

Chińskie tw. o resztach i funkcja Eulera

Stefan Sokołowski

Elbląg, 11 V 2025

1 Chińskie twierdzenie o resztach

Poniższe twierdzenie służy do wyznaczania liczby (x w poniższej ramce) na podstawie znajomości reszt z jej dzielenia przez znane „moduły” $m_1, m_2, \dots, m_k$. Okazuje się, że przy pewnych założeniach to się daje zrobić z dokładnością do dodawania wielokrotności iloczynu $m_1 \cdot m_2 \cdot \dots \cdot m_k$.

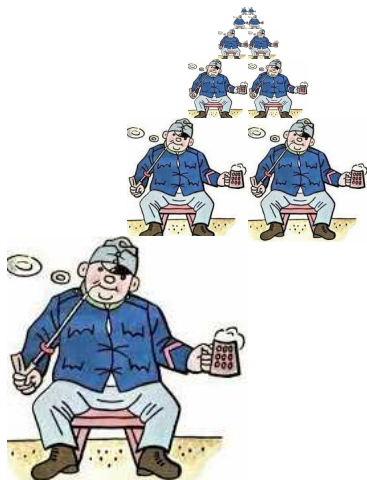
Na następnej stronie zilustrowana jest próba ustawienia oddziału x żołnierzy w różne szyki, przy czym okazuje się, że

- w szyku dwójkowym jeden pozostaje bez swojej dwójki, czyli $x \equiv_2 1$;
- w szyku trójkowym dwóch pozostaje bez swojej trójki, czyli $x \equiv_3 2$;
- w szyku piątkowym trzech pozostaje bez swojej piątki, czyli $x \equiv_5 3$.

Okazuje się, że stąd już wynika, że x może być każdą z liczb postaci $23 + 30 \cdot k$ dla dowolnego całkowitego k . Jeśli więc „widać na oko”, że liczba żołnierzy w oddziale jest dodatnia, ale nie większa niż 50, to jedyną możliwością jest $x = 23$.

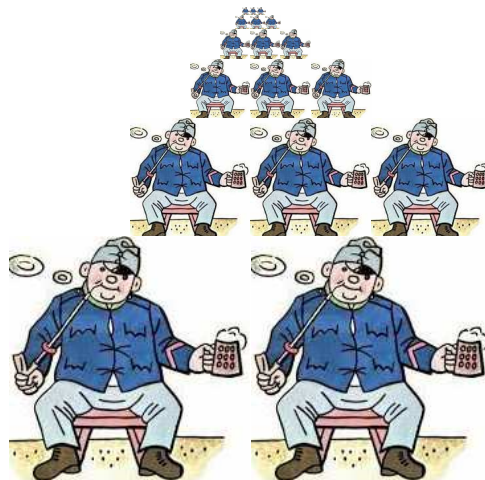
Chińskie twierdzenie o resztach służy do rozwiązywania takich właśnie układów kongruencji, czyli do ustalania wielkości x w oparciu o jej reszty z dzielenia przez ustalone moduły.

Przy ustawieniu parami...



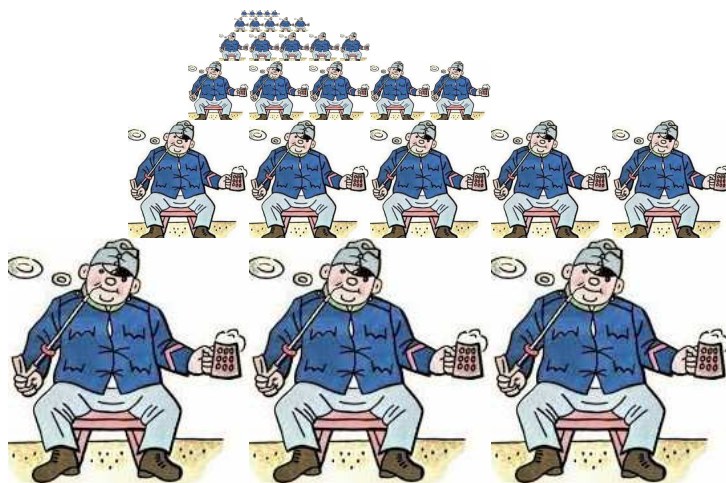
...jeden został bez pary.

