

Strona główna

Strona tytułowa

Spis treści



Strona 1 z 25

Powrót

Full Screen

Zamknij

Koniec

# Kongruencje

## oraz przykłady ich zastosowań

Andrzej Śladek, Instytut Matematyki UŚI

[sladek@ux2.math.us.edu.pl](mailto:sladek@ux2.math.us.edu.pl)

Spotkanie w LO im. Powstańców Śl w Bieruniu Starym

27 października 2005

Strona główna

Strona tytułowa

Spis treści



Strona 2 z 25

Powrót

Full Screen

Zamknij

Koniec

## Spis treści

1	Wstęp	3
2	Kongruencje	4
3	Cechy podzielności - zadanie 1	8
4	Tw. chińskie o resztach - zadanie 2	12
5	Funkcja Eulera - zadanie 3	16
6	Dwa zadania z Olimpiady Matematycznej	19
7	Zadania domowe	21
8	Literatura	24

# 1. Wstęp

Poznamy nowe fakty matematyczne, które pozwolą nam w łatwy sposób rozwiązać poniższe zadania.

**Zadanie 1.** W szkole uczniowie poznają cechę podzielności przez 3 oraz przez 9. Znajdź cechę podzielności przez inne liczby jak np. 7, 11, 13.

**Zadanie 2.** Liczba kostek w bardzo dużej czekoladzie równa jest  $x$ . Jeśli podzielić czekoladę na 3 części, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada?

**Zadanie 3.** Znajdź trzy ostatnie cyfry liczby  $3^{14404}$ .

## 2. Kongruencje

**Definicja** Niech  $n$  będzie liczbą naturalną oraz niech  $a$  oraz  $b$  będą liczbami całkowitymi. Mówimy, że  $a$  **przystaje do  $b$  modulo  $n$** , jeśli  $n$  dzieli  $a - b$ .

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b) \Leftrightarrow \text{istnieje l. całk. } k, \text{ że } a - b = k \cdot n$$

**Uwaga** Dwie liczby całkowite przystają do siebie modulo  $n$  wtedy i tylko wtedy, gdy dają tą samą resztę z dzielenia przez  $n$ .

*Które z poniższych kongruencji są prawdziwe?*

$$10 \equiv 1 \pmod{9}, \quad -1 \equiv 113 \pmod{6}, \quad -12 \equiv 13 \pmod{5},$$

$$-5 \equiv 31 \pmod{7}, \quad -26 \equiv 44 \pmod{10}, \quad 23 \equiv 71 \pmod{11}$$



## Własności kongruencji

1. Przystawanie modulo  $n$  jest relacją równoważnościową, tzn.

- $a \equiv a \pmod{n}$ ,
- $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ ,
- $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ .

Przykładowo udowodnimy ostatnią z nich (własność przechodniości).

Jeśli  $a \equiv b \pmod{n}$ ,  $b \equiv c \pmod{n}$ , to  $a - b = k \cdot n$ ,  $b - c = l \cdot n$ .

Wtedy  $a - c = (a - b) + (b - c) = k \cdot n + l \cdot n = (k + l) \cdot n$ ,  
a to oznacza, że  $a \equiv c \pmod{n}$ .

*Udowodnij dwie pierwsze własności!*

2. Kongruencje można stronami dodawać, odejmować i mnożyć, tzn.

$$a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$$

⇓

$$a+c \equiv b+d \pmod{n}, \quad a-c \equiv b-d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

*Spróbujesz to udowodnić?*

W szczególności,  
jeśli  $a \equiv b \pmod{n}$ , to dla dowolnych liczb całkowitych  
 $a_0, \dots, a_n$  mamy

$$a_n a^n + \dots + a_1 a + a_0 \equiv a_n b^n + \dots + a_1 b + a_0 \pmod{n},$$

tzn.

$$f(a) \equiv f(b) \pmod{n}, \text{ gdzie } f(X) = a_n X^n + \dots + a_1 X + a_0$$

Strona główna

Strona tytułowa

Spis treści



Strona 7 z 25

Powrót

Full Screen

Zamknij

Koniec

Rozwiąż następujące kongruencje:

- $3X + 2 \equiv 1 \pmod{5}$ ,
- $25X \equiv 12 \pmod{7}$ ,
- $3X \equiv 1 \pmod{6}$
- $37X \equiv 23 \pmod{73}$ .

