sme mohli tiež upraviť takto

$$\begin{aligned} 5^6 x &\equiv 1 \pmod{64}, \\ x &\equiv 5^{26} \pmod{64}, \\ 5^6 x &\equiv 5^{32} \pmod{10^6}. \end{aligned}$$

Pretože $B = 5^6 x$, platí

$$\begin{aligned} B &= 5^{32} \text{MOD } 10^6 = 25^{16} \text{MOD } 10^6 = \\ &= 625^8 \text{MOD } 10^6 = 390\,625^4 \text{MOD } 10^6 = \\ &= 890\,625^2 \text{MOD } 10^6 = 890\,625. \end{aligned}$$

V poslednom výpočte sme potrebovali päť umocnení na druhú, pretože $32 = 2^5$. Jedno (a to posledné) umocnenie sme si mohli ušetriť pomocou vzťahu $5^{16} \equiv 1 \pmod{64}$, ktorý síce nevyplýva z Eulerovej vety, ale ľahko ho dostaneme napríklad z binomického rozvoja pre $(4 + 1)^{16}$.

Úloha 5.9. Určte posledné trojčíslie čísla $A = 9^{9^9}$.

Riešenie I (s tabuľkami). Pretože $\varphi(1000) = 400$, budeme potrebovať 9^9 MOD 400. Priamo z tabuliek zistíme, že posledné štvorčíslice čísla 9^9 je 0489, teda 9^9 MOD $400 = 89$. Potom platí (počítame modulo 1000)

$$A \equiv 9^{89} = 3^{178} = 3^3.(3^{35})^5 \equiv 27.707^5 =$$
$$= 27.101^5.7^5 \equiv 27.501.807 \equiv 27.307 \equiv$$
$$\equiv 289 \pmod{1000}.$$

Teda A MOD $1000 = 289$, čo je hľadané posledné trojčíslie. □

Poznamenajme, že namiesto $\varphi(1000) = 400$ sme mohli uvažovať $\lambda(1000) = 100$, teda $9^{100} \equiv 1 \pmod{1000}$. Exponent 89 by sme tým však neznížili.

Riešenie II. Najprv zistíme 9^9MOD 100.
Počítame modulo 100 a používame binomickú vetu, pričom násobky 100 už vynechávame.

$$9^9 = (10 - 1)^9 \equiv \binom{9}{1}.10 - 1 = 89 \pmod{100}.$$

Teraz ľahko zjistíme poslednú číslicu čísla $\binom{9^9}{2}$, pretože (počítame modulo 10)

$$\binom{9^9}{2} = 9^9.\frac{9^9 - 1}{2} \equiv 9.4 \equiv 6 \pmod{10}.$$

Ďalej znova používame binomickú vetu, ale počítame modulo 1000:

$$9^{9^9} = (10 - 1)^{9^9} \equiv -\binom{9^9}{2}.100 + \binom{9^9}{1}.10 - 1 \equiv$$

$$\equiv -600 + 890 - 1 \equiv 289 \pmod{1000}.$$

Teda posledné trojčíslie čísla 9^{9^9} je 289. □

Iný možný postup by bol určiť, že

$$A \text{ MOD } 125 = 39, \qquad A \text{ MOD } 8 = 1$$

a pomocou týchto hodnôt určiť A MOD 1000.

Úloha 5.10. Určte posledné trojčíslie čísla $B = 8^{8^8}$.

Riešenie. Využijeme rozklad $1000 = 125.8$. Aby sme mohli určiť B MOD 125, určíme najskôr 8^8MOD 100. Platí (počítame modulo 100)

$$8^8 = 64^4 = 4\,096^2 \equiv (-4)^2 = 16 \pmod{100}.$$

Preto (teraz počítame modulo 125)

$$B \equiv 8^{8^8 \text{ MOD } 100} = 8^{16} = 2^{48} = 256^6 \equiv 6^6 =$$
$$= 216^2 \equiv (-34)^2 = 1\,156 \equiv 31 \pmod{125}.$$

Potom platí

$$B \text{ MOD } 1000 = 31 + k.125$$

pre nejaké celé číslo k; zrejme $0 \leqq k \leqq 7$. Pretože

$$(B \text{ MOD } 1000) \text{ MOD } 8 = B \text{ MOD } 8 = 0,$$

máme

$$31 + k.125 \equiv 0 \pmod 8,$$
$$5k \equiv 1 \pmod 8,$$
$$k \equiv 5 \pmod 8,$$

a teda $k = 5$. Potom

$$B \text{ MOD } 1000 = 31 + 5\,.\,125 = 656.$$

Teda hľadané posledné trojčíslie čísla B je 656. $\square$

Úloha 5.11. Určte posledné trojčíslie čísla $C = 7^{8^9}$.