Przy ustawieniu trójkami...



...dwaj zostali bez trójki.

Przy ustawieniu piątkami...



...trzej zostali bez piątki.

Stąd wynika, że wszystkich było 23.

Chińskie twierdzenie o resztach

Założmy, że

1. $m_1, \dots, m_k \in \mathbb{N} \setminus \{0\}$ są parami względnie pierwsze, oraz
2. $a_1, \dots, a_k \in \mathbb{N}$.

Dla rozwiązania układu kongruencji

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \dots \\ x \equiv_{m_k} a_k \end{cases}$$

(1)

$$\begin{cases} \frac{M}{m_1} \cdot s_1 \equiv_{m_1} 1 \\ \frac{M}{m_2} \cdot s_2 \equiv_{m_2} 1 \\ \dots \\ \frac{M}{m_k} \cdot s_k \equiv_{m_k} 1 \end{cases}$$

najpierw znajdujemy $s_1, s_2, \dots, s_k$ takie że

Układ (1) ma dokładnie jedno rozwiązanie x_0 modulo $M = m_1 \cdot \dots \cdot m_k$, dane wzorem

$$x_0 = \frac{M}{m_1} \cdot s_1 \cdot a_1 + \frac{M}{m_2} \cdot s_2 \cdot a_2 + \dots + \frac{M}{m_k} \cdot s_k \cdot a_k$$

Zadanie 1:

Z chińskiego twierdzenia o resztach wyznaczyć najmniejsze dodatnie rozwiązanie układu kongruencji:

$$\begin{cases} x \equiv_3 2 \\ x \equiv_7 4 \\ x \equiv_{10} 6 \end{cases} \quad (2)$$

Rozwiązanie:

Moduły 3, 7 i 10 są parami względnie pierwsze (**proszę nigdy nie zapominać o sprawdzeniu tego warunku!**), więc można stosować chińskie twierdzenie o resztach. Zaczynamy od rozwiązania kongruencji¹:

$$\begin{cases} \frac{3 \cdot 7 \cdot 10}{3} \cdot s_1 \equiv_3 1 \\ \frac{3 \cdot 7 \cdot 10}{7} \cdot s_2 \equiv_7 1 \\ \frac{3 \cdot 7 \cdot 10}{10} \cdot s_3 \equiv_{10} 1 \end{cases} \quad \text{Rozwiązaniami są:} \quad \begin{cases} s_1 \equiv_3 1 \\ s_2 \equiv_7 4 \\ s_3 \equiv_{10} 1 \end{cases}$$

Wobec tego rozwiązaniem oryginalnego układu (2) kongruencji jest

$$\begin{aligned} x_0 &= \frac{3 \cdot 7 \cdot 10}{3} \cdot 1 \cdot 2 + \frac{3 \cdot 7 \cdot 10}{7} \cdot 4 \cdot 4 + \frac{3 \cdot 7 \cdot 10}{10} \cdot 1 \cdot 6 \\ &= 140 + 480 + 126 = 746 \equiv_{3 \cdot 7 \cdot 10} 116 \end{aligned}$$

¹Dla przyspieszenia obliczeń można użyć programu

`iis.ans-elblag.pl/~stefan/Dydaktyka/MatDysk/Programy/euklides.c`
stosującego rozszerzony algorytm Euklidesa.