### Uwaga

Można pokazać, że kongruencja  $aX \equiv b \pmod{n}$  ma rozwiązanie wtedy i tylko wtedy, gdy  $\text{NWD}(a, n) | b$ .



### 3. Cechy podzielności - zadanie 1

Liczbę naturalną  $N$  w systemie dziesiętkowym można zapisać następująco:

$$N = (c_1c_2\dots c_n)_{10} = c_110^{n-1} + c_210^{n-2} + \dots + c_{n-1}10^1 + c_n.$$

Jeśli  $f(X) = c_1X^{n-1} + c_2X^{n-2} + \dots + c_{n-1}X^1 + c_n$ , to  $N = f(10)$

$$10 \equiv 1 \pmod{3}$$



$$N = f(10) \equiv f(1) = c_1 + c_2 + \dots + c_{n-1} + c_n \pmod{3}$$

tzn. 3 dzieli liczbę  $N$  wtedy i tylko wtedy, gdy dzieli sumę jej cyfr.

*Czy wiesz jak udowodnić cechę podzielności przez 9 oraz przez 11?*

Strona główna

Strona tytułowa

Spis treści



Strona 9 z 25

Powrót

Full Screen

Zamknij

Koniec

$$10 \equiv -1 \pmod{11}$$



$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \dots - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę  $N$  wtedy i tylko wtedy, gdy dzieli

naprzemienną sumę jej cyfr.

### Przykład

Aby sprawdzić podzielność liczby 12345678906 przez 11 obliczamy sumę naprzemienną cyfr

$$6 - 0 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 11,$$

która jest podzielna przez 11.

Zatem liczba 12345678906 jest podzielna przez 11.



Cechy podzielności przez inne liczby są bardziej skomplikowane. Przyjrzyjmy się cesze podzielności przez 7 oraz przez 13.

Liczbę naturalną

$$N = (c_1c_2\dots c_n)_{10} = c_110^{n-1} + c_210^{n-2} + \dots + c_{n-1}10^1 + c_n$$

możemy zapisać w postaci

$$N = \dots + 1000^1(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}.$$

Zauważ, że jeśli

$$g(X) = \dots + X(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10},$$

to

$$N = g(1000).$$

Strona główna

Strona tytułowa

Spis treści



Strona 11 z 25

Powrót

Full Screen

Zamknij

Koniec

$$1000 \equiv -1 \pmod{7, 13} \quad (\text{bo } 1001 = 7 \cdot 11 \cdot 13)$$



$$N = g(1000) \equiv g(-1) \pmod{7, 13}$$

$$g(-1) = \dots + (-1)^1(c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}$$

Stąd 7 (tak samo 13) dzieli liczbę  $N$  wtedy i tylko wtedy, gdy dzieli ”naprzemienną sumę” liczb powstałych z podziału liczby  $N$  na trójki.

## Przykład

7 dzieli 23697678872, bo  $-23 + 697 - 678 + 872 = 868 = 7 \cdot 124$

## 4. Tw. chińskie o resztach - zadanie 2

**Zadanie 2** Liczba kostek w bardzo dużej czekoladzie równa jest  $x$ . Jeśli podzielić czekoladę na 3 części, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada?

### Twierdzenie (chińskie o resztach)

Jeśli  $n_1, \dots, n_k$  są parami względnie pierwsze oraz  $r_1, \dots, r_k$  są liczbami całkowitymi, to istnieje liczba całkowita  $x$  taka, że

$$\begin{cases} x \equiv r_1 \pmod{n_1} \\ x \equiv r_2 \pmod{n_2} \\ \dots \dots \dots \\ x \equiv r_k \pmod{n_k} \end{cases}$$

Liczba  $x$  jest wyznaczona jednoznacznie modulo  $n_1 \cdot \dots \cdot n_k$ .

