

Równania „modulo” i chińskie twierdzenie o resztach

Stefan Sokołowski

Elbląg, 25 kwietnia 2025

Równania „modulo”

Zadanie 1:

Rozwiązać kongruencje:

$$(a) \quad 10 \cdot x \equiv_{14} 5$$

$$(b) \quad 10 \cdot x \equiv_{14} 4$$

Rozwiązanie:

Sformułowanie (a) oznacza, że $10 \cdot x$ i 5 różnią się o całkowitą wielokrotność liczby 14 :

$$10x + 14y = 5 \quad \text{dla pewnego } y \in \mathbb{Z}$$

Wobec tego zamiast rozwiązywać równanie (a) możemy rozwiązać powyższe równanie diofantyczne.

Ale $\text{nwd}(10, 14) = 2$ a $2 \nmid 5$, dlatego równanie (a) nie ma rozwiązania.

Równanie (b) jest z tych samych powodów równoważne równaniu diofantycznemu

$$10x + 14y = 4 \quad \text{dla pewnego } y \in \mathbb{Z} \tag{1}$$

i może być rozwiązywane tak jak równania diofantyczne.

Przy pomocy rozszerzonego algorytmu Euklidesa (albo przez nietrudne w tym przypadku bezpośrednie zgadnięcie) łatwo znajdziemy rozwiązanie szczególne tego równania:

$$10 \cdot (-1) + 14 \cdot 1 = 4$$

Dla znalezienia rozwiązania ogólnego równania (1) należy podzielić to równanie przez $\text{nwd}(10, 14) = 2$, przyjmując zerowy wyraz wolny

$$5x + 7y = 0$$

i „skrzyżować współczynniki”:

$$5 \cdot (-7t) + 7 \cdot (5t) = 0 \quad \text{dla dowolnego } t \in \mathbb{Z}$$

Ogólne rozwiązanie równania diofantycznego (1) jest sumą tych dwóch rozwiązań:

$$10 \cdot (-1 - 7t) + 14 \cdot (1 + 5t) = 4 \quad \text{dla dowolnego } t \in \mathbb{Z}$$

Przy przejściu do reszt modulo 14 to daje:

$$10 \cdot (-1 - 7t) \equiv_{14} 4$$

Tak więc rozwiązaniem równania (b) jest $x = -1 - 7t$ dla dowolnego $t \in \mathbb{Z}$. Oczywiście można to rozwiązanie zapisać prościej, jako $x = 6 + 7t$, bo modulo 14 to jest to samo.

Zadanie 2:

Znaleźć wszystkie takie liczby x , że

(a) $5x \equiv_7 4$

(d) $96x \equiv_{324} 84$

(g) $2912x \equiv_{3060} 284$

(b) $4x \equiv_8 5$

(e) $35x \equiv_{79} 3$

(c) $7x \equiv_{11} 2$

(f) $99x \equiv_{13} 12$

Zadanie 3:

Rozwiązać układy równań „modulo”:

(a)
$$\begin{cases} 2x + 3y \equiv_{11} 1 \\ 6x + 5y \equiv_{11} 5 \end{cases}$$

(b)
$$\begin{cases} 2 \cdot x - 3 \cdot y + z \equiv_{11} 1 \\ x + 4 \cdot y - 2 \cdot z \equiv_{11} 10 \\ -3 \cdot x - 2 \cdot y + 9 \cdot z \equiv_{11} 2 \end{cases}$$

Zadanie 4:

Skonstruować tabelkę dodawania oraz tabelkę mnożenia dla pozycyjnego układu liczenia o podstawie:

(a) 6

(b) 7

(c) 12

W przypadku (c) należy oczywiście wprowadzić dwie nowe cyfry, bo wszystkich powinno być 12.

Zadanie 5 (domowe na punkty):

Program w C, pokazany obok, czterokrotnie podnosi do kwadratu wartość zmiennej `p`, a następnie ją drukuje. Jaki wynik zostanie wydrukowany?

Proszę „ręcznie wykonać” program, a następnie uruchomić go na komputerze. Wyjaśnić ew. rozbieżności między wynikiem symulacji a wynikiem naprawdę wydrukowanym.

```
#include<stdio.h>

int main() {
    int i, p=10;
    for (i=0; i<4; i++) p = p*p;
    printf("\n p == %i\n\n", p);
    return 0;
}
```

Uwaga:

Czas na przysłanie (na s.sokolowski@ans-elblag.pl): 2 tygodnie od zajęć 6 — potem już nie przyjmuję rozwiązań. Liczba punktów zależy od oryginalności i elegancji rozwiązania. W mailu proszę koniecznie podać swoje **nazwisko**, **numer zajęć** i **numer zadania**.

Chińskie twierdzenie o resztach

Zadanie 6:

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

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

(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 7:

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

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

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

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

¹Dla przyspieszenia obliczeń można użyć programu
`iis.ans-elblag.pl/~stefan/Dydaktyka/MatDyskZaocz/Programy/euklides.c`
stosującego rozszerzony algorytm Euklidesa.