Sprawdzian 3

1. Wyznaczyć resztę z dzielenia liczby 541^{541} przez 37.
2. Kapral przygotowuje oddział liczący mniej niż 150 żołnierzy do defilady. Gdy ustawi go trójkami lub piątkami, zawsze zostaje mu jeden żołnierz. Gdy ustawi go siódemkami, każdy rząd jest wypełniony. Ile osób liczy oddział?

Rozwiązania

1. Szukamy rozwiązania kongruencji:
$$X \equiv 541^{541} (\mathsf{mod}\, 37)$$
w zbiorze $\{0, 1, \ldots, 36\}$. Ponieważ $541 \equiv 23 (\mathsf{mod}\, 37)$, więc $541^{541} \equiv 23^{541} (\mathsf{mod}\, 37)$ i badana kongruencja sprowadza się do:
$$X \equiv 23^{541} (\mathsf{mod}\, 37).$$
Ponieważ $NWD(23, 37) = 1$, więc wobec twierdzenia Eulera $23^{\phi(37)} \equiv 1 (\mathsf{mod}\, 37)$. Oczywiście $\phi(37) = 36$ i $541 = 36 \cdot 15 + 1$, tak więc:
$$23^{541} = 23^{36 \cdot 15 + 1} = (23^{36})^{15} \cdot 23^1 \equiv 23 (\mathsf{mod}\, 37)$$
i rozważana kongruencja przyjmuje postać:
$$X \equiv 23 (\mathsf{mod}\, 37).$$
Zatem resztą z dzielenia 541^{541} przez 37 jest 23.
2. Szukamy rozwiązania układu kongruencji:
$$\begin{cases} X \equiv 1 (\mathsf{mod}\, 3) \\ X \equiv 1 (\mathsf{mod}\, 5) \\ X \equiv 0 (\mathsf{mod}\, 7) \end{cases}$$
w zbiorze $\{1, 2, \ldots, 150\}$. Ponieważ $3, 5, 7$ są parami względnie pierwsze, możemy zastosować chińskie twierdzenie o resztach. Niech $M = 3 \cdot 5 \cdot 7 = 105$ oraz niech
   - y_1 będzie rozwiązaniem kongruencji
   $$\frac{105}{3} y_1 = 35 y_1 \equiv 1 (\mathsf{mod}\, 3),$$
   - y_2 będzie rozwiązaniem kongruencji
   $$\frac{105}{5} y_2 = 21 y_2 \equiv 1 (\mathsf{mod}\, 5),$$
   - y_3 będzie rozwiązaniem kongruencji
   $$\frac{105}{7} y_3 = 15 y_3 \equiv 1 (\mathsf{mod}\, 7).$$

   Rozwiązujemy po kolei dane kongruencje:
   - Rozwiązanie $35 y_1 \equiv 1 (\mathsf{mod}\, 3)$ to y_1 z rozwiązania równania $35 y_1 - 3 z_1 = 1$. Wobec algorytmu Euklidesa:
   $$35 = (-3) \cdot (-11) + 2, \quad -3 = 2 \cdot (-2) + 1,$$
   skąd:
   $$1 = -3 + 2 \cdot 2 = -3 + 2(35 + 11 \cdot (-3)) = 35 \cdot 2 - 3 \cdot 23,$$
   czyli $y_1 = 2$.
   - Rozwiązanie $21 y_2 \equiv 1 (\mathsf{mod}\, 5)$ to y_2 z rozwiązania równania $21 y_2 - 5 z_2 = 1$. Wobec algorytmu Euklidesa:
   $$21 = (-5) \cdot (-4) + 1,$$
   skąd:
   $$1 = 21 \cdot 1 - 5 \cdot 4,$$
   czyli $y_2 = 1$.
   - Rozwiązanie $15 y_3 \equiv 1 (\mathsf{mod}\, 7)$ to y_3 z rozwiązania równania $15 y_3 - 7 z_3 = 1$. Wobec algorytmu Euklidesa:
   $$15 = (-7) \cdot (-2) + 1,$$
   skąd:
   $$1 = 15 \cdot 1 - 7 \cdot 2,$$
   czyli $y_3 = 1$.

   Wobec tego $X = \frac{105}{3} \cdot 2 \cdot 1 + \frac{105}{5} \cdot 1 \cdot 1 + \frac{105}{7} \cdot 1 \cdot 0 = 70 + 21 = 91$ jest jedynym rozwiązaniem układu kongruencji $(\mathsf{mod}\, 105)$. Następne rozwiązanie $105 + 91 = 196$ jest już większe od 150, tak więc oddział liczył 91 żołnierzy.