Strona główna

Strona tytułowa

Spis treści



Strona 12 z 25

Powrót

Full Screen

Zamknij

Koniec

*Strona główna*

*Strona tytułowa*

*Spis treści*



*Strona 13 z 25*

*Powrót*

*Full Screen*

*Zamknij*

*Koniec*

# Czy wiesz jak rozwiązać zadanie 2?

*Strona główna*

*Strona tytułowa*

*Spis treści*



*Strona 14 z 25*

*Powrót*

*Full Screen*

*Zamknij*

*Koniec*

Należy rozwiązać układ kongruencji

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Strona główna

Strona tytułowa

Spis treści



Strona 15 z 25

Powrót

Full Screen

Zamknij

Koniec

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Analizujemy pierwszą kongruencję.

$$x \equiv 1 \pmod{3} \implies x = 3t + 1$$

Wstawiamy tak obliczone  $x$  do drugiej kongruencji i wyliczamy  $t$ .

$$3t + 1 \equiv 3 \pmod{5} \implies 3t \equiv 2 \pmod{5} \implies t \equiv 4 \pmod{5} \implies t = 5u + 4$$

$$\text{Zatem } x = 3(5u + 4) + 1 = 15u + 13.$$

Wstawiamy to do trzeciej kongruencji.

$$15u + 13 \equiv 2 \pmod{7} \implies u - 1 \equiv 2 \pmod{7} \implies u \equiv 3 \pmod{7} \implies u = 7s + 3$$

$$\text{Ostatecznie } x = 15(7s + 3) + 13 = 105s + 58.$$

**Odp.** Liczba kostek czekolady równa jest 58.

## 5. Funkcja Eulera - zadanie 3

**Zadanie 3** Znajdź trzy ostatnie cyfry liczby  $3^{14404}$ .

Do rozwiązania potrzebować będziemy tzw. funkcji Eulera.

Nazwa tej funkcji pochodzi od nazwiska szwajcarskiego matematyka L.Eulera, który żył w latach 1707-1783.



## Funkcja Eulera

$\varphi(n) :=$  liczba elem. zbioru  $\{k : 1 \leq k \leq n - 1, \text{NWD}(k, n) = 1\}$

### Własności:

(1) Jeśli  $\text{NWD}(n, m) = 1$ , to  $\varphi(nm) = \varphi(n)\varphi(m)$ .

(2) Jeśli  $p$  jest liczbą pierwszą, to  $\varphi(p^k) = p^{k-1}(p - 1)$ .

W szczególności  $\varphi(p) = p - 1$ .

### Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) = 2^2(2 - 1)5^1(5 - 1) = 80$ .

### Twierdzenie Eulera

Jeśli  $\text{NWD}(a, n) = 1$ , to  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

### Wniosek (Małe Twierdzenie Fermata)

Jeśli  $p$  jest liczbą pierwszą i  $p \nmid a$ , to  $a^{p-1} \equiv 1 \pmod{p}$ .

**Przykład**  $3^{80} \equiv 1 \pmod{200}$ .

**Zadanie 3** Znajdź trzy ostatnie cyfry liczby  $3^{14404}$ .

*Rozwiązanie.*

Należy znaleźć resztę z dzielenia liczby  $3^{14404}$  przez 1000.

Obliczmy  $\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = 400$ .

Zatem

$$3^{14404} = 3^{400 \cdot 36 + 4} = (3^{400})^{36} 3^4 \equiv 3^4 \pmod{1000},$$

bo  $3^{400} \equiv 1 \pmod{1000}$  na podstawie twierdzenia Eulera.

Ponieważ  $3^4 = 81$ , więc

**ostatnie trzy cyfry liczby  $3^{14404}$  to 081.**



## 6. Dwa zadania z Olimpiady Matematycznej

Rozwiążmy teraz dwa zadania, które pojawiły się kiedyś na Olimpiadzie Matematycznej.

### Zadanie 1.

Wykaż, że jeżeli  $m \equiv n \pmod{4}$ , to liczba  $53^m - 33^n$  jest podzielna przez 10.

*Rozwiązanie.*

Zauważ najpierw, że  $53^n - 33^m \equiv 3^n - 3^m \pmod{10}$ .