Riešenie. Budeme počítať C MOD 1000, pričom využijeme Eulerovu vetu pre moduly 8 a 125 a skutočnosť, že

$$nsn(\varphi(8), \varphi(125)) = 100.$$

Počítajme modulo 1000 ; platí

$$C \equiv 7^{8^9 \text{ MOD } 100} \equiv 7^{512^3 \text{ MOD } 100} \equiv 7^{12^3 \text{ MOD } 100} \equiv 7^{28} \equiv$$

$$\equiv 2401^7 \equiv (400 + 1)^7 \equiv 7\,.\,400 + 1 \equiv 801 \pmod{1000}.$$

Teda číslo C končí trojčíslím 801. $\square$

Úloha 5.12. Určte poslednú číslicu sedmičkového zápisu čísla $A = 10^{10^{10}}$.

Riešenie. Máme vlastne určiť A MOD 7. Pri počítaní modulo 7 platí

$$A \equiv 3^{10^{10}} \equiv 3^{10^{10} \text{ MOD } 6} \equiv 3^4 \equiv 4 \pmod 7.$$

Teda hľadaná posledná číslica je štvorka. $\square$

Určenie poslednej číslice z-adického zápisu čísla A pre ostatné základy menšie než 10 je ešte ľahšie, a čitateľ by to mal bez ťažkostí spraviť i spamäti.

Úloha 5.13. Určte posledné trojčíslie deviatkového zápisu čísla $A = 10^{10^{10}}$.

Riešenie. Budeme počítať modulo 9^3 a používať binomickú vetu; zrejmé násobky 9^3 budeme ihneď vynechávať, a využijeme tiež $9 \mid (10^{10} - 1)$, tedy aj $9 \Big| \binom{10^{10}}{2}$.

$$A = (9 + 1)^{10^{10}} \equiv \binom{10^{10}}{2} . 9^2 + \binom{10^{10}}{1} . 9 + 1 \equiv$$
$$\equiv 0 + 10^{10} . 9 + 1 = (9 + 1)^{10} . 9 + 1 \equiv$$
$$\equiv (10 . 9 + 1) . 9 + 1 \equiv 1 . 9^2 + 1 . 9 + 1 \pmod{9^3}.$$

Teda posledné trojčíslie deviatkového zápisu čísla A je 111. □

Úloha 5.14. Určte posledné trojčíslie sedmičkového zápisu čísla $A = 10^{10^{10}}$.

Riešenie. Budeme počítať modulo $7^3 = 343$ a využívať Eulerovu vetu. Počas výpočtu používame dekadické zápisy. Naprv určíme $10^{10} \mathrm{MOD}\, \varphi(343)$, t. j. $10^{10} \mathrm{MOD}\, 294$. Využijeme rozklad $294 = 6 . 49$. Platí

$$10^{10} \mathrm{MOD}\, 49 = 100^5 \mathrm{MOD}\, 49 = 2^5 \mathrm{MOD}\, 49 = 32,$$

a preto $10^{10} \mathrm{MOD}\, 294 = 32 + 49\, k$ pre vhodné celé číslo k. Pretože $10^{10} \mathrm{MOD}\, 6 = 4$, má byť aj $(32 + 49k) \mathrm{MOD}\, 6 = 4$, teda $(2 + k)\, \mathrm{MOD}\, 6 = 4$, odkiaľ vyplýva $k \equiv 2 \pmod 6$.
Pretože však zrejme $0 \leqq k \leqq 5$, máme $k = 2$ a

$$10^{10} \mathrm{MOD}\, 294 = 32 + 49 . 2 = 130.$$

Teraz počítajme modulo 343. Platí

$$A \equiv 10^{10^{10} \mathrm{MOD}\, 294} = 10^{130} = 100^{65} = 4 . 8^{21} . 50^{65} =$$
$$= 4 . (7 + 1)^{21} . (49 + 1)^{65} \equiv 4 . \left(\binom{21}{2} . 7^2 + 21 . 7 + 1\right) .$$

$$.(65.49 + 1) \equiv 4.(0 + 3.7^2 + 1).(2.7^2 + 1) \equiv$$
$$\equiv 4.(5.7^2 + 1) = 20.7^2 + 4 \equiv$$
$$\equiv 6.7^2 + 0.7 + 4 \pmod{343}.$$

Teda posledné trojčíslie sedmičkového zápisu čísla A je 604. $\square$