

- a) Kako je eksponent relativno mali, odmah ćemo primijeniti metod “kvadriraj-i-množi”:

$$\begin{aligned}([7]_{91})^2 &= [49]_{91} \\ ([7]_{91})^4 &= ([49]_{91})^2 = [2401]_{91} = [\text{mod}(2401, 91)]_{91} = [35]_{91} \\ ([7]_{91})^8 &= ([35]_{91})^2 = [1225]_{91} = [\text{mod}(1225, 91)]_{91} = [42]_{91} \\ ([7]_{91})^{16} &= ([42]_{91})^2 = [1764]_{91} = [\text{mod}(1764, 91)]_{91} = [35]_{91}\end{aligned}$$

Konačno je:

$$([7]_{91})^{20} = ([7]_{91})^{16} ([7]_{91})^4 = ([35]_{91}) ([35]_{91}) = [1225]_{91} = [42]_{91}$$

- b) Kako je $80 > 65$ i $\text{NZD}(4, 65) = 1$, isplati se reducirati eksponent prema Fermat-Eulerovoj teoremi. Imamo:

$$\varphi(65) = \varphi(5 \cdot 13) = \varphi(5) \varphi(13) = (5 - 1)(13 - 1) = 48.$$

Sada, na osnovu Fermat-Eulerove teoreme imamo:

$$([4]_{65})^{80} = ([4]_{65})^{\text{mod}(80, \varphi(65))} = ([4]_{65})^{\text{mod}(80, 48)} = ([4]_{65})^{32}.$$

Dalje nastavljamo prema metodu “kvadriraj-i-množi”:

$$\begin{aligned}([4]_{65})^2 &= [16]_{65} \\ ([4]_{65})^4 &= ([16]_{65})^2 = [256]_{65} = [\text{mod}(256, 65)]_{65} = [61]_{65} \\ ([4]_{65})^8 &= ([61]_{65})^2 = [3721]_{65} = [\text{mod}(3721, 65)]_{65} = [16]_{65} \\ ([4]_{65})^{16} &= ([16]_{65})^2 = [61]_{65} \\ ([4]_{65})^{32} &= ([61]_{65})^2 = [16]_{65}\end{aligned}$$

Ovdje smo samo prepisali rezultate koji su već jednom izračunati. Dakle, imamo:

$$([4]_{65})^{80} = ([4]_{65})^{32} = [16]_{65}$$

- c) I ovdje je isplativa redukcija eksponenta, jer je $100 > 79$ i $\text{NZD}(3, 79) = 1$. Kako je 79 prost broj, to je $\varphi(79) = 79 - 1 = 78$. Stoga je:

$$([3]_{79})^{100} = ([3]_{79})^{\text{mod}(100, \varphi(79))} = ([3]_{79})^{\text{mod}(100, 78)} = ([3]_{79})^{22}.$$

Dalje nastavljamo prema metodu “kvadriraj-i-množi”:

$$\begin{aligned}([3]_{79})^2 &= [9]_{79} \\ ([3]_{79})^4 &= ([9]_{79})^2 = [81]_{79} = [\text{mod}(81, 79)]_{79} = [2]_{79} \\ ([3]_{79})^8 &= ([2]_{79})^2 = [4]_{79} \\ ([3]_{79})^{16} &= ([4]_{79})^2 = [16]_{79}\end{aligned}$$

Konačno je:

$$\begin{aligned}([3]_{79})^{100} &= ([3]_{79})^{22} = ([3]_{79})^{16} ([3]_{79})^4 ([3]_{79})^2 = ([16]_{79}) ([2]_{79}) ([9]_{79}) = \\ &= ([16]_{79}) ([18]_{79}) = [288]_{79} = [\text{mod}(288, 79)]_{79} = [51]_{79}\end{aligned}$$

- d) Redukcija eksponenta ovdje bi bila veoma korisna, jer je eksponent 100000 prilično velik. Nažalost, imamo $\text{NZD}(6, 24) = 6 \neq 1$, pa Fermat-Eulerova teorema ne vrijedi. Srećom, vidjećemo da to ovdje nije problem. Zaista, imamo:

$$\begin{aligned}([6]_{24})^2 &= [36]_{24} = [\text{mod}(36, 24)]_{24} = [12]_{24} \\ ([6]_{24})^4 &= ([12]_{24})^2 = [144]_{24} = [\text{mod}(144, 24)]_{24} = [0]_{24}\end{aligned}$$

Dakle, imamo $([6]_{24})^4 = [0]_{24}$, pa je jasno da je $([6]_{24})^k = [0]_{24}$ za sve $k \geq 4$ (zapravo, ovo vrijedi već za $k \geq 3$). Stoga je:

$$([6]_{24})^{1000000} = [0]_{24}.$$

- e) Bespredmetno je i govoriti da je u ovom slučaju redukcija eksponenta od velike koristi. Kako je 23 prost broj, to je $\varphi(23) = 23 - 1 = 22$. Sada prema Fermat-Eulerovoj teoremi imamo:

$$([7]_{23})^{1000000} = ([7]_{23})^{\text{mod}(1000000, 22)} = ([7]_{23})^{12}$$

Dalje, imamo:

$$\begin{aligned}([7]_{23})^2 &= [49]_{23} = [3]_{23} \\ ([7]_{23})^4 &= ([3]_{23})^2 = [9]_{23} \\ ([7]_{23})^8 &= ([9]_{23})^2 = [81]_{23} = [12]_{23}\end{aligned}$$

Konačno je:

$$([7]_{23})^{1000000} = ([7]_{23})^{12} = ([7]_{23})^8 ([7]_{23})^4 = ([12]_{23})([9]_{23}) = [108]_{23} = [16]_{23}$$