Jeśli  $n = 4k + m$ , to

$$3^n - 3^m = 3^{4k+m} - 3^m = 3^m((3^4)^k - 1) = 3^m((81)^k - 1) \equiv 3^m(1-1) \pmod{10}.$$

## Zadanie 2.

Znajdź wszystkie takie liczby naturalne  $n$ , aby liczba  $1! + 2! + \dots + n!$  była kwadratem pewnej liczby naturalnej.

*Rozwiązanie.*

$$\underline{1! = 1 = 1^2}, \quad 1! + 2! = 3, \quad \underline{1! + 2! + 3! = 9 = 3^2}, \quad 1! + 2! + 3! + 4! = 33$$

Jeśli  $n \geq 5$ , to

$$1! + 2! + 3! + 4! + \underbrace{5! + \dots + n!}_{\text{podzielne przez 5}} \equiv 1! + 2! + 3! + 4! \equiv 3 \pmod{5},$$

a kwadraty liczb naturalnych przystają modulo 5 jedynie do 0, 1 lub 4.

**Odp.** Jedynie dla  $n = 1$  oraz  $n = 3$  liczba  $1! + 2! + \dots + n!$  jest kwadratem pewnej liczby naturalnej.



## 7. Zadania domowe

1. Rozwiąż kongruencje
  - $3X + 31 \equiv 15 \pmod{47}$
  - $3X \equiv 8 \pmod{13}$
  - $14X \equiv 22 \pmod{36}$
2. Znajdź i uzasadnij cechę podzielności przez 101.  
*Wsk.*  $100 \equiv -1 \pmod{101}$ .
3. Wykorzystując kongruencję  $1000 \equiv 1 \pmod{27, 37}$  wyprowadź cechy podzielności przez 27 oraz 37.
4. Wykorzystując kongruencję  $100 \equiv -2 \pmod{51}$  wyprowadź cechę podzielności przez 51.
5. W sadzie zebrano jabłka, których nie było więcej niż 1000. Gdyby podzielić jabłka równo do 7 koszy, to zostanie 1 jabłko.



Gdyby podzielić jabłka równo do 13 koszy, to zostanie 6 jabłek. Można jednak podzielić jabłka równo na 11 części. Ile zebrano jabłek?

6. Znajdź ostatnie dwie cyfry następujących liczb  $7^{6042}$ ,  $289^{289}$ ,  $7^{99}$ .  
Wsk. Oblicz  $\varphi(100)$ .
7. Wyznacz reszty z dzielenia:
  - (a)  $15^{231}$  przez 14
  - (b)  $3^{80} + 7^{80}$  przez 11
  - (c)  $208^{208}$  przez 23
8. Dopisać z prawej strony liczby 523 takie trzy cyfry, aby otrzymana liczba sześciocyfrowa była podzielna przez 7, 8 i 9.
9. Wykazać, że setna potęga dowolnej liczby całkowitej przy dzieleniu przez 125 daje resztę 0 lub 1.

Strona główna

Strona tytułowa

Spis treści



Strona 23 z 25

Powrót

Full Screen

Zamknij

Koniec

10. Znajdź resztę z dzielenia liczby całkowitej  $a$  przez 73 wiedząc, że  $a^{100} \equiv 2 \pmod{73}$  oraz  $a^{101} \equiv 69 \pmod{73}$ .
11. Wykazać, że iloczyn trzech kolejnych liczb naturalnych, z których środkowa jest sześcianem liczby naturalnej, jest podzielny przez 504 (*zadanie z Olimpiady Matematycznej*).

Strona główna

Strona tytułowa

Spis treści



Strona 24 z 25

Powrót

Full Screen

Zamknij

Koniec

## 8. Literatura

1. N.Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa 1995.
2. P.Ribenboim, *Mała księga wielkich liczb pierwszych*, WNT, Warszawa 1997.
3. W.Sierpiński, *Wstęp do teorii liczb*, Biblioteczka Matematyczna 25, PZWS, Warszawa 1965.
4. L.A.Steen (redaktor), *Matematyka Współczesna, Dwanaście esejów*, WNT, Warszawa 1983.

Strona główna

Strona tytułowa

Spis treści



Strona 25 z 25

Powrót

Full Screen

Zamknij

Koniec

I to już koniec!



Dziękuję za uwagę