

Równania „modulo”

Stefan Sokołowski

Elbląg, 8 V 2025

Przypomnienie:

1. Dla liczb całkowitych m , n i k (przy $k > 0$) poniższe stwierdzenia są równoważne:

$m \bmod k = n \bmod k$ reszta z dzielenia m przez k jest taka sama jak reszta z dzielenia n przez k

$m \equiv_k n$ m przystaje do n modulo k
--

$[m]_k = [n]_k$ m i n należą do tej samej klasy modulo k , czyli do tego samego elementu $\mathbb{Z}_k$
--

Wszystkie oznaczają, że $k \mid (m - n)$; innymi słowami: że m i n różnią się o całkowitą wielokrotność liczby k .

2. Relacja $\equiv_k$ jest **kongruencją** ze względu na dodawanie, odejmowanie i mnożenie liczb całkowitych. To znaczy, że jeśli $m_1 \equiv_k n_1$ oraz $m_2 \equiv_k n_2$, to

$$\begin{array}{ll} m_1 + m_2 \equiv_k n_1 + n_2 & \text{i} \\ m_1 - m_2 \equiv_k n_1 - n_2 & \text{i} \\ m_1 \cdot m_2 \equiv_k n_1 \cdot n_2 & \end{array}$$

Z tego wynika na przykład, że jeśli $m \equiv_k n$, to $m^p \equiv_k n^p$ dla dowolnej całkowitej $p \geq 1$.¹

Zadanie 1:

Rozwiązać kongruencje:

- (a) $10 \cdot x \equiv_{14} 5$
(b) $10 \cdot x \equiv_{14} 4$

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.

¹Dla $p = 0$ problemem może być podnoszenie zera do potęgi zerowej: 0^0 nie ma żadnej określonej wartości.

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

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

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

$$x = -1 - 7t \quad \text{dla dowolnego } t \in \mathbb{Z}$$

Oczywiście można to rozwiązanie zapisać prościej, jako $x = 6 + 7t'$, bo modulo 14 to jest to samo².

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

²Można to sprawdzić przez podstawienie $t + 1$ za t' : $6 + 7(t + 1) \equiv_{14} 6 - 7(t + 1) = 6 - 7t - 7 = -1 - 7t$

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 9 — 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**.
