Řešené příklady na „poslední dvě cifry“

1. $23^{24^{25}}$ Hledáme poslední dvě cifry.

   $\varphi(100) = (4-2)(25-5) = 40$, takže pro libovolné a nesoudělné se 100 platí podle Eulerovy věty $a^{40} \equiv 1(mod\ 100)$. Takže kdyby se nám podařilo zjistit zbytek 24^{25} modulo 40, věděli bychom, že 23 (nesoudělné se 100) umocněno na ten zbytek má stejné poslední dvě cifry jako $23^{24^{25}}$. Jenže jednoduše pomocí Eulerovy věty to nezjistíme, protože 24 a 40 nejsou nesoudělná (takže předpoklady Eulerovy věty nejsou splněny).

   První plán nám nevyšel - nevadí, jdeme sbírat dílčí informace.

   Můžeme si pomoci tím, že najdeme poslední cifru - zbytek po dělení 10. $\varphi(10) = (2-1)(5-1) = 4$. Největší společný dělitel 23 a 10 je 1. Tedy můžeme použít Eulerovu větu. Podle ní je $23^4 \equiv 1(mod\ 10)$. Je $24^{25} = 4 \cdot 6 \cdot 24^{24}$. Tedy $23^{4 \cdot 6 \cdot 24^{24}} \equiv 1^{6 \cdot 24^{24}}(mod\ 10)$, neboli $23^{24^{25}} \equiv 1(mod\ 10)$. Poslední cifra je tedy 1.

   Další informaci získáme pomocí zbytků po dělení čísla $23^{24^{25}}$ čísly 25 a 4. Víme, že 100 je dělitelné 4 a 25, takže každé přirozené číslo n dává po dělení 4 a 25 stejné zbytky jako číslo, které získáme, když od n odečteme všechny stovky (např. 19987 jako 87).

   Hledáme zbytek $23^{24^{25}}$ po dělení 25. $\varphi(25) = (25-5) = 20$. Největší společný dělitel 23 a 25 je 1. Tedy podle Eulerovy věty je $23^{20} \equiv 1(mod\ 25)$.

   Hledáme zbytek 24^{25} po dělení 20. Je

   $$24^{25} = 4 \cdot 6 \cdot 24^{24} = 4 \cdot (5+1) \cdot (25-1)^{24}$$

   $$4 \cdot (5+1) \cdot (25-1)^{24} \equiv (20+4) \cdot (25-1)^{24} \equiv 4 \cdot (25-1)^{24}(mod\ 20)$$

   Zajímá nás zbytek $4 \cdot (25-1)^{24}$ po dělení 5.

   $$(25-1)^{24} \equiv (-1)^{24} \equiv 1(mod\ 5)$$

   (V poslední úpravě si uvědomíme, že jde o 24 závorek ve kterých je v každé vždy jeden člen nedělitelný 5, takže celý součin musí dávat stejný zbytek po dělení 5 jako $(-1)^{24} = 1$.)

   Tedy $24^{25} \equiv 4 \cdot (5k+1)(mod\ 20)$ pro nějaké celé k, neboli

   $$24^{25} \equiv 4 \cdot (5k+1) \equiv (20k+4) \equiv 4(mod\ 20)$$

   $$23^{24^{25}} \equiv 23^4 \equiv (25-2)^4 \equiv (-2)^4 \equiv 16(mod\ 25)$$

   Získali jsme informaci, že $23^{24^{25}}$ dává zbytek 16 po dělení 25.

   Teď hledáme zbytek $23^{24^{25}}$ po dělení 4. $\varphi(4) = (4-2) = 2$. Největší společný dělitel 23 a 4 je 1. Tedy podle Eulerovy věty je $23^2 \equiv 1(mod\ 10)$. Je $24^{25} = 2 \cdot 12 \cdot 24^{24}$. Tedy je to sudé číslo, a proto

   $$23^{24^{25}} \equiv 1(mod\ 4)$$

   Dejme nyní tyto informace dohromady. Poslední cifra omezuje řešení na prvky množiny $\{01, 11, 21, 31, 41, 51, 61, 71, 81, 91\}$. Zbytek po dělení 25

říká, že řešení je v množině $\{16, 41, 76, 91\}$. Zbytek po dělení 4 říká, že řešení je v množině

$\{01, 05, 09, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97\}$

Takže jsme dospěli k výsledku 41. (Na určení výsledku by nám stačila dělitelnost 4 a 25 a určitě nemusíme vypisovat tu poslední množinu celou, stačí ověřit zbytek po dělení 4 z dosud nabízených možností.)

2. 7^{9^9} - máme najít poslední dvě cifry (příklad ze skript).

$$\varphi(100) = (4-2)(25-5) = 40$$

7 je nesoudělné se 100. Podle Eulerovy věty $7^{40} \equiv 1(mod\ 100)$.

Takže kdyby se nám podařilo zjistit zbytek 9^9 modulo 40, věděli bychom, že 7 (nesoudělné se 100) umocněno na ten zbytek má stejné poslední dvě cifry jako 7^{9^9}.

Hledáme zbytek $9^9 = 3^{18}$ **modulo** 40. $\varphi(40) = (8-4)(5-1) = 16$, 3 je nesoudělné se 40. Podle Eulerovy věty $3^{16} \equiv 1(mod\ 40)$. Takže $3^{18} \equiv 3^2 \equiv 9(mod\ 40)$ Zbytek 9^9 po dělení 40 je tedy 9.

Takže podle Eulerovy věty platí

$$7^{9^9} \equiv 7^9(mod\ 100)$$

$$7^9 \equiv (7^3)^3 \equiv 343^3 \equiv 43^3 = 79507 \equiv 7(mod\ 100)$$

Poslední dvě cifry jsou 07.

Definice svazu (převzatá z teorie množin a teorie svazů)

Řekneme, že *uspořádaná* množina S je **svazem** s operacemi infimum a supremum, pokud je neprázdná a pro každou její dvouprvkovou podmnožinu $\{x, y\}$ existuje supremum a infimum této množiny v S.

Poznámka: supremum a infimum počítáme vzhledem k danému uspořádání (reflexivní, antisymetrická, tranzitivní relace - nemusí být úplné) na množině S s argumentem - množinou - ne uspořádanou dvojicí (x, y), takže je automaticky komutativní, a argumentem může být i víceprvková množina, takže je i asociativní. Nemusí být distributivní.