(bo $3 \cdot 7 \cdot 10 = 210$). Wobec tego wszystkie rozwiązania mają postać

$$x = 116 + k \cdot 210 \quad (\text{dla } k \in \mathbb{Z})$$

Zadanie 2:

Sprawdzić, że w przykładzie na stronach 1–2 rozwiązanie $23 + 30 \cdot k$ istotnie wynika z chińskiego twierdzenia o resztach.

Zadanie 3:

Z chińskiego twierdzenia o resztach wyznaczyć najmniejsze dodatnie rozwiązania układów kongruencji:

$$(a) \begin{cases} x \equiv_3 2 \\ x \equiv_5 3 \\ x \equiv_{11} 4 \end{cases}$$

$$(b) \begin{cases} x \equiv_{16} 13 \\ x \equiv_{27} 4 \\ x \equiv_{59} 16 \end{cases}$$

$$(c) \begin{cases} x \equiv_3 1 \\ x \equiv_8 6 \\ x \equiv_{11} 5 \\ x \equiv_{25} 4 \end{cases}$$

2 Funkcja Eulera

Definicja funkcji φ Eulera:

$\varphi(n) \stackrel{\text{def}}{=} \text{liczba takich } k \in \{1, 2, \dots, n\}, \text{ że } \text{nwd}(k, n) = 1$

czyli liczba liczb między 1 a n (włącznie) względnie pierwszych z n .

Obliczanie wartości funkcji φ Eulera:

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

gdzie $p_1, p_2, \dots, p_k$ są wszystkimi pierwszymi dzielnikami liczby n .

Twierdzenie Eulera:

Jeśli n i a są względnie pierwsze i $n \geq 2$, to

$$a^{\varphi(n)} \equiv_n 1$$

Zadanie 4:

Policzyć resztę z dzielenia liczby 49^{1500} przez 300.

Rozwiązanie:

Najpierw policzmy $\varphi(300)$. Jej dzielnikami pierwszymi są 2, 3 i 5:

$$\varphi(300) = 300 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 300 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 80$$

Wobec tego z twierdzenia Eulera mamy $49^{80} = 49^{\varphi(300)} \equiv_{300} 1$, bo 49 i 300 są liczbami względnie pierwszymi. Dlatego

$$\begin{aligned} 49^{1500} &= 49^{80 \cdot 18 + 60} = (49^{80})^{18} \cdot 49^{60} \equiv_{300} 1^{18} \cdot 49^{60} \\ &= 49^{60} = (49^2)^{30} = 2401^{30} \equiv_{300} 1^{30} = 1 \end{aligned}$$

Zadanie 5:

Policzyć następujące reszty z dzielenia:

(a) $8^{1000000}$ przez 63

(b) $110^{10^{25}}$ przez 73

(c) $77^{2 \cdot 7^7}$ przez 17

3 Małe twierdzenie Fermata

Małe twierdzenie Fermata

Jeśli p jest liczbą pierwszą i $a > 0$ nie jest wielokrotnością liczby p , to

$$a^{p-1} \equiv_p 1$$

Zadanie 6:

Wyznaczyć resztę z dzielenia 7^{2021} przez 13.

Rozwiązanie:

Z małego twierdzenia Fermata mamy

$$7^{12} = 7^{13-1} \equiv_{13} 1$$

Ponieważ $2021 = 168 \cdot 12 + 5$, to

$$\begin{aligned} 7^{2021} &= 7^{12 \cdot 168 + 5} = (7^{12})^{168} \cdot 7^5 \equiv_{13} 1^{168} \cdot 7^5 = 7^5 = (7^2)^2 \cdot 7^1 \\ &= 49^2 \cdot 7 \equiv_{13} 10^2 \cdot 7 = 100 \cdot 7 \equiv_{13} 9 \cdot 7 \equiv_{13} 11 \end{aligned}$$

Zadanie 7:

Z pomocą małego twierdzenia Fermata wyznaczyć reszty z dzielenia

(a) 28^{123456} przez 41;

(b) 57^{666666} przez 29;

(c) 1111^{111111} przez 59.